Misbehavior Detection and Attacker Identification in Vehicular Ad hoc Networks

dem Fachbereich 20 Informatik
der Technischen Universität Darmstadt
genehmigte

DISSERTATION

zur Erlangung des akademischen Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
von

M.Sc. Norbert Bißmeyer
geboren in Osnabrück

Referenten der Arbeit:	Prof. Dr. Michael Waidner Technische Universität Darmstadt
	Prof. Dr. Frank Kargl Universität Ulm
Tag der Einreichung:	07.10.2014
Tag der mündlichen Prüfung:	27.11.2014

Darmstädter Dissertation 2014
D 17

Acknowledgments

I would particularly like to thank my supervisor Prof. Dr. Michael Waidner who gave me the opportunity and freedom to research in this interesting field of technology at the Fraunhofer Institute for Secure Information Technology (SIT). His guidance and scientific advice were a great help on the way to write this dissertation. In addition, I would like to express my gratitude to Prof. Dr. Frank Kargl who supported my research and provided helpful feedback in several discussions.

The work in the department Mobile Networks at Fraunhofer SIT was a great pleasure thanks to the continuous support and encouragement of my colleagues. I would like to thank in particular my supervisor and mentor Dr. Kpatcha Bayarou to believe in my work and support me with outstanding effort. Very special thanks also to Dr. Peter Ebinger and Dr. Frank G. Weber who helped me a lot by proof-reading this thesis and my colleagues at Fraunhofer for all the fruitful discussions we had together.

I would also like to thank the people of the working group security of the Car2Car Communication Consortium, the people involved in the ETSI ITS security working groups, and the experts I cooperated with in the research projects sim^{TD} and PRESERVE. Further, I would like to thank the participants of the Harmonization Task Group (HTG#6) to discuss the topic of V2X communication security and privacy in an international context at some of the greatest places on earth. I am sure the results we worked out will help to make V2X communications become reality in the coming years

Finally, thanks to my parents, my sister, my brother, and all my friends for their unconditional support and patience during the course of this work. Last but not least I would like to thank Jennifer Malberg for our great time together and to believe in me and the success of my work. Without all their encouragement and understanding this thesis would not have been possible.

Abstract

The objective of the research presented in this dissertation is to detect misbehavior in vehicular ad hoc networks (VANETs) and to identify the responsible attackers or faulty nodes in order to exclude them from active network participation. Vehicles and roadside units use wireless ad hoc communication in VANETs to increase traffic safety and efficiency by exchanging cooperative awareness information and event-based messages. Considering both presence and status of vehicles moving in a defined range drivers can be notified instantly about upcoming potentially dangerous situations such as a sudden braking action of a vehicle driving in front or the tail end of a traffic jam ahead. VANET nodes frequently broadcast mobility-related information (i.e. absolute values for position, time, heading, and speed) within a communication range of several hundred meters to establish a cooperative awareness of single-hop neighbors. Due to the ad hoc communication between network nodes traffic safety applications become feasible that have low latency requirements.

The protection against external attackers in VANETs is provided by applying cryptographic methods. Only registered nodes of the VANET are equipped with valid keys that are certified by a trusted certificate authority. Internal attackers who possess appropriate hardware, software, and valid certificates must be considered as a dangerous threat. Attackers who either extract valid keys and certificates from a communication unit or install a malware on VANET devices on board of vehicles or on roadside units are able to send bogus messages that are accepted by unsuspecting vehicles. We demonstrate that the processing of fake information may affect the safety and efficiency of the overall traffic in the attackers' single or multi-hop communication range.

Most existing solutions in the context of misbehavior detection in VANETs are based on data-centric plausibility and consistency checks. We propose in this dissertation new methods and frameworks to evaluate the behavior of VANET nodes based on cooperatively exchanged location-related information. Most existing solutions are only tested within simulations. In contrast we analyzed the applicability of misbehavior detection in VANETs under real conditions. Long-term experiments in outdoor field operational tests and dedicated trials with test vehicles revealed new insights with respect to misbehavior detection and attacker identification which are presented in this dissertation. Based on this knowledge a novel strategy has been developed that consists of three main contributions: local misbehavior detection, local short-term identification of potential attackers, and central long-term identification of attackers.

The concept for *local misbehavior detection on VANET nodes* is based on different information sources such as received packets or sensor measurements to perform data consistency and data plausibility checks. In case of detected inconsistencies or implausible movement characteristics the suspicious node is observed and its trustworthiness is locally evaluated.

The contributions for *local short-term identification of potential attackers* consider explicitly the frequent change of neighbor node identifiers as stipulated by European standards and international

industrial regulations. Based on test results gained from a large field operational test a concept for the local misbehavior evaluation of neighbor nodes is proposed. The resulting node trustworthiness is further used to generate misbehavior reports that are transmitted to a central evaluation authority. Consequently, the central authority is informed about suspicious nodes and hence potential attackers of the VANET.

The third main contribution is the processing of misbehavior reports for *central long-term identification of attackers*. If sufficient evidence is reported by a significant number of independent VANET nodes the central misbehavior evaluation authority is authorized to request information whether different pseudonymous IDs contained in related misbehavior reports belong to the same suspicious node. This process is supported by the central certificate authorities which ensure the consideration of drivers' privacy while processing critical information. After the assessment of the reported suspects the central misbehavior evaluation authority is able to identify the attacker and exclude his or her from active participation in any VANET communication.

Based on the knowledge gained from our practical experiments with test vehicles we developed an effective concept to enable the secure and reliable long-term operation of VANETs. Attackers and faulty nodes can reactively be excluded from the network after independent network nodes have locally detected their misbehavior and a central authority has identified the offenders. This approach is more effective in terms of long-term attacker exclusion and minimization of false-positive detections compared to related approaches that are only deployed on VANET nodes. Consequently, the proposed concept will help to minimize the motivation of potential attackers to aim on VANETs. Due to the detection of abnormal node behavior even novel attack methods that may emerge in the future should be effectively counteracted by applying these concepts.

Zusammenfassung

In dieser Dissertation werden Methoden ausgearbeitet, die die Erkennung von Fehlverhalten in Vehicular Ad-hoc Netzwerken (VANETs) ermöglichen, sowie die Identifizierung der verantwortlichen Angreifer oder fehlerhaften Knoten. Das Ziel ist es, die störenden Netzwerkknoten langfristig von der aktiven VANET-Kommunikation auszuschließen. Fahrzeuge und Infrastruktureinheiten am Straßenrand nutzen die drahtlose Ad-hoc-Kommunikation um Informationen zur Verkehrssicherheit und Effizienz mit benachbarten Netzwerkknoten auszutauschen. Durch den konstanten Austausch von Statusinformationen sind Netzwerkknoten in der Lage ihr Umfeld in einem definierten Bereich wahrzunehmen. Bei potenzieller Gefahr können Fahrer rechtzeitig über bevorstehende Verkehrssituationen, wie zum Beispiel den plötzlichen Bremsvorgang eines voraus fahrenden Fahrzeugs oder ein nahendes Stauende, informiert werden. Die Knoten des VANETs verbreiten regelmäßig präzise Informationen bezüglich ihres eigenen Standortes und ihrer Bewegung innerhalb einer Funkreichweite von mehreren hundert Metern. Unter anderem wird die absolute Position, die Fahrtrichtung und die Geschwindigkeit in Verbindung mit einem Zeitstempel per Broadcast versendet. Durch die Ad-hoc-Kommunikation zwischen den Netzknoten werden im Besonderen verkehrssicherheitsrelevante Anwendungen ermöglicht, die eine niedrige Latenz beim Informationsaustausch voraussetzen und daher durch eine mobilfunkbasierte Kommunikation nicht realisiert werden könnten.

Der Schutz vor externen Angreifern wird in VANETs mit Hilfe von kryptographischen Verfahren sichergestellt. Nur registrierte Netzwerkknoten sind mit gültigen Schlüsseln und Zertifikaten ausgestattet, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt werden. Interne Angreifer, die entsprechende Hardware, Software und gültige Schlüssel bzw. Zertifikate besitzen, stellen eine Bedrohung für das Netzwerk und den drauf basierenden Anwendungen dar. Ein Angreifer, der entweder gültige Schlüssel mit den dazugehörigen Zertifikates aus einer Kommunikationseinheit extrahiert oder eine Malware auf einem VANET-Knoten installiert hat, ist in der Lage gültige Nachrichten mit gefälschtem Inhalt zu senden. Diese Nachrichten werden dann von ahnungslosen Fahrzeugen akzeptiert und können zu Falschmeldungen und fehlerhaften Entscheidungen der Fahrer führen. In dieser Arbeit wird gezeigt, dass die Verarbeitung von gefälschten Informationen Einfluss auf die Verkehrssicherheit und Effizienz des gesamten Verkehrs im Kommunikationsbereich des Angreifers haben kann.

Die meisten existierenden Lösungen anderer Autoren im Bereich der Fehlverhaltenserkennung in VANETs basieren auf datenbezogenen Plausibilitäts- und Konsistenzprüfungen. Wir schlagen in dieser Dissertation neue Methoden und Konzepte vor, die das Verhalten von Nachbarknoten in VANETs unter Nutzung von positionsbezogenen Informationen bewerten. Da die meisten existierenden Lösungen nur in Simulationen unter Verwendung von theoretischen Annahmen getestet wurden, fehlen Erkenntnisse bezüglich der Fehlverhaltenserkennung unter realen Bedingungen. Dagegen konnten wir durch unsere Langzeitexperimente in einem Feldversuch neue Erkenntnisse bezüglich der lokalen Fehlverhaltenserkennung und Angreiferidentifizierung gewinnen. Basierend auf diesem Wissen wurde

eine neuartige Strategie entwickelt, um den Gefahren durch interne Angreifer zu begegnen und um damit die langfristige Zuverlässigkeit der VANET-Kommunikation zu erhöhen: Die lokale Erkennung von Fehlverhalten durch Knoten des VANETs, die lokale kurzfristige Identifizierung potentieller Angreifer und die zentrale langfristige Identifizierung von Angreifern.

Der Ansatz zur *lokalen Erkennung von Fehlverhalten auf VANET-Knoten* nutzt verschiedene Informationsquellen. Primär sind das die empfangenen Datenpakete der Nachbarn, aber auch Messungen lokaler Sensoren werden zur Durchführung von Datenkonsistenzprüfungen und Plausibilitätsprüfungen verwendet. Sobald Inkonsistenzen oder ein unplausibles Bewegungsverhalten eines benachbarten Knotens detektiert wurden, wird dessen Verhalten lokal bewertet.

Bei der *lokalen kurzfristigen Identifizierung potentieller Angreifer* werden explizit die kurzzeitig gültigen und regelmäßig wechselnden pseudonymen Identifizierer der VANET-Knoten berücksichtigt, wie sie durch europäische Standards und internationale Industriegremien gefordert werden. Basierend auf Testergebnissen eines umfangreichen Feldtests werden Konzepte und Mechanismen zur lokalen Auswertung von verdächtigen Nachbarknoten vorgeschlagen. Die resultierende Vertrauenswürdigkeit der jeweiligen Nachbarknoten wird lokal verwendet, um Berichte über beobachtetes Fehlverhalten zu generieren. Diese Berichte werden anschließend zur einer zentralen Auswertungsbehörde übertragen, um langfristig verdächtige Knoten und damit mögliche Angreifer des VANETs zu identifizieren.

Der dritte Hauptbeitrag ist die Verarbeitung von Fehlverhaltensberichten für die *zentrale langfristige Identifizierung von Angreifern*. Wenn eine ausreichend große Anzahl von Berichten mit entsprechenden Beweisen von unabhängigen VANET-Knoten an die zentrale Auswertungsbehörde geschickt wurden, ist die Behörde berechtigt den möglichen Zusammenhang verschiedener pseudonymer Identifizierer von verdächtigen Knoten aus unterschiedlichen Fehlverhaltensberichten zu untersuchen. Dieser Schritt wird benötigt um Angreifer zu identifizieren, die ihre pseudonymen Identifizierer wechseln um ihr Fehlverhalten zu verschleiern. Der Prozess wird durch die zentrale Zertifizierungsstelle unterstützt unter Berücksichtigung der Anforderungen zum Schutz der Privatsphäre der Fahrzeugführer. Nach Auswertung der gemeldeten Fehlverhaltensberichte und der Bewertung der verdächtigen Knoten ist die zentrale Stelle in der Lage den Angreifer von der aktiven Teilnahme an der VANET-Kommunikation auszuschließen.

Basierend auf dem Wissen, das durch die praktischen Experimente erlangt wurde, haben wir ein effektives Konzept entwickelt, mit dem der sichere und langfristige Betrieb eines VANETs ermöglicht wird. Angreifer und fehlerhafte Knoten können reaktiv aus dem Netzwerk ausgeschlossen werden nachdem unabhängige Netzwerkknoten ihr Fehlverhalten erkannt haben und eine zentrale Stelle die Verursacher identifiziert hat. Dieses Konzept ist effektiver bezüglich des langfristigen Ausschlusses von Angreifern sowie der Minimierung von Falsch-Positiv Erkennungen im Vergleich zu Mechanismen, die nur auf VANET-Knoten eingesetzt werden. Durch die drohende Gefahr langfristig erkannt und aus dem Netzwerk ausgeschlossen zu werden, können potentielle Angreifer bereits im Voraus davon abgeschreckt werden Angriffe durchzuführen. Da die vorgeschlagenen Mechanismen auf der Erkennung von abnormalem Knotenverhalten basieren, sollten auch zukünftige Angriffsmethoden erkannt werden, die derzeit noch nicht bekannt sind.

Contents

List of Tables

List of Figures

The world is a dangerous place, not because of those who do evil, but because of those who look on and do nothing.

Albert Einstein

Part I.

Background

1. Introduction

The detection of misbehavior and the identification of the corresponding offender are topics that concern both security and safety aspects in vehicular ad hoc networks. This chapter serves as an introduction to these topics. By focusing on security aspects we substantiate why these mechanisms are needed in order to make vehicular communications more reliable for long-term operation. After a general motivation, related key terms are defined in Section 1.2 and a dedicated problem statement is discussed in Section 1.3. Subsequently, the goals of the work are presented in Section 1.4 and the scientific contributions are summarized in Section 1.5. A discussion of the dissertation structure concludes this chapter.

1.1. Motivation

In principle, a cooperative system is based on rules that are commonly agreed on to ensure correct processes for information processing, proper interactions between all system entities and fair distribution of rights and responsibilities. This principle is not necessarily restricted to technical communication systems. For example, in social communities laws are created to organize a fair cooperative living. Violating the rules could endanger the overall system goals or may leverage single entities to get additional advantages at the expense of others. In general, a well designed system may prevent illegal action such as fraud through integrated countermeasures. In complex systems, however, it may be impossible or extremely costly to guarantee the absence of faults and vulnerabilities in the design. Moreover, due to costs and disproportional effort it may not be reasonable to include all available counter mechanisms in a system design to prevent misuse. Therefore, mechanisms for misbehavior detection are used in cooperative systems in addition to basic instruments that aim for misuse prevention. In politics for example, processes typically do not prevent misbehavior by design but inspections are scheduled that discover people or legal entities that do not follow the rules. Similarly, in cooperative information and communication technologies (ICT) monitoring systems are used to detect abnormal behavior and misbehavior based on predefined signatures.

As a result, in different systems (not exclusively in the domain of ICT) mechanisms are used to monitor the system quality and its long-term reliability. Especially in systems with a long life time, the design may not be able to consider all future developments that could endanger the system's functionality and reliability. In ICT, for example, attacks could become possible due to new technologies and inventions such as side channel attacks or quantum cryptography whereby implemented security mechanisms become obsolete. A misbehavior detection mechanism that observes the activities in the cooperative system is able to detect abnormal behavior and may identify the initiator of problems such as an attacker. Depending on the kind of misbehavior, appropriate reactions may be triggered, e. g.

prosecution of the user, technical deactivation of the ICT entity or revocation of cryptographic credentials.

A vehicular ad hoc network (VANET) is affected in particular as its long-term operation is an important aspect. Usually vehicles are operated over long periods of time in contrast to other ICT devices such as mobile phones for instance, and they are not controlled and observed by a central entity. An owner may be able to customize his or her own vehicle with additional communication hardware or install individual software that could affect the functionality of the overall cooperative communication system negatively. However, proactive security mechanisms (i. e. encryption and digital signing of messages) that aim to prevent unintended system usage are an essential measure in order to exclude external attackers from the network. Nevertheless, these measures are not able to prevent misbehavior of internal attackers who are in possession of valid credentials of the security system. With reference to the mandate of the European commission [Com09] and the memorandum of understanding of automobile manufacturers [Con11] it can further be estimated that after the initial deployment phase has passed, the number of connected vehicles will likely reach several million nodes. Due to the scale of a VANET and its decentralized character, full control of each and every node in the network becomes unlikely. An attacker is not necessarily a malicious hacker that tries to disrupt the cooperative system's functionality. Even ordinary drivers might be motivated to selfishly misuse vehicular ad hoc communications in order to free the fast lane on a highway or switch a traffic light to green. As a result, a reactive mechanism is needed that constantly observes the system functionality and ensures fairness in the network.

We concentrate in this dissertation on two aspects:

a) How can misbehavior and possible vulnerabilities be detected and identified as early as possible?

b) How can the initiator of misbehavior be identified in order to react appropriately (e. g. exclude the attacker or faulty node until the problem is solved)?

With the two measures of misbehavior detection and subsequent attacker identification the long-term reliability of proper VANET functionality can be ensured.

1.2. Misbehavior in Inter-Vehicle Communications

In general, misbehavior can be defined as an action of someone who is behaving inappropriate. With respect to cooperative ICT, misbehavior are active and passive actions performed by communication end points that are not behaving according to predefined rules. Active misbehavior is for example the distribution of wrong information, while passive misbehavior is for example the illegal collection of specific information of individuals.

According to Buchegger [Buc04] misbehavior detection is not restricted to any particular kind of misbehavior as long as it is detectable, i. e. observable and classifiable as such with a high probability. A classical intrusion detection system (IDS) observes network links and endpoint systems to detect predefined attack signatures or anomalies differing from a predefined normal state. A misbehavior detection system (MDS) is related to cyber-physical systems (CPS) that handle physical input and output. A CPS can be described as a system of collaborating computational elements controlling physical entities. In addition to IDS misbehavior detection approaches are extended by measurements

of physical sensors and contextual information such as time and location. The mechanisms discussed in this dissertation focus on the detection of active misbehavior performed intentionally by attackers or accidentally by faulty network nodes that show abnormal behavior. However, in productive systems detected anomalies that differ to some extend from expected normal states are not necessarily misbehavior. Inaccuracies must be considered in order to avoid false detections and consequently possible false reactions. The threshold between valid and invalid behavior may be vague in real-world vehicular ad hoc networks. Furthermore, vehicles in an exceptional state such as involved in a traffic accident might distribute abnormal information.

In this dissertation we focus on abnormal behavior considering aspects of location-related information distributed and processed within the domain of traffic safety and efficiency.

1.3. Problem Statement

Coping with misbehaving nodes in communication networks is important in order to guarantee trustworthy exchange of information. Accordingly, different mechanisms are applied to ensure the most important security goals: sender authenticity and authorization, message integrity and confidentiality. As argued in the motivation the application of cryptographic mechanisms can ensure the adherence of common rules of the cooperative network. Internal attackers, however, possess valid credentials and necessary communication technology to overcome these proactive security mechanisms. To reduce the risk of internal attackers the systems of the communication endpoints can additionally be protected by firewalls and trusted computing solutions [HAF+09, OYN+08]. Nevertheless, manipulation of vehicular systems cannot be prevented since side channel attacks [Tar10] and malicious software manipulation (e. g. flashing of system software [MBZ+12] or exploiting vulnerabilities) are additional risks. In any case, securing the complete network of vehicles is costly and challenging since data have to be protected seamlessly on their way from the source of information such as a sensor to the destination such as a display or transmitter. For example, in the use case *Emergency Electronic Brake Lights* [ETS09], information from a braking vehicle has to be transmitted to neighboring vehicles whereupon the sender has to secure every component, interface, and network between the brake sensor and the transceiver. Additionally, the receiving vehicle has to secure every component, interface, and network between the transceiver and the human machine interface (HMI) in order to be sure that an attacker has not manipulated the information [HAF+09]. Full protection of data on the way between the source component of the sender (e. g. braking sensor) and destination component at the receiver (e. g. display) is very expensive with respect to complexity, overhead, and cost. However, even if all channels are fully protected by means of cryptography the physical manipulation of sensor inputs cannot be prevented. An attacker could for example manipulate the global navigation satellite system (GNSS) signal that is received and processed by the VANET nodes.

Hence, detecting attackers with malicious behavior is important to impede their negative influence and ensure long-term reliability of VANETs functionality. Applying an IDS as security mechanism is a well-known concept in different kinds of computer networks. However, VANETs have unique characteristics and features, hence different requirements have to be considered compared to wired networks, classical wireless networks, or mobile ad hoc networks (MANETs). The main challenges in VANETs are:

a) decentralized character due to rare infrastructure connections,
b) possibly short connection times between network nodes (e. g. vehicles or roadside units),
c) frequent change of temporary pseudonymous node identifiers,
d) handling of physical input and output,
e) imprecise and not synchronized data originating from different nodes.

Additionally, detecting adversaries is challenging, especially since no practical experience from a real network is available in the current status of VANET deployment.

1.4. Goals

As addressed in the motivation and the problem description, reactive security mechanisms in form of misbehavior detection and long-term attacker identification are important to ensure the reliable long-term operation of vehicular ad hoc networks. The main goal of this work is to develop mechanisms to detect faulty vehicles and attackers in the wireless ad hoc communication by applying autonomous data consistency and plausibility checks on every node in a VANET.

It has to be considered that the structure of communication networks is usually organized in layers (cf. open systems interconnection (OSI) model) [Tan03]. In general, every layer is responsible for a different functionality and upper layers can rely on services provided by lower layers. For example, the packet routing functionality is provided by the network layer and applications on upper layers assume that outgoing packets are equipped with appropriate routing information so that they are routed correctly through the network to the destination. In principle, the check of information plausibility is reasonable for the individual data on every layer. However, in this work we focus on location data-based plausibility checks that validate the correctness of mobility information (i. e. absolute position, heading, speed and time) of neighboring network nodes. This kind of information is exchanged frequently (i. e. with a frequency up to 10 Hz [ETS10d]) and basically all VANET applications rely on location-related data received from neighbors [ETS09]. Consequently, network nodes that attract attention due to repeatedly non-plausible behavior should be detected and considered as potential attackers.

Since privacy protection plays an essential role in VANETs, the design of a mechanism for long-term attacker identification has to consider different privacy preserving requirements. In order to protect the driver privacy, vehicles use temporary pseudonymous identifiers in the wireless ad hoc communication that are changed randomly [GG07]. This privacy protection mechanism aims to hinder internal and external attackers to create long-term traces and traffic profiles based on recorded communication traffic. In the same way, single central entities should not be able to link pseudonymous identifiers to long-term vehicle identifiers. A credential provider, for example, should not be able to link on its own pseudonymous identifiers from wireless communications to a number plate or a vehicle identification number (VIN). Likewise, the measures for misbehavior detection and attacker identification must not weaken the driver privacy.

Figure 1.1 shows our proposed general strategy for misbehavior detection and long-term attacker identification in VANETs. The attacker vehicle A and the benign vehicle B communicate through a VANET using cryptographic credentials such as asymmetric keys and certificates that ensure the authentication and authorization of the sender as well as the message integrity. After a while, vehicle B

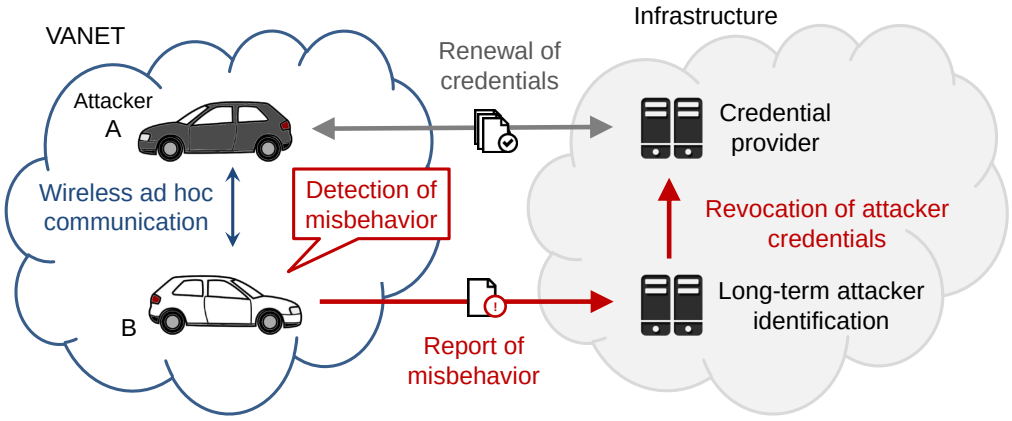


Figure 1.1.: Strategy for misbehavior detection and attacker identification in VANETs

detects a potential misbehavior of vehicle *A* based on mobility data consistency and plausibility checks. As soon as the suspicion is substantiated vehicle *B* reports the misbehavior to the infrastructure for attacker identification. It has to be considered that vehicles can frequently change their pseudonymous identifiers in order to preserve drivers' privacy. Therefore, it may be necessary to involve the credential provider such as a public key infrastructure (PKI) in order to identify the source of misbehavior. After the identification of the attacker, the credential provider revokes the attacker's credentials or rejects certificate renewal requests originating from the identified attacker. The disturbing network nodes should be prevented to actively participate in VANET communications until their correct behavior can be ensured. Furthermore, it has to be ensured in this process that attackers are not able to discredit benign nodes with faked misbehavior reports.

In addition to the reporting of misbehavior, the results of mobility data plausibility checks can be used locally by vehicular applications on upper layers to decide whether received information can be considered trustworthy or if information provided by suspicious neighbors should be handled with caution.

1.5. Contributions

We address specific scientific challenges by dividing the topic into two separate steps: misbehavior detection and attacker identification.

In the first step different mechanisms for misbehavior detection are analyzed that are based on incoming messages originating from neighboring nodes as well as local sensor data of the own node. Based on generic approaches and frameworks of published research (cf. Section 3.1.2 and 3.1.3), we propose several distinct frameworks for plausibility checking of mobility data received from neighbor nodes. Since most existing solutions are only evaluated within simulations we comprehensively analyzed the applicability of misbehavior detection in VANETs under real conditions. By participating in a large scale field operational test and performing dedicated trials with test vehicles we gained new insights with respect to misbehavior detection and attacker identification. Based on this knowledge

we developed the framework illustrated in Figure 1.1 that considers the local detection of misbehavior on VANET nodes and the central long-term identification of attackers and faulty nodes. As a result, we can show that plausibility checking by means of probabilistic instruments is applicable in VANETs under consideration of realistic system requirements and privacy protection aspects.

In order to increase the detection rate of non-existing, so-called "ghost" vehicles, we propose in this dissertation a new mechanism to detect conflicting location claims of nodes within single-hop communication range. The proposed mechanisms enable the detection of location-based attacks without creating additional communication overhead on the wireless ad hoc channel and without requiring specific hardware sensors at the network nodes. We evaluated our contribution by means of simulation and by using movement and message data from recorded real vehicle traces. Moreover, the applicability of the misbehavior detection system has been analyzed with test vehicles on dedicated test areas and public roads. In these tests, our framework was deployed over 15 weeks on 220 different stations and approximately 17 billion messages were checked. The evaluations have shown that attacks on the VANET communication can be detected reliably by nodes of the VANET using our proposed mechanisms.

In the second step the applicability of results from the local misbehavior detection system is analyzed in order to temporarily identify the attacker on the decentralized VANET node. An optimal MDS would allow to immediately exclude attackers as soon as they are detected without exchanging further information with other local or central entities. We demonstrate a mechanism to evaluate neighbor node trustworthiness based on received location-related data and observed behavior. The resulting information about node trust can be used by VANET applications in order to support their decision-making process in critical situations. If, for example, a vehicle *B* receives from an ahead driving vehicle *A* an emergency braking notification while the misbehavior detection system at vehicle *B* rates vehicle *A* not to be trustworthy, the application on vehicle *B* might suppress a driver notification until further trustworthy information is collected. However, we show that a reliable long-term attacker identification on the network nodes is not possible due to the dynamic topology of VANETs and applied privacy enhancing technologies (PETs). In particular, the VANET nodes can identify other nodes only based on their pseudonymous identifiers that change frequently. Our evaluations, based on recorded real vehicle traces, substantiate the fact that locally on the VANET nodes a long-term identification of attackers is not possible (as intended by the applied PET).

As a consequence, it is analyzed whether attackers can be identified more reliably at a central entity. Based on this analysis we developed a new mechanism for the centralized evaluation of misbehavior reports and the subsequent exclusion of attackers. In the context of VANET security our centralized mechanism is unique as it takes operational aspects such as scalability and node identification into account while considering necessary privacy protection requirements. In this concept, VANET nodes detect misbehavior based on local data plausibility checks and create misbehavior reports that are transmitted to a central misbehavior evaluation authority (MEA). The central entity is able to filter fake reports that are created by an attacker aiming to hide its malicious behavior or blame benign nodes arbitrarily. This is possible as the MEA can check whether two pseudonyms from related reports belong to the same node. In order to support the latter function, the integration of a privacy-friendly pseudonym resolution protocol with the pseudonym credential provider infrastructure (i. e. PKI) is proposed.

Based on simulation we show that the detection of attacker nodes is possible even if colluding attackers are reporting fake misbehavior reports.

The main research questions answered in this dissertation can be summarized as follows:

(1) How is it possible to detect internal misbehaving network nodes?

It is analyzed whether the inspection of mobility data is sufficient to distinguish messages sent by faulty or malicious nodes and messages sent by benign nodes. Considering realistic movements of network nodes including abrupt driving behavior is important. Moreover, outstanding traffic events such as accidents should not lead to an exclusion of involved vehicles. In this dissertation the hypothesis should be verified that location-related abnormalities introduced in Section 1.2 can be detected as long as the abnormal behavior happens within a sensor observed area of a benign single-hop communication neighbor.

(2) Are VANET nodes able to identify attackers under consideration of privacy protection mechanisms?

In order to protect the privacy of drivers, the identifiers of the different layers of the vehicular communication system (e. g. MAC address on data link layer, IP address on network layer, station ID on application layer) change frequently by applying a simple random algorithm [GG07] or a more sophisticated context-based algorithm [ESG+10]. In this dissertation the hypothesis should be verified that attackers cannot be excluded permanently from active participation in VANET communications as long as the pseudonymous identifiers can be changed frequently. We assume that linking information related to different pseudonymous identifiers must not be exchanged between the nodes of the vehicular ad hoc network in order to protect the drivers' privacy.

(3) Is a central identification of attackers feasible in order to support the long-term operation of the VANET?

Local MDS running on the decentralized VANET nodes are able to detect potential misbehavior but, however, a reliable long-term identification of attackers may only be possible at a central entity. It should be investigated whether a central mechanism is able to exclude faulty nodes and attackers from active VANET participation in order to support the operational reliability of the network. The hypothesis should be verified that faulty and malicious nodes can be excluded having a majority of benign independent misbehavior reporters. On the other hand, false-positive detections and fake reports should not lead to an exclusion of benign nodes.

(4) Is it possible to apply a central attacker identification scheme that meets relevant privacy protection requirements?

According to the privacy protection requirements in VANETs third parties must not be able to arbitrarily track vehicles. Additionally, internal security entities such as credential providers should not be able to track and identify vehicles over long periods of time. Therefore, the central misbehavior report evaluation authority has to be designed privacy-friendly. It should be studied how misbehavior detection and evaluation effect the drivers' privacy. The hypothesis should be verified that the central processing of misbehavior is possible without revealing long-term identifiers of benign nodes.

Moreover, the fundamentals of location-related data checking are analyzed in detail in this dissertation. Based on these checks, the principle possibilities for misbehavior detection, temporary attacker identification, long-term attacker identification, and attacker exclusion are evaluated in the context of VANETs. Beyond the consideration of basic fundamentals, relevant practical requirements such as reliability, efficiency, scalability, and applicability are taken into account in our proposals.

Our research results might also be relevant for other ICT domains since detection and identification of internal attackers is desired in most communication systems. However, the IDS applied in enterprise networks is only partially comparable with mechanisms for misbehavior detection in VANETs as discussed in Section 1.2. More relevant are cyber-physical systems that handle physical input and output. For example, the aerospace and automotive domain primarily focus on location and mobility-related data. However, other CPS domains such as manufacturing, chemical processing, energy, or transportation may focus on other system and environmental information such as power consumption, temperature, pressure, composition of material, liquid or gas. In this context our research results may be relevant to improve misbehavior detection and attacker exclusion. Although we focus on the processing of location-related information our proposed methods for misbehavior detection are flexible by means of input data, cf. Sections 3.2 and 3.6. Moreover, with the local and central evaluation of node trustworthiness under consideration of PETs we contribute to the research in the context of CPS security. For instance, CPS devices applied in domains energy, entertainment, consumer electronics, or home automation may be equipped with short-term pseudonymous IDs in order to protect the users' privacy. Although we focus on VANET communications in this dissertation our work is aiming for contributing to the general scientific research in the field of flexible and adaptable security architectures with respect to misbehavior detection and attacker identification.

1.6. Structure of the Dissertation

This dissertation is arranged in three main parts. In Part I we introduce and motivate our work and provide necessary foundations of misbehavior detection and attacker identification in VANETs. The main contributions of our work are presented in Part II and Part III. First we provide our contributions to the local misbehavior detection that are applied by autonomous implementations on network nodes. Subsequently, the contributions to the attacker identification both performed locally on network nodes and centrally at a misbehavior evaluation authority are detailed. In Part IV we conclude the dissertation and provide appendices to our work.

2. Vehicular Ad hoc Networks

As motivated in Chapter 1 the detection of misbehavior is an important aspect in order to increase the dependability of communication networks. This chapter introduces the vehicular ad hoc network (VANET) as the field of application for our research on misbehavior detection and attacker identification. A definition of the VANET-specific participants and communications is given in Section 2.1. Section 2.2 introduces general security and privacy mechanisms that aim for network protection against external attackers in VANETs. Finally in Section 2.3 different attack types are discussed and the adversary model is presented.

2.1. Characteristics, Participants and Communications of VANETs

A vehicular ad hoc network aims to enable for vehicles a wide range of new traffic safety and efficiency applications but also multimedia and convenience applications. In addition, a VANET exhibits unique characteristics compared to mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs) that require specific measures for misbehavior detection and attacker identification. It is assumed that every node of the VANET is aware of its own current position. Vehicles are equipped with a global navigation satellite system (GNSS) receiver, for example of the global positioning system (GPS), to determine their absolute position. Vehicles may further correct positional errors using differential GNSS services, dead reckoning technologies based on movement information from local sensors (e. g. velocity sensor, angle of steering wheel), and information derived from digital maps. The main characteristics of VANETs are summarized in Table 2.1 in combination with their challenges for misbehavior detection and attacker identification.

Table 2.1.: Relevant characteristics and challenges of VANETs with respect to misbehavior detection and attacker identification

Attribute	Description	Challenges
Synchronization	Information from different sources is received at different times in different intervals.	Updates of own sensors such as the GNSS position or radar measurements must be synchronized with received location information.

Attribute	Description	Challenges
Scalability	The communication range covers a radius of up to 1 km [ETS10b, IEE10] and more than 100 nodes are assumed to be in reception range. Theoretic models and simulations show incoming packet rates of 1,000 packets per second [SBK+11].	The communication systems and the applications running on the nodes have to handle a large number of incoming messages without adding large delays.
Mobility	Vehicles are possibly driving with high speeds and the behavior of the driver is not necessarily predetermined.	The connections between vehicles are ephemeral.
Bandwidth and connectivity limitations	The bandwidth of the wireless channels is limited to the frequency band of VANET communications [ETS10b]. Additionally, a permanent connection to the infrastructure cannot be assumed.	Security solutions that need to cooperatively exchange data with neighbor nodes are not able to broadcast a large amount of security related data such as neighborhood tables, radar detections, etc.
Pseudonymity	In order to protect the privacy of drivers the node identifiers (i. e. vehicle identifiers) are changing frequently and unexpectedly.	Applications running on the nodes cannot rely on long-term node identifiers and the use of pseudonyms impede a long-term observation of the node's behavior. Attackers could misuse this feature to hide malicious behavior by frequently changing the node's ID.

Main participants of the VANET are vehicles and roadside facilities that aim to support the ad hoc communication between vehicles. The access points at the roadside act as gateways between the vehicles and backend services (e. g. central traffic management or fleet management) and additionally support multi-hop packet routing between distant vehicles. Access to cellular networks that may be used by vehicles to communicate with backend services are not assumed to be available in all vehicles. In this work, we focus on three participants in VANET communications: *vehicle station*, *roadside station*, and *central station* as depicted in Figure 2.1.

The representation of participants and communication channels in this figure is based on the description of the intelligent transportation system (ITS) architecture provided by the U.S. Department of Transportation [RA12] and ETSI [ETS10a]. Since these participants form a network with the depicted communication channels the participants are further named *node* of the VANET and *station* of the ITS. In the following listing, the main participants of a VANET are discussed including their most important components.

- **Vehicle stations** consist of an on-board unit (OBU) that is running the VANET applications, the communication facilities (i. e. radio, communication stack, etc.) and connects to the on-board network. The security subsystem of the station is connected to the OBU or comes as part of it.

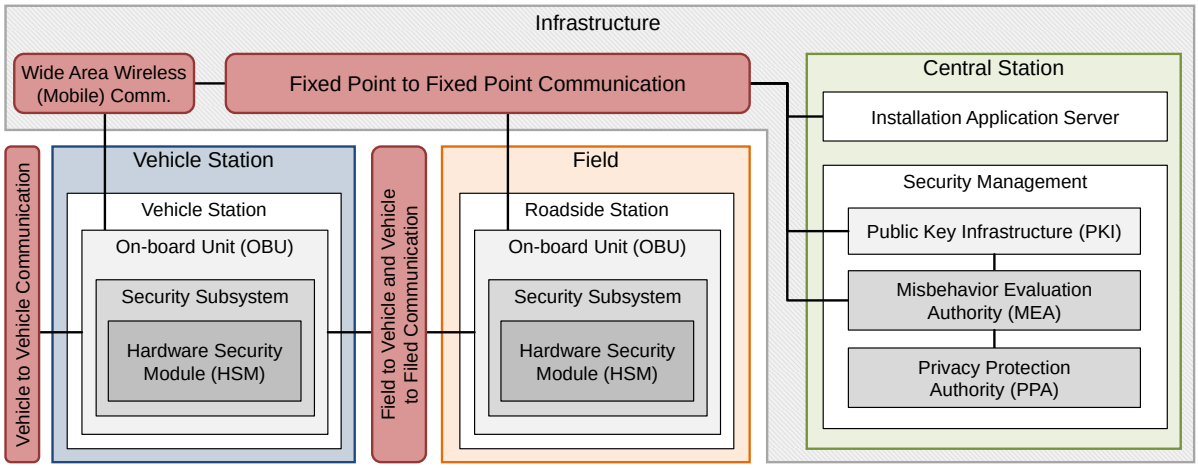


Figure 2.1.: Participants and communication links of an Intelligent transportation system architecture [ETS10a, RA12]

The subsystem provides security services to protect the on-board communication and the external VANET communication. A hardware security module (HSM) is used in the security subsystem to store cryptographic credentials (e. g. private keys) and accelerate cryptographic operations. In parallel it acts as a trust anchor.

- In the **field**, the most important participants are roadside stations:
  - The **roadside station**, also known as **roadside unit (RSU)**, consists of the same components as a vehicle station (i. e. OBU, security subsystem, HSM). The roadside station is able to act as gateway between the vehicle communication and fixed point communication.
- The **central stations** provide the backend services. In our work, we focus on the installation application server and the security management:
  - The **installation application server** provides software for vehicle stations and roadside stations (i. e. OBU and security subsystem). Possible operators of the server may be vehicle manufacturers or suppliers. The server is able to communicate with vehicles via wide area wireless communications (e. g. UMTS, LTE) or via fixed point entities such as RSUs.
  - The **security management** in the backend is running a security credential provider such as a PKI that is used to protect the VANET communication against external attackers. The security management is connected to the vehicles via fixed point communications or wide area wireless mobile communications. Additionally, the security management may contain a misbehavior evaluation authority (MEA) and a privacy protection authority (PPA). The MEA is responsible to process misbehavior reports that are provided by vehicle stations or roadside stations via fixed point communications. The PPA is responsible to verify that in the related processes all privacy policies are followed.

According to Figure 2.1 different communication channels are used in VANETs. However, we focus in this dissertation on the wireless ad hoc data transmission between vehicles (V2V) and between vehicles and the infrastructure (V2I). This kind of communication is further denoted as **V2X**. It is

based on the IEEE standard 802.11p [IEE10] and the European profile standard for ITS operating in the 5 GHz frequency band [ETS10b].

On top of the access layer, a geographic networking routing protocol is assumed to be applied as depicted in Figure 2.2. This routing protocol is based on position information of neighboring nodes in order to forward multi-hop messages to distant nodes as unicast packet or towards a geographic area as multicast or broadcast packet [Mai04]. On top of the network & transport layer a facilities layer is

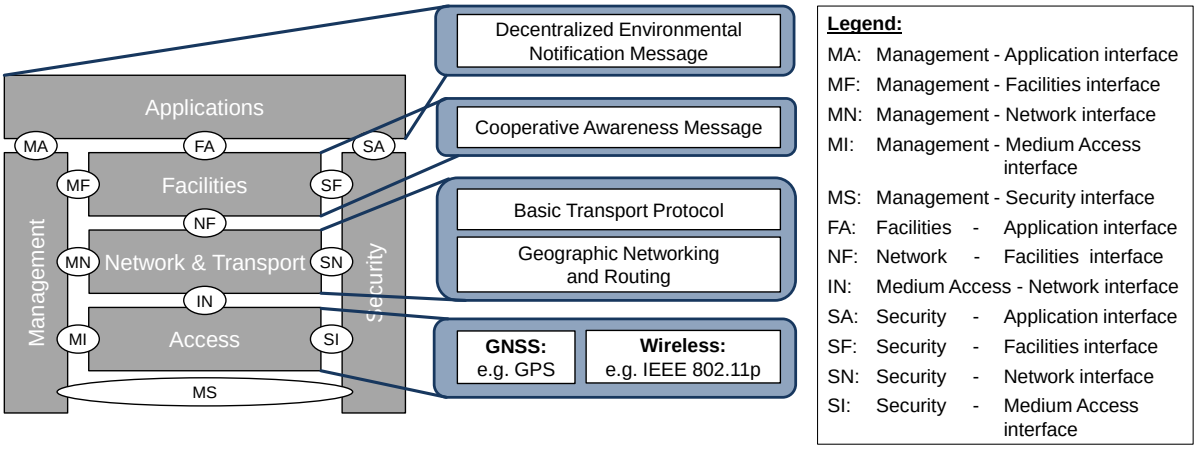


Figure 2.2.: Communication stack of VANET nodes based on ETSI [ETS10a] showing exemplary functions, message types, and technologies

located that is responsible for V2X message generation and processing.

Two basic message types are further considered in this dissertation. The **cooperative awareness message (CAM)** [ETS10d] is broadcasted periodically by all VANET nodes with up to a frequency of 10 Hz in order to publish their current position and operating state to single-hop neighbors. The **decentralized environmental notification message (DENM)** [ETS10e] however is only created and sent when a specific event occurs, for example in case of an emergency braking notification or a post crash notification. The interfaces shown in Figure 2.2 are used to hand over data between the communication layers. Additionally, orthogonal layers (i. e. management and security) are connected via interfaces to add security information to packets or update management information.

Figure 2.3 illustrates the generic message format of a V2X message that is structured in blocks. The elements of the message with a colored background are involved in the data consistency and plausibility checks discussed in this dissertation. The identifiers are highlighted with a dark blue background and the mobility data is highlighted with a light blue background. The payload shown on the right hand side of Figure 2.3 is created by the application or facilities layer. After payload generation the packet is handed over to the next lower layer. Here, the transport header and the network header is added by the network & transport layer. The position of the security header inside the packet may vary since it depends on the data that should be protected by the signature. Finally, the access layer adds a MAC header in front of the packet and a MAC frame check sequence to the end of the packet before it is sent to single-hop neighbors.

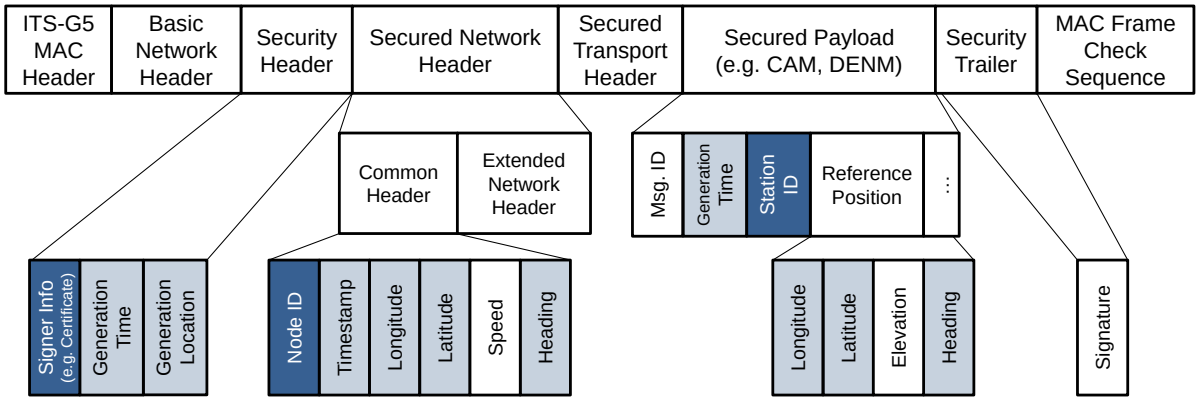


Figure 2.3.: V2X packet format used in ITS communications [ETS10d, FGJ+10, IEE13]

The combination of the wireless data transmission technology and the frequent broadcast of position information of neighbors enables V2X applications that may increase the safety and efficiency of future driving. In contrast to other environment sensors such as cameras or radar, wireless communication is not restricted to the line-of-sight environment. At the same time a relatively large amount of data can be transmitted with low latency. According to the IEEE standard 802.11p [IEE10] messages can be transmitted within a communication radius of several hundred meters by the use of one transmitter. However, this single-hop communication range can be increased to several kilometers by the use of multi-hop message forwarding techniques. As a result, V2X communications enable new applications that require low latency data transmissions between VANET nodes as described in the ETSI basic set of applications [ETS09] to create a cooperative location awareness of neighbors.

2.2. Security and Privacy in Vehicular Ad hoc Networks

In contrast to wired networks, the access to wirelessly transmitted data in VANETs cannot be restricted in general, since messages can be received by every transmitter that is tuned to the respective frequency. Consequently, a wireless network is more vulnerable to attacks from external attackers than a wired network. In order to exclude external attackers appropriate security mechanisms must be integrated [ETS13c, GFL+05]. Relevant protection mechanisms are extensively discussed in scientific research papers [LSM07, PBH+08]. These mechanisms have been refined to be applied in field operational tests as discussed by the author of this dissertation in [BSM+09], [MBS+09], and [SBK+11].

With cryptographic security mechanisms in place, access to message content can be restricted as discussed in Section 2.2.1. Nevertheless, internal attackers, coming as nodes that are in possession of valid cryptographic credentials, are still able to distribute bogus information. In order to detect authenticated but misbehaving nodes, the VANET security architecture shall consider data plausibility checks according to emerging standards [ETS10c], [ETS12a], and [ETS13a]. Data plausibility checks are subsequently discussed in detail in Section 2.2.2.

2.2.1. Cryptographic Mechanisms

The protection of wireless networks by means of cryptographic credentials is a common approach. Classical wireless networks that use a central access point and that are based on IEEE 802.11 a/b/g/n are mostly protected by the IEEE 802.11i security protocols or the comparable protocols from the Wi-Fi alliance (i. e. WPA and WPA2). These security protocols basically support two different strategies for user authentication. Furthermore they usually encrypt the traffic which is possible due to unicast communication and the centralized topology. By using WPA-Personal for user authentication, a pre-shared key (PSK) is used. However, using the second option, WPA-Enterprise, a RADIUS[1] authentication server is required. Applying IEEE 802.11i security mechanisms in VANETs is not reasonable due to the following reasons.

a) A connection to a central authentication server is not available as used in IEEE 802.11i and WPA-Enterprise.

b) After the initial deployment phase, likely several million of nodes may belong to a VANET. Sharing a long-term PSK with all nodes as done in WPA-Personal cannot be protected against attacks. The introduction of short-term PSKs would result in a complex management and, at the same time, may require a periodic connection between vehicle nodes and the infrastructure.

c) The extensible authentication protocol (EAP) as applied in WPA-Enterprise for key exchange may introduce high delays in the ad hoc message exchange. VANET nodes have to exchange messages with low latency also under consideration of a fast changing topology, since vehicles enter and leave the communication range of adjacent nodes very fast.

d) Basic V2X messages (i. e. CAM and DENM) are broadcasted. In this case, only sender authentication and integrity of the message content is required, but the confidentiality of the transmitted data is not needed.

As a result, a customized security solution for VANETs is proposed by IEEE [IEE13] and ETSI [ETS10c, ETS13b] that is based on asymmetric keys and related certificates issued by a trusted third party. In order to ensure sender authentication and message integrity, the sender of a V2X message signs the payload (e. g. CAM) with a private key. The signature and the related certificate with the public key are appended to the packet to enable a verification at the receiver. Figure 2.3 shows the essential parts of the security header containing the signer information in form of a certificate and the signature. All receivers of the message are able to check the authentication of the sender by verifying the contained sender certificate. Additionally, the receivers have to check that the certificate is issued by a trusted third party. Subsequently, the receiver is able check the integrity of the message content by verifying the signature with the public key of the provided certificate.

In addition to the cryptographic mechanisms that care for sender authentication, message integrity, and optionally for data confidentiality, the privacy of the driver has to be protected. That means, a receiver of V2X messages must not be able to track and identify another node over long periods of time by monitoring the wireless channel. Consequently, the nodes frequently change all their identifiers contained in outgoing packets. According to Figure 2.3 the nodes can be identified by the MAC address, the network header node ID, the security signer information, and the station ID inside the CAM

[1] The remote authentication dial in user service (RADIUS) provides a centralized authentication, authorization, and accounting service for network nodes.

or DENM. Since the security signer information contains the sender's certificate, several unlinkable certificates have to be managed by the nodes which are denoted as pseudonym certificates (PCs).

The PKI concept of the Car-to-Car Communication Consortium[2] (C2C-CC) was jointly developed by the members of the task force in which the author of this dissertation was essentially involved. Several parts of the conceptional work of the C2C-CC PKI task force were driven and organized by the author of this dissertation [BSS+11]. Figure 2.4 illustrates the architecture of this PKI that issues the certificates aiming for protecting the V2X communication [BSS+11, ETS10c, oTRA12]. Three different certificate authority (CA) types are defined for the PKI. The root CA (RCA) is the trust anchor of the VANET and it issues certificates for the long-term CA (LTCA) and the pseudonym CA (PCA). Since all nodes of the VANET trust the root certificate of the RCA, the nodes consequently trust the certificates of the LTCA and PCA as well. Before a node is allowed to request new PCs for the V2X communication, it has to be enrolled at the LTCA. In the enrollment process every node is equipped with a long-term certificate (LTC). This LTC must only be used to sign requests of new PCs that are sent to the PCA. If the PCA can successfully verify the validity of the LTC, a set of different PCs is issued and provided to the requester. An equipped node can use the PCs to authenticate itself in the V2X communication and can protect at the same time the driver's privacy by frequently changing the PC and all other identifiers in outgoing packets.

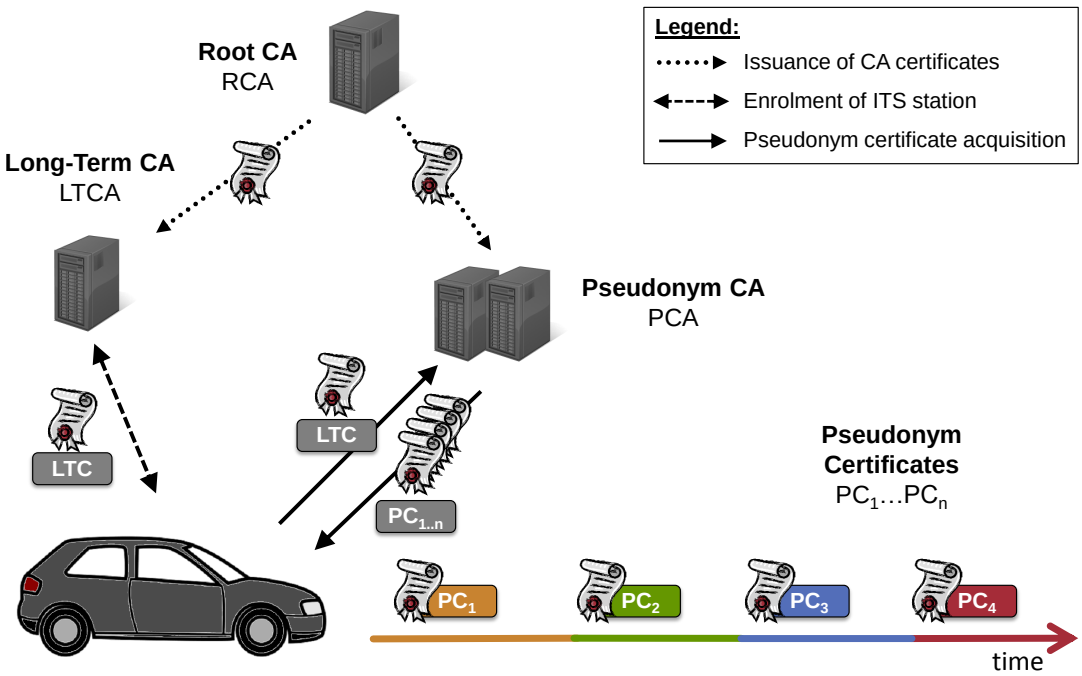


Figure 2.4.: Security and privacy in VANETs using public key cryptography [BSS+11, ETS10c, oTRA12]

[2] http://www.car-to-car.org/

2.2.2. Data Consistency and Plausibility Checks

As motivated in Chapter 1 this dissertation focuses on data plausibility checks in order to detect faults and misbehavior in the single-hop communication range. This mechanism is designed to be applied in addition to cryptographic mechanisms. An important information element in VANET communications is the position of adjacent nodes because most applications rely on it. Functions such as the geographic routing on network layer or the V2X applications require genuine, accurate and reliable location data of neighbors. As a result, we propose to verify the consistency and plausibility of location-related data of adjacent nodes that are broadcasted frequently as CAMs or geo-networking beacons. In order to be able to compare all location-related data contained in a packet it is reasonable to perform the consistency and plausibility checks on facilities or application layer. Since several V2X applications require information about the movement plausibility of neighbor nodes, the integration of a single instantiation of a location data-based check may be reasonable to save valuable resources.

Figure 2.3 shows that information about a sender's position may be placed at different parts of a V2X packet. The network header contains a common header with ID as well as location and timing information of the sender [FGJ+10]. The security header contains the signer information and possibly also a generation time and location according to the IEEE 1609.2 standard [IEE13] or the ETSI TS 103 097 standard [ETS13b]. Finally, the payload (e. g. CAM [ETS10d] or DENM [ETS10e]) contains the sender's ID and location with a related timestamp. In order to perform data plausibility checks and consistency verifications a standardized way is required to represent this relevant information from packets irrespective of specific message formats. The relevant information is denoted as Position Vector (PV). Table 2.2 summarizes the PV contents.

Table 2.2.: Content of a position vector

Entry	Description	Example
Identifier	The pseudonymous identifiers of a neighbor node are provided with every V2X message. The IDs on the layers of the communication stack may have different formats but should be derived from the certificate ID that is created by the security layer. The certificate ID can be generated by hashing the bytes of the certificate according to IEEE 1609.2 [IEE13] or ETSI TS 103 097 [ETS13b]. Since these identifiers periodically change, the IDs can only be used to temporarily distinguish the neighbors.	Certificate ID: 0ec6e51b5a7a722a
		MAC address: 5a:7a:72:ff:fe:2a
		Network layer node identifier: 1064790267564552746
		Station identifier: 7564552746
Timestamp	The absolute timestamp is derived from the GNSS and is therefore synchronized between all VANET nodes. It shows the number of milliseconds since a defined point in time, for example since 1st January, 1970 (UTC).	11 September 2012 17:30:59.000 = 1347377459000

Entry	Description	Example
Position	Absolute position encoded as world geodetic system coordinate (WGS84) or as universal transverse mercator (UTM) coordinate.	WGS84: latitude = 49.871654°, longitude = 8.638208°
		UTM: easting = 474002.49m, northing = 5524423.53m, zone = 32U
Heading	Course angle of the position. 0° = north, 90° = east, 180° = south, 270° = west.	Driving direction towards north-west = 45.00°
Velocity	Optionally, the velocity reported by neighbors can be used. Alternatively, it is calculated based on the driven distance between two messages.	30m/s
Yaw velocity	The yaw velocity describes the speed of a vehicle rotation around the yaw-axis (z-axis). A value is positive if the rotation is in counterclockwise direction from the bird's eye view.	0.5 rad/s
Lateral acceleration	Describes the linear acceleration parallel to the lateral axis of the node. A positive value is given if the node turns left and a negative value is given if the node turns right.	1.2 m/s^2
Longitudinal acceleration	Describes the linear acceleration parallel to the longitudinal axis of the node. A positive value is given for accelerations and a negative value is given for decelerations.	-3.5 m/s^2

In addition to the information included in messages received from V2X neighbors, the consistency and plausibility checker requires mobility information of the own station. At minimum, a frequently updated PV of the own system is required in order to verify the plausibility of received information. To increase the quality of plausibility checking the framework can further leverage different independent sources of information that confirm or disprove a specific situation. Table 2.3 describes secondary local information sources that may be used to check whether a stated position of a neighbor node is plausible.

Table 2.3.: Secondary local information sources used by data plausibility checks

Information source	Description
Digital road map	Digital maps provide accurate representations of a particular area, detailing most road arteries and further give other traffic related information.
Environment sensors	Cameras, radar, lidar or ultrasonic sensors are able to provide information about the environment in line of sight. For example, a lidar or two camera arranged side by side allow a three dimensional recognition of the environment.
Directional antennas	Antenna arrays or directional antennas allow a rough position estimation of senders in wireless networks, cf. [SJWH11].

2.3. Adversary Model

This section presents the adversary model which serves as a basis for the development of countermeasures within this dissertation. The severity of a threat caused by an adversary depends on its abilities, technical knowledge and methods on accessing the attack target. Different types of attackers can be clustered into different groups according to their possibilities, motivations and situations [MBS+09, SBK+11]. Therefore different motivations for attacks on VANETs are discussed in Section 2.3.1. Further, different variants and situations can be distinguished as presented in Section 2.3.2. However, this dissertation focuses on misbehavior detection that is caused by location-based attacks. Therefore, this kind of attack is presented in detail in Section 2.3.3.

2.3.1. Attacker Motivation

Understanding the motivation of an attacker is important to determine the risk of specific attacks. Table 2.4 categorizes the motivation of possible attackers and provides examples for a related attack [SBK+11]. In this dissertation we focus on incentives that may motivate location-based attacks.

Table 2.4.: Classification of attacker motivations

Motivation	Examples
Physical harm, vandalism, terrorism, robbery, kidnapping	Causing an accident
	Denial of Service of VANET nodes and communications
	Reduce trust in V2X communications by provoking false driver warnings
	Reducing road traffic efficiency such as provoking traffic congestions in order to reroute the traffic
Financial incentives	Insurance fraud: After an accident, the vehicle owner could try to manipulate the recorded location data stored in the vehicle in order to obscure liable behavior
	Create and distribute personal advertisement without agreement of the receiver
	Infringement of car manufacturer's intellectual property
Non monetary personal motivation	Gain reputation as hacker
	Get the ability to run own malware on VANET nodes in order to increase the hacker's reputation or to prepare other attacks
	Enhancement of the attacker's traffic conditions, e. g. freeing the fast lane on a highway

2.3.2. Attack Variants

In general, different different attack variants can be distinguished: passive vs. active attacks, online vs. offline attacks, and external vs. internal attacks.

Passive vs. Active Attack In a passive attack, the attacker is not able to manipulate the attacked system. For instance, an attacker could eavesdrop critical data such as private keys or certificates containing privacy relevant information. In an active attack, however, the attacker actively interacts with the system to be attacked. Typical examples for active attacks are the injection or alteration of software as well as the modification of stored data on system endpoints such as VANET nodes. Moreover, active attackers may inject or alter transmitted data within the communication between the nodes.

Passive attacks are relevant for the privacy in VANET communications as the extensive collection of wireless transmitted data within large areas may enable attackers to create movement traces of vehicles that can be linked to individuals. However, we focus in this dissertation on the detection of active attackers that actively transmit fake information. According to the definition in Section 1.2 misbehavior must be observable and classifiable. A passive attacker that does not emitting signals may only be indirectly detectable utilizing side channel information.

Online vs. Offline Attack For performing an offline attack, the attacker requires physical access to the hardware under attack. As the attack type already indicates, the system under attack is offline. That means that the software environment is not running. The attacker may access the storage of the attacked system by the use of another computer or by transplanting certain hardware components into a system controlled by the attacker. Both ways may allow for the manipulation of files or databases. Consequently, the attacker may be able to access or modify sensitive data, e. g. credentials or account data, that are not protected by appropriate mechanisms such as a Hardware Security Module [WWZ+11]. In addition, the code of V2X applications or the operating system could be modified by an attacker, which allows him to disable parts of the software or significantly change the functionality of the software.

In online attacks the executed software of the system under attack is not manipulated but vulnerability in the operating system or the applications are exploited. A vulnerability may be used to bypass a security enforcement system or to inject malicious code that is subsequently executed on the system. This may result in a temporary or permanent change of the system behavior.

We assume that an attacker is able to use both, online and offline attacks to perform location-based attacks.

External vs. Internal Attack External attackers are not authenticated and authorized to actively participate in the network. By the use of cryptography external attackers can be excluded from the network. In this case only authenticated network nodes can be equipped with valid cryptographic credentials that are not accessible by external attackers. As a result, external attackers can passively tap the communication but are not authorized to transmit messages. However, if an external attacker sends an invalid message, the receiver can detect and discard it since only messages from authenticated and authorized senders are verified successfully. In contrast, an internal attacker is equipped with valid cryptographic credentials in order to participate as a valid network node. Using only cryptographic security mechanisms, malicious activities cannot be detected and bogus messages are accepted by the receivers.

2.3.3. Location-Based Attacks in VANETs

In this section the attacker model is presented that is applied as basis for the remaining dissertation. Only with an substantiated attacker model appropriate countermeasures can be developed. In contrast to the situation given in wired networks, Wifi networks, and MANETs typically location-related information is distributed within VANETs. Therefore, we focus on internal active online attackers that distribute false position data. In particular, the attacker can simply broadcast fake CAMs with a false position vector but with a valid digital signature. Consequently, the illusion of a vehicle can be created that exists not in the reality. We denote this kind of simulated node further as *ghost vehicle*. In general, location-based attacks can be used to create a fake event (e. g. emergency braking of a non-existing vehicle) or, in contrast, to deny a real event (e. g. denying the existence of a present traffic jam). Figure 2.5 exemplary shows a location-related attack. The ghost vehicle A_1 is created in front of a real vehicle R and performs a virtual emergency braking action. If the driver of R brakes as a reaction on a warning it could be endangered by the truck T that may not be equipped with a V2X communication unit.

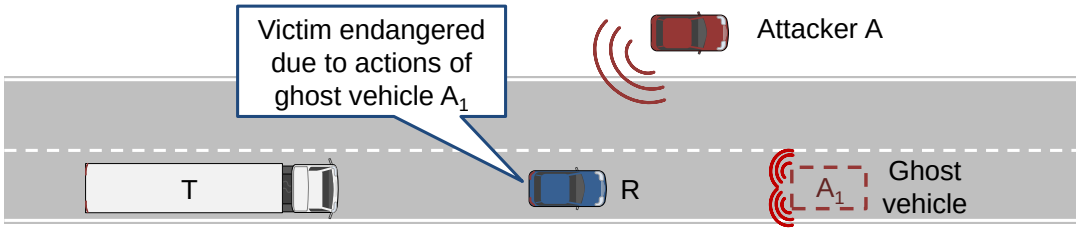


Figure 2.5.: Location-based attack: Ghost vehicle A_1 is created and placed by an attacker A in front of a real vehicle R

Furthermore, it is assumed that an internal active attacker might be able to present multiple identities in parallel to create the illusion of several ghost vehicles at the same time. This kind of attack is named *Sybil attack* and was first described by Douceur [Dou02]. Even though a central trusted authority (i. e. PKI, cf. Section 2.2.1) is used in V2X communications, VANET nodes may be equipped with a set of pseudonym certificates that have overlapping periods of validity. As a result, an attacker could use multiple pseudonym certificates in parallel to mount a Sybil attack.

In the following subsections we demonstrate the impact of location-related attacks on the traffic efficiency and on traffic safety applications. In addition to the simulation of the attacks with a traffic and communication simulator real V2X communication equipment is used to demonstrate the impact of location-based attacks.

2.3.3.1. Simulation of Location-Based Attacks

Compared to highly complex and expensive real field tests a simulation framework allows the study of effects on the traffic flow in larger scenarios with multiple variations. The simulator allows the evaluation of different scenarios with flexible configurations such as several test runs with different V2X communication unit equipment rates at involved vehicles. The evaluations can also be repeated using the setup described afterwards in this section in order to reproduce the evaluation results. For

these reasons, a software simulator is used to particularly demonstrate the impact of location-based attacks on road traffic efficiency. The design and concepts of the simulated attacks were elaborated by the author of this dissertation [BSRS11]. The subsequent implementation of required software components and the configuration of the simulation framework was supported by Christian Schmidt as part of his Bachelor thesis [SSB10] which was supervised by me.

In fact, the simulations are used to study different driver behavior schemes. However, traffic simulation itself is complex as most mathematical traffic flow models are incomplete [KHRW02]. Moreover, according to Schünemann et al. [SMR08] traffic simulation itself does not suffice for the field of V2X communications. To study the impact of attackers, a wireless communication network simulator is needed and own applications have to be executed on the simulated VANET nodes. Therefore, the framework *V2X simulation runtime infrastructure* (VSimRTI) [fAITI13, QSR08] was used that allows the integration of several simulators. The objective is to verify the hypothesis that an internal attacker is able to negatively affect the road traffic efficiency in order to motivate the application of appropriate countermeasures. As far we know this kind of evaluation of possible attacker's impact on road traffic efficiency has not been performed previously. The authors in related work mostly focus on malicious impact on packet routing in VANETs [HRM10, LS06]. In order to quantify the influence of the attacker we measured the travel time of vehicles between a starting point and a destination location.

The VSimRTI system architecture is inspired by the IEEE standard for modeling and simulation (M&S) high level architecture (HLA) [oEE00]. However, the complexity of the HLA standard and its implementation exceed the scope of a V2X simulation framework. Instead, a subset of the standard and some of its fundamental concepts were used to realize the V2X simulation framework. Hence, a lightweight framework for simulator integration was created by the Daimler Center for Automotive Information Technology Innovations [fAITI13] that facilitates the simulation of V2X communication scenarios. Communication among the simulators is enabled by the VSimRTI which is accessible by ambassadors similar to the HLA standard.

This simulation environment is further used to implement and execute attacks on the VANET by considering a subset of possible driver reactions. In the following scenarios, an attacker A is broadcasting bogus V2X messages in order to negatively affect the traffic efficiency.

Scenario 1: Attacker creates ghost vehicle on single lane road In the first scenario as shown in Figure 2.6, the attacker has a fixed position at the road side. The transmitter of the attacker is located approximately in the middle of an urban road segment of 1200 meters in length. A laptop, a compromised RSU or a parked vehicle could be used to broadcast messages with bogus content. In this first scenario, vehicles drive with 50 km/h on one lane of the road segment. Due to the mobility model applied in the traffic simulator, vehicles are not allowed to overtake by using lanes of the opposite driving direction. As a result, slow vehicles slow down also following vehicles on the same lane. As argued by Schmidt et al. [SLH09] a fixed roadside attacker can be assumed to be realistic due to the minimal effort for the attacker. In this first scenario, the attacker A is periodically broadcasting bogus CAMs and DENMs stating a ghost vehicle A_1 in an abnormal state such as being involved in a traffic accident. Vehicles in approximately 300 meters distance to the attacker receive the bogus messages and react immediately by slowing down.

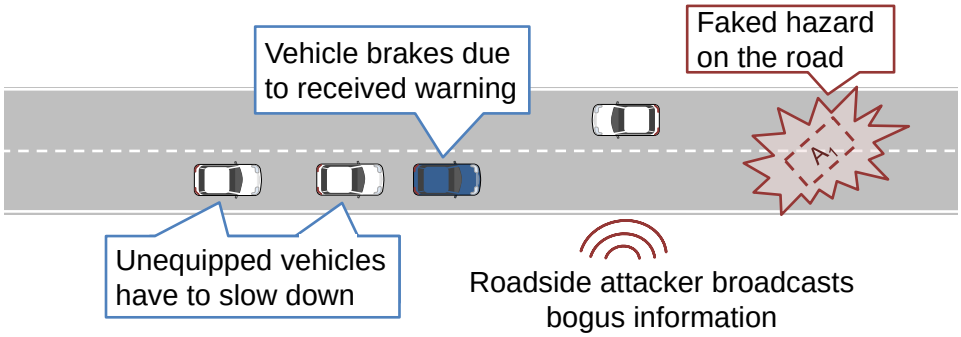


Figure 2.6.: Active internal roadside attacker creates a ghost vehicle A_1 on a single lane road

Scenario 2: Attacker creates multiple ghost vehicle on multilane highway In a second simulated scenario, illustrated in Figure 2.7, a Sybil attack is executed on a highway by a roadside attacker similar to the first scenario. In this case a road segment with a length of 1700 meters is configured. The static attacker located approximately 1100 meters behind the starting point broadcasts CAMs with different identifiers and faked positions in order to simulate a traffic congestion on a highway with 3 lanes per direction. It is assumed that vehicles equipped with a V2X communication system detect a congestion if the speed of a vehicle in the transmission range is below a defined threshold and its distance to another vehicle is smaller than the usual safety zone. In our simulations, we assume that vehicles driving slower than 10 m/sec and exhibit, additionally, a safety distance smaller than 9 meters are involved in a congestion. Vehicles that detect such a situation on the same road segment in front of their own position react on this event by slowing down such as shown in Figure 2.9.

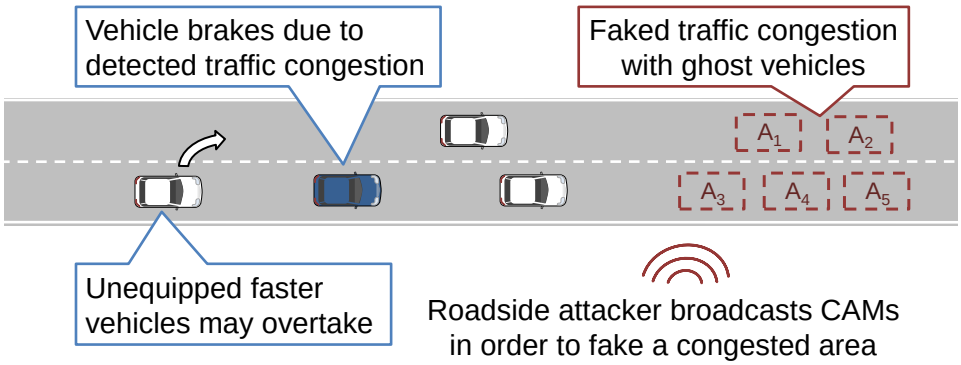


Figure 2.7.: Active internal roadside attacker executes a Sybil attack on a multilane highway

Evaluation of attack scenarios A major challenge for the evaluation of attacks is the definition of appropriate driver behavior. The behavior can not be statically defined due to the fact that different drivers may have different perceptions. Consequently two possible behavior schemes of the driver are considered in order to evaluate the impact of the attacks.

In the first scheme, the driver reduces its speed permanently to 8 m/sec as soon as the road hazard is detected. This reduced speed is kept until the end of the simulated road segment is reached. This kind of driver behavior may reflect cautious drivers who reduce their speed for a longer period of time even if no real danger can be identified on the road. The first graphs in Figures 2.8 and 2.9 represent this permanent reduction of the vehicles' velocity.

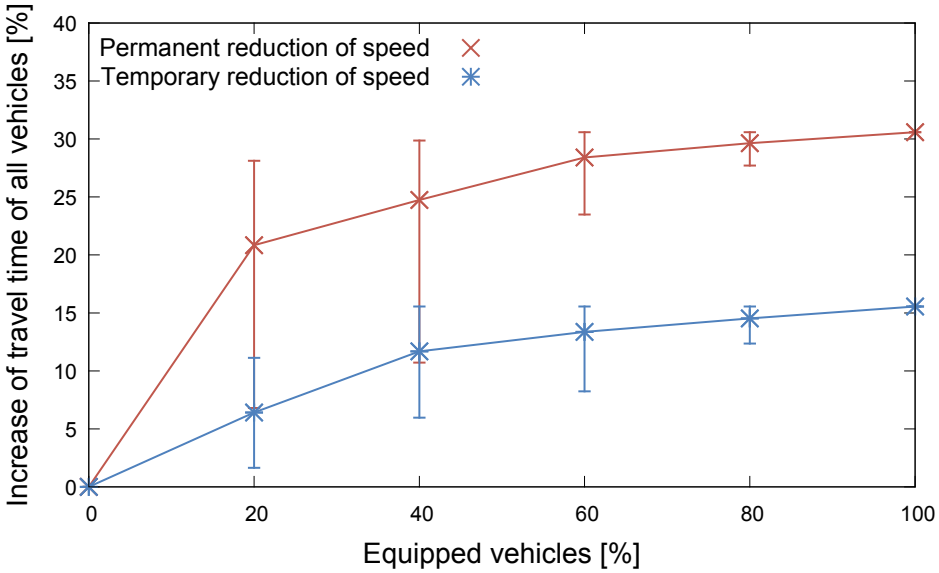


Figure 2.8.: Impact on single lane road traffic efficiency with an attacker in communication range

In the second scheme, the speed of the vehicle is reduced as soon as the transmission range of the attacker is entered and malicious messages are received. The communication simulator is configured to a communication radius of approximately 300 meters per node. Vehicles that approach the attacker's communication range are immediately informed about the road hazard and reduce their speed for approximately 250 meters to 8 m/sec. This scheme is probably the normal behavior because vehicle drivers in the real world approaching and passing a faked danger spot would see that no real danger exists and accelerate to normal speed until they have passed this area. The second graphs in Figures 2.8 and 2.9 represent this temporary reduction of the vehicles' velocity.

The graphs in Figures 2.8 and 2.9 show the effect on the overall traffic that is analyzed with increasing numbers of reacting vehicles. The figures show the average of driving time of 10 vehicles that is required between the starting point and the destination. In order to measure the reference trip time no simulated vehicle is equipped with a V2X communication unit and consequently no bogus message is processed. Further, a vehicle equipment rate of 20 %, 40 %, 60 %, 80 %, and 100 % is considered in independent simulation runs. Unequipped vehicles do not reduce their speed and may overtake slower vehicles if there is a free lane available.

As shown by the results in Figure 2.8 the impact on the overall road traffic is already significant if only 20 % of all vehicles are equipped with V2X communication units on a single lane road that is attacked (cf. Figure 2.6). Due to missing opportunities to overtake, drivers that are assuming a hazard on the road will also slow down following vehicles on the same road segment. As a result, even

unequipped vehicles may be influenced by the attacker. This impact is similar for both reaction types as distinguished by the different graphs in Figure 2.8. With 20 % equipped vehicles, the mean travel time increases up to 21 % in case of permanent speed reduction and 6 % in case of temporary speed reduction. The maximum delay exceeds 31 % and 16 % to vehicles that slow down permanently and temporarily, respectively.

Similarly, in the second scenario, depicted in Figure 2.7, vehicles equipped with a V2X communication system react as soon as they detect the congested road segment based on received bogus CAMs. However, in contrast to the single lane road segment, unequipped faster vehicles are allowed to over-

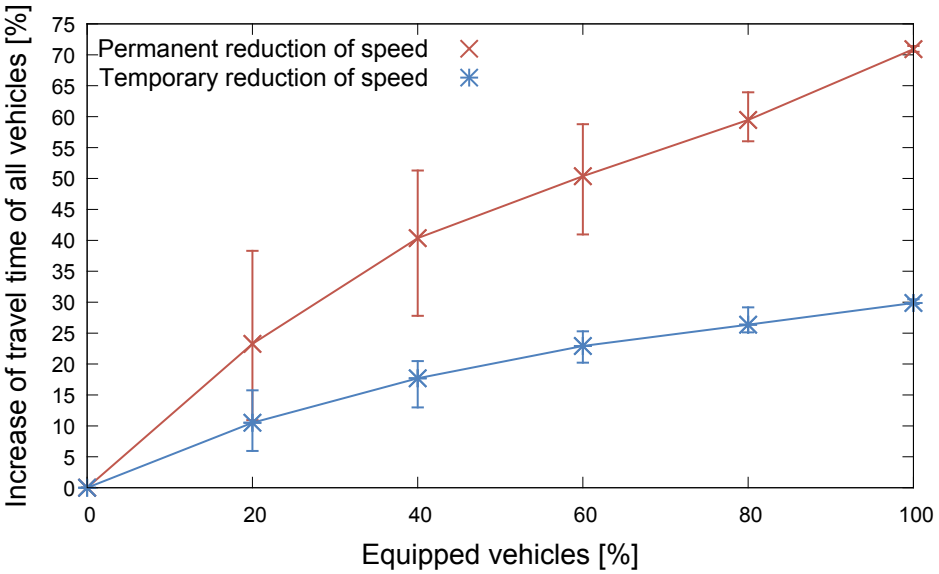


Figure 2.9.: Impact on multilane highway traffic efficiency with an attacker in communication range

take the slow vehicles. As a result, Figure 2.9 shows a linear increase of driving time. The minimal mean travel time for all vehicles from the start point to the destination is used as reference. Compared to the first scenario a different road length and another road type is used in this second scenario. Consequently the difference between normal travel speed and reduced speed due to received warnings is higher in this second scenario. For the equipped vehicles that detect the faked traffic congestion, the delay of mean travel time exceeds 71 % in case of permanent speed reduction and 30 % in case of temporary speed reduction. However, if only a subset of vehicles react on bogus information, attacks on multilane roads may have a limited impact on the overall traffic efficiency because vehicles without having a V2X communication system may not be affected.

Both kinds of attacks may exhibit an even larger impact on the traffic if faked hazard notifications are forwarded via multi-hop communication to distant nodes which take another route to their destination. In this case, the attacker may be able to reroute other vehicles in order to get a less occupied road. Nevertheless, with this experiments we have demonstrated that internal attackers are able to negatively influence the road traffic efficiency by broadcasting fake V2X messages. As a result, countermeasures have to be applied that are able to detect the attacks and identify the responsible attacker nodes.

2.3.3.2. Real Location-Based Attacks

Since the calibration of the simulator requires detailed knowledge of parameters related to communications, vehicle movement, driver behavior, and the environment the performance of real world experiments are indispensable. As a consequence we analyzed the attacker's possibilities concerning the distribution of fake location-based information using three test vehicles equipped with prototypical V2X communication units on a dedicated test track. With these experiments we analyze whether attackers are able to send false traffic safety warnings that are accepted, processed and displayed as driver warnings at vehicles in communication range. In our test setup the attacker was able to control the V2X communication system of a vehicle. The attacker manipulated only the contents of the position vector (cf. Table 2.2 on page 18) which may result in abnormalities as defined in Section 1.2.

As far we know location-based attacks on VANET communications have not previously been performed in real world scenarios. The attack variants presented in the following have been elaborated and designed by the author of this dissertation [BSP+13]. Henrik Schröder implemented and performed the experiments and evaluated subsequently the test results as part of his Master thesis [SWB13] which was supervised by me.

Our experimental location-based attack deploys a malware on the application layer of a vehicle that is equipped with a V2X communication system. This malware is able to create messages (e. g. CAMs or DENMs) with forged content that are sent out via facilities layer, network & transport layer and access layer (cf. Figure 2.2 on page 14). Without appropriate misbehavior detection and prevention mechanisms in place an application layer attacker does not need to modify the communication stack to send valid V2X messages containing faked PVs in the application payload. The PVs of the security header and the network header are not affected as they are created by the security subsystem and network layer implementation, respectively. Assuming a strict separation of layers, every layer has to cryptographically protect its own data by adding a dedicated security header. In practice this strategy would dramatically enlarge the packet size and would impede reliable high frequency broadcast communication. Consequently, a single security header is considered per packet as depicted in Figure 2.3 and targeted by field operational tests (FOTs) [Wei09, Sch13], related security projects [WWZ+11, SBK+11] and industrial consortia [WBF+13]. The applications on the receiver station consequently consider only the PV of the payload (i. e. generation time, station ID and reference position of CAMs and DENMs). An application layer attacker is able to even forge the movement paths of multiple stations by using different station IDs. However, more powerful attackers who control the complete communication stack including the security subsystem would be able to send messages that contain consistent PVs in all headers of a V2X packet.

An application layer attacker requires only limited access to components of the OBU to impact the traffic safety of other nodes when misbehavior detection is not applied. A malware on application layer can use well defined interfaces to get mobility data of the own station (i. e. time and position). Such a malware can further use the communication channels to send fake messages, has access to the local navigation support and gets the list of V2X neighbors. The developed experimental malware creates ghost vehicles by forging the PV of self generated messages. Due to the navigation support and access to the V2X neighbor list, the malware can automatically select a location on the road where a ghost vehicle has most impact on neighbors. Since the malware aims to affect V2X functions that rely on

single-hop CAMs and DENMs, the attacker has to make sure that malware-generated CAMs do not conflict with CAMs generated automatically by the facilities layer.

V2X Application: Emergency Electronic Brake Lights In order to demonstrate the impact of an application layer attacker misuse scenarios for the emergency electronic brake lights (EEBL) are discussed in the following. The EEBL application is specified by ETSI in its basic set of applications [ETS09]. Instead of using simulations, as done by most related work, an implementation on real vehicles is used in this dissertation to demonstrate the feasibility of location-based attacks. Consequently, the detailed specification of the functionality of the application has to be known by the attacker. The results of this location-based attack are applicable to several other location-related applications specified by ETSI [ETS09].

- Slow vehicle and stationary vehicle warning
- Wrong way driving warning
- Signal violation warning
- Overtaking vehicle warning and lane change assistance
- Pre-crash sensing warning
- Co-operative glare reduction
- Across traffic turn and merging traffic turn collision risk warning
- Intersection collision warning
- Co-operative merging assistance
- Co-operative forward collision warning
- Intersection management combined with traffic light optimal speed advisory
- Co-operative adaptive cruise control and platooning
- etc.

The co-operative road safety application EEBL aims to warn following vehicles of a sudden slow-down of the traffic to limit the risk of longitudinal collisions. A strong braking vehicle, equipped with a V2X communication system, immediately broadcasts a DENM that informs the receivers about a panic braking action. After the reception of the DENM, the EEBL application on single-hop neighbors calculates whether the braking vehicle is in its area of relevance. If it is relevant, the application calculates its individual time-to-crash (TTC). The relevance area is spanned in front of the receiver's vehicle with an angle rel_α and a length rel_l as depicted in Figure 2.10. If the DENM sender is inside the relevance area of the receiver R, an information or warning is shown to the driver depending on the TTC value. In case the receiver's velocity is above a defined threshold and TTC $\leq TTC_{warn}$ then the driver is warned. Otherwise, a less important EEBL information is displayed. In the experiments, the EEBL configuration is used as shown in Table 2.5.

Without appropriate misbehavior detection and prevention mechanisms, false EEBL warnings can be provoked at unmodified victim vehicles as illustrated in Figure 2.10. The malware deployed on the attacker's vehicle A analyzes the V2X neighborhood and automatically selects a victim as further detailed in the following paragraph. Subsequently, in front of victim R a ghost vehicle A_1 is created that pretends to drive in the same direction with a valid movement. After a lead time $attack_{lead}$ the

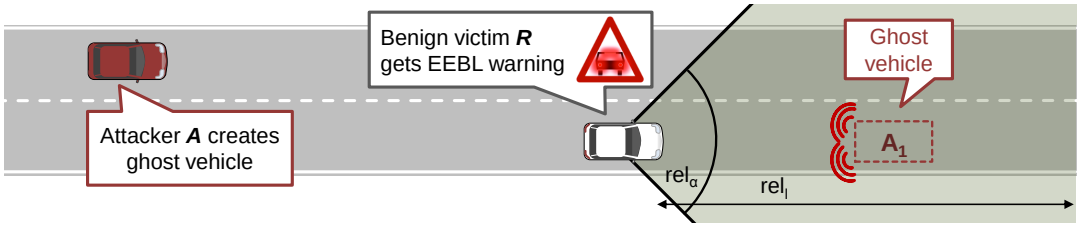


Figure 2.10.: Simulation of braking ghost vehicle by singe driving attacker

attacker broadcasts in the name of A_1 an EEBL-DENM that informs about the fake braking action. The DENM and subsequent CAMs from the attacker contain each a PV with aligned position data and a negative acceleration value of $attack_{dec}$. Since A_1 is modeled in the relevant safety area of R, the EEBL application of the victim displays a false driver warning. This may lead to an unexpected and possibly dangerous reaction of the driver.

Victim Selection The application layer malware deployed on the OBU of A is designed to trigger the unmodified EEBL application on equipped neighbors. The malware is working autonomously with data from the attacker's OBU without manual interaction or support of external entities. As soon as there is at least one single-hop vehicle station, the malware checks whether the neighbor's distance to A is below $attack_{range}$ (cf. Table 2.5). If several neighbors fulfill the conditions, the vehicle with the most straight trajectory and the highest speed is selected as victim. The malware starts to iteratively attack this vehicle for a time $attack_{dur}$ until another victim with better conditions is found. This means that the ghost vehicle is replaced after $attack_{dur}$ to a position in front of the victim.

Table 2.5.: EEBL application configuration and attacker's malware configuration

EEBL Application		**Attacker**	
Parameter	Value	Parameter	Value
rel_α	90°	$attack_{dec}$	-7.5 m/s^2
rel_l	400 m	$attack_{range}$	500 m
TTC_{warn}	5 sec	$attack_{dur}$	4 sec
		$attack_{lead}$	1 sec

Implementation of the EEBL Attack For the experimental analysis of the exemplary location-based attack three test cars were used that were fully equipped with a V2X communication system. At one of the vehicles the malware application was installed and the original CAM generation of the facilities layer was deactivated. All remaining components and functionalities on this attacker station were left unchanged. The other two cars were not modified at all and served as victims.

The OBU of the test cars provides interfaces to the vehicle's CAN bus, GPS and the wireless ITS-G5A channel based IEEE 802.11p. The applications are executed in a Java OSGi framework [All13] which provides an vehicular API to access information about the own station and the communication

channels. The application execution framework is separated from the communication stack implementation on a automotive grade personal computer with an Intel Atom D510 processor at 1.66 GHz and 2 GB of RAM.

The experiments were conducted on a dedicated test area where low speed and high speed tests could be done without endangering public road traffic. Although different test variants were performed in the experiments the next paragraph focuses on the evaluation of a test situation as illustrated in Figure 2.10.

Evaluation of the EEBL Attack The sent and received messages of the attacker and the victim as well as the mobility information of both vehicles were recorded while the tests. This enabled us to replay the attack scenario subsequently with V2X communication units in a laboratory environment. However, since only two vehicles were used in the experiments the results can easily repeated using the setup information provided in this section.

In the selected attack scenario an unmodified vehicle R is driving on a straight 2200 meters long road with constant speed of 14 m/sec. The attack outcome on unprotected receivers is shown in Figure 2.11 with time and distance on the diagram axes. The diagram shows the attack over a time of 70 seconds.

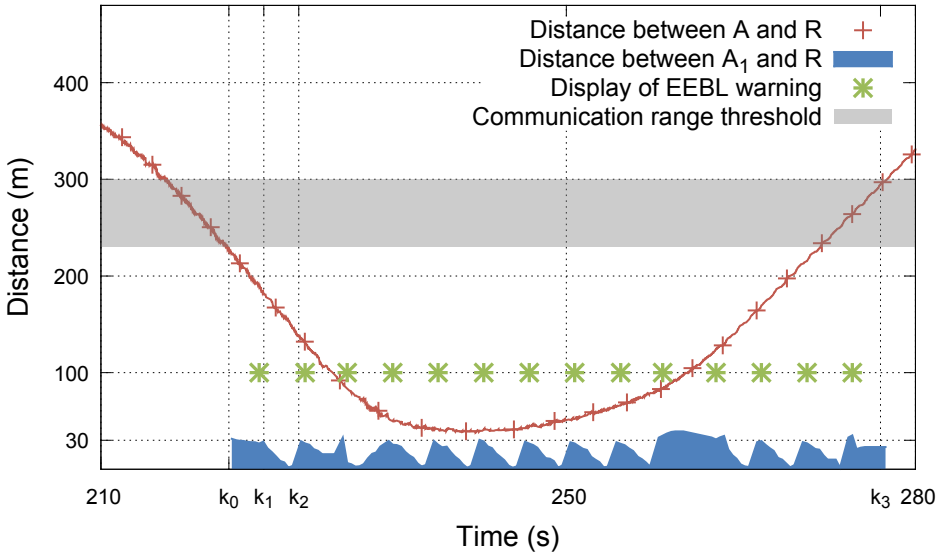


Figure 2.11.: Attacker A creates a braking ghost vehicle A_1 that provokes false driver warnings at receiver R. The victim R is not running location data-based misbehavior detection mechanisms.

At the beginning of this test, vehicle A with the running malware drives 350 meters behind the receiver vehicle R outside its communication range. The first curve shows the distance between attacker A and receiver R over the test time. As soon as A enters the communication range of R, the malware automatically detects R as victim and executes the EEBL attack by creating the ghost vehicle A_1. Shown by the filled blue curve in Figure 2.11, the attacker creates CAMs for a ghost vehicle A_1 at time k_0 and waits $attack_{lead}$ before an EEBL warning is broadcasted in the name of A_1. At this point in time A_1 is placed approximately 30 meters in front of R. After the time $attack_{lead}$ the ghost vehicle simulates an emergency braking action, decelerates and sends an EEBL-DENM at k_1 which is received

and displayed by the victim R. Since the driver of R is not (intentionally) reacting to the false warning the vehicle passes the position of the ghost vehicle a few seconds later.

As soon as the malware detects that the ghost vehicle's position is passed by the victim, it places a new ghost vehicle in front of R at time k_2 and starts another emergency braking attack. As a result, the victim R gets a new warning at each iteration. This attack is repeated until A leaves the single-hop communication range of the selected victim at time k_3. Figure 2.12 illustrated the sequence of actions and related events at time k_0, k_1, and k_2.

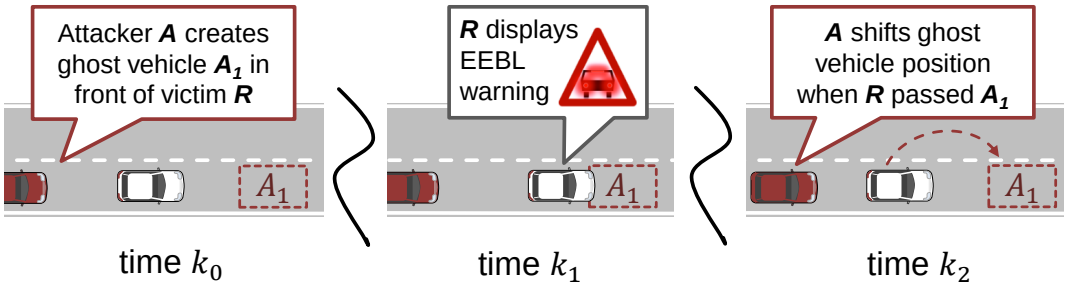


Figure 2.12.: Sequence of a ghost vehicle attack created by Attacker A

This evaluation shows that real attacks on V2X applications are possible by using an application layer malware. As long as the receiver is not protected appropriately by misbehavior detection mechanisms, an attacker can misuse the OBU with its communication stack including the security subsystem that handles valid cryptographic credentials. The attacker analysis of Bißmeyer et al. [BSP+13] has considered in addition to the application layer attacker more sophisticated attackers who are able to control the complete communication stack or parts of it. Attackers who control for example the CAN bus interface could forge the GNSS position and the movement of the local station. This attacker would additionally be able to manipulate the PV of the V2X network header and the security header without manipulating the communication stack implementation. An unrestricted attacker that is for example using a laptop is assumed to be the most powerful adversary. It operates a complete V2X communication system and possesses valid cryptographic credentials. In this dissertation we aim to detect location-based misbehavior created by all kinds of adversaries.

Extension and Limitation of the Location-Related Attacks Our experimental attack is relatively simple since the attacker does not consider the environment of the ghost vehicle. A more sophisticated attacker would probably try to imitate plausible movement of the ghost vehicle. First, the attacker would probably aim to create the ghost vehicle at the border of the communication range of the victim in order to avoid the sudden appearing of the node. However, with other vehicles in the attacker's communication range there is a high chance that other vehicles detect the ghost vehicle to be suddenly appearing. Moreover, the attacker might aim to avoid vehicle overlaps and position jumps as depicted in Figure 2.12 at time k_1 and k_2, respectively. This, however, might become challenging with increasing traffic density. The attacker has to maneuver the ghost vehicle through the road traffic without creating overlaps with other vehicles by avoiding at the same time position jumps.

In conclusion, we have demonstrated the impact of location-related attacks performed by active inter-

nal attackers. Since location and time information is consumed by most V2X applications an internal attacker is able to trigger false driver warnings at neighbors in single-hop communication range. Due to our experiments with test vehicles we confirm in this dissertation for the first time the hypothesis that internal attacks are the reality if the following conditions are given. The attacker is able to install a malware application on vehicles that is equipped with appropriate communication devices and security credentials. Additionally, the receivers are not appropriately protected by misbehavior detection systems such as consistency and plausibility checks.

Part II.

Misbehavior Detection

3. Local Misbehavior Detection on VANET Nodes

The detection of misbehavior in VANETs is essential in order to exclude internal attackers that are in the possession of V2X transceivers and valid cryptographic credentials. This part of the thesis is dedicated to mechanisms for consistency and plausibility checks of mobility data that are received from single-hop neighbors via CAMs or DENMs. The evaluation of these approaches is discussed in this chapter in relation to the single messages but also in relation to its sender node.

After the discussion of related work in Section 3.1, misbehavior detection algorithms are classified in Section 3.2. General criteria for the evaluation of the proposed mechanims are discussed in Section 3.3.

Our main contributions are discussed in the subsequent sections. A module-based misbehavior detection framework is proposed in Section 3.4 using different kinds of checks. Basic message-based value range checks and consistency checks are performed at first in this scheme. Subsequently, node-based checks are used to verify the movement of neighbor vehicles by performing a tracking based on Kalman filters. The framework has been tested and evaluated with 120 vehicles and 100 RSUs over a period of 76 days. A new scheme for detecting abnormal vehicle overlaps, is developed in Section 3.5. Finally, a misbehavior detection framework based on particle filters is presented in Section 3.6. The particle filter-based framework allows the integration of incoming data for plausibility checking and simplifies consequently the local misbehavior detection.

3.1. Related Work

Data plausibility checking and misbehavior detection in V2X communications is discussed in several publications since 2004. In the following three subsections related work regarding location-based attacks, detection mechanisms and related frameworks is discussed (Sections 3.1.1, 3.1.2, and 3.1.3). In Section 3.1.4 an evaluation of this related work with respect to this dissertation is presented.

3.1.1. Location-Based Attacks

Reactive misbehavior detection mechanisms are required to detect location-related attacker in a VANET as analyzed in [ETS13c, LHSW04, LSM07, SBK+11]. Leinmüller et al. [LHSW04, LSM07] identified that the application of classical network intrusion detection systems is limited because they primarily base on signature and anomaly detections. In contrast, a context-related verification of position and timing data is more promising in VANETs. The authors further argue that reactive concepts such as plausibility checking and misbehavior detection are key security concepts for securing active safety applications. The authors in [LSS+08] and [LSKM05] showed that position forging attacks with created ghost vehicles are most severe for VANET security. They assume that an attacker is able to apply the following attack variants: forging single positions, forging multiple positions with different IDs,

forging a movement path of a single node or forging multiple movement paths with different node IDs. Similarly, Papadimitratos [Pap08] argues that the most dangerous adversary is an internal attacker that possesses cryptographic keys and credentials to participate in V2X communications.

3.1.2. Location Data-Related Plausibility Checking

In order to detect ghost vehicles, the following context-related mobility data plausibility and consistency checks are proposed by different authors of research papers [FCCP13], [Ger10], [GGS04], [LMSK06], [LSK06], [SLH09], [SLS+08], [Sch09] and within research projects such as SEVECOM [Kun08] or sim^{TD} [MBS+09]. In the following listing related mechanisms are presented in an unstructured manner. A categorization of relevant mechanisms is subsequently proposed in Section 3.2.

- Different authors of related work propose to consider an acceptance range related to received messages in order to detect senders that are not inside the receivers communication range. This test has been first proposed by Golle et al. [GGS04]. The behavior related to this attack is also known as wormhole attack in wireless networks [HPJ06]. In addition to the position freshness check, the authors of IEEE 1609.2 [IEE13] and ETSI TS 102 731 [ETS10c] propose to check the freshness of timestamps in order to detect replayed messages.
- Leinmüller et al. [LSK06] and Gerlach [Ger10] propose to observe the mobility of nodes in order to detect implausible movement traces that contain for example position jumps.
- Yan et al. [YOW08] propose a concept that is used to verify position claims of single-hop neighbor nodes with omni-directional radar sensors. Several authors of related work propose to use context and environment information in order to verify mobility data provided by neighboring VANET nodes.
- Douceur [Dou02] proposes to verify the maximum vehicle density in order to detect Sybil attacks.
- Leinmüller et al. [LSK06] and Gerlach [Ger10] propose to verify the stated positions provided in V2X messages in relation to digital maps.
- Jaeger et al. [JBSH11] propose to verify of the maximum beaconing frequency in order to detect denial-of-service (DoS) attacks.
- Different authors of related work propose to eavesdrop messages in order to monitor the forwarding behavior of neighboring nodes. A first mechanism is described by Marti et al. [MGLB00] in the context of MANET routing. Kozma et al. [KL08] and Tian et al. [TWLY10] adopted this approach to perform intrusion detection in VANETs. However, only the related work is relevant that consider geographic routing protocols because ETSI standards focus on this type of packet forwarding in the multi-hop routing strategy of V2X communication [ETS11].
- The proactive and reactive exchange of neighbor tables for consistency verification is proposed by different authors, such as Leinmüller et al. [LSK06], Schmidt et al. [SLS+08], and Yan et al. [YCO09]. In particular, in [YCO09] Yan et al. propose the distribution of a list that contains radar confirmed neighbor vehicle positions in order to detect Sybil attacks cooperatively.

- Schmidt et al. [SLS+08] propose the check of a minimum moved distance in order to identify static roadside attackers. The authors argue that location-related attacks performed by static attackers are more likely than attacks performed by mobile attackers due complexity reasons.
- Schmidt et al. [SLS+08] propose also the detection of suddenly appearing nodes in the receiver's vicinity. The authors aim to detect in particular static attackers with this mechanism.
- Hubaux et al. [HCL04] are the first that propose to detect invalid location claims based on a received signal strength indicator (RSSI). The protocols proposed by Hubaux et al. [HCL04] and Demirbas et al. [DS06] need at least four static RSUs that analyze the transmission power of a sender in order to detect false position claims and Sybil attacks. Unfortunately, the RSSI-based position estimation technique is not very accurate. Therefore, Laurendeau et al. [LB09] and Xiao et al. [XYG06] propose to consider only the direction of the signal source. Ren et al. [RLY+09] propose further a relative location verification by using directional antennas to distinguish between vehicles in front and behind.
- Fiore et al. [FCCP13] propose an active protocol for neighbor position verification based on time-of-flight radio frequency ranging technologies. This active challenge-response protocol can be used to reliably detect attackers who fake their location. However, this protocol might need an additional communication channel in order to exchange the challenge-response messages.

The authors of [LHSW04] and [ODS07] propose to consider additionally application-specific knowledge for misbehavior detection. In the latter reference, the authors focus on misbehavior detection based on received hazard messages by comparing notifications about the same event from different originators. Gosh et al. [GVKG09] propose to check the consistency of post crash notifications in order to identify false warnings. They compare vehicle trajectories and driving habits in order to detect application specific misbehavior.

In order to detect Sybil attacks, the authors of [CWHZ09], [PATZ09], [XYG06], and [ZCNC07] assume a dense network of RSUs that can assist the verification of stated vehicle positions. These approaches assume that a tracking of vehicles is possible over a large area so that RSUs can recognize a vehicle at different locations. However, the authors of [ZCNC07] propose to use a trusted third party that allows only RSUs to recognize the vehicles. In a similar way, the authors of [CWHZ09] assume that RSUs broadcast frequently special messages and certificates that are used to detect Sybil nodes based on timestamps contained in the signed RSU messages. Anonymous credentials are another kind of specific certificates that are used in [CNW11, SWS+12] to detect Sybil nodes based on a cryptographically protected usage restriction of the credentials. This approach allows a reliable detection of Sybil nodes as the sender is allowed to use only one credential per time. However, the schemes suffer from increased overhead and bad performance compared to the elliptic curve cryptography which is considered by ETSI [ETS13b] and IEEE [IEE13] in their draft standards.

In Section 3.2 we propose a strategy to categorize the aforementioned mechanisms with respect to misbehavior detection in VANETs.

3.1.3. Misbehavior Detection Frameworks

In this section related misbehavior detection frameworks are discussed that are based on the methods to verify location-related data discussed in the previous section .

In [SLS+08] Schmidt et al. describe a VEhicle Behavior Analysis and Evaluation Scheme (VEBAS) that combines misbehavior detection approaches in a module-based security system. This scheme maintains different positive rating modules and negative rating modules that implement a selection of the previously mentioned data plausibility checks. In a further step the outcomes of the different modules are weighted and aged by a function called *exponentially weighted moving average* (EWMA) before they are aggregated within the respective group of positive and negative ratings. Finally, the authors propose to combine the aggregated ratings in order to get a local trust value for the evaluated node. This extensible module-based structure is designed to calculate reputation values for neighboring nodes. It allows also the exchange of locally generated recommendations with neighbors.

In a similar way, in [Ger10] Gerlach proposes a scheme that evaluates the trustworthiness of received messages based on different modules (here denoted as observers) whose results are aggregated by a *Bayesian network* (BN). Every observer contains a rule for evaluating the given mobility data and translates the results into entries of a conditional probability table. By querying the BN, a trust value of a single message can be obtained as well as the trustworthiness of the related node. A unique attribute of this framework is the consideration of confidence values within received mobility data such as position + confidence, speed + confidence, heading + confidence.

3.1.4. Evaluation of Related Work

Most descriptions of adversary models given by authors of related work are in line with our assumptions about internal attackers. Single or multiple ghost vehicles could be generated by an attacker in order to fake traffic safety-related events. Even if the generation of a single ghost vehicle is more likely than multiple Sybil nodes that are generated simultaneously, it is assumed that an attacker with sufficient knowledge and control of a V2X communication system is able to create a Sybil attack. As argued by the author of this dissertation [BSP+13] an internal attacker might be able to forge multiple IDs at the same time when the sender and receiver do not apply appropriate consistency checks.

The mechanisms presented in Section 3.1.2 are partially based on different assumptions. In this dissertation, we do not focus on eavesdropping and monitoring the routing behavior as discussed in [KL08], [LSK06], and [TWLY10]. However, we aim to generally detect fake location claims of single-hop neighbor nodes. Geographic routing protocols benefit from this detection since they rely on correct location information of single-hop neighbors in order to forward packets correctly and reliably.

The proactive and reactive exchange of neighbor tables as discussed in [LSK06] and [YCO09] is another critical issue. All received data from neighbors can be equally trusted as long as valid cryptographic credentials are used to sign the messages. Therefore, attackers would also be able to distribute faked neighbor tables. Moreover, the exchange of additional data for security purposes would increase the load on the wireless channel dramatically. According to Schoch [Sch09] the reactive exchange of position information creates unacceptable communication overhead and the verification does not profit much or even suffers from it. Increasing the load of the wireless V2X communication channel is critical since the security overhead is already substantial due to relatively large security credentials [BSS+11, ETS13b, IEE13]. Additionally, the exchange of security-related data may create new vulnerabilities and attack vectors that could be misused. As a result, we argue to avoid or at least minimize the amount of additional redundant data that are transmitted for plausibility checks.

In contrast to the authors of [CWHZ09], [PATZ09], [XYG06], and [ZCNC07], we argue that a comprehensive network of roadside infrastructures cannot be assumed in VANETs due to its large area and consequently high costs [KCD+09]. Mechanisms that require a constant connection to the infrastructure may only be applicable in urban scenarios with a dense network of RSUs. In our system model defined in this work (cf. Figure 2.1 on page 13) only a sporadic field-vehicle communication via RSUs is assumed. Moreover, it is unlikely that all vehicles in a VANET are equipped with cellular network transceivers that can be permanently used to communicate with the infrastructure.

In the following sections we propose reasonable algorithms and instruments for plausibility and consistency checks without relying on unrealistic requirements such as static node IDs or permanent RSU-vehicle connections. Our solutions are based on fundamentals elaborated by Schmidt et al. [SLS+08] in their module-based VEBAS scheme and by Gerlach [Ger10] in his observer-based scheme. Unfortunately, the authors of VEBAS do not provide an evaluation at all (cf. [SLS+08]). The author of [Ger10] limits the evaluation of the observer-based scheme to a fixed receiver station that processes messages generated by a simulation environment. The practical applicability of these schemes is therefore not proven. However, in this dissertation we combine most relevant approaches within practically relevant frameworks that are deployed on test vehicles and evaluated under real conditions, partially over long periods of time. Additionally, we propose a new plausibility check based on the principle of having a maximum vehicle density as first discussed by Golle et al. [GGS04] and further mentioned in [Ger10, LSK06].

3.2. Categorization of Misbehavior Detection Checks in VANETs

In this section we propose a strategy to categorize methods for misbehavior detection proposed by authors of related work (cf. Section 3.1.2) and own methods developed within this dissertation. The mobility data consistency and plausibility checks discussed in this section are aimed to be applied in addition to cryptographic security measures as described in Section 2.2.1. These checks are used to filter messages with obviously wrong position vectors and to collect evidence for a misbehavior detection.

In general every node in the VANET autonomously perform the checks of the position vector after reception and decoding of a V2X message. First, mobility data and sender IDs from different packet headers are extracted by the responsible communication stack layers and handed over to the plausibility tester. Finally, after performing the checks, an evaluation of the message and sender node trustworthiness is performed which may be used by local applications and for local misbehavior detection.

An overview of the proposed classification is illustrated in Figure 3.1. A message-based plausibility check of information is performed to filter malformed data that violate predefined range of values. If the same piece of information is available multiple times in a message a consistency check should be done in addition. Related methods are detailed in Section 3.2.2. The received mobility data of neighbor nodes should also be checked against locally available trusted first hand information as explained in Section 3.2.3 and 3.2.4. This data verification using local static knowledge and local sensor information can be done either on message basis or on node basis. Finally, received data can be compared with second hand information received from other VANET nodes. If received information is not consistent with other received second hand information it might be challenging for the related mechanisms to

interpret the results correctly, since both information sources are usually trusted equally. Mechanisms handling second hand information are discussed in Section 3.2.5. A summarization of all mechanisms is provided in form of a table in Section 3.2.6.

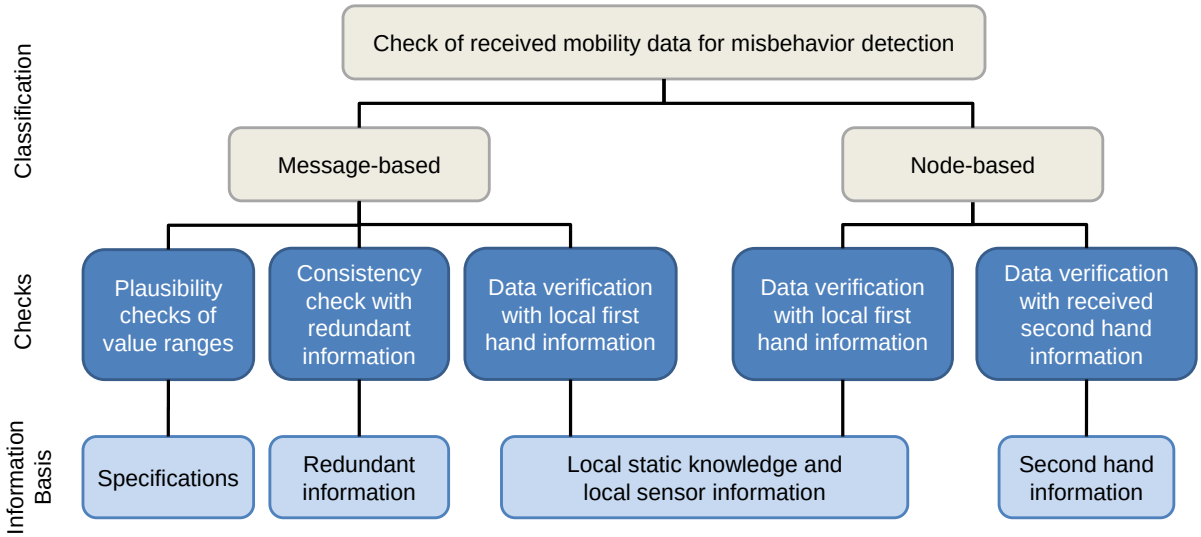


Figure 3.1.: Checking data for misbehavior detection in VANETs

In Figure 3.1 it is shown that the three checks on the left hand side are message-based and the two checks on the right hand side are node-based. The value range checks and the consistency checks are message centric and consider V2X messages separately. The data verification with received second hand information is in contrast node centric since previous messages have to be received that provide information about prior node behavior.

3.2.1. Message-Based Data Plausibility Checks

A message-based plausibility check is using predefined rules and physical boundaries. These checks are using a transmitted position vector (PV) that includes the position of the sender, its current speed and heading at a specific point in time. In these basic checks the given values of a PV are compared with the predefined domain of definition.

The heading value shall follow the domain of definition according to related standardization for CAM and DENM as well as for network layer headers. A heading value larger than 360° for example should be considered to be not plausible. Furthermore, the velocity values shall be checked as well as the position of the sender. The position is usually encoded in the WGS84[1] format that includes a latitude and longitude value [ETS10d, ETS10e]. For example, a velocity of a vehicle below -30 $\frac{m}{s}$ and beyond 100 $\frac{m}{s}$ is suspicious in normal road traffic.

[1] Geodetic standard of world geodetic system (WGS) used in cartography, geodesy, and navigation, established in 1984 and last revised in 2004.

3.2.2. Message-Based Data Consistency Checks with Redundant Information

A message-based consistency check is possible if information is redundant, e. g. due to reception of multiple messages over different communication channels or due to redundant information on different layers of the OSI layer model. The general packet format of a V2X message as depicted in Figure 2.3 on page 15 shows that position information is available in different parts of a packet. Even though this position information is not equal due to possibly different interpretations on different layers, a comparison by means of consistency checks allows at least a detection of unexpected deviations. Large deviations consequently may indicate a misbehavior of the sender station since a malware could have modified the position data on one layer only. However, it is necessary to be aware about variations between comparable information. For example, the position vector applied on one layer may be more inaccurate as the vector applied on another layer because in one case the raw GNSS signal is used and in the other case a dead reckoning optimized position is used. Another reason for variations could be a slightly different position reference point.

In order to additionally detect Sybil attacks the consistency of identifiers contained in V2X packets have to be checked as motivated and proposed by Bißmeyer et al. [BSP+13]. Therefore it is required that at least the node ID of the network header and the station ID of the payload are linked to the certificate coming as part of the security header. To create the linking the security subsystem of the ITS station creates a hash value from the currently used pseudonym certificate and uses parts of the value as certificate ID (cf. ETSI TS 103 097 [ETS13b]). This certificate ID is further used by the layers of the communication stack to derive their header specific identifiers. On packet reception the identifiers from the MAC header, network header, security header and payload are collected and finally compared on the top most message processing layer. If the IDs are not consistent or cannot be linked to the certificate or its certificate ID, the packet can be considered as malformed.

3.2.3. Message-Based Data Verification with Local First Hand Information

By using static local first hand knowledge two different checks of the message content are considered that focus on the detection of replayed data. The application of local sensor information, however, might be important for application-related checks such as temperature value verifications.

Check of maximum communication range (MCR): In a communication range check, the distance between the position of a single-hop sender and receiver is calculated. If this distance exceeds the maximum transmission range the location of the sender can be assumed to be not plausible. It is assumed that radios are used that follow the maximum specified transmission power according to IEEE 802.11p [IEE10] and ETSI ES 202 663 [ETS10b]. The mechanism was first mentioned by Golle et al. [GGS04] and corresponds to the *Acceptance Range Threshold* sensor described by Leinmüller et al. [LSK06]. In general, this kind of check aims to detect location-based replay attacks that are also known as tunnel or wormhole attack [HPJ06]. In this attack an attacker records an authenticated message at a location l_1, transmits it quickly to a location l_2 and re-broadcasts it at l_2.

Check of maximum transmission delay (MTD): In addition to a distance check, the maximum transmission delay of single-hop messages shall be verified by receiving stations. According to ETSI TS 102 637-2 [ETS10d] the maximum transmission delay of CAMs shall not be larger than 100 ms. As a result, messages with an outdated timestamp or a future timestamp should be considered as not

plausible. This kind of check is already part of emerging standards, i. e. IEEE 1609.2 [IEE13] and ETSI TS 102 731 [ETS10c]. The MTD check aims to detect time-based replay attacks where an attacker records a valid message at time k_1 and replays it later at the same location at a time k_2.

3.2.4. Node-Based Data Verification with Local First Hand Information

In addition to the message-based checks, a node-based verification is reasonable using two types of local first hand information. Static local knowledge about the network and its communication systems may be used to detect implausible behavior of adjacent nodes. Furthermore, local sensors may be used to verify the PV of received messages.

3.2.4.1. Checks based on Static Local Knowledge

In this paragraph, four options are denoted that are based on static knowledge and standardized rules to check location-related data. These checks were first mentioned by Leinmüller et al. [LSK06] and Schmidt et al. [SLS+08]. However, their practical applicability has not been addressed. Within this dissertation, different strategies are proposed how to integrate these checks into a misbehavior detection framework.

Check of maximum beacon frequency (MBF): Since the wireless V2X channels are used cooperatively, the maximum transmission frequency of CAMs is limited. A plausibility check on the receiving station is able to count the received messages from the single-hop neighbors and is consequently able to detect violations according to ETSI TS 102 637 [ETS10d, ETS10e].

Check of suddenly appearing station (SAS): In normal traffic conditions it can be assumed that new vehicles first appear at the boundary of the communication range. As a result, a first CAM from a station with an unknown ID shall contain a PV that states a certain distance between the sender's station and the receiver station. However, ID changes and hidden stations that might be caused by large buildings in urban traffic require a context depended check of suddenly appearing stations.

Check of plausible movement (PM): Based on a physical mobility model for vehicles a position can be predicted using previously received position statements. When a new message is received, the predicted position can be compared with the stated position whereupon large deviations are suspicious, hence may result in misbehavior detection. Since CAMs are broadcasted with a maximum frequency of 10 Hz [ETS10d], an accurate position vector of the next CAM can be assumed. By checking the movement plausibility, position jumps and unexpected mobility behavior can be detected.

Check of map related position (MRP): A digital road map can be used to check the position of a sending vehicle station assuming that every receiving VANET station is equipped with a digital map. A digital road map may be required by traffic safety and efficiency applications anyway. However, a vehicle that cannot be assigned to a valid road segment of the local map is possibly driving on a private road or is parked beside a road. It has to be further considered that the local map may be outdated. In any case, the exclusive check of a map related position is not robust enough for misbehavior detection. Performing the MRP check in combination with other verification methods should be preferred.

3.2.4.2. Checks Based on Local Sensors

Stations that are equipped with local environment sensors can use their measurements to confirm or refute a stated location of a neighbor node. For example a local front radar transceiver is able to track different vehicles that are driving ahead of the own station. In the same way, other local distance and proximity sensors such as cameras, lidar or infrared-based detectors can be used to check the stated PV of neighbors. Since front radar systems are already widely used in vehicles for autonomous cruise control, the plausibility checks discussed in this work focus on applying a radar transceiver as local sensor. The concept of using local sensors to verify stated locations in VANETs has been first comprehensively discussed by Yan et al. [YOW08] and was subsequently used within other related concepts [Ger10, SLS+08]. Within this dissertation, we integrated a radar sensor into a misbehavior detection framework and evaluated the practical applicability by using recorded traces and radar measurements from test vehicles [JBSH11, QBa11].

Radar approved position (RAP): If a received position of a neighbor node can be mapped to a radar object of the local sensor, then this vehicle position information can be assumed to be trustworthy. However, RSUs are in general not confirmable with a radar sensor.

Radar conform position (RCP): In addition, the object detection of a local radar can be used to refute a stated location. If a neighbor vehicle claims a position that is located between the own station and an object that is detected by the radar, then this vehicle position is not trustworthy. Assuming that the stations trust their own sensors and on-board networks, a detected false position claim can be trusted. If however received second hand information is used to check the plausibility of received position claims the verification might not be trustworthy as discussed in Section 3.2.5.

3.2.5. Node-Based Data Verification with Received Second Hand Information

A station that receives conflicting – but equally trusted – information from two different nodes cannot directly determine which statement is true and which is false. However, by collecting additional information about the same or a similar statement from different independent senders, the receiver may be able to take a decision assuming that the majority of provided information is correct.

Neighborhood table exchange (NTE): As discussed in the related work neighbors may distribute their local first hand information (e. g. radar tracked nodes) or reputation information about their neighbor nodes. A receiver of this information is able to compare the received tables with other received tables and with its local neighbor information. This mechanism has been first discussed by Leinmüller et al. [LSK06] and is listed in this section for completeness. However, it is not further considered as reasoned in Section 3.1.4.

Check of vehicle overlaps (VO): Since vehicles are periodically broadcasting CAMs with their absolute position and their rough stations' dimensions, a check of position overlaps can be performed by comparing the PVs of near-by stations. The VO check has been newly developed by the author of this dissertation [BSB10] and is further discussed in detail in Section 3.5.

3.2.6. Summary of Misbehavior Detection Check Categorization

A summarization of relevant mechanisms for local misbehavior detection performed on VANET nodes is presented in Table 3.1. This table shows the correlation of the methods applied in this dissertation with the classification and information basis illustrated in Figure 3.1.

Table 3.1.: Summary of misbehavior detection check categorization

Abbreviation	Name of method	Classification	Information Basis	Comment
	Plausibility checks of value ranges	Message-based	Specifications	
	Consistency checks	Message-based	Redundant information	
MCR	Maximum communication range	Message-based	Local static knowledge	
MTD	Maximum transmission delay	Message-based	Local static knowledge	
MBF	Maximum beacon frequency	Node-based	Local static knowledge	
SAS	Suddenly appearing station	Node-based	Local static knowledge	
PM	Plausible movement	Node-based	Local static knowledge	
MRP	Map related position	Node-based	Local static knowledge	
RAP	Radar approved position	Node-based	Local sensor information	
RCP	Radar conform position	Node-based	Local sensor information	
NTE	Neighborhood table exchange	Node-based	Received second hand information	Not further considered
VO	Vehicle overlap test	Node-based	Received second hand information	Developed by author of dissertation

3.3. Evaluation Criteria for Misbehavior Detection in VANETs

The evaluations of our approaches in Sections 3.4, 3.5, and 3.6 are based on the aspects introduced in this section: *accuracy*, *scalability*, *extensibility*, *generalizability*, *complexity*, *bandwidth & connectivity*, and *privacy*. In Section 3.7 we compare our proposals with related work based on these criteria which are described in more detail in the following.

- **Accuracy:** We focus on the detection of misbehavior as defined in Section 1.2 by considering the PV defined in Table 2.2 on page 18. The accuracy of the proposed frameworks is measured based on the following criteria.
  - Abnormal deviation of time, absolute location, heading, and velocity
  - Abnormal vehicle movement, i. e. position jumps

  - Abnormal occupancy of space, i. e. position overlaps with other nodes and position conflicts with the observed area of environment sensors such as radar
  - Abnormal sudden appearance of VANET nodes

The number of correct detections of maliciously manipulated PV should be maximized (true-negative) but the number of incorrect detections (false-positive) and the number of not detected attacks (false-negative) should be minimized. Table 3.2 subsumes the applied evaluation metric.

Table 3.2.: Evaluation metric for data consistency and plausibility checking

Stated mobility information is correct	**Outcome of plausibility check is true** (Plausibility confirmed)	**Outcome of plausibility check is false** (Implausibility detected)
False	False, False-negative	Correct, True-negative
True	Correct, True-positive	False, False-positive

- **Scalability:** The scalability with respect to computational performance and memory consumption is relevant since automotive computer systems might be more restricted as personal computers. It should be ensured that respective hardware is able to handle the misbehavior detection solution.
- **Extensibility:** The extensibility of a solution for misbehavior detection is important since new attacks might come out in the future and should be considered.
- **Generalizability:** It should be considered whether the solution can be generalized to be applied in other domains.
- **Complexity:** The complexity of misbehavior detection solutions should be as less as possible in order to avoid vulnerabilities and faulty implementations. Less complex solutions might also simplify their extensibility and generalization.
- **Bandwidth & Connectivity:** Since the wireless ITS-G5 [ETS10b] control channel must only be used to transmit traffic safety related data, misbehavior detection mechanisms should be able to work autonomously on the nodes.
- **Privacy:** The misbehavior detection system of a VANET should not weaken the drivers' privacy. For example, private information of individuals such as names or addresses must not be revealed and vehicle traces should be protected in order to complicate the linking between movement traces and information of individuals.

3.4. Module-Based Misbehavior Detection Framework using Kalman Filters

The concepts and the design of the Kalman filter-based plausibility check presented in this dissertation is the result of a group work of Hagen Stübing, Attila Jaeger and the author of this dissertation.

Basics of the Kalman filter-based approach for vehicle movement plausibility checking are described in the PhD Thesis of Hagen Stübing [Stü12]. Beyond the results achieved in the group work a comprehensive evaluation of the Kalman filter-based plausibility check concept is performed by the author of this dissertation. Within this dissertation we developed a concept to integrate and evaluate the accuracy of the Kalman filter-based plausibility check within a large scale Field Operation Test (FOT) [SES+13, BSS13]. The evaluation of the applicability of the plausibility checker is based on long-term measurements that were performed by using a logging framework of the FOT. The automated evaluation of the recorded log data was supported by Tobias Gundlach in his Bachelor thesis [GWB12] which was supervised by the author of this dissertation. Within this dissertation we evaluated the applicability of plausibility checks in a VANET for the first time with a noteworthy number of real vehicles and roadside units.

Furthermore, a module-based misbehavior detection framework is developed by the author of this dissertation that uses the Kalman filter-based plausibility check as one module. In addition, the developed framework integrates the checks categorized in Section 3.2 and subsumed in Table 3.1 as separated modules. The results from different plausibility modules are aggregated in a fusion process to determine the trustworthiness of V2X messages and neighbor nodes. We consider all categories introduced in Section 3.2 with the module-based misbehavior detection framework. Daniel Quanz has supported the work by implementing and evaluating the data fusion concept as part of his Bachelor thesis [QBa11] which was supervised by the author of this dissertation.

In the following, a brief introduction of the Kalman filter theory is given, followed by a description how the filter is adapted for the purpose of vehicle tracking. Subsequently, the module-based misbehavior scheme is described in Section 3.4.3 that applies a Kalman filter among other instruments to check the plausibility of stated movement data sent by single-hop neighbor nodes. Finally, an evaluation of a related plausibility check is discussed in Section 3.4.4 that is based on long term measurements gathered in a large FOT.

3.4.1. System State Prediction with Kalman Filters

A Kalman filter [Kal60] is a well-known tool for predicting the state of linear dynamic systems based on a series of noisy measurement data. Especially for object tracking, a Kalman filter represents an efficient solution [BP99]. The Kalman filter generates an optimal prediction if the measurement error is Gaussian distributed. This is typically the case for position data delivered in wireless V2X communications even if some areas around the predicted position are more likely than others as discussed by Bißmeyer et al. [BB11] and Gerlach [Ger10]. The limitations of the Kalman filter-based prediction become obvious when unexpected deviations occur in the trajectory of a tracked object, e. g. caused by sharp driving maneuvers in case of vehicle tracking. This aspect has been further considered in more detail by Stübing et al. [SFH11]. Within this dissertation, that limitation of the Kalman filter is taken into account by elaborating a particle filter-based misbehavior detection framework, cf. Section 3.6.

A Kalman filter is a recursively operating filter that is able to estimate a statistically optimal system state based on previous states and noisy input data. In general, the filter is based on a prediction and correction step for every time step k as depicted in Figure 3.2. The prediction $\hat{x}_k$ of a system state is calculated by multiplying the last predicted state $\hat{x}^+_{k-1}$ with the state transition matrix F_k as shown in

Equation 3.1. The state transition matrix is the mathematical representation of the underlying system model. The prediction accuracy can be further increased by incorporating a control value u_k and using a control matrix B_k.

$$\hat{x}_k = F_k \cdot \hat{x}_{k-1}^{+} + B_k \cdot u_k \tag{3.1}$$

Additionally, a prediction error P_k is calculated that estimates the inaccuracy of the current prediction $\hat{x}_k$. P_k is also known as covariance that considers the fact that states depend on previous states through the linear matrix F_k. As shown in Equation 3.2 P_k is calculated based on the transition matrix F_k, the calculated prediction error from the previous recursion round P_{k-1}^{+}, and a system fault matrix Q_k which represents inherent errors in the system model.

$$P_k = F_k \cdot P_{k-1}^{+} \cdot F_k^T + Q_k \tag{3.2}$$

In the correction phase, the predicted state is then corrected in order to achieve a more accurate system state by adding measured system state information. As shown in Equation 3.3 the predicted value $\hat{x}_k$ is multiplied with a transition matrix H_k before it is subtracted from the measured data $\tilde{y}_k$.

$$\begin{aligned} \Delta y_k &= \tilde{y}_k - \hat{y}_k \\ &= \tilde{y}_k - H_k \cdot \hat{x}_k \end{aligned} \tag{3.3}$$

In order to decide how much Δy_k is needed to be considered in the corrected system state $\hat{x}_k^{+}$ as established in Equation 3.5, a Kalman gain K_k is calculated based on the prediction error and measurement variances R_k as shown in Equation 3.4. Finally, the prediction error P_k^{+} is updated as shown in Equation 3.6 with the Kalman gain in order to support the prediction step of the next round (cf. Equation 3.2).

$$K_k = P_k \cdot H_k^T \cdot (H_k \cdot P_k \cdot H_k^T + R_k)^{-1} \tag{3.4}$$

$$\hat{x}_k^{+} = \hat{x}_k + K_k \cdot \Delta y_k \tag{3.5}$$

$$P_k^{+} = P_k - K_k \cdot H_k \cdot P_k \tag{3.6}$$

The corrected system state and prediction error is then used in the succeeding prediction phase at time step $k+1$. The schematic in Figure 3.2 illustrates the Kalman filter phases. Thereby, z^{-1} denotes the time shift between step $k-1$ and k, respectively.

3.4.2. Tracking with Kalman Filters

In V2X communications, both CAMs and DENMs contain a position vector providing mobility information in the form of position, speed, heading, and time as listed in Table 2.2 on page 18. For the purpose of vehicle tracking, the state vector of the Kalman filter $\hat{x}_k$ at time k consists of the vehicle's position (p_{x_k}, p_{y_k}) as Cartesian UTM data and the velocity (v_{x_k}, v_{y_k}) in the xy-plane as shown in Equation 3.7.

$$\hat{x}_k = \begin{pmatrix} p_{x_k} \\ p_{y_k} \\ v_{x_k} \\ v_{y_k} \end{pmatrix} \tag{3.7}$$

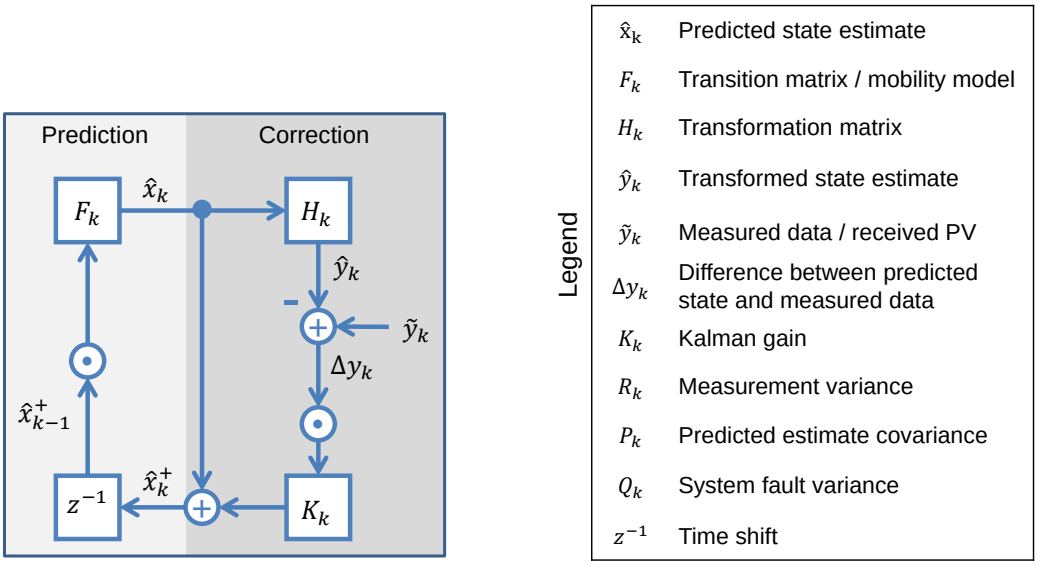


Figure 3.2.: Schematic Kalman filter structure with a legend of used variables

In order to predict both position and velocity a vehicle mobility model is then applied, which is based on the equation of linear motion as shown in Equation 3.8. Here, p_{x_k} and p_{y_k} denotes the position, v_{x_k} and v_{y_k} the velocity, and a_{x_k} and a_{y_k} the acceleration at time k.

$$\begin{aligned} p_{x_k} &= p_{x_{k-1}} + v_{x_{k-1}} \cdot \Delta t_k + a_{x_{k-1}} \cdot \frac{\Delta t_k^2}{2} \\ p_{y_k} &= p_{y_{k-1}} + v_{y_{k-1}} \cdot \Delta t_k + a_{y_{k-1}} \cdot \frac{\Delta t_k^2}{2} \end{aligned} \tag{3.8}$$

Based on variable message frequencies according to ETSI [ETS10d], the time difference Δt_k between the current time k and the time of the previous step $k-1$ is assumed to be not constant. According to Equation 3.8 and the form of the chosen system state shown in Equation 3.7, the state transition matrix F_k results in a four by four matrix as depicted in Equation 3.9. Since acceleration is not transmitted in CAMs and DENMs, its value is calculated from speed differences of the last received messages. Due to the fact that the acceleration is assumed to be constant within each time step, $\Delta t_k^2/2$ is added to the respective speed entries with a factor a_k before F_k is applied in the final prediction step.

$$F_k = \begin{pmatrix} 1 & 0 & \Delta t_k & 0 \\ 0 & 1 & 0 & \Delta t_k \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.9}$$

The application of the control value u_k (cf. Equation 3.1) is not taken into account as only received location data is used as measurement input. If, however, local sensor data would be available for nearby tracked vehicles, the sensor measurements could be incorporated as u_k.

In the subsequent correction step, the PV from the received message is taken as measurement input $\tilde{y}_k$. The contained values for position, velocity, and heading are converted into a system state as shown in Equation 3.7. Therefore, the state $\hat{y}_k$ and the measurement vector $\tilde{y}_k$ are of identical form and the transition matrix H_k can be eliminated in the corresponding corrections steps (cf. Equation 3.3, 3.4, and 3.6).

As mentioned by Jaeger, Stübing, and the author of this dissertation [JBSH11, SJB+10] the system fault matrix Q_k can be chosen dynamically according to the road type as the prediction accuracy heavily depends on driving maneuvers. In [SFH11] Stübing et al. additionally propose a maneuver recognition that modifies the Kalman gain K_k to correct the system state in a way that measurements are considered more than predictions. In analogy, the measurement variances matrix R_k can be chosen dynamically from a position confidence value contained in received V2X messages as proposed by Gerlach in [Ger10]. Based on the adoptions and chosen matrices, the Kalman filter can now be used as a vehicle tracker in a local mobility data verification mechanism that aims to detect misbehavior caused by attackers and faulty nodes.

3.4.3. Module-based Misbehavior Detection

A misbehavior detection framework involving a Kalman filter is able to identify different mobility data plausibility violations as mentioned in Section 3.2.4. By tracking adjacent nodes with the Kalman filter deviations of speed, heading, and position are observed and a comparison between the stated PV and its corresponding predicted PV is performed. As long as for every single-hop node within the communication range V2X messages are received periodically, a separate Kalman filter instance is maintained for the node in form of a vehicle tracker object.

Integration of PM and SAS Checks into Module-based Framework The different steps of tracking with the Kalman filter are illustrated in the activity diagram in Figure 3.3. As soon as a V2X message is received, the mobility data and node ID are extracted from the message and the list of locally managed vehicle trackers is searched for this node ID. If a tracker is found for the ID in step (1), then the Kalman filter prediction is performed as shown in Equation 3.1. By calculating Δy_k, cf. Equation 3.3, the predicted state $\hat{x}_k$ is compared with the received mobility data $\tilde{y}_k$. If the deviation is above a defined threshold, the received PV is not in accordance with the mobility model. As a consequence the PM module returns the lowest possible result value (i. e. Result = 0.0) in step (2). Otherwise, if the deviation is below the defined threshold then the highest possible result value (i. e. Result = 1.0) is returned. Irrespective of the result, the correction phase of the Kalman filter is performed following step (2) in order to get the corrected state $\hat{x}_k^+$ (cf. Equation 3.5).

If no tracker was found, two possible reasons can be distinguished (step (1) in Figure 3.3): Either an unknown vehicle is entering the receiver's communication range or an already known vehicle has performed an ID change. The ID change of a tracked vehicle is detected by iterating the tracker list to identify the candidate which is most likely to fit the received mobility data. For the most reasonable tracker a prediction and correction phase of the Kalman filter is entered and the deviation is determined. If the vehicle movement fits the prediction of this tracker, then an ID change is detected (see step (3) in Figure 3.3) and the maximum result value (i. e. Result = 1.0) is returned. Consequently, the associated

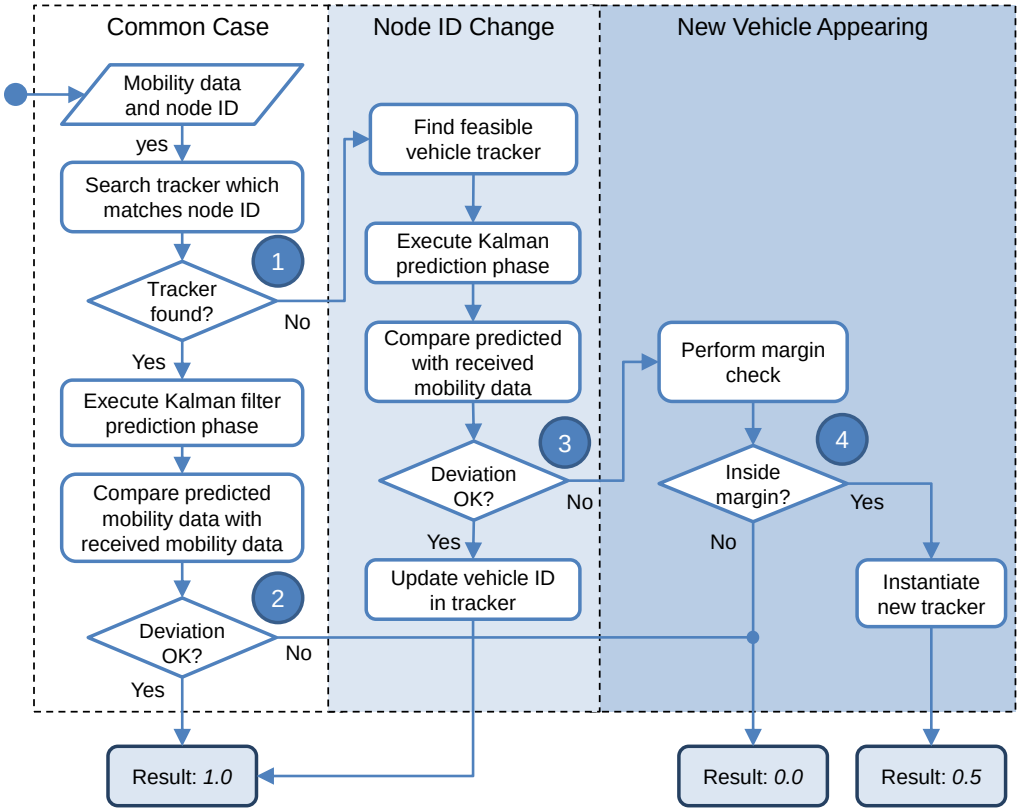


Figure 3.3.: Tracking of adjacent nodes with the Kalman filter

vehicle tracker ID is updated and the next prediction is performed. The ID change detection is further discussed in more detail in Section 4.2.

If a V2X message is received from an unknown node and an ID change of known nodes can be ruled out, a sudden appearance check is performed before a new Kalman filter instance is created with the sender's pseudonymous node ID. In this case, a margin check is performed in step (4). The margin check examines whether the new node first appears on the border of the current communication range of the receiver. If the new node is located inside the margin then the result of the PM module is neutral (i. e. Result = 0.5). Otherwise, the lowest result value (i. e. Result = 0.0) is returned.

Integration of Consistency and Threshold Checks into Module-based Framework For additional checks such as MRP, RAP, RCP, and VO tests, mentioned in Section 3.2, additional algorithms have to be applied. Some basic checks can be subsumed in a module that performs general consistency and threshold checks as shown on the left-hand side of Figure 3.4. This consistency and threshold check verifies first that only single-hop messages are considered. Multi-hop DENMs cannot be reliably tested in a node-based misbehavior detection scheme since they are not received periodically. Subsequently, the threshold check verifies the PV contents on a message-basis by checking the correctness of the value range of the position, heading, and velocity. Additionally, a message-based consistency check

is performed that compares the PV of the network header with the PV of the payload (e. g. CAM or DENM) and optionally with the security header. Finally, the consistency and threshold check verifies the sender's maximum communication range, maximum transmission delay, and maximum beacon frequency based on static local knowledge, i. e. standardization documents [ETS10d, ETS10e, ETS10b, IEE10]. However, the maximum beacon frequency (MBF) is the only node-based check in this module.

Aside from the consistency and threshold checks, further different specific plausibility checks are performed in separate modules, as depicted in Figure 3.4. One check detects vehicle position overlaps as further detailed in Section 3.5 and another module is using local sensor information, for example a radar transceiver, to analyze the plausibility of stated vehicle positions. In the latter check, roadside stations are ignored as they do not create a radar echo that can be used. Finally, a test method is executed that analyzed whether a vehicle position can be linked to a segment of a digital map.

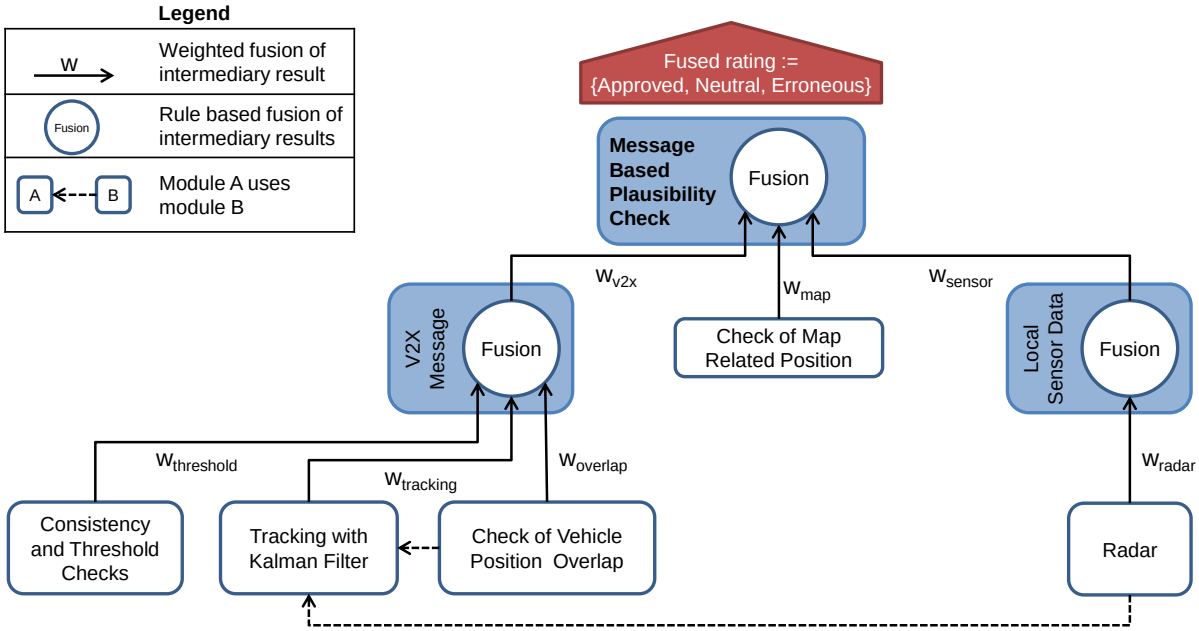


Figure 3.4.: Fusion of results from different data plausibility checks to rate the message-based plausibility

Fusion of Module Outputs In order to evaluate the trustworthiness of the message a fusion of intermediate module results is realized with a tree [QBa11]. The tree consists of a root, internal vertices V and leafs where every internal vertex has a set of child vertices VC. The leafs in Figure 3.4 represent the plausibility modules which check the PV of received V2X messages. The different results are subsequently combined in the intermediate vertices and then finally consolidated in the root in order to get a single plausibility rating of the analyzed V2X message. The fusion tree T is defined as $T = (V, E, w, r, R)$ at which V denotes the set of vertices, E denotes the set of edges, w denotes the weighting function, r denotes the rating function and R denotes the set of rules that are applied by the vertices. The weight function $w : V \times V \rightarrow \mathbb{N}_0$ gives the weight of the edge that is spanned between two vertices and the rating function $r : V \rightarrow [0, 1]$ gives the result of a plausibility or consistency check that is performed by

a single vertex. The set of rules contains triples of the form $R := \{x | x := (v,o,n), v \in V, o \in O, n \in \mathbb{R}_0^+\}$ at which the set $O := \{=, \neq, <, >, \leq, \geq\}$ denotes the possible operations, v denotes the vertex that the rule is related to, and n is a value that is used to compare the rating r with.

The weights at the edges are used in the fusion process to prioritize results. For example, the rating of a radar-based position verification is considered with high weighting due the usage of highly trusted local first hand sensor information. However, in contrast, ratings of a map-based plausibility test are considered in the fusion process with low weighting. Explicit values of the weights have not been elaborated in this dissertation. The rules are built into the fusion process in order to allow for the consideration of thresholds before the ratings are aggregated. If, for example, the consistency and threshold check fails because a sender is outside the acceptable communication range then the message should be rated as erroneous even if other modules rate the specific mobility information to be plausible.

The fusion process starts when the leaf vertices have processed the position vector of a V2X message by providing their specific plausibility ratings. First the rule that is related to a child vertex $v_c \in VC$ is applied to the rating of v_c. If no rule is assigned to the vertex then the rating value is used unmodified in the fusion function as shown in Equation 3.10.

$$r(v) = \frac{\sum_{v_c \in VC} w(v, v_c) \cdot r(v_c)}{\sum_{v_c \in VC} w(v, v_c)} \tag{3.10}$$

In order to simplify the misbehavior detection, the final merged result, gathered from the root vertex $r(v_{root})$ is classified as *Approved* when $0.5 < r(v_{root}) \leq 1$, *Neutral* when $r(v_{root}) = 0.5$, and *Erroneous* when $0 \geq r(v_{root}) < 0.5$. A message is rated as *Neutral* only in special cases such as the initial tracking phase when no past movement information is available at the Kalman filter but all other modules approve the message.

In case of an erroneous result, further action should be taken by the local misbehavior detection system. At this point, only a message-based evaluation of the PV is performed. Additionally, an evaluation of the nodes' trustworthiness can be created by collecting the message-based ratings and evaluate the short-term and midterm behavior of respective neighbor nodes.

In order to maximize the tracking time of neighbor nodes and therefore their evaluation time a local detection of ID changes is proposed. This is necessary as an attacker could exploit the pseudonym change mechanism (cf. Section 2.2.1 and [BSS+11]) by changing its IDs after performing an attack. As a consequence the attacker might be rated neutral after an ID change by the misbehavior detection system of neighbors. With the proposed ID change detection the local misbehavior detection system is able to track vehicles irrespective of their used identifiers. However, the detection of ID changes can only be performed by the Kalman filter if the specific node is accurately tracked based on frequently received CAMs. If the tracked node applies countermeasures to complicate the detection of ID changes, for example by applying random silent periods [HMYS05] or mix-contexts [GG07], then the probability decreases for receivers to link messages with old and new IDs.

3.4.4. Evaluation of the Module-based Misbehavior Detection

The following evaluation of the module-based misbehavior detection framework is structured according to the evaluation criteria defined in Section 3.3. After presenting details about the test setup, the

evaluation criteria are discussed with respect to the module-based misbehavior detection framework. This discussion is based on the defined criteria: *accuracy, scalability, extensibility, generalizability, complexity, bandwidth & connectivity, and privacy*. By means of these criteria a comparison of related solutions is presented in Section 3.7.

Evaluation Setup - Strategy An experimental evaluation of the module-based plausibility framework has been selected to be most reasonable since the overall applicability of the framework should be analyzed. The correct processing of the single module operations has previously been tested [SJB+10, Stü12] using different parameters and input values. In order to evaluate the practical applicability of the proposed framework data from real V2X communications has to be processed that may also contain usual inaccuracies. Most simulation tools are not able to create at the same time realistic communication conditions including environment-related shadowing, realistic vehicles movements, and realistic driver behavior. The experimental evaluation is consequently the best choice to evaluation the proposed framework.

Evaluation Setup - Tools For the evaluation a Java OSGi [All13] implementation has been used that was deployed on several test vehicles and RSUs of a FOT. The system architecture of the vehicles and RSUs follows the description of the ITS architecture as discussed in Section 2.1. However, the function of the communication stack is split in two parts as illustrated in Figure 3.5. Both, the access layer and the network & transport layer come as a part of a communication & control unit (CCU).

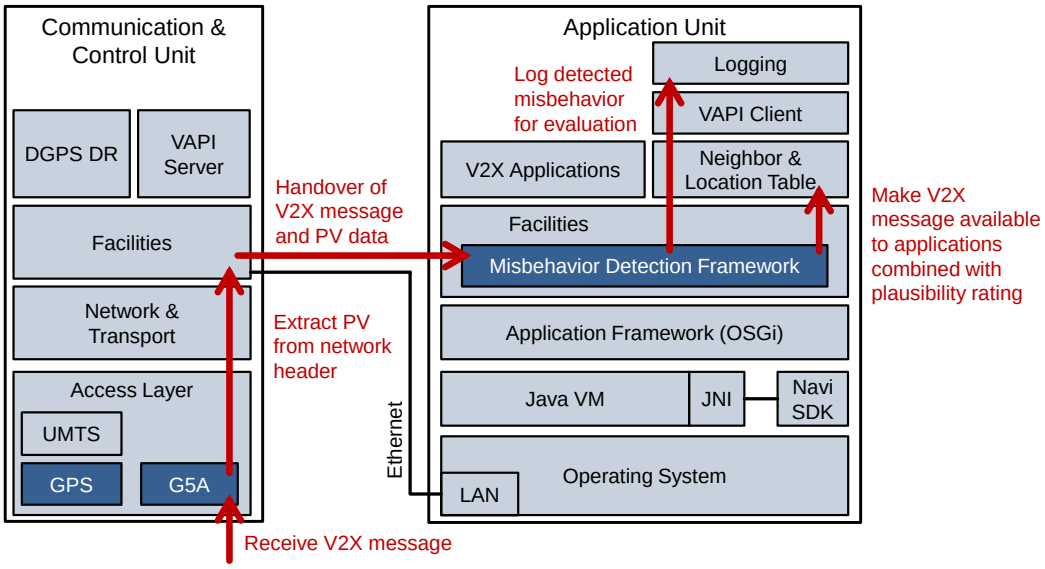


Figure 3.5.: Integration of the module-based misbehavior detection framework into the on-board V2X communication architecture of the FOT [SBH+10, JBSH11]

The application layer is operated by an application unit (AU) and functions of the facilities layer can be found on both the CCU and AU. The security solution of the FOT implementation [BSM+09] is also in line with the descriptions in Section 2.2 regarding all relevant aspects. The implementation

of the module-based misbehavior detection framework is operated on the facilities layer of the AU as depicted in Figure 3.5. The AU is realized with an automotive grade personal computer hardware equipped with an Intel Atom D510 processor at 1.66 GHz and 2 GB of RAM. On a Windows-based operating system the Java OSGi virtual machine is operated. On the facilities layer of the AU, the plausibility checker is able to access the local mobility information of the own station and receives all incoming messages before they are provided to the V2X applications. As illustrated in Figure 3.5, V2X messages received by the CCU via ITS-G5A are processed by the different communication layer implementations. The message object is extended on the network & transport layer with the PV of the network header before it is provided to the AU facilities layer. Before the message object is stored in the neighbor & location table the module-based misbehavior detection framework analyzes the PV content of the V2X message. In order to check the PV the misbehavior detection implementation needs access to up-to-date information about location and time of the station the implementation is running on. This information is provided by the vehicular application programming interface (VAPI) that uses GPS-based positioning improved by differential GPS (DGPS) and dead reckoning (DR).

Evaluation Setup - Measurements The author of this dissertation created for the FOT an extensive evaluation concept with respect to security and plausibility in order to measure the required parameters related to misbehavior detection on 120 vehicles and 100 RSUs over a test period of 76 days [WBB+12]. This measurement was realized with the logging framework as shown in Figure 3.5. Within the FOT, the AU logging application has collected on all vehicles and RSUs relevant log information generated by local system components. At the end of every day the logs were transmitted to a central infrastructure entity. The misbehavior detection framework created log entries for V2X messages that showed abnormal behavior of neighbor nodes or invalid values as listed in the following.

- `THRESHOLD_CHECK__TIMESTAMP_CHECK_NOT_PASSED`
- `THRESHOLD_CHECK__RANGE_CHECK_NOT_PASSED`
- `THRESHOLD_CHECK__VELOCITY_CHECK_NOT_PASSED`
- `THRESHOLD_CHECK__MOBILITY_DEVIATION_CHECK_NOT_PASSED`
- `THRESHOLD_CHECK__HEADING_DEVIATION_CHECK_NOT_PASSED`
- `THRESHOLD_CHECK__C2X_MESSAGE_FREQUENCY_CHECK_NOT_PASSED`
- `NEW_STATION__MARGIN_CHECK_NOT_PASSED`

As indicated by these evaluation parameters the misbehavior detection implementation deployed on the test stations focuses on the main subset of plausibility checks: the consistency and threshold checks (i. e. MCR, MTD, MBF) and the PM and SAS checks based on the Kalman filter-supported tracking of adjacent nodes. After completion of the FOT the evaluation of the log entries has been performed with an automated process. In order to minimize the size of the log entries exact values could not be logged in the FOT. Instead we prepared value classes (e. g. 100, 200, ... , 1000) and rounded the exact value to match a class. For example, a value of 156 is assigned to the class 200. The algorithms used in the evaluation process, elaborated by the author of this dissertation, are further detailed in the evaluation concept of the FOT project [WBB+12]. For the sake of simplicity, the following evaluation is focused on measurements created by the vehicles and is ignoring the measurements created by RSUs. Since the

module-based plausibility checks use only mobility data, the measurements created by RSUs are not the primary focus of the evaluation.

Evaluation Setup - Environment In the course of the FOT urban roads, rural roads, and highways of a test area around the city of Frankfurt am Main were used. The test vehicles has been steered by twelve expert drivers and 450 test drivers who were specifically recruited for that purpose. During the field operational test more than 150 kilometers of test drives has been traveled per day and per vehicle. The test drivers performed specific experiments based on scripted road scenarios [Wei12]. This ensured that most of the test time several vehicles were in common communication range.

Evaluation Setup - Reproducibility Based on the logs recored within the test drives XML encoded trace files including V2X messages can be generated. Every XML file contains locally available information of the respective station provided by the VAPI such as GPS location and time, speed, heading, etc.. In addition, the sent and received V2X message objects can be included. These files can be replayed with a trace player that is connected to CCU and AU devices in a laboratory environment. As a consequence all test scenarios of the FOT are reproducible and repeatable.

Evaluation Setup - Configuration The configuration of the module-based misbehavior detection framework used in the FOT is provided in Table 3.3. The values in the first three rows are fixed due to physical limitations of the IEEE 802.11p radios and due to definitions in ETSI standards (i. e. [ETS10d, ETS10e]).

Table 3.3.: Configuration of the module-based misbehavior detection framework

Plausibility check	Value	Description	
Maximum communication range (MCR)	1 km	If the location of a single-hop message claims to be within the MCR then the receiver considers the position vector as plausible.	**Defined by standards**
Maximum transmission delay (MTD)	500 ms	If the timestamp of the message generation is below the MTD, compared with the receivers' system time, the provided message is considered to be fresh.	
Maximum beacon frequency (MBF)	15 Hz	A sender that distributes V2X messages with a higher frequency than MBF is considered to be suspicious.	
Suddenly appearing station (SAS)	200 m	Stations that claim to be in a distance below SAS are considered to be not plausible.	**Variable**
Plausible movement (PM)	5 m	A claimed position that deviates more that 5 meters from a predicted position is considered to be implausible.	
	111 $\frac{m}{s}$	A stated velocity value larger than 111 m/s is not trustworthy.	
	10°	A heading that differs more than 10° from the predicted heading is considered to be implausible.	

The MCR is for example limited by the maximum transmission power allowed for IEEE 802.11p transceivers and the MTD and MBF are limited by specifications of the ETSI standards [ETS09, ETS10d]. The remaining configuration values of the SAS and PM check are determined in dedicated tests with a small number of test vehicles. Consequently, the variable configuration values may differ in later deployments.

Accuracy In order to calibrate the Kalman filter-based tracking algorithm for the practical outdoor tests, recorded traces from multiple test drives in cities, on country roads, and on highways has been used. In these position prediction accuracy tests, CAM frequencies with a dynamic rate according to ETSI [ETS10d] are compared with static frequencies between 1 Hz and 10 Hz. In particular, message frequencies of 1 Hz, 2 Hz, 10 Hz, and the dynamic ETSI frequency are applied on the corresponding CAM generation algorithm in a trace player to evaluate the Kalman filter accuracy. The test results provided in Figure 3.6 show that the prediction accuracy of the advocated Kalman filter-based vehicle tracker is optimal at the highest CAM frequency.

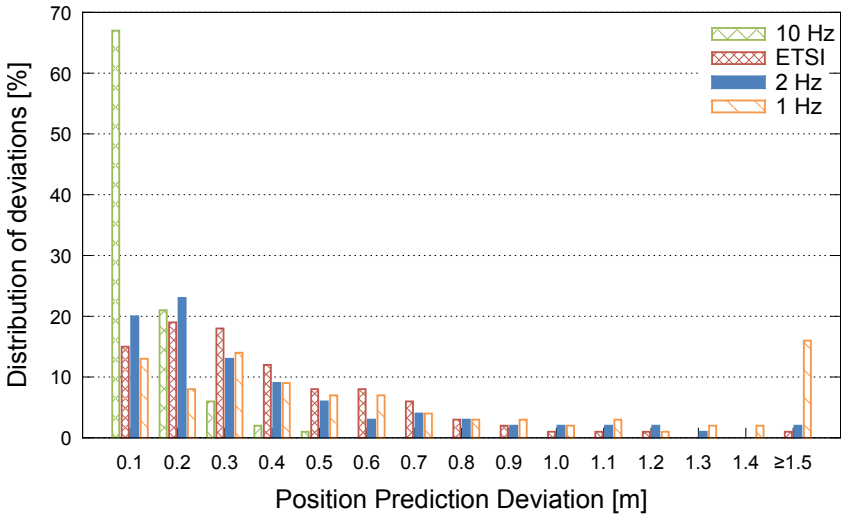


Figure 3.6.: Evaluation of the impact of different CAM frequencies on the Kalman filter-based position prediction accuracy

For the test shown in Figure 3.6 an exemplary trace is used that comprises highway sections allowing speeds of more than 90 km/h, and inner-city road sections. Even with the variable CAM generation interval, the prediction deviation is lower than 1 meter in the majority of all cases (i. e. 96% of received PVs). In addition, the effect of different road classes on the prediction accuracy is evaluated. Therefore, highway traces are compared with city traces, each with CAM intervals according to the CAM generation rules based on ETSI specifications [ETS10d]. The position prediction accuracy depends on the mobility and the behavior of the tracked object. We analyzed the hypothesis that the accuracy of predictions is best having vehicles moving with high speed on highways that motivate less to change the heading and velocity. On the contrary, vehicles moving with low speed in urban environments produce higher prediction inaccuracies because they might change their heading and velocity spontaneously.

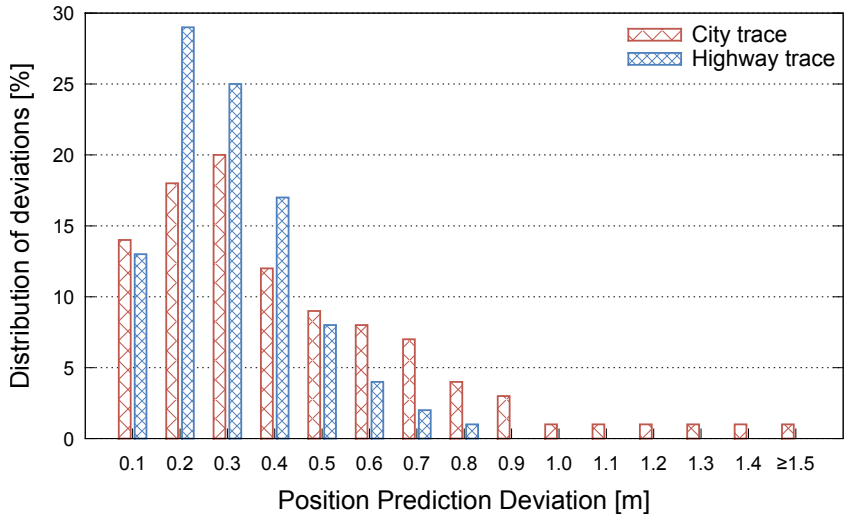


Figure 3.7.: Evaluation of the Kalman filter-based position prediction accuracy. Measuring the impact of different road types using CAM generation rules according to ETSI [ETS10d]

The measurements with the Kalman filter implementation confirm this hypothesis. In Figure 3.7 it is shown that a less predictable vehicle movement in urban scenarios has a negative effect on the prediction accuracy. However, even in city traces the position inaccuracy is still negligibly low, but in special situations, e. g., in a situation where a vehicle performs an emergency braking or suddenly starts to overtake another vehicle, the prediction accuracy decreases.

In addition to Kalman filter-based measurements under laboratory conditions the module-based misbehavior detection framework has been deployed in a field operational outdoor tests over a time period of 76 days. The goal is analyze the applicability of our approach under real conditions. The following evaluation is based on log data created by the misbehavior detection implementation installed on the test vehicles. Further, it has to be considered that within this FOT attacks were not performed. Consequently, the number of anomalies caused by authenticated and authorized VANET nodes is analyzed in the following. Even if the implementations of the FOT are partly based on immature prototypes the results might provide valuable information for future productive implementations. This also applied for anomaly and misbehavior detection.

In summary, the outdoor tests with real vehicles produced a false-positive rate of $\approx$ 9.25%. Consequently, over 9% of the processed V2X messages are rated as erroneous in the tests. The pie diagram in Figure 3.8 shows the distribution of the plausibility violations related to the different checks. A detailed discussion of the false-positive rate is given in the following including an analysis and a classification of the errors.

Figure 3.9 depicts the results of the MCR check. Only the detections above the threshold of 1 km, cf. Table 3.3, are considered. The bar chart shows on the x-axis different ranges of distance between the message sender and receiver. The y-axis shows the portion of MCR violations related to the total number of processed messages. At the same time the y-axis shows the distribution of MCR violations. The results show that some single-hop messages in the tests violate the predefined MCR but in relation

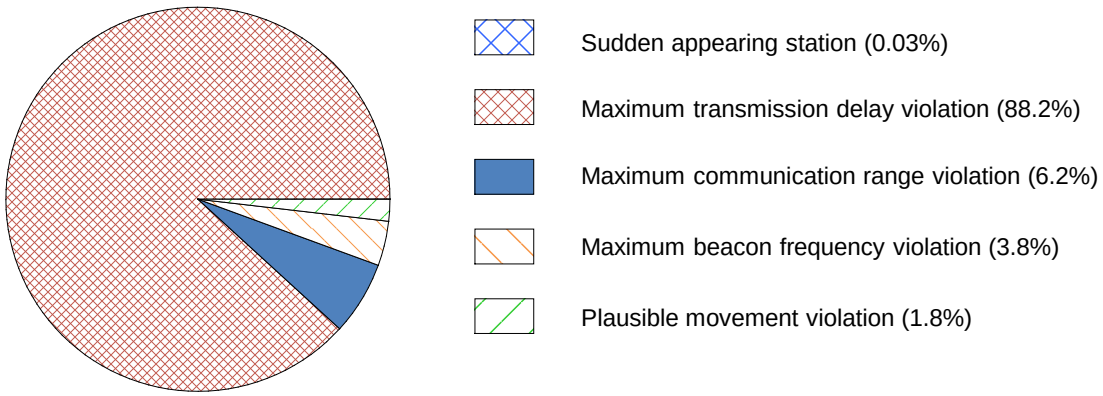


Figure 3.8.: Distribution of plausibility violations in long-term tests with real vehicles

to the total number of processed messages these violations are marginal (i. e. subsumed $\approx 0.57‰$). More than 40% of the anomalies are caused by messages that are sent beyond 2000 meters which is twice as much as allowed according to MCR configuration, cf. Table 3.3. After an analysis of this effect we identified that RSUs sent V2X messages with increased transmission power for test purposes.

Figure 3.10 shows the results of the MTD check. The construction of the chart is comparable with Figure 3.9 with respect to the meaning of axis and bars. In the figure it is shown that the majority of MTD faults are violating the threshold four times more than allowed. Moreover, the bars shows that this check detects most implausible messages in the FOT. If all MTD faults added up $\approx 8.2\%$ of the received V2X messages processed on vehicle stations provide a timestamp older than the configured MTD. The pie chart in Figure 3.8 acknowledges that most false-positive detections (88.2%) are caused by the MTD check. In most cases the timestamp is older than 2 seconds. This effect was primarily caused by

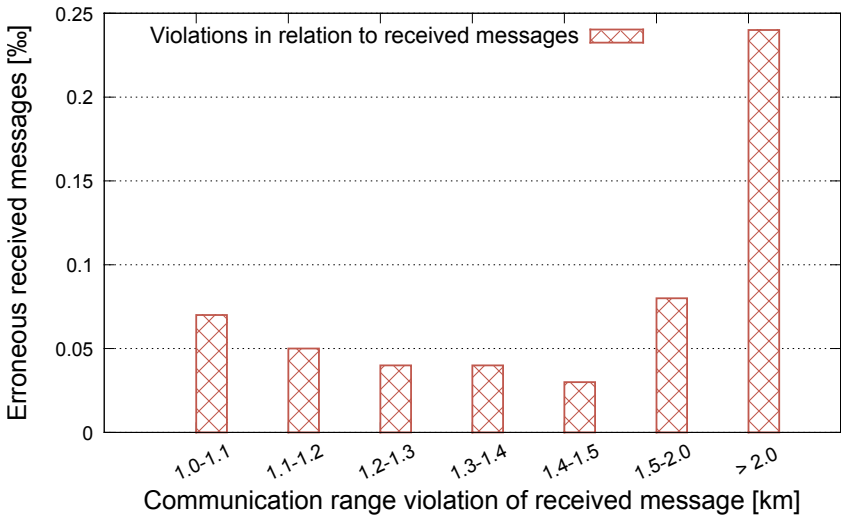


Figure 3.9.: Violation of maximum communication range in long-term outdoor tests with real vehicles

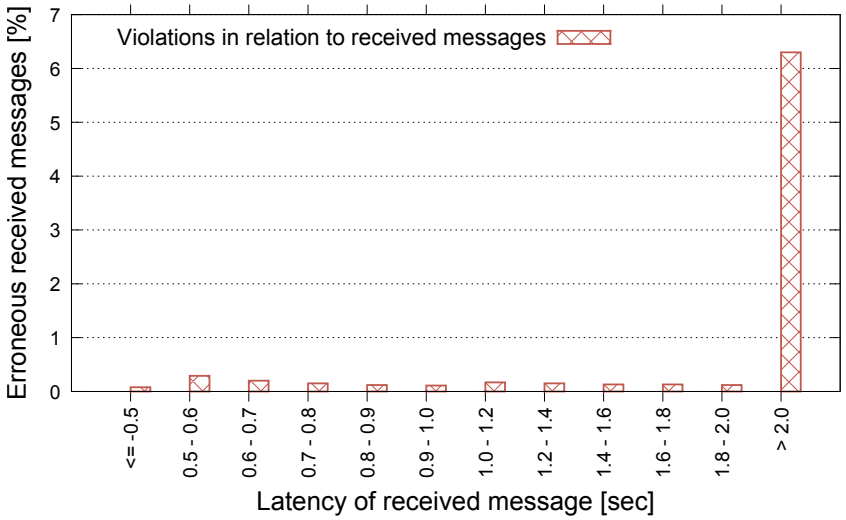


Figure 3.10.: Violation of maximum transmission latency in long-term outdoor tests with real vehicles

unsynchronized nodes and overloaded systems unable to send outgoing messages in time. Furthermore, some systems in the tests were not able to provide incoming messages to the plausibility checker on the AU in time. It has to be considered that this MTD check is the first test that is performed by the module-based misbehavior detection framework when a V2X message is received. If the generation timestamp of the message is above the predefined threshold listed in Table 3.3 then the message is considered to be erroneous. In this case no further check is performed and consequently no evaluation with respect to the other parameters has been done. As a result, multiple implausibilities per message are not considered.

Another threshold check is the MBF check that is not represented by a diagram. However, the FOT evaluations have shown that 3.8% of the plausibility errors are caused by nodes that send more V2X messages per second than allowed by the standards. In total, approximately 3.3‰ of the received V2X messages violate the ETSI standard [ETS10d] with respect to the maximum beacon frequency.

The detection of suddenly appearing stations is evaluated in Figure 3.11. On the x-axis, the distance between the new station and the receiver is grouped. The y-axis shows the number of SAS detections within the corresponding range. It is shown that the number of suddenly appearing stations is higher at the SAS threshold and decreases with a smaller distance to the receiver. This evaluation shows that in real VANETs the sudden appearing of previously unknown nodes is not negligible even if only $\approx 0.3‰$ of the received messages were related to this kind of anomaly. Most reasonable explanations are shadowing effects caused by buildings, large trucks or geographical conditions such as hilltops. As a consequence this kind of detection should probably not be used to exclude vehicles.

The evaluations shown in Figure 3.9, 3.10, and 3.11 are related to the threshold checks and do not require a tracking of nodes. In contrast, Figure 3.12 depicts the evaluation of the Kalman filter-based vehicle tracking.

The x-axis shows the different deviations between a stated position and the corresponding expected position. In particular, this is the deviation between a stated position contained in a V2X message

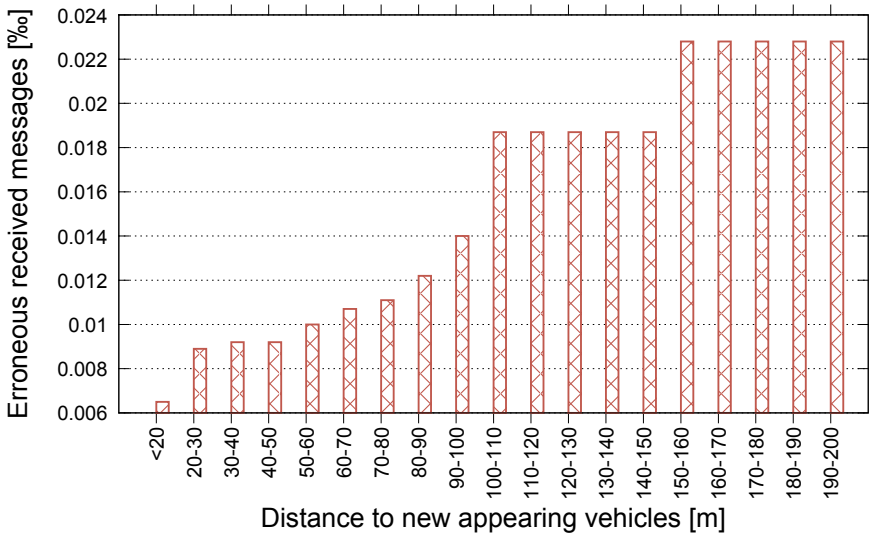


Figure 3.11.: Detection of suddenly appearing stations in long-term outdoor tests with real vehicles

and the Kalman-filter predicted position. The y-axis shows the portion of PM violations related to the total number of processed messages and at the same time the distribution of violations in relation to all PM errors. The figure shows that most violations ($\approx 40\%$) appear in the range between 5 and 6 meters and that the number of detections decreases with higher distance values. By adding up all values it can be shown that in total approximately 1.6‰ of all received V2X messages cause a PM violation. Compared with the evaluations under laboratory conditions shown in Figures 3.6 and 3.7 the FOT evaluation revealed that a few position jumps larger than 5 meters can be assumed in real VANET implementations. As a consequence a local misbehavior detection system should be robust with respect to single violations. However, if several detections are caused by a specific node then this node could be considered as faulty and further actions such as local exclusion or misbehavior reporting should be performed.

Since no attack has been performed in the long-term outdoor tests the author of this dissertation has elaborated and performed dedicated experiments with attackers in place. This has been done to measure the number correctly detected misbehavior (true-negative) and the number of undetected misbehavior (false-negative). For this purpose an application-layer attacker is used to perform generic location-related attacks in dedicated tests as presented in the adversary model in Section 2.3.3.2. Figure 3.13 shows the misbehavior that is detected by receiver R. Three types of points are used in this figure to indicate the detection events with reference to the kind of consistency and plausibility check. The misbehavior is caused by a ghost vehicle A_1 over a test time of 70 seconds. The diagram shows the misbehavior detections based on the same attack scenario as illustrated in Figure 2.10 on page 29. In comparison to Figure 2.11 on page 30, in this diagram only the distance between the ghost vehicle A_1 and the receiver R is shown by the filled curve.

The sudden appearance of the ghost vehicle is detected when the attack is started at time k_0. According to Table 3.3 new vehicles that appear within a range of 200 meters around the receiver are considered as suspicious. In the evaluated attack A_1 appears in front of R with a distance of approx-

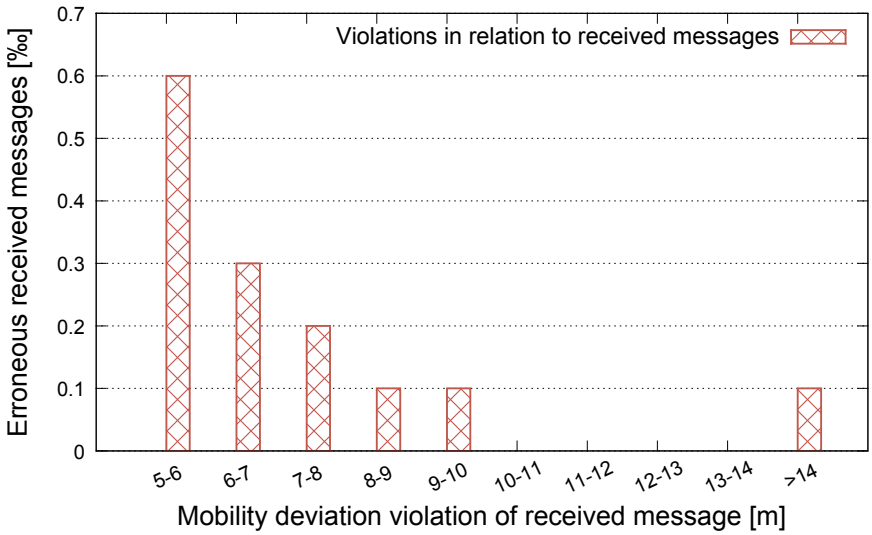


Figure 3.12.: Detection of implausible movement in long-term tests outdoor with real vehicles

imately 30 meters which leads to a plausibility violation. The PM check identifies further position jumps of the ghost vehicle every time A_1 moves to a new position in front of the receiver, cf. time k_2 in Figure 2.12 on page 31 and time k_2 in Figure 3.13. Position jumps larger than 5 meters are considered to be suspicious, cf. Table 3.3. At the times 231, 235, and 262 position jumps are not detected as the distance computed based on position information from two sequential CAMs has not exceeded the threshold. Only abrupt jumps larger than 5 meters are considered as inconsistency as shown by the distance curve in Figure 3.13. The third plausibility test detects position overlaps of A_1 and R as further detailed in Section 3.5. In total, receiver R detects in this exemplary attack scenario 24 plausibility violations caused by one ghost vehicle within a time frame of approximately 50 seconds. False-positive detections have not been appeared in this dedicated attack scenario.

It has to be considered that the performed attack is based on the EEBL application. However, the purpose of the attack and the ghost vehicle's behavior is comparable with other location-based application that aim for increasing traffic safety and efficiency. As a result, we can confirm the hypothesis that the module-based misbehavior detection framework is able to detect abnormalities as introduced in Section 1.2. Nevertheless, a more sophisticated attacker would try to present a fully plausible movement of the ghost vehicle. These possibilities decrease with increasing traffic density as detailed in Section 2.3.3.2.

Summarizing the results, both the evaluations of laboratory tests and outdoor tests with several equipped test vehicles have shown that the module-based mobility data plausibility check applying Kalman filters is an appropriate instrument to detect deviations of a defined mobility model. The detection requires, however, that the attacker produce abnormalities that can be detected. Further, it has been shown that the combination of different specific plausibility verification modules is possible in order to evaluate the plausibility of a PV on both message basis and node basis. Since a simple message-based plausibility rating with the classification *approved*, *neutral*, and *erroneous* is provided, the V2X applications on the AU could decide not to process erroneous messages. Nevertheless, the results of the

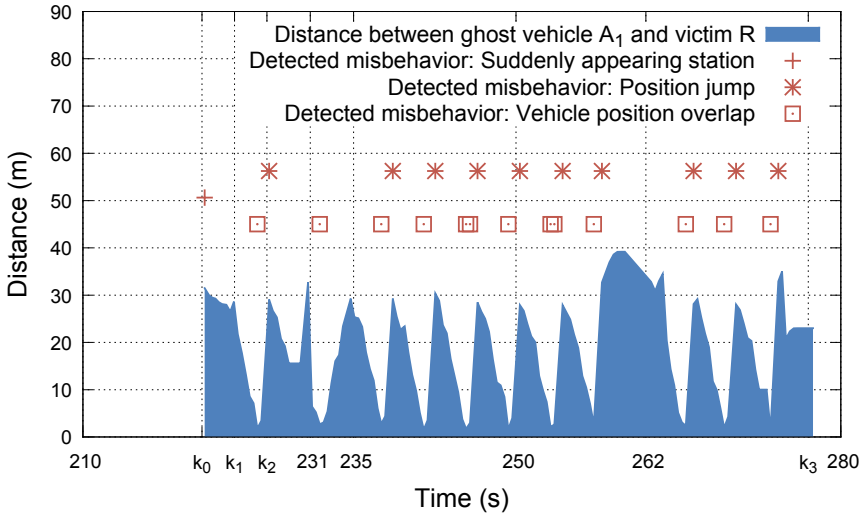


Figure 3.13.: Ghost vehicle caused misbehavior detection using a Kalman filter

outdoor tests show that approximately 9.25% of the received messages are rated as *erroneous*. From a security perspective, it is reasonable to discard received messages that are not approved by message-based plausibility checks. In particular, replayed messages and messages containing a PV with false value ranges or with inconsistent PVs are detected by the MCR and MTD checks. The corresponding erroneous V2X messages should be dropped and should not provided to the applications.

Implausible messages that are detected by the node-based checks (i. e. MBF, SAS, and PM), however, should not be dropped but handled by the application on the AU with low confidence. Based on the ratings of the single messages a short and mid term evaluation of node trustworthiness can be created. According to the evaluation involving the test vehicles, approximately 98% of the measured implausibilities are caused by message-based checks and only 2% are caused by node-based plausibility checks. Consequently, approximately 5‰ of the incoming single-hop V2X messages lead to a node-based implausibility.

Since no evaluation results related to accuracy are published by authors of related work [SLS+08, Ger10, oTRA12] a comparison based on figures cannot be done. For the comparison of our own proposals with related solutions we estimate the accuracy of related works based on argumentations provided in the respective publications. A summary of this comparison is provided in Section 3.7.

Scalability The performance of the prototypical plausibility checker is measured under laboratory conditions using different recorded vehicle traces. In these performance tests the previously described AU hardware of the test vehicles has been used. Even though such high-performance hardware may not be used in the later deployments it is assumed that more efficient implementations, for example code written in C instead of Java, will probably show similar results on less powerful embedded hardware. The evaluations show that the total execution of the plausibility check of an incoming V2X message takes on average $\approx$ 2.7 ms but exceptional values of approximately 190 ms have been measured with higher numbers of neighbor nodes. The exceptional values are potentially caused by the Java environ-

ment that sporadically executes internal processes such as the garbage collector that consumes system resources. Furthermore, the plausibility checker has to share its CPU and memory with other applications that are executed on the same system, e. g. V2X message generation and handling, local dynamic map, navigation support. Moreover, it is measured that a minor part ($\approx 20\%$) of the processing time is consumed by consistency and threshold checks (i. e. MCR, MTD, MBF) and the major part ($\approx 80\%$) is consumed by the PM and SAS verifications. This evaluation shows that the module-based plausibility check is basically able to verify up to 370 messages per second by predicting vehicle positions accurately. However, this number strongly depends on the applied system and its performance and is closely related to other applications that are executed on the system.

Since the concepts of related work [SLS+08, Ger10] have not been evaluated with implementations a comparison with respect to scalability and performance is not possible. The performance of our module-based misbehavior detection framework depends on the performance of the different modules. The evaluated setup provides good results with respect to processing performance and latency. However, implementers should consider that operations required by different modules should be performed only once in order to save resources. This might be the case, for example, for vehicle tracking.

Extensibility The proposed module-based misbehavior detection framework is extensible by adding or exchanging single modules. Due to the approach for fusion of results provided by modules the functionality of local misbehavior detection can be split in subordinated module implementations. The modularity of our approach is comparable with the VEBAS concept proposed by Schmidt et al. [SLS+08].

Generalizability Both frameworks, the proposed module-based framework and VEBAS, rely on highly specialized modules to verify different aspects of location-related information. Consequently, the generalization of the module-based misbehavior detection is limited. The consistency and threshold check, for example, is designed to analyze the specific elements of V2X packet contents and the Kalman filter is designed to track mobile network nodes. In the same way the verification of node positions with local sensors such as radar or camera might be designed for specific inconsistency detections.

Complexity The module-based approach follows the simple paradigm *divide and conquer* which is well known in computer science. Every module focuses on a specific aspect of the problem in location-related misbehavior detection. This reduces on the one hand the complexity. On the other hand, different modules may depend on the existence and operation of other modules which increases the complexity. The Kalman filter-based vehicle tracking depends on correctly performed consistency and threshold checks and the modules using local sensors rely on correct position predictions of the Kalman filter. With an increasing number of modules the complexity of the framework increases.

Bandwidth & Connectivity In the proposed module-based framework no exchange of information related to misbehavior detection is required. This saves valuable bandwidth of the ITS-G5 channels. Moreover the proposed framework is working autonomously and is not depending on infrastructure entities or specific misbehavior detection related information provided by VANET neighbors. The reporting of misbehavior to a central entity is optionally from perspective of the module-based misbehavior detection framework.

Privacy The module-based framework is able to work with pseudonymous IDs as targeted in standardization [IEE13, ETS12a, ETS13b] and deployment activities [WBF+13]. The module-based approach in contrast impacts the privacy since single-hop neighbor nodes are tracked by the Kalman filter. This tracking allows the observation of ID changes of nodes as discussed in more detail in Section 4.2. As long as the information about the linking of pseudonymous IDs is not distributed or centrally collected the effort remains high to reveal personal information such as the home address of drivers.

3.5. Position Overlap-Based Misbehavior Detection

As introduced in Section 3.2.5 second hand information provided by other nodes can be used to check the location plausibility of adjacent nodes. In this section a new kind of node-based location data consistency check is proposed that solely uses second hand information (i. e. CAMs) from single-hop neighbor nodes to verify their location plausibility and consistency. This novel concept has been elaborated by the author of this dissertation and bases on the idea that different physical vehicles cannot occupy the same certain space at the same time. An implementation and evaluation of the concept was supported by Christian Stresing within his Master thesis [SHB10] which was supervised by me.

The proposed check aims to detect implausibilities caused by non-existing ghost vehicles that are created by an attacker as described in the adversary model in Section 2.3. These ghost vehicles frequently exhibit inconsistencies when real vehicles move through the claimed position of the ghost. As a result, this knowledge is used to make assumptions about possible misbehavior by modeling a position verification strategy that compares the PVs of adjacent vehicles. While using a generic vehicle model and taking typical GNSS position errors into account, physically impossible position overlaps can be detected. This framework can be used by the local misbehavior detection system performed on receiver stations.

3.5.1. Vehicle Overlap Model

Ideally, a received position vector represents the location of the center of a corresponding vehicle. Obviously, two vehicles that virtually drive through each other are possibly not broadcasting the exact same position data. PVs contain a single position that allows a centimeter exact resolution (cf. Table 2.2 on page 18). In general, the vehicles' dimensions combined with a possible safety clearance is not taken into account by the PVs. Therefore, the proposed overlap detection scheme models the vehicle dimensions based on width $w(N_A)$ and length $l(N_A)$ information provided by a vehicle N_A within its CAMs. This model is based on an approach of Anurag et al. [DGB08] where it is used in a collision warning system. Having the dimensions and the heading a vehicle the vertices of a rectangle can be calculated. In particular, the left front (LF), the left rear (LR), the right front (RF), and the right rear (RR) vertex can be identified as shown in Figure 3.14.

With the help of this vehicle model it is possible to calculate whether rectangles of different vehicles overlap. In order to observe any overlap of two rectangles an hyperplane overlapping test is performed that is well known as *separating axis test* in the literature [GT96, SIF97]. Two rectangles of vehicles N_A and N_B overlap if any point $P(x_p, y_p, z_p)$ of one rectangle lies inside the area of the other rectangle.

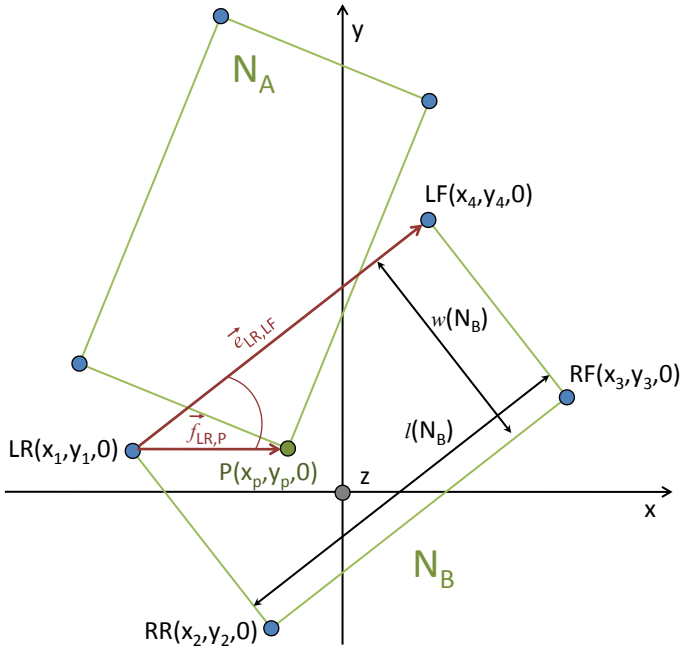


Figure 3.14.: Vehicles modeled as a rectangular shape with dimensions w and l

More specifically, the algorithm tests whether a vertex of the rectangle of one vehicle N_A is on the right side of all edges (traversing the rectangle's edges clockwise) of the rectangle of vehicle N_B. This rule implies that this corner would be inside vehicle N_B, and thus the vehicles overlap.

In every rectangle overlap test the algorithm starts with one edge of the rectangle of vehicle N_B, for example the leg between point $LR(x_1, y_1, 0)$ and $LF(x_4, y_4, 0)$ and computes its representing vector $\vec{e}_{LR,LF}$. Similarly, the vector $\vec{f}_{LR,P}$ from $LR(x_1, y_1, 0)$ to the testing point $P(x_p, y_p, 0)$ is determined. The testing point is one of the corners of the other vehicle N_A. These two vectors span a parallelogram whose surface can be calculated as euclidean norm of the resulting vector from the vector product of the two vectors $\vec{e}_{LR,LF}$ and $\vec{f}_{LR,P}$ as shown in Equation 3.11.

$$\begin{aligned} \chi_1 &= |\vec{e}_{LR,LF} \times \vec{f}_{LR,P}| \\ \chi_1 &= |(x_p - x_1)(y_4 - y_1) - (y_p - y_1)(x_4 - x_1)| \end{aligned} \tag{3.11}$$

The resulting value χ may be positive or negative, depending on the sign of the angle (either positive or negative) between the two vectors. Consequently, the sign of the result indicates on which side of the vector $\vec{e}$ the testing point $P(x_p, y_p, 0)$ is located. Subsequently, the algorithm continue clockwise picking the next edge and test χ on the remaining edges.

If all test results, i. e. all χ_i with $i \in 1...4$, have the same sign (in the example depicted in Figure 3.14: positive), the tested point $P(x_p, y_p, 0)$ of N_A is inside the rectangle of N_B. If not, the calculation is repeated with the next corner point of N_A. Once all four corners have been tested and an overlap is not detected then the algorithm tests whether the corner points from the other vehicle N_B are inside the rectangle of N_A. This algorithm fails only if the two rectangles form a cross-like shape with all

corner points outside the rectangle model of the other vehicle but their bodies crossing. In this case, the overlap will be detected in the next test when at least one of the vehicles has moved slightly. Indeed, this implies a valid movement behavior which can be ensured by the vehicle tracking discussed in section 3.4 and 3.6.

Due to possible imprecisions of the distributed position data, the vehicle overlap detection model needs to be extended. The previously discussed algorithm incorporates only two results: either an overlap is detected or not. The extension assesses the certainty of overlaps by addressing the area close to the vehicles. Even in a traffic jam, there is always a certain amount of space between neighboring vehicles: the safety area. A vehicle that claims its position to be inside the safety area of another vehicle is suspicious and should further be observed in more detail. However, due to the former mentioned imprecisions in position data, vehicles that move close to another vehicle might unintentionally create slight overlaps. This should not lead to immediate misbehavior detection, but should raise awareness. As such, the area outside the physical vehicle dimensions shall be considered with a reduced weighting. Therefore, differently sized rectangles are used to model the vehicles as illustrated in Figure 3.15. Vehicle overlaps of inner rectangles result in detections with higher certainty than overlaps of outer rectangles. The certainty of an overlap $c_{overlap} \in \mathbb{R}$ with values in the range $[0,1]$ can be calculated as presented in Algorithm 3.1.

Algorithm 3.1 Algorithm to calculate the certainty of a vehicle overlaps

1: **while** $i < i_{max}$ **and** $c_{overlap} = 0$ **do**
2: $\quad c_{overlap} \leftarrow \frac{overlaps(N_A,N_B,i)}{(i+1)^{\gamma}}$
3: $\quad i \leftarrow i+1$
4: **end while**

The function $overlaps()$ is a predicate that checks whether two specific rectangles of node N_A and N_B overlap. More precisely, the predicate tests the particular rectangles at level $i \in \mathbb{N}_0$ with values $i = 0,\ldots,i_{max}$. Based on the parameter i several virtual rectangles with different dimensions are calculated for a vehicle as illustrated in Figure 3.15. The exponent γ in the second line is used to decrease the weight of $c_{overlap}$ with increasing i as subsequently discussed in more detail. The predicate function $overlaps()$ in the numerator returns 1 if the rectangles overlap, or 0 otherwise. This function implements the algorithm that is described in the vehicle overlap model, but re-calculates the rectangle length l and width w based on the loop iterator i.

It is assumed that the sizes of the vehicles' physical safety area correlate to the speed of travel. Additionally, the vehicles' velocities influence the dimensions of the outer certainty rectangles. With higher velocities, the safety area increases predominantly in the direction of travel which is modeled as length l_{rect} as shown in Equation 3.12.

$$l_{rect} = \frac{i}{i_{max}} \cdot \frac{v(N_A)}{d_s} + \alpha \cdot l_{N_A} \tag{3.12}$$

The variable i_{max} in equation 3.12 is the maximum number of iterations to be executed, i. e. the maximum number of rectangles in the vehicle model. The fraction $\frac{v(N_A)}{d_s}$ depends on the velocity of vehicle N_A and is added to the original length of the innermost rectangle of vehicle model of N_A. The dimensionless parameter d_s calibrates the influence of the velocity on the length of the rectangles and the

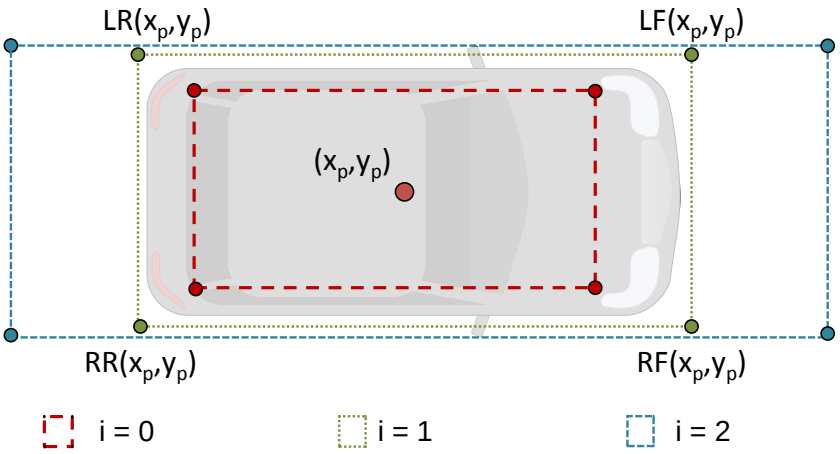


Figure 3.15.: Vehicle modeled using differently sized rectangles to observe overlaps

factor α reduces the original length of the vehicle for overlap detection. A reduction of the inner rectangle size may be interesting in order to increase the severity of inner rectangle overlaps. While l_{rect} depends on $v(N_A)$, the calculation of w_{rect} ignores the vehicle's velocity since it has marginal impact. However, under consideration of lateral position inaccuracies, w_{rect} is also enlarged with increasing i as shown in Equation 3.13.

$$w_{rect} = \frac{i}{i_{max}} \cdot (w_l - \alpha \cdot w_{N_A}) + \alpha \cdot w_{N_A} \tag{3.13}$$

The rectangle width w_{rect} increases slightly, but shall not exceed the width of the lane the vehicle is traveling on since otherwise overlaps would occur in the case that vehicles travel next to each other on neighboring lanes. In the following evaluations, a typical lane width of $w_l = 2.5$ m is assumed to be the upper bound. The predicate $overlaps()$ in Algorithm 3.1 uses equation 3.12 and 3.13 in order to obtain appropriate values for l_{rect} and w_{rect}. With increasing i, and therefore increasing dimensions of the rectangles, the overlap certainty decreases. The denominator in the equation of the second line of Algorithm 3.1 determines the fraction of certainty of an overlap of the two rectangles that can be adjusted with the exponential weight γ.

3.5.2. Node Evaluation based on Vehicle Overlaps

By applying the vehicle position overlap check, a ghost vehicle can be detected that claims a similar position as another vehicle at a specific point in time. The overlap certainty indicates the probability of the overlap. However, even in the case of high overlap certainty an attack is not necessarily the cause. For example, two benign vehicles that are sending PV updates with a low frequency may cause a false-positive vehicle overlap detection. As a result, a certain number of evidences should be collected by the overlap detection module before a possible misbehavior is assumed.

In the above described evidence collection process, the overlap detection results gained from Algorithm 3.1 are summed up in variable $s \in \mathbb{R}$ for every vehicle within the communication range. Every time the algorithm is executed, new overlap detections $s(k)$ are added to the value of previous detec-

tions $s(k-1)$ with k being the time, cf. Equation 3.14. In addition, an aging factor $a \in [0,1]$ is used in Equation 3.14 that enables previous overlap detections to fade. For instance, a neighbor vehicle that has created in the past overlaps with other vehicles may has a considerable level of distrust. This distrust should be decreased over time when no further overlaps are detected.

$$s(k) = c_{overlap} + a \cdot s(k-1) \tag{3.14}$$

Obviously, variable s increases with respect to the certainty of overlap detections in each measurement. In order to define an overall certainty of misbehavior, parameter $s_{min} \in \mathbb{N}$ is introduced. This value determines the level of evidence that is required to assume a misbehavior detection based on vehicle overlaps. Equation 3.15 calculates the certainty of having detected overlap-based misbehavior.

$$c_{misbehavior} = \frac{s_{min} \cdot s}{2 \cdot (s_{min} - s) + s_{min} \cdot s} \tag{3.15}$$

When the node-based collection of overlap evidence s reaches s_{min}, then the misbehavior certainty $c_{misbehavior}$ reaches 1. Equation 3.16 shows the adaption of Equation 3.14 by constraining the results to the range $[0, s_{min}]$.

$$s(k) = min(c_{overlap} + a \cdot s(k-1), s_{min}) \tag{3.16}$$

3.5.3. Evaluation of the Position Overlap-Based Misbehavior Detection

The following evaluation of the vehicle overlap detection mechanism is structured according to the criteria defined in Section 3.3. In the first paragraph, the implementation, the evaluation instrument, and the setup is presented. Subsequently, the evaluation results are discussed in respect to the defined criteria: criteria *accuracy, scalability, extensibility, generalizability, complexity, bandwidth & connectivity, and privacy*. We aim to examine the hypothesis whether the proposed mechanism can be applied in VANETs to detect misbehavior.

Evaluation Setup In order to evaluate the functionality and applicability of the proposed mechanism a simulation framework has been used. In contrast to the evaluation of the module-based misbehavior detection framework all parameters of the communication channel, the vehicle movement, and the driver behavior can be configured. Moreover, the required system configurations and components that are required to analyze the functionality of the proposed mechanism are not available in prototypical FOT implementations. The overlap detection mechanism requires in particular lane accurate positions. This accuracy cannot permanently be achieved with FOT implementations that are available at this time. Furthermore, a simulation study allows to calibrate the mechanism with different configurations and the subsequent evaluation runs can be reproduced and repeated with the parameters given in this section.

The *V2X simulation runtime infrastructure* (VSimRTI) simulator as previously introduced in Section 2.3.3.1 was applied. This framework has been developed by the Daimler Center for Automotive Information Technology Innovations (DCAITI) to integrate several time-discrete simulators. VSimRTI is in particular optimized for the testing of VANET applications. This simulation framework combines the traffic simulator *simulation urban mobility* (SUMO) [KHRW02] that allows for the modeling of vehicle

behavior in road scenarios and the network simulator JiST/SWANS [Bar06, Bar04] that is taking care of the wireless communication between the vehicles and RSUs. The application interface simulator of VSimRTI allows to implement applications that are running on each simulated station as depicted in Figure 3.16.

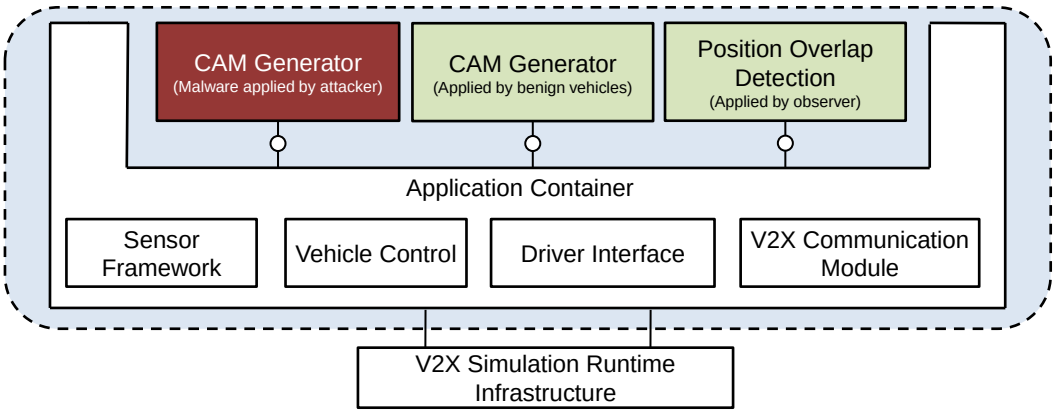


Figure 3.16.: Integration of applications into the VSimRTI simulation framework

VSimRTI comes with an implementation of a CAM generator that periodically distributes them among relevant nodes in the network. These CAMs are periodically sent according to a predefined frequencies between 1 Hz and 10 Hz. Every benign vehicle in the simulation is equipped with an application that broadcasts CAMs. For evaluation purposes there is a single observer vehicle being in communication range of the attacker that runs the application to detect the position overlap-based anomalies.

The attacker malware that generates the ghost vehicle is designed to run on a RSU. At this station the benign CAM generator is exchanged by the malicious CAM generator depicted on the left hand side of Figure 3.16. That way, it is possible with VSimRTI to model a roadside attacker without affecting traffic simulation due to a vehicle on the road. Based on recorded previous vehicle movements, the malware replays these CAMs in order to create the illusion of correctly positioned or even plausibly moving vehicles. The replayed CAMs are then received by approaching vehicles that check the obtained position information.

Before the detection mechanism can be deployed, appropriate configurations for the vehicle overlap model and its dimensions have to be determined. The following parameters have to be configured: i_{max}, γ, d_s, α, and w_l. Furthermore, reasonable values for the algorithm execution frequency must be found. Finally, appropriate values for the overlap detection certainty related parameters such as s_{min} and the aging a need to be determined.

The usage of multiple rectangles that represent the vehicles' dimensions and their safety areas (cf. Figure 3.15), allows to allocate less weight to overlaps at outer distances than to overlaps in the core of the vehicle overlap model. This functionality is verified with the attacker scenario depicted in Figure 3.17. A stationary ghost vehicle A_1 is overlapped by a moving vehicle R. At time k_0 the rectangles of both nodes do not overlap. At a later time k_1 the core of both rectangles overlap almost completely

and at time k_2 only the outer rectangle of the moving vehicle R is still overlapping with the rectangle of A_1.

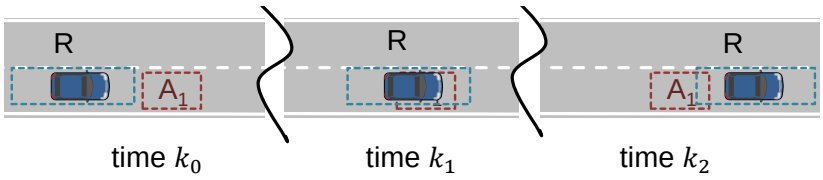


Figure 3.17.: Attacker scenario considered for vehicle overlap detection

This attack scenario is used in the simulations to determine a reasonable value for i_{max}. Depending on the value of d_s, which affects the length of the rectangles (see Equation 3.12), position overlaps of the two vehicles are detected throughout the simulations. Figure 3.18 shows the simulation results of the overlap scenario with different i_{max} and constant $d_s = 1.25$. Since only a small difference between the overlap level $i_{max} = 6$ and $i_{max} = 10$ can be determined, it is reasonable to select the smaller value for the remaining evaluations. For the detection of misbehavior the appropriate execution interval of the overlap testing algorithm has to be elaborated. This interval should not be related to the frequency of received CAMs because an attacker should not be able to manipulate the overlap detection by adjusting its message broadcasting frequency. Nevertheless, the execution interval must be high enough in order to allow a reliable overlap detection even with high vehicle mobilities.

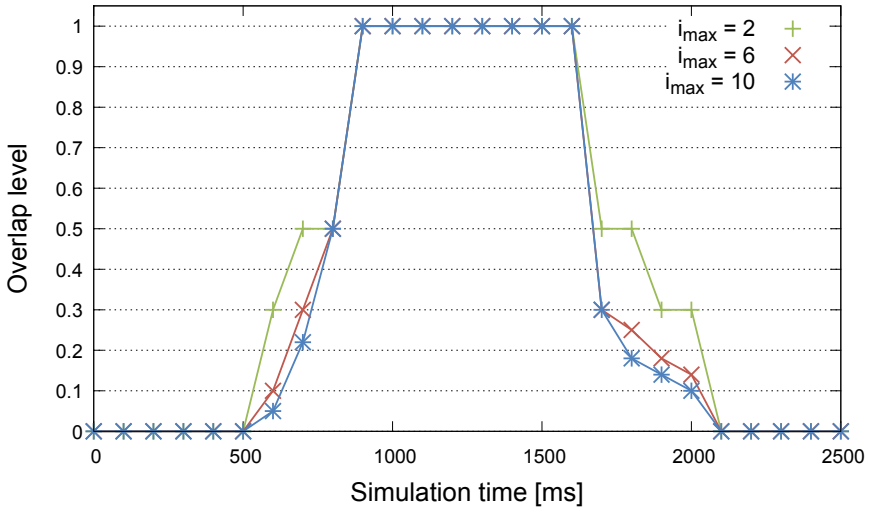


Figure 3.18.: Test results of the overlap detection algorithm used to calibrate i_{max} of the misbehavior detection module

Considering the anticipated application for misbehavior detection, it may happen that a stationary ghost vehicle A_1 is overlapped by another vehicle R that travels with maximum speed. In this situation, the overlap time is reduced to a minimum. Figure 3.19 shows the course of an overlap of two vehicles with a random GNSS error of 2 meters. In contrast to Figure 3.18, each curve has been recorded at a different speed of vehicle R. At an execution frequency of 10 Hz, at least one overlap at the core

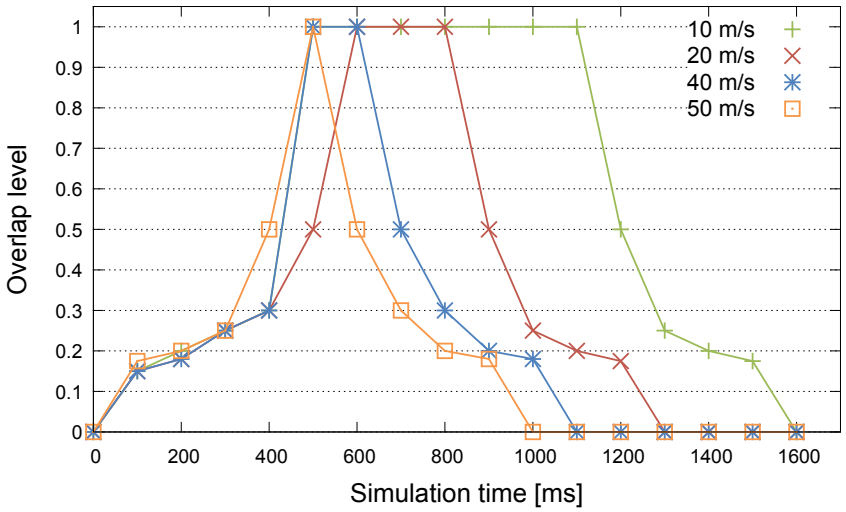


Figure 3.19.: Test results of the overlap detection algorithm used to calibrate the execution interval of the misbehavior detection module

rectangle is observed, despite the simulated GNSS position inaccuracy. Since a single overlap at the core provides a quite low level of evidence, the value of the overlap level at outer rectangles is set to $\gamma = 0.5$ in Algorithm 3.1. Based on further evaluations, detailed in [BSB10], an aging factor of $a = 0.9$ (cf. Equations 3.16) is used as well as a threshold value $s_{min} = 4$ that determines the number of sufficiently collected evidences. Using these configuration settings combined with a maximum random GNSS position inaccuracy of 6 meters, several evaluations of the overlap detection approach were performed with the simulation framework VSimRTI as detailed in [BSB10]. All configuration parameters are subsumed in Table 3.4.

Table 3.4.: Proposed configuration for position overlap-based misbehavior detection

Vehicle Model				**Evaluation of Vehicle Overlaps**		
Parameter	Value	Algorithm	Equations	Parameter	Value	Equations
γ	0.5	3.1		s_{min}	4	3.15, 3.16
i_{max}	6	3.1	3.12, 3.13	a	0.90	3.16
d_s	1.25		3.12	Execution frequency	10 Hz	
w_l	2.50		3.13	of overlap detection		

Accuracy In order to evaluate the accuracy of the proposed overlap detection, both the false-positive and false-negative errors are measured, and both the true-positive and true-negative detections are counted. The following three test scenarios have been evaluated with the simulation framework.

(1) Attacker fakes road traffic congestion by creating several ghost vehicles In a first test setup, a fake traffic congestion is created that consists of several ghost vehicles (e. g. A_1, ... , A_5, as exemplarily depicted in Figure 2.7 on page 24) that are generated by the malware of the attacker. Subsequently, benign vehicles overlap the positions of the ghost vehicles as they are driving through the non-existing congestion area. As a result, it has been shown that all ghost vehicles are correctly detected and no real vehicle is accused to be an attacker, despite random position inaccuracies of 6 meters, cf. test scenario 1b in Table 3.5. In order to distinguish between benign real vehicles and ghost vehicles, it is assumed that the observer of vehicle overlaps has traveled together with the benign vehicles in single-hop communication range for a predefined distance and time. Consequently, real vehicles have reached a higher trust and confidence level than the ghost vehicles. This concept to distinguish between real vehicles and ghost vehicles has obviously limitations as further discussed in test scenario 2.

(2) Attacker tries to deny existence of real road traffic congestion In this second test case it is analyzed whether an observer is able to distinct between the benign neighbor node and the ghost vehicle, both involved in an overlap, if no history about these nodes is available. This case may happen if an attacker aims to deny the existence of a real congestion. In such a scenario, the attacker creates a single ghost vehicle that drives virtually through a congestion area. In this case, the benign real vehicles involved in the traffic congestion have an equally low trust and confidence level than the ghost vehicle because the history of all nodes is equally long. Since no vehicle has reached a sufficient high trust and confidence level the observer cannot recognize the ghost vehicle as shown in Table 3.5. Consequently, we propose in Chapter 4 and Chapter 5 the reporting of detections to a central authority to evaluate detections from different reporters that have observed the same overlap. By combining other types of reported misbehavior a central entity is assumed to be able to identify the attacker.

(3) Overlap detection with high lateral positional shifts In general the results of the local overlap detection show that all vehicle overlaps are observed as expected. However, with increasing random GNSS position inaccuracy the false-negative detection rate increases. A third simulation setup is used to measure the false-positive rate without attackers in communication range that create ghost vehicles. For this test, a multi-lane highway scenario is selected in which vehicles overtake each other while traveling in the same direction with different velocities. With low position inaccuracies, the simulation shows that no overlap detections occur, cf. test scenario 3a in Table 3.5. However, with high lateral positional shifts, a high false-positive rate can be observed.

The results of the performed test scenarios are subsumed Table 3.5.

The evaluation has shown that the detection of position inconsistencies can be done reliable with the proposed mechanism. However, we figured out that accurate position information is required to minimize the number of false-positive detections. Different traffic safety applications (e. g. lane change assistance, intersection management, etc. as specified in the basic set of applications of ETSI [ETS09]) also rely on accurate PVs. Therefore, it is likely that techniques such as dead reckoning, differential GNSS, and relative positioning algorithms [BLB11] will be applied in future VANETs to allow a lane-level accurate positioning [PB11]. In addition, a research project in the domain of automated driving

Table 3.5.: Evaluation of the overlap detection algorithm

Test case	Random GNSS error	Detection of overlaps with distinction between of real vehicle and ghost vehicle	Detection of overlaps without distinction
(1) Attacker fakes road traffic congestion	0 m	100 %	0 %
	6 m	100 %	0 %
(2) Attacker tries to deny existence of traffic congestion	0 m	0 %	100 %
	6 m	0 %	80 %
(3) Overlap detection with high lateral positional shifts	0 m	0 %	0 %
	6 m	0 %	100 %

target the goal that vehicles can continuously determine their positions on the road to within 20-10 centimeters [MAG14].

Scalability The applied separating axis test [GT96, SIF97] applied for the position overlap detection has in principle no high performance requirements with respect to computation and memory consumption. The memory consumption is acceptable since only one vehicle model with several rectangles has to be stored per neighbor node. This vehicle model can be updated in every execution step of the algorithm.

Most relevant computations are related to simple vector operations and the processing of two dimensional polygons. Nevertheless, the algorithm has to be executed per single-hop neighbor vehicle with up to 10 Hz for several rectangles (cf. Table 3.4 for configuration of i_{max}). Additionally, a straightforward implementation would verify the position of a neighbor vehicles with the position of all other neighbor vehicles. In this case a complexity $O(N^2)$ is given with N being the number of single-hop neighbor vehicles and assuming a maximum execution interval and a static number of rectangles i_{max}. This complexity would result in an unacceptable high number of executions per second. In order to reduce the complexity and therefore the number of executions we propose the application of a relevance filter. Only neighbors that have nearby neighbors are verified. Since vehicles can have only a limited number of flanking neighbors the complexity is reduced to $O(N)$. Additionally, neighbor nodes that are not in the relevant area of the verifying node could optionally be ignored. For example, vehicles moving in the opposite direction behind the verifying node might be not relevant for local V2X applications. If this consistency check should, however, be used for misbehavior reporting it is reasonable that all single-hop vehicles are verified.

Extensibility The proposed mechanism provides most benefit in dense road traffic scenarios. With only a few vehicles on the road attackers could easily create ghost vehicles with plausible movement. If the traffic density increases the attackers might forced to create unintended location-related conflicts with other vehicles. For that reason, it is reasonable to deploy the overlap detection in a misbehavior detection framework together with a PM and SAS check. Then an attacker cannot arbitrarily position ghost vehicles on the road without provoking inconsistencies with other real vehicles, in particular in

dense road traffic. An attacker that tries to avoid vehicle overlaps might be forced to create position jumps of the ghost vehicle that can be detected by the PM and SAS checks.

Generalizability The proposed mechanism is designed for the application in transportation systems. Therefore, its adaptation for other use cases is probably limited. In the domain of location-related data consistency and plausibility checking this mechanism is generic and fundamental. Compared to related mechanisms for misbehavior detection in VANETs it shows the following advantages. Our mechanism is able to detect inconsistencies of single-hop vehicular neighbors that are not in line of sight. This is not possible for example with mechanisms based on local sensors such as radar or cameras. Furthermore, the overlap detection does not require additional knowledge such as digital road maps or neighborhood tables. The proposed scheme also works independently from traffic situations and movement patterns. Some related mechanisms are designed only for urban or highway traffic [CWHZ09] and others must be trained and updated with specific knowledge [SFH11]. Moreover, no support by roadside infrastructures is required and no specific information need to be exchanged between VANET nodes.

Complexity The complexity of the proposed mechanism in terms of implementation and integration is relatively low. As mentioned in the previous paragraph there are no dependencies on hardware such as local sensors or infrastructure components. The overlap detection works autonomously on VANET nodes and requires only permanently updated location-related information provided by neighbors via CAMs.

We propose in this dissertation a simple vehicle model that is based only on rectangles that describes the occupied area of a vehicle. In future work more complex vehicle models for trucks and buses should be considered in addition in order to allow flexible vehicle structures. While driving through sharp corners or while turning on intersections a long truck may not occupy a road area with a rectangular shape. However, the applied algorithm for overlap checking of two vehicle models supports also more complex polygon structures.

Bandwidth & Connectivity The proposed mechanism is based on received second hand information contained in CAMs. No additional security-related information has to be exchanged in order to detect possible inconsistencies. This is an advantage in contrast to related mechanisms that require for example the periodic exchange of neighborhood tables between VANET nodes. Since only CAMs from the adjacent nodes are processed an attacker can not influence the overlap detection mechanism to its advantage without affecting the mobility of the ghost vehicle.

Privacy In order to create the vehicle model for neighboring nodes it is required to get their accurate position and their rough dimensions. As a consequence it is not necessary to include very accurate vehicle dimension information into CAMs that may allow a distinction between different vehicles. The format of the CAM allows only to insert vehicle dimension matching to a predefined vehicle class. No additional information is required to be inside the CAM format that may weaken the drivers' privacy.

As a conclusion of the evaluation, the proposed mechanism for vehicle overlap-based misbehavior detection can be successfully applied in upcoming VANETs. Most relevant for an practical application is the position accuracy of mobility information provided with CAMs.

3.6. Particle Filter-Based Misbehavior Detection Framework

The concept for mobility data plausibility checks presented in Sections 3.4 and 3.5 is based on different separate modules that perform PV-related tests in combination with local first hand information or received second hand information. Other related approaches also separate tests into modules in order to process different information sources as proposed e. g. in [Ger10, SLS+08, LSK06, YOW08]. These approaches, however, suffer from a complex aggregation of results (cf. Figure 3.4 on page51) and sharing of information with different modules. Additionally the status of the neighbor nodes is redundantly managed within different modules. In order to consider these issues, we present in this section an alternative framework that combines different location information from a broad variety of input sources using only one instance of a particle filter per single-hop neighbor node. This particle filter is used to determine the trustworthiness of the node and allows a search for possible misbehavior as shown in Figure 3.20.

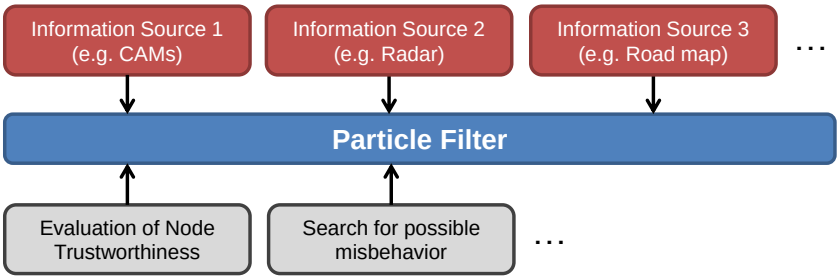


Figure 3.20.: Data source aggregation for plausibility checking with a particle filter

This framework has been elaborated by the author of this dissertation [BMBK12]. Some application details of the particle filter-based misbehavior detection were further elaborated by Sebastian Mauthofer in his Master thesis [MBH12] which was supervised by me. As part of this thesis he also implemented and evaluated the concept under laboratory and real conditions using test vehicles.

In this section it is shown that a probabilistic particle filter [HMdPS05, TBF05] is an appropriate instrument to implement data plausibility and consistency checks for VANETs. Usually Particle filters are used to increase position accuracy of moving devices such as robots [TBF05] or persons equipped with mobile devices [Ebi13]. As far we know this is the first time that a particle filter is applied to verify location-related information in the context of vehicular ad hoc networks. In particular we elaborated in this dissertation the possibilities to assign positive and negative particle weights in order to represent plausible and implausible areas within an observed area. In the following subsections, first the principles of a particle filter are described, followed by the utilization concept to check data plausibility and detect misbehavior. Finally, an evaluation of the concept under laboratory conditions is discussed, and tests with three real vehicles on a test track are described.

3.6.1. The Particle Filter

Particle filters belong to the family of Bayesian filters. In general the algorithm of a particle filter consists of predict/update cycles that are performed repeatedly to estimate the state of a dynamic system [TBF05]. In a first step the filter performs a prediction of a prior system state, where a new believe state is calculated. The second step is the so called measurement update. Here, the predicted believe state is corrected by the use of sensor observations. The basic idea of particle filters is that any probability density function (PDF) can be approximated by a set of samples. With a sufficient amount of samples, the density of samples in a given area represents the probability of that area. With particle filters, each sample is represented by a particle, containing a whole set of state variables. This allows for the sampling of arbitrary density functions and therefore of several complex models.

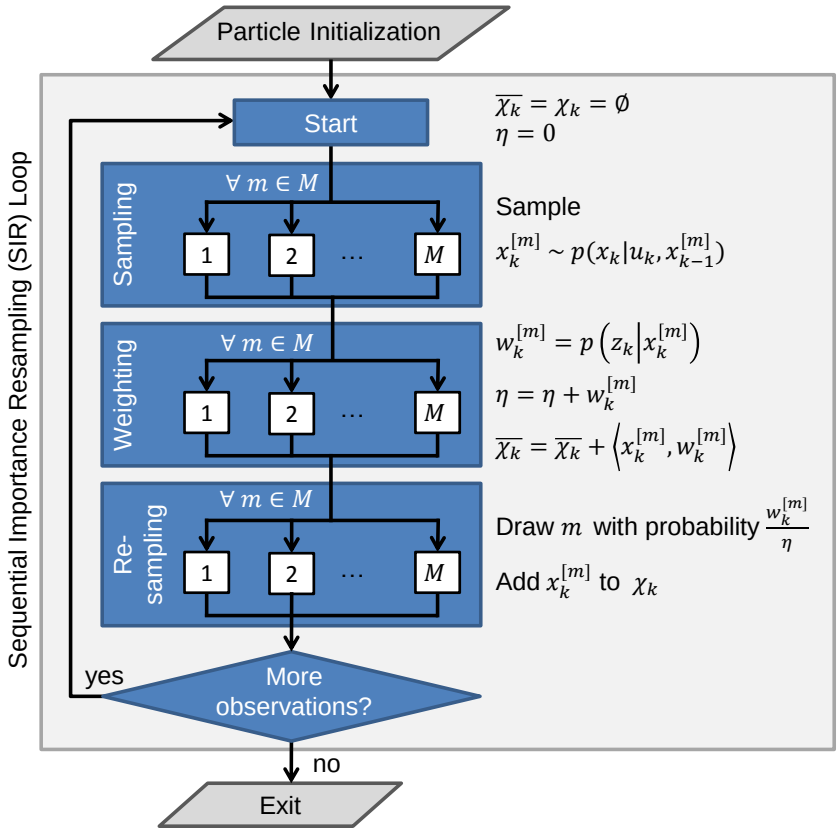


Figure 3.21.: The particle filter algorithm using sequential importance resampling

For the application as mobility data plausibility check it is reasonable to choose a particle filter algorithm that is using the common sequential importance resampling (SIR) approach [TBF05]. Each particle $x_k^{[m]}$ of the filter comes as a instantiation of the system state at a time k and represents a sample of the posterior distribution. χ_k is the particle set at time k containing all particles $x_k^{[m]}$ (with $1 \leq m \leq M$) of that time step where M denotes the total number of particles. A reasonable value for parameter M is evaluated later in this section by using a V2X communication test system. The algorithm depicted in

Figure 3.21 takes a set of particles χ_{k-1} together with the most recent control information u_k to calculate the required state shift of the particles by sampling the state transition distribution with $p(x_k|u_k, x_{k-1})$.

In the weighting step following, the most recent sensor measurement z_k is used as an input for the weighting in which the conditional probability is calculated with $p(z_k|x_k^{[m]})$ for each particle. For normalization purposes, a counter η is used which sums up all particle weights in the SIR loop. After the weighting is done, the particle is added to a new temporary particle set $\overline{\chi_k}$. The most important step of the particle filter algorithm is the *resampling*. The algorithm draws M particles with replacement from the temporary particle set $\overline{\chi_k}$. The probability of drawing a particle corresponds to its normalized particle weight $w_k^{[m]}/\eta$. Finally, the drawn particles are added to the output particle set χ_k. The resulting particle set χ_k is used in the next iteration with $k = k+1$ when the SIR loop is executed again.

3.6.2. Data Fusion and Plausibility Checking with Particle Filters

In order to check the plausibility of mobility data sent by single-hop neighbor nodes the particle filter algorithm performs a fusion of data from several location-related data sources. In this approach, a separate particle filter is used for each tracked vehicle. Particle filters show a high efficiency with respect to tracking purposes and allow the inclusion of both negative and positive weighting factors. However, the VANET scenario differs from typical utilizations of particle filters where a hypothesis is corrected by fully trusted sensor data. In contrast to other usage areas, e. g. the robotics domain, the incoming PV of a tracked vehicle is an essential part of the data z_k that is used to correct the sampling. This received data however can be forged or flawed by an attacker. Consequently, the goal of the tracking is not to identify the most likely position of the vehicle but to determine the plausibility of a stated PV. We elaborated [BMBK12] that the following location data-based verification methods can be applied with one particle filter per node without managing additional information in external modules.

- Tracking of adjacent nodes to verify their movement and detect position jumps of ghost vehicles
- Consideration of local first hand sensor information to confirm or disprove a stated neighbor node position (e. g. information received from radar, lidar, cameras, directional antennas)
- Consideration of local first hand knowledge to confirm or disprove a stated neighbor node position (e. g. information gathered from digital road maps, a sudden appearance area [SLS+08], a maximum communication range [SJB+10])
- Consideration of received second hand information (e. g. overlap detection [BSB10])
- Functions for misbehavior detection support (e. g. consideration of moved distances [SLH09], pseudonym change detection [WKMP10], tracking of own position)

Therefore, the particle filter-based concept comes as an alternative instrument to the module-based concept described in Sections 3.4 and 3.5 for location data-based plausibility checking.

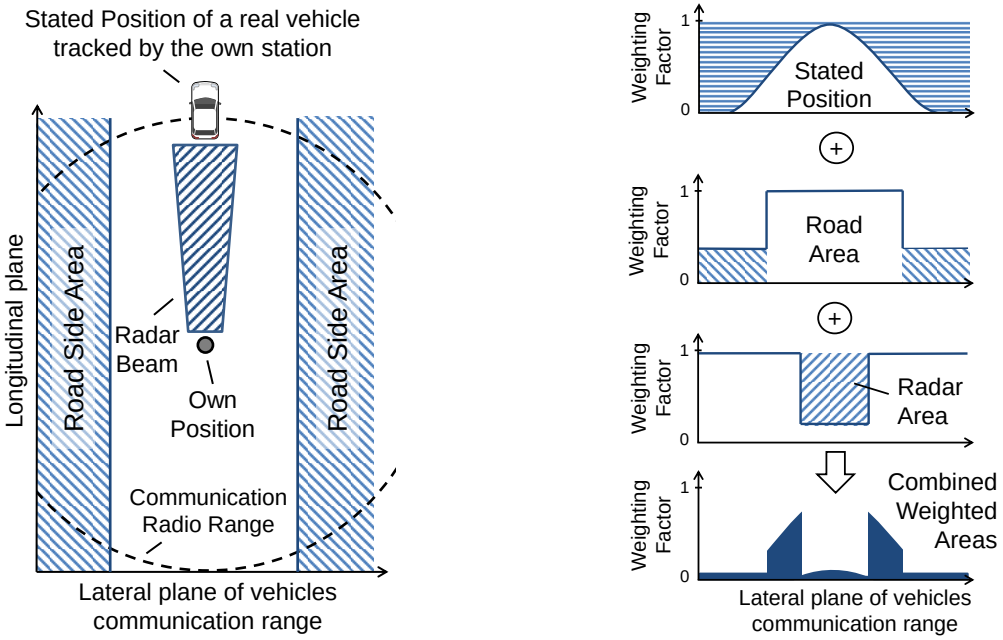
In order to apply the particle filter for mobility data plausibility checking, the sampling step is used to predict the state transition from a previous state to the following state according to the given control information. In this scheme, the state transition function is based on the positional shift between two incoming messages. From the PV of a previous message, the vehicle speed and the heading is derived[2].

[2]The node's gear rate may also be available in V2X messages and could therefore be used to consider direction changes in more detail. However, for the sake of simplicity this approach is not used in this proof of concept.

This vector is multiplied with the time difference between the previous PV and the current PV. Since the positional shift is assumed to be independent from the location of the tracked vehicle, all particles are shifted identically. The actual fusion of the different location-related data sources is performed in the weighting step. This step is dedicated to the correction of the predicted believe state calculated in the sampling step. In order to do so, sensor data is provided to the particle filter to inform about the current state of the environment.

In this misbehavior detection approach, two types of information are provided to the particle filter in order to weight the particles.

The first type of information is the stated position of the tracked neighbor vehicle which is gathered from received V2X messages. Figure 3.22(a) and Figure 3.22(b) depict the same situation from different perspectives. In this scenario a single-hop neighbor node claims to be located in front of the own vehicle. The top view in Figure 3.22(a) shows the own vehicle in the center. The horizontal view from the own vehicle towards the tracked vehicle that is driving ahead is shown in Figure 3.22(b).



(a) Top view

(b) Front of view

Figure 3.22.: Fusion of multiple weight factors with a primary Gaussian distribution

The four stacked diagrams show how separate information sources are combined to a single weighted area. As shown in the topmost layer of Figure 3.22(b) a Gaussian distribution of particle weights is created based on the stated position of the tracked vehicle. Although this information is not reliable, as it might be forged, it represents the claimed state of the tracked vehicle. This position is actually the key information which has to be matched with the predicted current position to identify deviations from the movement pattern. If the stated position does not match at all, there is a high probability that the received message is flawed. In order to weight the particles, the information about the stated position

needs to be mapped onto a PDF as shown in Figure 3.21 and Equation 3.17.

$$w_k^{[m]} = p(z_k|x_k^{[m]}) \tag{3.17}$$

With an increasing distance from the original position, the uncertainty of the stated position is increasing but still a roughly circular shape is generated. The center of the area created by the PDF corresponds to the highest probability. The reduction of probability is approximated by a Gaussian distribution in the evaluated implementation.

The second type of information is local first hand information that is assumed to provide additional reliable knowledge about the environment. This knowledge involves data obtained from local sensors such as radar, environmental databases such as street maps, and general laws of physics, such as communication distances assuming a maximum transmission power. This knowledge is used to reduce the particle weight at implausible locations and raise the particle weight at locations with a high likelihood. In Figure 3.22(a) and Figure 3.22(b), the influence of road side areas and a radar area are shown exemplarily in form of hatched polygons. According to the plausibility model vehicles driving next to the road should be detected as well as vehicles that are located within the radar beam area that is spanned between the own vehicle and another vehicle traveling ahead. Consequently, the weight of particles is reduced that are located inside the road side areas and inside the radar beam area. As a result, particles of a ghost vehicle claiming a position inside the radar beam area are assigned a low weight.

In principle, every information can be used as a weighting factor as long as it can be described as a single polygon or a combination of multiple polygons that represent the knowledge about the environment. In the module-based framework discussed in Section 3.4, each sensor information is processed in a separate plausibility check module. In contrast, the particle filter-based scheme allows to add knowledge and sensor results in a single step. The factor assigned to each polygon area represents the importance of the information.

The process of weighting particles is performed in two steps. First, the bivariate normal distribution of the stated position is used to weight the particles as shown by $p(z_k|x_k^{[m]})$ of Equation 3.18. In the second step, the total of all area factors as expressed by the second factor of Equation 3.18 is applied to increase or decrease the particle weights.

$$w_k^{[m]} = p(z_k|x_k^{[m]}) \cdot \frac{1}{f_1^{[m]} + f_2^{[m]} + ... + f_n^{[m]}} \tag{3.18}$$

If Equation 3.18 is applied the stated position information is dominant in the weighting process. This is required since the next prediction step at time $k+1$ relies on the information included in the message at time k. However, the area factors might have a high influence on the plausibility rating but not necessarily on the correction of a predicted believe state.

The actual core of the concept is to use the normalization factor of the particle filter as a measurement of the plausibility of the stated position and therefore of the content of the received message. The normalization factor, further denoted as Ω, contains the summarized weights of all particles. It is assumed that a high particle weight - which results either from the proximity to the center of the bivariate normal distribution or from a positive area factor - represents a high probability of being in a plausible state. Accordingly, a low particle weight results from high uncertainty that could be caused

by conflicting information. Therefore, a high normalization factor (= high probability of being in a plausible state) is caused by a large number of high-rated particles, and a low factor (= low probability of being in a plausible state) by many low-rated particles - with a smooth transition between the two extremes.

3.6.3. Misbehavior Detection with Particle Filters

As shown in Figure 3.22 different checks can be simply integrated as weighted polygon areas in order to detect misbehavior based on the MCR, SAS, PM, MRP, and RCP check. The particle filter further allows to check whether an object at a given location is matching with the particle cloud of one of the tracked vehicles. This mechanism can be used to test if any of the tracked vehicles is detected by the radar or if a tracked vehicle has performed an ID change. In order to perform this kind of check normally distributed particles at the interested location are added to the particle cloud. For these checks the sampling and resampling steps can be skipped since only the particle weights and the respective normalization factor Ω are needed. The rest of the procedure, e. g. mapping of the normalization factor, is done as usual (cf. Figure 3.21).

Moreover, the particle cloud can also be used to check whether the stated positions of neighboring vehicles overlap as detailed in Section 3.5. For this task, the particle filters are applied in the following way: All particles of the respective filters are mapped onto a two-dimensional grid. In this concept, the size of a grid cell has approximately the size of the involved vehicles, and the cells are partly overlapping each other. Every cell, identified by its x and y coordinate, maintains a separate counter variable $\vartheta_{x,y}$ that is used to detect possible overlaps. For each particle of the filters in question, the closest cells of the grid are searched and the counters $\vartheta_{x,y}$ of the affected cells are incremented. After all particles are assigned, the cells with high values of $\vartheta_{x,y}$ represent vehicle locations. For cells its counter ϑ exceeded the maximum number of particles assigned to a single particle filter indicate an overlap of two or more vehicles.

Finally, an additional particle filter instance can be used to track the own vehicle's position. It is not relevant if imprecise map data, winding roads, or an inaccurate own GNSS information are the cause, the own vehicle should always be able to serve as a reference with respect to plausibility. If the own station is not able to achieve high position accuracy, the whole plausibility check should be paused until the accuracy is sufficiently high.

3.6.4. Evaluation of Plausibility Checking with Particle Filters

The goal of this evaluation is to analyze whether a particle filter can be applied to detect the location-related misbehavior defined in Section 1.2. The paragraphs of this section are structured according to the evaluation criteria defined in Section 3.3. Further, we analyze whether the particle filter provides better properties with respect to extensibility, generalizability, and complexity than a module-based misbehavior detection framework. By means of these criteria a comparison of proposed and related solutions is finally presented in Section 3.7.

Evaluation Setup Similar to the evaluation of the module-based approach, discussed in Section 3.4.4, practical experiments have been performed to analyze the overall applicability of the particle filter framework. After the functionality of the particle filter implementation has been tested recorded vehicles traces have been used in a laboratory setup to calibrate and evaluate the framework. We utilized the same evaluation setup as used for the module-based framework as illustrated in Figure 3.5 on page 53 and described in Section 3.4.4 to enable a comparison of both approaches. Within the performed experiments only the Java OSGi implementation of the module-based misbehavior detection framework has been substituted by a Java OSGi implementation of the particle filter-based framework. However, a long-term evaluation within a large scale FOT has not been performed due to missing opportunities. Instead, dedicated tests has been conducted with several test vehicles. In these real world experiments XML encoded vehicle traces were recorded per vehicle that include all on-board information of the station and all V2X messages that were exchanged in the test runs. These files have been replayed with a trace player that is connected to a CCU and AU device in a laboratory environment to analyze the particle filter-based approach with different configurations. Based on these recored traces and the configuration parameters presented in this section our evaluations can be reproduced and repeated.

In the real world experiments three test vehicles were used on a testing area to perform various test drives including different maneuvers. In all tests one particle filter instance was used for every neighbor vehicle. Each filter contained 1000 particles and used a filter area size of 800×800 meters. The configuration parameters of the particle filter are subsumed in Table 3.6. In contrast to the module-based framework only location-related information can be checked by the particle filter. As a result, the MTD and MBF checks are not performed by the particle filter.

Table 3.6.: Configuration of the particle filter-based plausibility check

Plausibility check	Value	Description
Maximum communication range (MCR)	0.8 km	If the location of a single-hop message claims to be within the MCR then the receiver considers the position vector as plausible.
Suddenly appearing station (SAS)	200 m	Stations that claim to be in a distance below this value are considered to be not plausible.
	15	Number of messages to be received until the sudden appearance area is deactivated.
	50	Weighting factor related to messages that violate the sudden appearance area, cf. Equation 3.18.
Plausible movement (PM)	4	Value for the sigma of the Gaussian kernel applied as PDF which corresponds approximately to a radius of 3 to 6 meters.
Radar conform position (RCP)	100 m	Maximum detection distance supported by the front radar transceiver.
	50	Weighting factor related to messages that violate the radar appearance area, cf. Equation 3.18.

Accuracy For the evaluation of the particle filter-based framework an implementation is tested that comprises the MCR, SAS, PM, and RCP checks. In order to measure both, the false-negative and the

false-positive rates (cf. Table 3.2 on page 45) several manually generated vehicle traces has been used as well as real vehicles traces. The results of the measurements performed in an environment free of attackers show that benign single-hop neighbor nodes are rated trustworthy. Figure 3.23 exemplarily show that no false detections are created by the plausibility checker in normal road traffic conditions even if some messages do not provide absolute accurate mobility data. In contrast to the evaluation of the module-based framework no long-term evaluations of the false-positive rates could be performed. However, several different test drives have been performed and different recorded traces have been used with the trace player setup to ensure that no false detections are created by the particle filter.

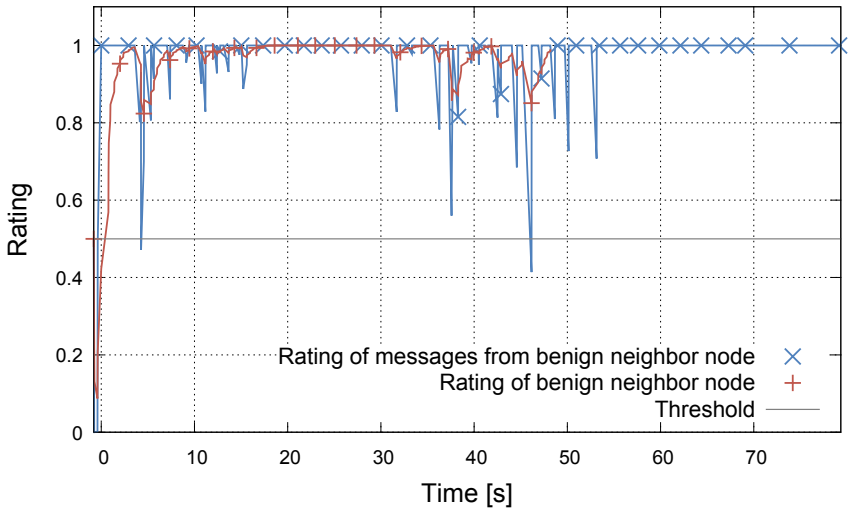


Figure 3.23.: Evaluation of particle filter-based MDS under real conditions using trace without attackers

In order to verify that attacks are correctly detected (cf. true-negative rate according to Table 3.2) with the particle filter-based framework different dedicated tests with respect to the MCR, SAS, PM, and RCP check has been performed with several test vehicles. The results are comparable with the results of the module-based framework with respect to detection rate and detection accuracy. In the following the misbehavior detection related to the radar conform position (RCP) verification is discussed in more detail since this kind of check has not been analyzed with the module-based framework.

The results depicted in Figure 3.25 show a ghost vehicle attack as introduced in Section 2.3.3 and extended in Figure 3.24 under optimal laboratory conditions. In this scenario a tracked ghost vehicle A_1 drives along with a vehicle R that runs the plausibility checker. At the beginning of the test A_1 moves with a constant speed identical to the speed of R, and keeps a constant distance. At time k_1, the tracked ghost vehicle enters the radar area that is spanned between vehicle R and another real vehicle T that is detected by the radar of R. Since it is very unlikely that a real vehicle is located in the radar-monitored area, this area has a weighting factor of 50 configured, which will result in a particle weight reduction of $\frac{1}{50}$ according to Equation 3.18.

As shown in Figure 3.25 the rating of vehicle A_1 increases rapidly after the initialization phase and stays at a high level until the ghost vehicle enters the radar area at time k_1. As expected, the rating of messages suddenly drops to a low value clearly below a defined threshold of 0.5. While the

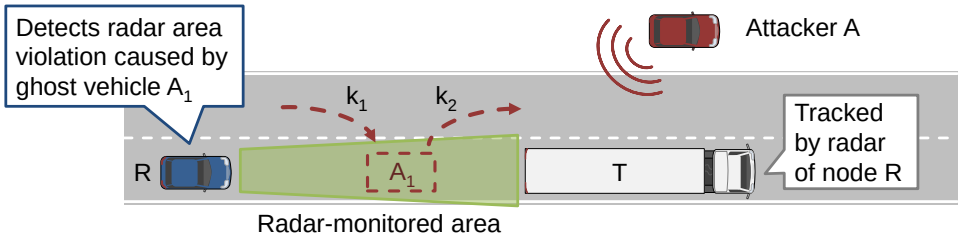


Figure 3.24.: Ghost vehicle A_1 violates the radar area spanned between R and T

ghost vehicle is within the radar-monitored area, the node-based trust value decreases also below this threshold. Shortly after the ghost vehicle has left the radar observed area at time k_2, the message-based

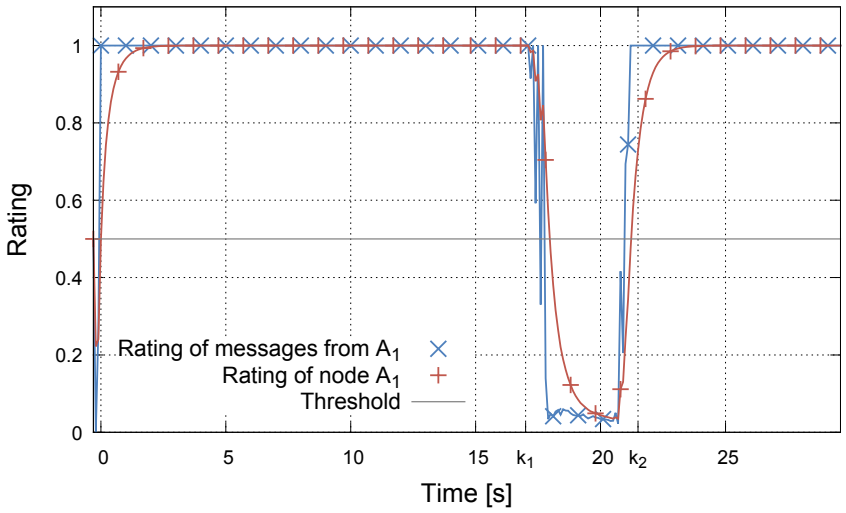


Figure 3.25.: Evaluation of particle filter-based MDS under laboratory conditions using trace with RCP violation

rating reaches a high value again. Figure 3.25 shows that the malicious behavior of ghost vehicle A_1 is clearly detected indicated by the decrease of the node-based rating caused by violation of the radar-monitored area. However, the detection of node-based anomalies should not lead to a permanent local exclusion of the affected node since unexpected situations such as an accident could also be the cause of an detected anomaly. The rating of the node should rather be used to created misbehavior reports that are evaluated by a central entity.

Additional tests performed under real conditions are based on traces recorded on a dedicated test area where several simple maneuvers, e. g. sudden braking and evasion of obstacles, were performed. The test results shown in Figure 3.26 address the impact of the radar object detection analogous to the tests under laboratory conditions. The tracked ghost vehicle A_1 starts a sudden overtaking maneuver and goes into the gap between the vehicle R and a heading vehicle T at time k_1. Afterwards, at time k_2 the ghost vehicle leaves the radar area but stays in communication range and performs some further driving maneuvers.

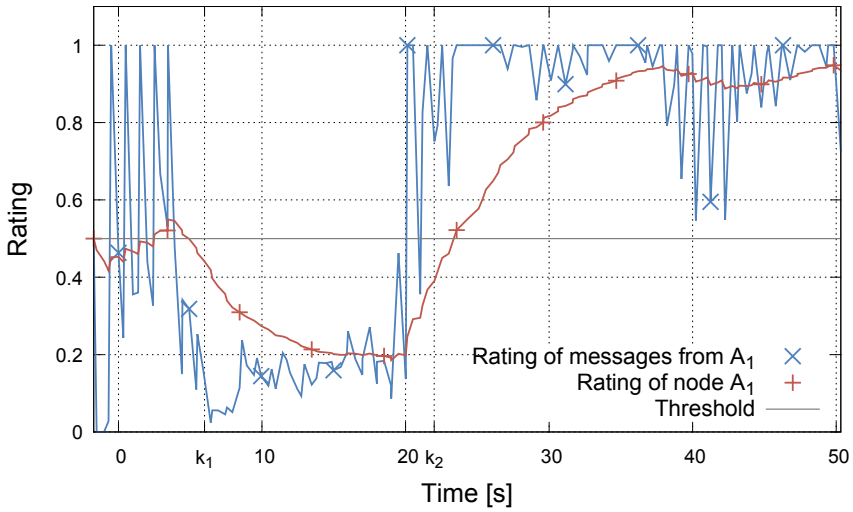


Figure 3.26.: Evaluation of particle filter-based MDS under real conditions using trace with RCP violation

Figure 3.26 shows the decrease of the message- and node-based rating below the threshold at time k_1, which indicates non-plausible behavior of the tracked vehicle A_1. Similar to the test results under laboratory conditions, the node-based trust rating of the A_1 increases as soon as the ghost vehicle leaves the radar area at time k_2. The alternating message trust values in Figure 3.26 are related to the applied Gaussian distribution function. This function is used to check whether a stated position of a tracked vehicle is valid as illustrated in the topmost layer of Figure 3.22(b) on page 78. An analysis of recorded messages from real vehicles has shown that many stated positions are not perfectly matching with this Gaussian bell curve, which results in low message ratings. It is therefore reasonable to adapt the probability distribution function in future prototypical implementations in order to ignore minor position inaccuracies in received V2X messages. However, in spite of alternating message trust values caused by inaccurate position data and insufficiently considered abrupt driving behavior, the expectations are fulfilled since the misbehavior of the ghost vehicle is clearly detected.

The evaluations show that in general both, the module-based and the particle filter-based framework are comparable with respect to misbehavior detection accuracy. The results of tests with real vehicles show that the particle filter algorithm is able to handle movement data that represent typical driving behavior, without producing false detections. At the same time, ghost vehicle attacks are detected as long as they show abnormal behavior according to the aspects defined in Section 1.2. A concluding comparison with other approaches is provided in Section 3.7.

Scalability The performance and therefore the scalability of the particle filter-based framework is directly related to the number of particles contained in the filters. On the other hand, the accuracy also directly depends on the number of particles. An increase of particles leads to a higher accuracy but, otherwise, needs more processing power. We evaluated the optimal number of particles that can be applied per filter to obtain optimal results. Figure 3.27 presents different graphs of a node-based rating that are related to different numbers of particles, starting from 10 particles up to 1000 particles per

filter. For these performance evaluations, the recorded real vehicle traces are reused, cf. rating curve of A_1 shown in Figure 3.26.

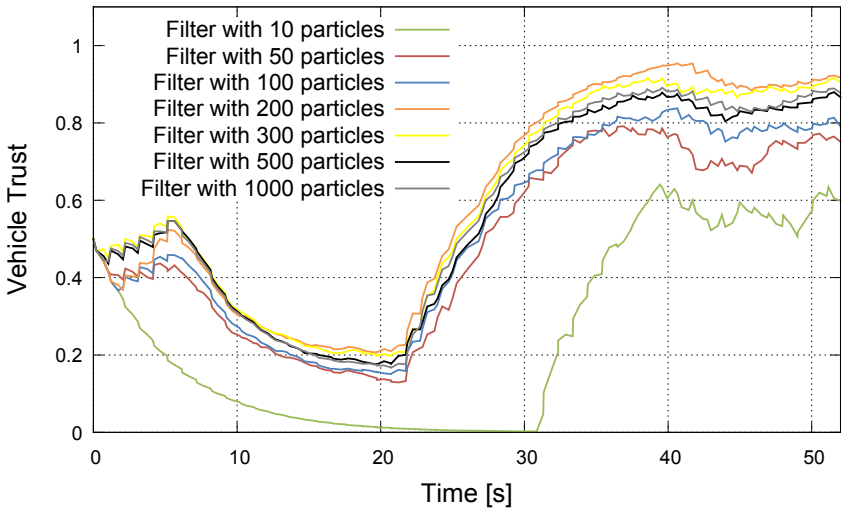


Figure 3.27.: Accuracy of particle filer measurements with different numbers of particles

All particle filters that are related to the graphs depicted in Figure 3.27 with marginal deviations from the reference vehicle trust graph can be assumed to handle appropriate particle numbers. In theory, a particle filter processing more particles produces more precise results. Consequently, the graph representing the particle filter with the highest amount of particles is used as reference that can be computed reliably on the test system. In the test setup the best results can be achieved with particle numbers between 500 and 1000. Filters with more than 2000 particles cannot be processed fast enough due to limited processing power on the tested automotive systems. In Figure 3.28 the deviations between the reference filter with 1000 particles and the filters with less particles are shown. For filter providing less than 300 particles, the results are still usable but cannot be deemed satisfyingly accurate (i. e. showing a mean deviation $\geq 4\%$).

Figure 3.29 shows the performance measurements of the particle filter with varying numbers of particles similar to the accuracy evaluation shown in Figure 3.27. Since the complexity of particle filters is $O(M)$, an increase of the number of particles M causes a linear increase of computational effort. This might be a problem in resource restricted environments. For practical application we propose to utilize between 100 and 500 particles per filter. When only 100 particles are used per particle filter, it is possible to handle up to 200 incoming messages per second, but using around 500 particles per filter, approximately 40 messages can only be processed. Consequently, the particle filter algorithm may be adapted to incoming message rates and only relevant neighbors may be tracked.

In comparison with a other probabilistic filters (e. g. the Kalman filter see Section 3.4) the particle filter can process in a single weighting step information from different information sources. The computational overhead caused by the number of different information sources is negligible with respect to the total order $O(M)$ of the particle filter-based plausibility check. As a result, the particle filter is a good choice if several different information sources have to be considered in order to detect mis-

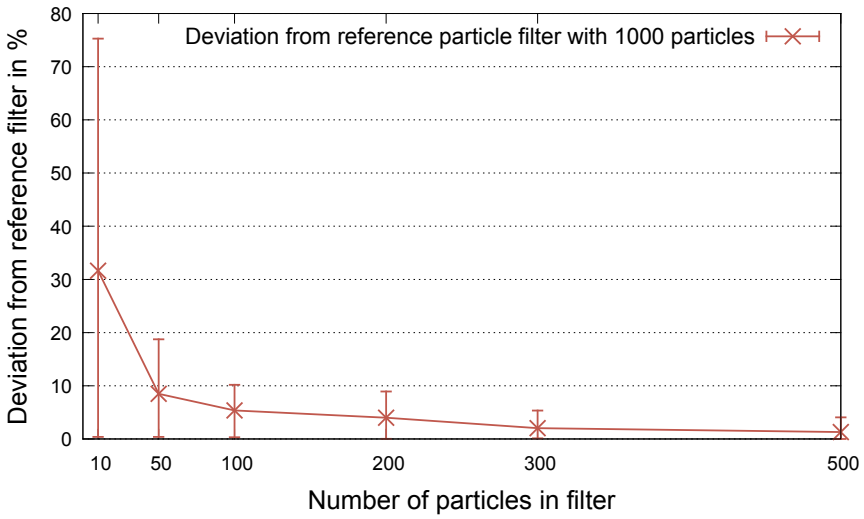


Figure 3.28.: Prediction deviations between a reference filter with 1000 particles and filters with less particles

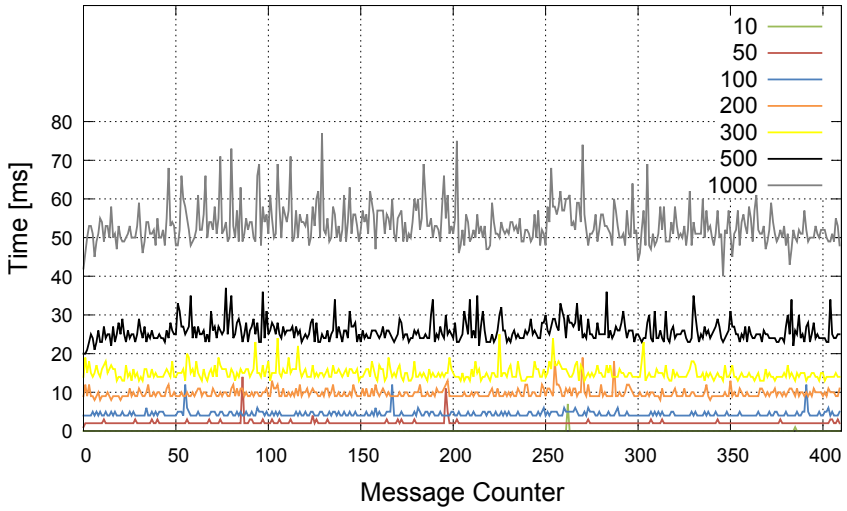


Figure 3.29.: Runtimes of the particle filer algorithm in dependence of particles numbers

behavior in V2X communications. For the sake of complexity and effort, the tested proof of concept implementation has not used enough information sources to outperform the module-based framework that is implemented with a Kalman filter.

Extensibility A particle filter is able to integrate different location-related information in order to increase the quality of the probabilistic state modeling and estimation. The information of the sources are considered by the particle filter using Equation 3.18 in order to influence the weights of the single particles. The extensibility of the particle filter is however limited to sources that provide location-related information. In particular, it is necessary that replayed messages are dropped before the location data

of an associated V2X message is processed by the particle filter. Additionally, the beacon frequency of observed neighbors cannot be verified with the particle filter concept. Therefore it is necessary to perform some basic checks before the location-related checks are performed by the particle filter.

Generalizability The generalizability of the particle filter concept with respect to misbehavior detection is high. In general, particle filters support non-linear state propagation functions and non-Gaussian noise. There is no limitation to the probability density function that is applied in a particle filter. In addition several different PDFs can be applied at the same time for different information sources. This property makes the particle filter to an adequate instrument for location data plausibility and consistency checking.

There are proposals to apply particle filters in the domain of mobile ad hoc networks to track persons that are equipped with wireless transceivers [Ebi13]. Moreover, the particle filter-based framework could be extended by other kinds of information, for example light, moisture, temperature or pressure, to support misbehavior and fault detection in wireless sensor networks.

Complexity In order to analyze the complexity related to the integration of information sources that may have mutual dependencies with other aspects of local-related information we performed several experiments with a radar sensor. In Figure 3.4 on page 51 the dependency of a RCP test on a probabilistic vehicle tracker is shown. The position of the tracked vehicle must be synchronized with the radar sensor in order to rate the location plausibility. When applying a particle filter it is not necessary to specify each single dependency between different aspects of location-related plausibility since the weight of the particles is automatically influenced by all existing information sources. For example, if a neighbor vehicle claims to be located within an area that conflicts with measurements of a local radar then the affected particles are assigned with low weights and consequently are drawn in the resampling state with low probability, cf. Section 3.6.2. Additional information sources with mutual dependencies are for example digital maps, differential antennas, or second hand location information used to detect vehicle overlaps. In the module-based framework the sequence of checks might be relevant. Since the particle filter framework include all information into one weighting process some dependency questions become obsolete.

Our experiments and related evaluations have shown that the integration of information sources with mutual dependencies is simple. This simplicity is in particular important to avoid vulnerabilities and faulty implementations.

Bandwidth & Connectivity In the same way as specified for the module-based approach the particle filter-based framework is designed to work autonomously on the nodes of the VANET. The exchange of information related to misbehavior detection via ITS-G5 with neighbors is not considered. A misbehavior report generation that is using the particle filter might need, however, capabilities to communicate sometimes with the infrastructure.

Privacy Personal or identifying information related to the driver of a vehicle is not processed by the particle filter-based approach. Similar to the module-based framework the application of pseudo-

nymous IDs is anticipated. However, the tracking of the nodes allows the detection of ID changes and therefore the linking of different IDs. In order to protect the privacy of drivers this linking information must not be shared with other VANET neighbors or external entities.

3.7. Comparison of Local Misbehavior Detection Approaches

In this section we summarize the comparison of the module-based framework with the particle filter-based framework, cf. Sections 3.4 and 3.6, respectively. Moreover, we compare our approaches with VEBAS, proposed by Schmidt et al. [SLS+08], the observer-based scheme proposed by Gerlach [Ger10] and a purely centralized approach. The later schemes are aiming to process random V2X messages that are reported by nodes of the VANET whereas the nodes do not evaluate the suspects beforehand. This comparison is based on the criteria defined in Section 3.3 and uses the four simple rating values: -- (very poor), - (poor), + (good), and ++ (excellent). The double minus and the double plus indicates a very negative or very positive rating, respectively. The single minus indicates that some requirements are unfulfilled or unsatisfactorily considered. The single plus indicates that most requirements are considered. Table 3.7 lists the ratings associated to the different approaches and subsumes the most relevant positive and negative aspects.

The accuracy of the module-based and particle filter-based frameworks is comparable with both, VEBAS and the observer-based approach. In all four cases the detection mechanisms can be configured and extended in order to provide a high detection rate and a low false-positive detection rate as long as benign vehicles provide accurate position information. However, Gerlach propose to apply RSSI that is prone to false and inaccurate detections [Ger10, Section 5.5.2]. The accuracy of a pure centralized approach is not sufficient if only reports containing inconsistent V2X messages are provided to a central misbehavior detection authority. Since VANET nodes can gather a large set of information about neighbors based on V2X messages and context information the local misbehavior detection can work more accurate. Furthermore, some misbehavior can only be detected if local first hand information can be accessed that is exclusively known by VANET nodes, cf. MBF, SAS, RCP.

With respect to scalability and performance the module-based framework shows better results than the particle filter-based approach. By comparing the performance of vehicle tracking in both approaches, at the first glance the Kalman filter seems to be more efficient than the particle filter. With increasing number of information sources and location-related plausibility checks the particle filter becomes more interesting since the particle processing step is executed only once regardless of the number of data sources and checks. Even if no performance numbers are available for the related works [SLS+08, Ger10], it can be assumed that VEBAS and the observer-based approach show similar performance values as the module-based approach. A purley centralized approach, however, has to process large data amounts which might cause problems with an increasing number of reporting VANET nodes.

The extensibility of a central mechanisms can be assumed to be better than solutions that are distributed on network nodes because a remote update might not be supported by most vehicles. However, in general all proposed schemes can be extended by additional mechanisms in order to detect location-related misbehavior that is unknown today.

Table 3.7.: Comparison of local misbehavior detection approaches

Approach	Pros	Cons	Accuracy	Scalability	Extensibility	Generalizability	Complexity	Bandwidth	Privacy
Module-based framework	High detection accuracy with specialized modules; Extensible with specialized modules; No exchange of additional data between VANET nodes; No permanent connection to central infrastructure required	Specialized modules responsible for specific tasks; Dependability of modules increase complexity of module-based framework.	++	+	+	--	-	+	+
Particle filter-based framework	High detection accuracy due to flexible PDF; Generalizable to be applied in other domains; Reduced complexity due to direct integration of information from different sources into particle cloud; No exchange of additional data between VANET nodes; No permanent connection to central infrastructure required	High computational performance requirements; Only location-related consistency or plausibility tests can be integrated that can be realized with particles	++	-	+	++	+	+	+
VEBAS [SLS+08]	High detection accuracy assumed since comparable with module-based approach; Extensible with specialized modules	No evaluation results published; Additional data exchange between VANET nodes	++	+	+	--	-	-	-

Approach	Pros	Cons	Accuracy	Scalability	Extensibility	Generalizability	Complexity	Bandwidth	Privacy
Observer-based approach by Gerlach [Ger10]	Extensible with specialized modules; Concept of Bayesian Networks can be used in other domains	Multiple processing of same data; Received signal strength observer prone to false-positive detections; Additional data exchange between VANET nodes	+	+	+	+	-	-	-
Purely centralized approach	Generation of long-term node reputation	Decreasing accuracy of misbehavior detection with less information gathered; Handling of large amounts of data at central infrastructure; High requirements regarding connectivity between VANET nodes and central infrastructure	--	-	++	+	-	-	--

Considering the generalizability, the particle filter can be easily adopted to other kinds of misbehavior detection in VANETs and also to other domains of computer networks. Since the observer-based solution is based on Bayesian networks the generalizability can also be assumed to be high.

The complexity of most approaches is rather high since dependencies and interoperability between different components have to be considered in the module-based approach, the observer-based approach, VEBAS and the centralized approach. The particle filter solves this problem in an elegant way. Since the location-plausibility of neighbor nodes is represented by a cloud of particles local first hand information and received second hand information can be integrated into this particle cloud. As a result, the rating of the neighbors' location is automatically influenced by the integrated information.

With respect to communication bandwidth and connectivity the module-based approach and the particle filter-based approach are rated positive since no additional data associated to misbehavior detection is transmitted via the ITS-G5 communication link. The authors of VEBAS and the observer-based approach propose to exchange information between VANET neighbors that is related to misbehavior detection. Due to the same reason the pure centralized approach is rated negative. If no filtering of possible misbehavior is performed on the local nodes then possibly high amounts of data has to be transmitted between the network nodes and the central entity. This may require in addition a constant communication link between the network nodes and the infrastructure.

In order to protect the privacy of drivers the module-based framework and the particle-filter based framework are rated positively because information that may simplify the vehicle tracking is not exchanged between neighboring nodes. VEBAS and the observer-based approach are rated negatively because they consider the exchange of neighborhood tables. However, local misbehavior detection mechanisms applied on VANET nodes can protect the driver's privacy better than purely centralized frameworks.

3.8. Limitations of Local Misbehavior Detection and Further Challenges

The local detection of anomalies is naturally limited with respect to the detection of misbehavior and attacks. According to our research results there is no difference between valid and expected anomalies such as a traffic accident and maliciously created anomalies introduced in Section 1.2. For example, two vehicles that collide on the road distribute mobility data via CAMs that may violate the boundary of regular negative acceleration and may cause vehicle overlap detections. In this case, the involved nodes must not be considered as attackers and must not be excluded from V2X communications.

A local misbehavior detection running of VANET nodes is consequently not able to distinguish in any case between valid expected anomalies and anomalies caused by maliciously generated ghost vehicles. A pure local misbehavior detection solution can therefore only detect the abnormal situation and related events but cannot reliably decide if the anomaly is caused due to an attack. This aspect is further analyzed in more detail in Chapter 4.

Additionally, the following aspects have to be considered that complicate data consistency and plausibility checking in general.

- **Synchronization**: Information from different sources in a multisensor environment might be received at different times, intervals and arbitrary orders. The fusion of information that are received with some delays is first named by Bar-Shalom [BS02] as *out-of-sequence measurements (OOSM)*. The problem of multisensor target tracking systems receiving out-of-sequence measurements is discussed in detail by Zhang and Bar-Shalom [ZBS12a]. They argue that the fusion of OOSM is not trivial and with respect to the particle filter they showed that optimal solutions have high performance effort [ZBS12b]. Sensor measurements provided by local sensors such as the GNSS position or a radar object detection need to be synchronized with the PV that is extracted from received V2X messages. With the tracking functionalities of the Kalman filter or the particle filter it is possible to calculate an accurate PV of the past and predict a PV of the near future. Synchronized mobility data are also required by the vehicle overlap detection.
- **Inaccuracy**: Broadcasted mobility data contain usually inaccuracies since the GNSS suffer from measurement inaccuracies of about 3 to 5 meters even if mechanisms for error reduction are applied, e. g. map-based positioning, dead reckoning and differential GNSS.

  Additionally, some constants in the CAMs such as the dimensions of a vehicle are inaccurate as only values can be used that are related to predefined classes. This is required to make vehicles to a great extend undistinguishable from other vehicles in the VANET and therefore to protect the privacy of the drivers.

- **Scalability**: Both theoretical situation analysis and simulations have shown that incoming packet rates of approximately 1000 packets per second can be expected [SBK+11] when wireless V2X channels are used that base on ITS-G5 [ETS10b] using IEEE 802.11p [IEE10]. If more than approximately 1000 packets are sent over one channel the number of packet collisions increases dramatically. However, for traffic safety and efficiency applications only a subset of neighbors may be relevant, e. g. only vehicles driving ahead in a similar direction. As a possible solution, a relevance filter can be applied that decides which neighbors have to be checked and observed.
  In order to minimize the performance requirements for misbehavior detection, a predefined execution interval of plausibility checks is reasonable. Alternatively, the execution might be done upon receipt of a new V2X message.
- **Bandwidth and connectivity limitations**: Since the wireless ITS-G5 control channel must only be used to transmit traffic safety related data, plausibility checks and misbehavior detection mechanisms should be able to work autonomously on the nodes. Additionally, constant or even sporadic connections to back-end services of the infrastructure cannot be assumed.
- **Privacy**: In order to protect drivers' privacy, identifiers of vehicles are changed frequently and unexpectedly. An attacker could misuse this feature to hide its malicious behavior when the identifier of the attacker vehicle is changed directly after an attack. Even if vehicle trackers are applied to detect the ID change of neighboring nodes, cf. Section 4.2 and related works of Wiedersheim et al. [WKMP10], an attacker could stop broadcasting messages before changing to another ID. This behavior would prevent others to be able to link different IDs owned by the attacker.

In the evaluations of the proposed module-based framework (Section 3.4) and the particle filter-based framework (Section 3.6) as well as the newly proposed vehicle overlap check (Sections 3.5) all these VANET-specific requirements are considered.

3.9. Summary and Conclusion

Within this chapter we depicted that location-based misbehavior can be reliably and autonomously detected by single-hop neighbor node applying consistency and plausibility checks of received mobility data. We proposed a categorization of plausibility checks that separates message-based checks from node-based checks (cf. Section 3.2).

Based on this categorization we developed a module-based misbehavior detection framework that applies these checks in separate modules. The message-based verification of correct value ranges, mobility data consistency, maximum communication range, and maximum transmission delay can be used to filter messages with erroneous content. The evaluations of the corresponding plausibility checks based on long-term outdoor tests have shown that the majority of false-positive detections are caused by single-hop messages that exceeded the maximum communication range or the maximum transmission delay. However, the node-based checks should not result in the discarding of affected messages since implausibilities could be caused by possible dangerous road traffic situations that may lead to the transmission of abnormal mobility information. The respective messages could be very important for the traffic safety applications to show appropriate reaction, e. g. through warning the driver. The

evaluations of the node-based plausibility checks based on outdoor tests show that suddenly appearing stations, vehicle overlaps and implausible movements of attacker nodes are detected.

Further, we developed a new kind of node-based location data consistency check that is based on received second hand information (cf. Section Section 3.5). Based on accurate position information the consistency check is able to reliably detect anomalies created by attackers. Compared to related mechanisms no additional information exchange with neighbor nodes is required.

Finally, we propose a particle filter-based framework in Section 3.6 that aims at integrating different information sources to perform both plausibility checks and misbehavior detection. In this approach one single particle filter instance is maintained per neighbor node in order to combine all relevant local first hand information and received second hand information. In contrast to the module-based schemes, sharing of the same information among different modules is avoided as well as the multiple management of a neighbor node's state in different modules. Moreover, a complex aggregation of module results is avoided. The detection of misbehavior and consequently an evaluation of node trustworthiness is possible by accessing the particle filter. Finally, the evaluation of the particle filter-based misbehavior detection scheme has been performed in dedicated tests under laboratory and real conditions. The results show that attacks are reliably recognized and that false-positive detections are avoided.

Own proposals and related concepts are compared in Section 3.7 based on seven evaluation criteria that are introduced and reasoned in Section 3.3. This comparison estimates that our module-based approach is comparable with the VEBAS concept proposed by Schmidt et al. [SLS+08] and the observer-based concept proposed by Gerlach [Ger10] with respect to most criteria. In contrast, our particle filter-based framework shows better properties with respect to generalizability and complexity than related proposals. However, the scalability of the particle filter is rated worse due to higher computation effort. Most comparisons are based on estimations since detailed evaluations of related work is missing. Compared to purely centralized mechanisms our proposals outperform them in mostly all categories.

As discussed in Section 3.8 the local autonomous detection of misbehavior on VANET nodes allow only a short-term identification of attackers with possibly low confidence. Details related to the location identification of attackers are further analyzed in Chapter 4. In order to identify attackers with high confidence and to allow a permanent exclusion of these affected nodes we propose in Chapter 5 the central evaluation of reported misbehavior.

Part III.

Attacker Identification

4. Local Short-term Identification of Potential Attackers

In addition to the detection of abnormal activities caused by attackers or faulty nodes the responsible nodes have to be identified in order to allow reactions on misbehavior events. As discussed in Part II of this dissertation misbehavior detection frameworks operated on VANET nodes detect the malicious activities of attackers. In this part mechanisms for both short-term and long-term identification of responsible attackers are proposed. Based on these mechanisms malicious and faulty nodes can be excluded from the active participation in VANET communications.

In Section 4.1 related work is analyzed that aims for local identification and exclusion of attackers in the context of wireless V2X communications. Subsequently, in Section 4.2 privacy enhancing technologies (PETs) are discussed and how they may complicate local attacker identification. The impact of the PETs on misbehavior detection and evaluation is analyzed in an example scenario using several test vehicles over a long period of time. Based on the results of the mobility data plausibility checks discussed in Chapter 3, the message and node trustworthiness can be assessed as presented in Section 4.3. Finally, Section 4.4 analyzes afterwards the applicability of local misbehavior evaluation mechanisms with respect to the local exclusion of attackers and faulty nodes.

4.1. Related Work

Both local identification of attackers and local reaction on attacks are discussed in different publications. Gosh et al. [GVKG09] identified that a local eviction of malicious and faulty nodes is desirable to minimize the time to detect, report, and exclude responsible nodes. However, more important than the time of exclusion is the accuracy of the doubtless identification of responsible nodes in order to minimize the false-positive and false-negative rates. In Section 4.1.1 related work is discussed that aim for the local identification of attackers by solely exchanging information between local VANET neighbors. In most cases a trust value is calculated for the neighbors in order to distinguish benign and misbehaving nodes. Related work regarding the evaluation of trustworthiness is discussed in Section 4.1.2. Finally, in Section 4.1.3 related work is discussed that aim for the local exclusion of attackers.

4.1.1. Local Identification of Attackers

Basically, the identification of attacks can be done event-based or node-centric. The authors of [DLJZ10, GVKG09, ODS07] focus on the identification of false traffic events such as fake post crash notifications [GVKG09] or fake local danger warnings [ODS07]. In these proposals, the consistency of reported event information is considered instead of the behavior of involved nodes. However, for this

event-centric attack identification, specific knowledge of the affected application is needed. Consequently, the node-centric identification of attacks is more universal since detection results reported by different applications can be aggregated. Related approaches for the node-centric attacker identification are discussed in the following.

Leinmüller et al. [LHSW04] and Crescenzo et al. [CLPZ10] propose a local evaluation architecture that is based on data plausibility checks to determine which neighbor is possibly attacking the network by maliciously sending false data. In order to identify the generator of Sybil nodes, the authors of [GGS04] and [XYG06] analyze the radio characteristics for a position verification. In these proposals, information about locally detected attackers is not shared with other neighbors. In contrast, Schmidt et al. [SLS+08] propose a framework that distributes local detections to neighbors and consequently considers recommendations from others. Similarly, the publications of Park et al. [PATZ09], Chen et al. [CWHZ09], and Zhou et al. [ZCNC07] rely on information sent by trusted RSUs in order to identify Sybil nodes.

4.1.2. Local Evaluation of Node Trustworthiness

Based on the observation of the neighbor nodes' behavior, the receivers of single-hop V2X messages are able to evaluate autonomously the trustworthiness of others. However, basic trustworthiness of VANET nodes is derived from the cryptographic verification of message signatures and certificates that are issued by a trusted PKI. Most related proposals distinguish between entity (node-based) trust and data (message-based) trust. Zhang [Zha11] provides a survey that analyzes relevant approaches for trust management in VANETs. According to this survey most trust management approaches use entity trust (also referred to as *reputation*) as a basis for trustworthy wireless VANET communications. In Sections 4.1.2.1 and 4.1.2.2 basics of state-of-the-art trust models are discussed as well as related implementations.

4.1.2.1. Trust Models

We focus on models that are related to the context of automated trust generation by machines. Trust models that are based on recommendations, rankings or ratings of human users in online environments such as commercial platforms or social networks are not considered. Furthermore, we focus on the application of direct evidence generated locally. Second hand recommendations provided by VANET neighbors are not considered. As discussed in Section 3.2.5 the exchange of second hand information does not provide much benefit but burdens the bandwidth-limited ad hoc communication channels.

Probabilistic Models Most relevant probabilistic trust models are Bayesian or reputation models as proposed by Jøsang et al. [JI02] and Buchegger at al. [BB04]. In the following the basis of Bayesian trust models is introduced [TBF05]. The Bayesian fundamentals are also used in general in Sections 3.4 and 3.6 to calculate the location plausibility using the Kalman filter and the particle filter, respectively. The Bayes' theorem, cf. Equation 4.1, can be used to calculate the probability of a belief based on a

measurement Y. The outcome can be used as probabilistic trust value with the range [0,1].

$$P(X|Y) = \frac{P(Y|X)P(X)}{P(Y)} = \frac{P(Y|X)P(X)}{\sum_{X'} P(Y|X')P(X')} \tag{4.1}$$

If X should be inferred from a measurement Y then the probability $P(X)$ is referred to as *prior probability distribution*. The probability $P(X|Y)$ is called the *posterior probability distribution*. As shown in Equation 4.1 the posterior $P(X|Y)$ can be computed using the "inverse" condition probability $P(Y|X)$ together with the prior probability $P(X)$.

Beta Distribution The beta distribution is a probabilistic distribution of a random variable $0 \leq p \leq 1$ over [0,1]. Jøsang et al. [JI02] propose its application in reputation systems. The posteriori probabilities of binary events can be represented as beta distributions using the probability density function Γ with two parameters $\alpha > 0$ and $\beta > 0$.

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \tag{4.2}$$

In addition, the following restrictions have to be considered in Equation 4.2: $p \neq 0$ if $\alpha < 1$ and $p \neq 1$ if $\beta < 1$. The outcomes of a misbehavior detection mechanism that is further denoted as *rating* can be represented as r denoting the observed number of positive evidences and s being the number of negative evidences. If no prior knowledge is available the beta distribution function is initialized with $f(p|1,1)$ according to Buchegger at al. [BB04]. As soon as ratings in form of r and s are available they are integrated in the beta distribution function as $\alpha := \alpha + r$ and $\beta := \beta + s$.

The probability expectation value of the beta distribution is given by Equation 4.3 according to [JI02] and the standard deviation is given by Equation 4.4.

$$E(p) = \frac{\alpha}{\alpha+\beta} \tag{4.3}$$

$$\sigma = \sqrt{\frac{\alpha\beta}{(\alpha+\beta+1)(\alpha+\beta)^2}} \tag{4.4}$$

The advantage of this expectation function is that rating information are continuously included into the model. It is in particular not necessary to store the rating information per processed event per node. Only the aggregated values α and β have to be managed per node. However, this function needs to be extended by a weighting mechanism to consider the recentness of rating information. If this would not be done new ratings become less important over time the more ratings are aggregated. The required mechanism is denoted as *aging* in related literature [BB04, Ebi13, Rie09]. Buchegger at al. [BB04] propose to integrate a static weight u as a discount factor for past experiences. They propose a modified Bayesian update approach as shown in Equation 4.5.

$$\begin{aligned} \alpha &:= u\alpha + r \\ \beta &:= u\beta + (1-r) \end{aligned} \tag{4.5}$$

In order to select the appropriate aging value Buchegger et al. propose to use an integer m that is used to define u as shown in Equation 4.6.

$$u = 1 - \frac{1}{m} \tag{4.6}$$

The magnitude m defines the number of new ratings that are required to assume stationary behavior. In addition, the aging factor ensures that the values of α and β will store finite numbers with respect to the rating values r.

Subjective Logic The subjective logic, proposed by Jøsang [Jøs01], allows to combine elements of the Bayesian probability theory (evidence) with elements of the belief theory. This approach is based on an opinion space o that consists of three parameters $b(x) \in [0,1]$, $d(x) \in [0,1]$, and $u(x) \in [0,1]$ representing the belief, disbelief, and uncertainty. The three coordinates of an opinion are depended by the function $b(x) + d(x) + u(x) = 1$ so that one element is redundant. In Figure 4.1 a graphical illustration shows the interrelation of these three parameters as an equal-sided triangle. As an example, the opinion $\omega_x = (0.4, 0.1, 0.5)$ is illustrated.

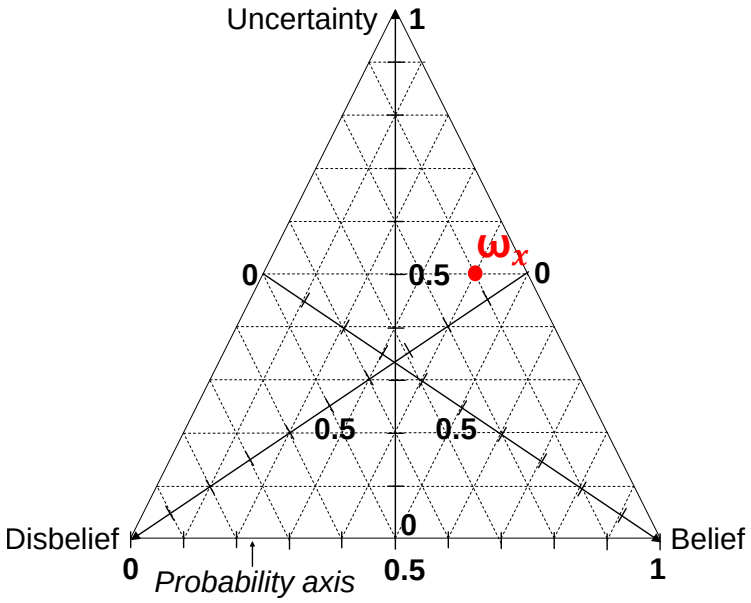


Figure 4.1.: Simplified illustration of the subject logic opinion triangle proposed by Jøsang [Jøs01]

The subjective logic can be used as basis for probability density functions such as the beta distribution. Jøsang [Jøs01] provides also mapping functions between the evidence space used in the beta distribution and the opinion space used in the subjective logic. As a consequence values can be transfered between both models. The opinion space is related to the uncertainty that an observer has about the evidence. In order to complete the model, Jøsang [Jøs01] proposes also methods to aggregate opinions and to integrate discounting functions.

4.1.2.2. Related Implementations of Systems for Node Evaluation

In order to apply node reputation for misbehavior detection probabilistic systems are useful that apply a two-value pair to distinguish *trust* and *certainty* [EB09,Ger07a,Rie07]. According to Gerlach [Ger07a] the reputation of nodes can be classified reflecting untrusted nodes, marginally trusted nodes, and completely trusted nodes. By calculating the entropy of the trust, a certainty value is allocated to the respective trust value. High entropy represents a high level of uncertainty and hence low trust in the node. Low entropy, on the other hand, results in high trust.

Mármol et al. present in [MP12] a *trust and reputation infrastructure-based proposal* (TRIP) which computes a reputation score based on both recommendations and self-estimated reputations. In TRIP every node locally computes a reputation value for all neighbors and maintains a comprehensive reputation table over a long period of time. The reputations are further shared with local neighbors and with a central infrastructure.

Both the *vehicle ad hoc network reputation system* (VARS) [DFM05] and the *vehicular security through reputation and plausibility* check (VSRP) [DOJ+10] scheme use neighbor reputation values that are built on local observations. VARS proposes the piggybacking of reputation opinions to allow for confidence decisions at neighboring nodes upon the reception of event messages. The VSRP scheme on the contrary allow for actively requesting reputation information when messages from unknown nodes are received.

4.1.3. Local Exclusion of Attackers

According to Liu et al. [LCH10] related approaches for attacker exclusion in VANETs can be classified into two categories: local and global eviction. In this chapter only mechanisms for local attacker eviction are discussed. The global attacker exclusion is considered in chapter 5. The authors of [MRC+08,RPA+07,RMFH08,YOW08] argue that the local eviction of attackers is possible without a central control system. In this context, the following general approaches are considered [RMFH08]: *abstain*, *voting*, and *self-sacrifice*.

If a node ignores the node eviction information sent by neighbors (*abstain*), it fully relies on its own local misbehavior detections to identify attackers and to ignore messages sent by these nodes. Yan et al. [YOW08] propose the local isolation of malicious nodes by allocating all neighbors to groups named: *trust*, *question*, and *distrust*. In their scheme, communication is generally granted with nodes of the groups *trust* and *question* whereby fully trusted nodes are preferred communication partners. The communication with nodes of the group *distrust* is not allowed.

By applying a *voting* protocol, a node informs its neighbors about potential attackers that should not be considered as trustworthy. The LEAVE (local eviction of attackers by voting evaluators) protocol proposed by Raya et al. [RPA+07] is used to periodically broadcast identities of nodes that have been locally tagged as misbehaving. Assuming both a majority of honest reporters and reliable local misbehavior detection, nodes identified as attackers are temporarily ignored by nodes that use LEAVE. Cao et al. [CKL+08] further propose a collection of event-based votes that inform about the trustworthiness of events. If a consensus is reached, then the related event is assumed to be true.

The protocol named *Stinger* is based on the mechanism of *self-sacrifice* that considers in particular the discrediting attack in contrast to the voting schemes [MRC+08]. Applying this protocol, a node S that accuses another node R to be an attacker in turn has to sacrifice its own reputation. Consequently, the certificate and the corresponding identities of node S and node R are both temporarily evicted from the VANET. This self-sacrifice mechanism should prevent that attackers are able to discredit benign nodes.

4.1.4. Evaluation of Related Work

We focus in this dissertation on trust models as introduced in Section 4.1.2.1 that consider machine associated trust values that are generated by machines. Probabilistic Bayesian models base on well defined mathematics and are applied in several domains. Both, the beta distribution and the subjective logic base on these probabilistic model and provide possibilities to express the uncertainty of trust values. As a consequence, these approaches are relevant for the local node trust evaluation in VANETs. We focus in this dissertation on the beta distribution since it works with a two value pair. However, if required a translation between the beta distribution model and the subjective model is possible.

Regardless of the approaches for local node exclusion discussed in Section 4.1.3, the authors of [LCH10] argue that a local eviction of attackers requires a reliable detection of misbehavior by honest nodes, which may not be possible in most situations. In particular, the simultaneous use of two or more certificates is identified as a potential weakness in both the *voting* and the *self-sacrifice* mechanism. Another critical aspect, as identified in [LCH10], is the circumstance that some honest nodes may not be able to vote as they are not equipped with appropriate detection devices such as a radar transceiver or do not perform the required plausibility checks. However, if available, such devices or mechanisms may have a limited range of influence. The temporary local exclusion of attackers as presented in related work is not a satisfying solution for safety-related VANET applications.

In conclusion, the node-centric observation of the behavior of neighbor nodes is most useful in order to discover potential attackers. This approach is more generic compared to event centric attack identification, and does not rely on application-specific knowledge. The evaluation of neighbor node trustworthiness based on data plausibility checks can be generally considered reasonable. However, all related publications presented in Section 4.1.2 require permanent never changing unique node identifiers. This assumption is not in line with those mechanisms applied to protect drivers' privacy as discussed in the VANET model in Section 2.2.

4.2. Change of Identifiers for Privacy Protection

The periodical change of the vehicles' identifier is obligatory in order to protect drivers' privacy. The following analysis of ID changes and related ID change observations, performed by the author of this dissertation [SES+13, BSS13], is based on measurements recorded in an outdoor test involving 120 vehicles over 76 days. As far we know this is the first time that aspects of ID changes in VANETs are measured over a long period of time using real traffic data. Wiedersheim et al. [WKMP10] have analyzed previously the detection of ID changes of single-hop neighbors by utilizing a simulation framework. They simulated 25 - 200 nodes in an urban environment of 1000×1000 meters over a period of 1000

seconds. In this dissertation we aim to validate their simulation results by real world measurements. This is an important aspect for local misbehavior detection and local short-term identification of potential attackers. In our tests we applied the Kalman filter described in Section 3.4.2 to track single-hop neighbor nodes. Details about the test and evaluation setup can be found in Section 3.4.4.

We analyzed in our long-term experiments three aspects.

- Are the ID changes performed as expected?
- Have temporary blocks of ID changes a negative effect on ID changes?
- Is it possible to observe the ID change of neighboring nodes?

Related to the evaluation criteria the following events were logged by all vehicles of the FOT. The first three event types are used to log relevant information of the vehicle's status when an ID change is performed. The last type is used to log ID changes of a single-hop neighbors that are detected by a local vehicle tracker.

- `PSEUDONYM_ID_CHANGE__ODOMETER`
- `PSEUDONYM_ID_CHANGE__BLOCK_ACTIVATED`
- `PSEUDONYM_ID_CHANGE__BLOCK_DEACTIVATED`
- `VEHICLE_TRACKER__PSEUDONYM_ID_CHANGE_OBSERVED`

Every log entry contains a timestamp that allows the synchronization of logs from different vehicles. In addition, several other information are logged by the Vehicular Application Programming Interface (VAPI) that allow a detailed evaluation of ID changes, ID change blocks, and ID change observations.

In the long-term experiment a predefined ID change interval of 30 minutes was configured. In Figure 4.2 the measurements from all 120 vehicles are subsumed with respect to performed ID changes. The logarithmic x-axis provides the driven distance between two ID changes. The y-axis is used to show the time between two changes. Apart from some premature change events, when the trip is interrupted, the ID is changed every 1800 seconds as shown by the first graph in Figure 4.2. If a trip is interrupted

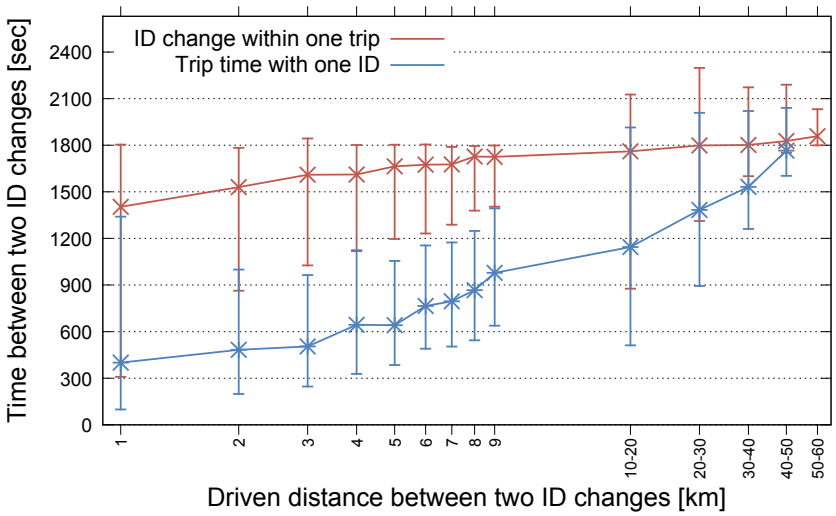


Figure 4.2.: Performed vehicle ID changes measured in long-term outdoor tests

earlier, e. g. by shutting down the vehicle including its OBU, a new pseudonymous ID is applied at the beginning of the next trip. As expected, the second graph shows that the duration of short trips (i. e. $\leq$ 1800 sec) increases with the driven distance.

A temporary blocking of ID changes is used by different V2X applications to prevent ID changes in critical traffic situations for a limited period of time. For example the application that is responsible for intersection collision warnings blocks the ID change if the own station is within the vicinity of an intersection. This mechanism was developed by the author of this dissertation within the sim^{TD} project [MBS+09]. Subsequently this mechanism was included into the ETSI standard TS 102 723-8 [ETS13a].

We analyzed with the FOT if a temporary block of ID changes has negative effects on the regularly performed ID change. Figure 4.3 shows the related evaluation results. In particular, the driven distance and duration with activated ID change block has been measured at all vehicles in the long-term outdoor test. On the x-axis the line graph depicts the driven distance in meters. The left y-axis shows the duration of active blocks in seconds. The filled curve depicts with the x-axis and the right y-axis that most blocks occur within a distance of up to 600 meters. Distances with activated blocks larger than 1 km were not measured in the FOT. Only few ID change blocks remain active for more than 600 meters

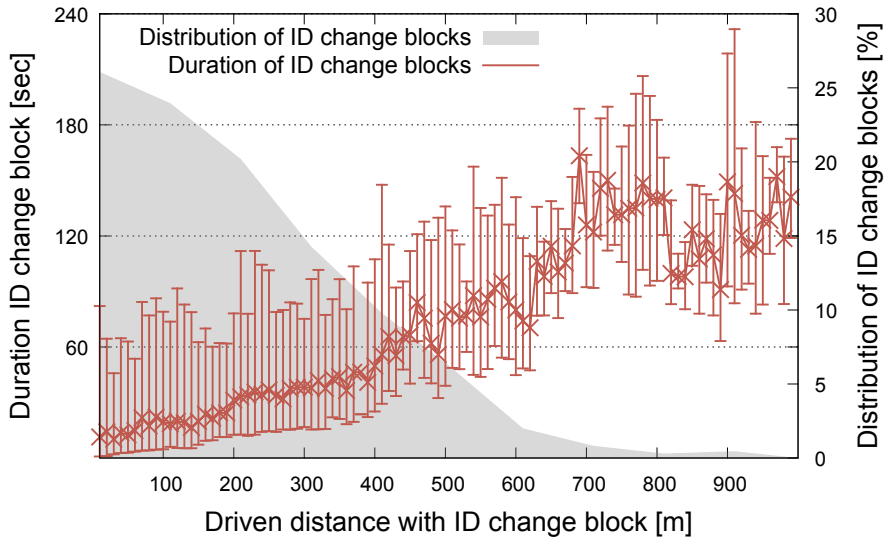


Figure 4.3.: Block of vehicle ID changes measured in long-term outdoor tests

and 90 seconds. The graph shows that on average the duration of an ID change block does not exceed the time of 150 seconds and the vehicles are not driving more than a few hundred meters with an active block. As a result, regular periodic ID changes that are performed probably every few minutes in future productive devices are only minimally affected by temporary ID change blocks.

As discussed in Section 3.2 the local plausibility checks depend on the tracking of single-hop neighbors. In order to track neighbor vehicles despite their periodic ID changes, probabilistic mechanisms for position estimation (e. g. Kalman filter or particle filter) can be used to observe ID changes of nodes in direct communication range. To protect drivers' privacy, the tracking information and ID change

detections must not be shared with other V2X communication neighbors or central infrastructures. As long as the ID change information is used by different stations autonomously, the privacy of the driver is preserved because the involved nodes are not able to create long-term movement profiles. Consequently, an attacker would need to follow a specific node within its single-hop communication radius over a relatively long period of time in order to collect data for useful movement statistics. Only with long-term statistics, an attacker would be able to create a link between the movement of a vehicle and its possible driver's identity by analyzing specific location information. In particular the start location of the vehicle's first trip in the morning could reveal the home address of the driver and the destination could reveal the address of his or her workplace [GP09].

Figures 4.4 and 4.5 show the accuracy of a Kalman filter-based ID change detection performed on 120 vehicles as evaluated in long-term outdoor tests. In this evaluation the number of correctly observed ID changes and the number of false-positive detections is measured. Based on the findings of Wiedersheim et al. [WKMP10] the hypothesis is analyzed that almost all ID changes can be detected by neighboring nodes as long as precise and frequent position information is received per V2X neighbor. The fraction of correctly observed ID changes is illustrated in Figure 4.4. The x-axis shows the number of neighbor nodes that were in communication range when an ID change occurred. The number of measured ID changes having more than 50 single-hop neighbors was negligible low in the FOT. The y-axis shows the percentage of correctly observed ID changes of all single-hop neighbors. The graph shows that the detection rate decreases with an increasing number of neighbors. While with one adjacent node, the observation rate is at 100%, the detection rate decreases to approximately 50% with 12 neighbors.

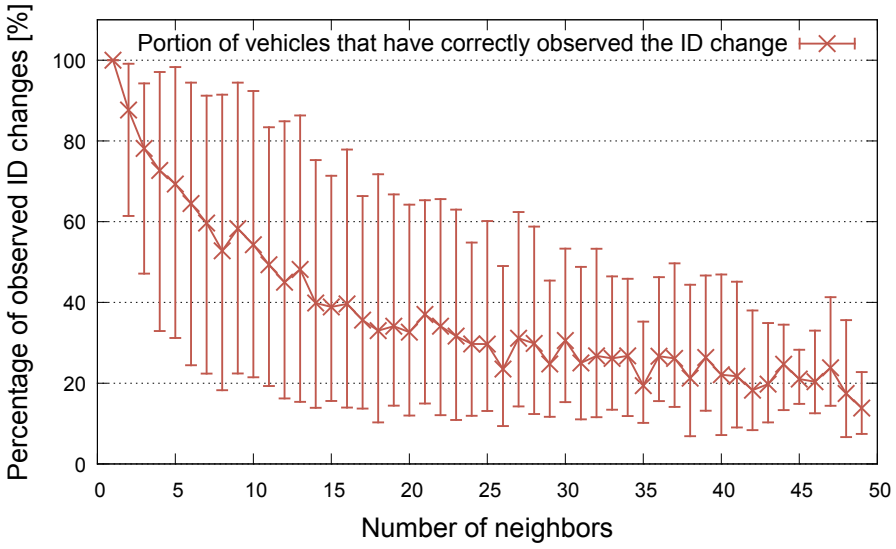


Figure 4.4.: Correct detection of ID changes in long-term outdoor tests

Figure 4.5 shows on the other hand the evaluation of false-positive detections. The red graph shows that on average 23.5% of the detections are false. However, it is additionally shown by the gray filled curve that most ID change detections were made with a low number of neighbors in the reception

range. Consequently, the results of the long-term evaluation show that nodes in the single-hop communication range can be tracked beyond their usage of single node IDs. The findings of Wiedersheim et al. [WKMP10] based on simulations are confirmed in general by our real world experiments. However, inaccurate position information in real systems and frequently appearing and disappearing vehicles complicate the detection and create some false-positive detections.

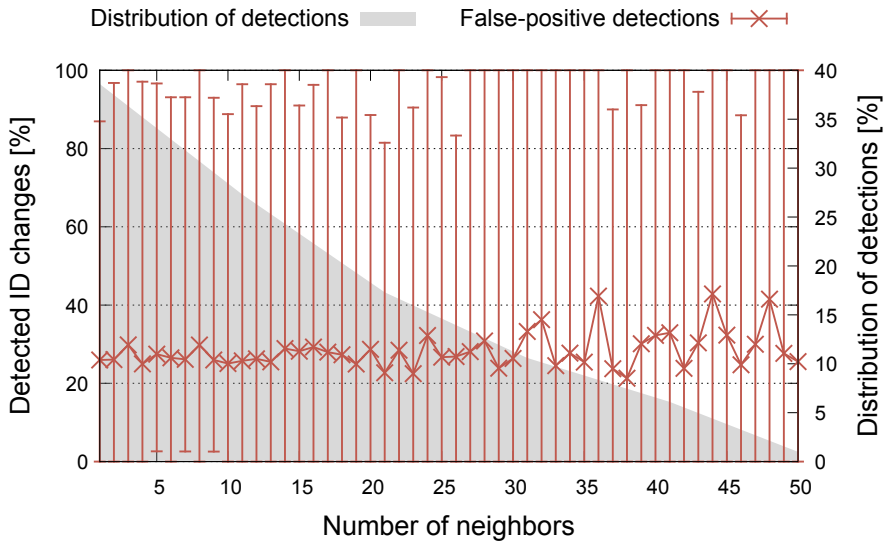


Figure 4.5.: False detection of ID changes in long-term outdoor tests

The analysis of related work in Section 4.1 shows that most related publications do not consider regular ID changes in the VANET at all. However, this assumption is not followed in this dissertation even if vehicle trackers are able to observe the majority of ID changes that are performed by single-hop neighbors. At latest when the neighbor leaves the communication range, its ID change cannot be observed and if the same neighbor enters the communication range again its new ID cannot be associated to previous IDs. A single central entity that is able to link all pseudonymous identifiers, as needed by the TRIP scheme [MP12], conflicts with the protection of drivers' privacy as well. Consequently, we assume that the stations can autonomously and arbitrarily change their identifiers without following global or local instructions. Even attackers could misuse this mechanism in order to hide malicious activities without coming into conflict with general ID change rules. That means that receivers of V2X messages can create short-term reputation profiles only.

4.3. Trust Model for Local Evaluation of Node Trustworthiness

The concept of trust is not easy to define since there is not a single definition based on universal consensus. However, Gambetta [Gam88] defines trust as "trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action". In the proposed

trust model the local evaluation of node trustworthiness is based on ratings related to V2X messages sent by this node. We propose to apply Bayesian logic to determine the relationship between message ratings and node trust. The rating of received messages is then again based on the outcome of the module-based data plausibility checker discussed in Section 3.4, and the particle filter-based plausibility checker discussed in Section 3.6.

In order to locally evaluate the trustworthiness of single-hop neighbors a trust model with three parameters *message rating*, *node trust*, and *node trust confidence* is applied.

- The **message rating** is based on the results of data consistency and plausibility checks as proposed in Chapter 3. The rating $r_{o,n,k}$ of a message sent by node n at time k is created by the receiving observer node o. Every locally processed V2X message is rated which is sent by a single-hop neighbor node. More details about the generation and processing of message ratings are described in Section 4.3.1.

Based on results of data consistency and plausibility checks as detailed in Chapter 3 we propose a local evaluation of node-centric trustworthiness [BMBK12]. For this task a pair of two values (i. e. node trust and node trust confidence) is used.

- The **node trust** is a probabilistic value that bases on message ratings. It expresses the trustworthiness of a *trustor*, in our case the receiver of V2X messages, into the *trustee*, which is in our context the sender of V2X messages. The mechanisms related to the establishment and management of node trust are discussed in more detail in Section 4.3.2.
- The **node trust confidence** represents the certainty a *trustor* has about the correctness of the node's trust value. In our concept, the node trust confidence depends on three parameters: the message rating, the node trust, and context information. In Section 4.3.3 the generation and management of node trust confidence is described in more detail.

Figure 4.6 depicts the relationship between trust and confidence. The labels *high distrust, low distrust, neutral, low trustworthiness, high trustworthiness* in this figure are only used to explain the relationship between node trust on the x-axis and node trust confidence on the y-axis. We do not apply functions to classify the unit intervals as done in the fuzzy logic [Zad75]. This might be necessary if the node trust assessment should be used locally by V2X applications to adapt their behavior accordingly. Since we aim to centrally evaluate detected node-related misbehavior for a long-term exclusion of attackers in this dissertation this local classification is not further considered.

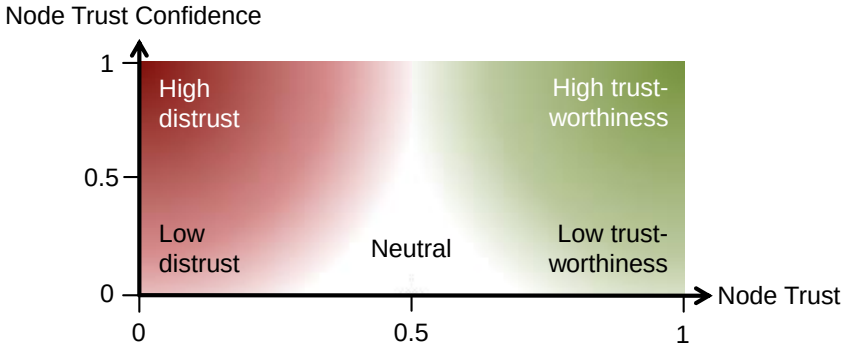


Figure 4.6.: Relationship between trust and confidence

A node can be fully trusted if both the values for trust and confidence show their respective maximum. A low confidence value means that the related node trust value should not be considered much. The local evaluation of node trustworthiness considers the *message rating* $r_{o,n,k}$ related to sender node n at time k separately from the *node trust* $t_{o,n,k}$ as further detailed in Sections 4.3.1, 4.3.2, and 4.3.3. Node trust values $t_{o,n,k} \in \mathbb{R}$ and associated node trust confidence values $c_{o,n,k} \in \mathbb{R}$ have values in the range $[0,1]$. A value of 1 represents the best possible rating, values around 0.5 indicates missing knowledge or uncertainty and 0 is the worst possible rating. The transition between the minimum and the maximum is smooth.

We focus on the computational trust model to discuss the processing of both, evidence derived from local misbehavior detection mechanisms and context-dependent parameters. The representation of results of this trust model is designed for software agents instead of humans. As discussed in the following sections the relationship between evidence (message rating) and node trust is based on the Bayesian approach introduced in Section 4.1.2.

4.3.1. Message Rating

The rating $r_{o,n,k}$ of a message sent by node n at time k and processed by a receiver o is based on consistency and plausibility checks of location-related data. A high value is achieved if the results of the checks substantiate the correctness of the message content regarding the following measures:

- compliance to specifications,
- consistency of duplicate data,
- verifications with both first hand information and second hand information.

In particular, the maximum is assigned to $r_{o,n,k}$ if the node's movement is in accordance with the predefined mobility model and own sensor measurements as well as with rules that do not indicate a violation. Deviations result in a gradual decrease of the message rating value. Low message rating can be the result of unforeseen movement patterns and/or violations of plausibility checks. Although low values might indicate a potential attack, it is also possible that they are caused by natural reasons such as inaccurate GNSS signals, not synchronized stations, or sudden driving maneuvers. In general, the outcome of the module-based data plausibility checker discussed in Section 3.4, and the particle filter-based plausibility checker discussed in Section 3.6, determines the message rating.

In the module-based plausibility framework, the values for message rating are calculated by the fusion of ratings provided by different modules as illustrated in Figure 3.4 on page 51. The description in Section 3.4 states that the final rating of the root vertex $r(v_{root})$ can be used to set the message rating.

In the particle filter-based framework, a normalization factor Ω is used to determine $r_{o,n,k}$. This factor Ω contains the summarized weights of all particles of a tracked neighbor node. In order to calculate the value for $r_{o,n,k}$, a factor Ω' with $\Omega' < \Omega$ is normalized to the range of values for the message rating $r_{o,n,k}$. It is reasonable to select a particle weight Ω' that is smaller than the maximum weight of all particles since some particles are randomly spread and a perfect matching of received location data with the PDF applied in the particle filter is unlikely. In order to do so, the upper limit of Ω' needs to be defined using the parameters for random particle spreading and the PDF. In the simplest way, a linear mapping function is used, where $\Omega'/2$ is mapped to a value of $r_{o,n,k} = 0.5$. If, for example, the maximum measured total particle weight is $\Omega = 100$, the maximum message rating $r_{o,n,k} = 1$ is mapped

to a value of about $\Omega' = 80$ and therefore the $r_{o,n,k} = 0.5$ is mapped to a value of $\Omega'/2 = 40$. In the same way, measured Ω' values like 20 and 60 would result in ratings of 0.25 and 0.75, respectively.

As argued in the conclusion of the local misbehavior detection in Section 3.9 the message-based checks should be used to filter messages with erroneous content. On the contrary, the node-based checks should not result in a discard of affected messages. Consequently, a local classification of message rating values according to Table 4.1 is proposed that bases on research of Jaeger, Stübing, and the author of this dissertation [JBSH11, SJB+10]. The message rating is created by applying the results of the message and node-based checks. The three validation classes can easily be interpreted and used by local V2X applications. Messages considered to be erroneous should be ignored or dropped by upper layers, and approved messages shall be used without constraints.

Table 4.1.: Simple validation classes used by local message-related plausibility checks

Validation Class	Interpretation	Message Rating
Erroneous	The security system recommends to ignore the message	$0 \leq r_{o,n,k} < 0.5$
Neutral	Due to missing information the consistency and plausibility checks cannot evaluate the message	$r_{o,n,k} = 0.5$
Approved	Mobility data of the message are checked and approved	$0.5 < r_{o,n,k} \leq 1$

However, V2X messages that are classified as *neutral* shall be used with caution because in this case the security subsystem is not able to take a reliable decision with respect to message-based checks. For example, if the plausibility framework does not get a periodical update of the own position and time, the plausibility of received PVs cannot be determined, which may result in neutral message rating evaluations with a $r_{o,n,k} = 0.5$. The node trust is not considered in this classification and shall not be used as a basis for decisions on message droppings. The node-based evaluation is discussed in Section 4.3.2.

4.3.2. Node Trust

The node trust $t_{o,n,k}$ is based on evidence derived from message ratings. $t_{o,n,k}$ is an indicator for general trustworthiness of trustor node o in a trustee neighbor node n at time k, i. e. whether a node is faked or its real existence can be approved. Here the probabilistic model based on the Bayesian approach is chosen in combination with the beta distribution as introduced in Section 4.1.2. In addition we extend the beta distribution model with a static aging factor u as proposed by Buchegger et al. [BB04]. The value of the message rating $r_{o,n,k}$ is applied as shown in Equation 4.7 which is based on Equation 4.5.

$$\begin{aligned} \alpha_{o,n,k} &:= u\ \alpha_{k-1} + r_{o,n,k} \\ \beta_{o,n,k} &:= u\ \beta_{k-1} + (1 - r_{o,n,k}) \end{aligned} \tag{4.7}$$

The node trust value is calculated with the formula introduced in Equation 4.3 on page 99 whereby the expectation value represents node trust $t_{o,n,k}$. Equation 4.8 shows the formula used to calculate the node trust.

$$t_{o,n,k} = \frac{\alpha_{o,n,k}}{\alpha_{o,n,k} + \beta_{o,n,k}} \tag{4.8}$$

The initial values for α_{o,n,k_0} and β_{o,n,k_0} are 0.5 which results in an initial node trust value of $t_{o,n,k_0} = 0.5$. This indicates that no prior knowledge is available about a neighbor node such as a tracked vehicle. The aging factor $u \in (0,1)$ determines the ratio of how much a new message rating value affects the node trust. Depending on the chosen value for the aging (e. g. $u = 1 - \frac{1}{m}$), a magnitude of m plausible messages have to be processed until stationary maximum node trust can be assumed. In the same way m implausible messages have to be sequentially received until the minimum trust value is reached. As a consequence, a single message with a bad trust rating will only effect the node trust marginally, but multiple successive bad ratings will result in a rapid decrease of $t_{o,n,k}$.

4.3.3. Node Trust Confidence

The purpose of the node trust confidence $c_{o,n,k}$ is to provide the certainty of the trustor o (receiver of V2X messages) regarding the node trust value $t_{o,n,k}$ at time k that is related to a single-hop neighbor node n. If the confidence value is low, either not enough information has been collected about a target node, or $t_{o,n,k}$ shows inconsistent trust information. The node trust confidence value represents the confidence of the security subsystem with respect to the rating of the node trust value $t_{o,n,k}$. Alternatively, $c_{o,n,k}$ can be described as the quality of the node trust value. In our model we apply a two-step approach to create the node trust confidence.

a) First, the standard deviation of the beta distribution is calculated, cf. Equation 4.9.

b) Subsequently, the standard deviation is multiplied by factors that consider the time and distance the sender and receiver of V2X messages have been in common single-hop communication range. With increasing time and distance the factor applied on the node trust confidence value increases.

Equation 4.9 is used to calculate the preliminary $c'_{o,n,k}$ based on the standard deviation of the beta distribution that is used to calculate the node trust $t_{o,n,k}$ according to [ZMHT05, ZMHT06]. Zouridaki [ZMHT05] extended the standard deviation by a parameter ζ to ensure that resulting confidence values are in the range [0,1].

$$c'_{o,n,k} = 1 - \sqrt{\frac{\zeta\alpha\beta}{(\alpha+\beta+1)(\alpha+\beta)^2}} \tag{4.9}$$

Since low values of $c'_{o,n,k}$ indicate inconsistency in the node's behavior, the confidence is also used to indicate potential attacks, in addition to confirm the plausibility of the node trust $t_{o,n,k}$. For example, a low value can be caused by a ghost vehicle that is suddenly entering a radar-monitored area that has to be free of vehicles (cf. location-based attack described in Section 2.3.3). The influence of the preliminary $c'_{o,n,k}$ is shown in Figure 4.7. In this figure, the evaluation of a tracked neighbor node is illustrated. It is shown that the node trust confidence value indicates differences between message

rating and node trust. At the beginning of the tracking of a new node, $c'_{o,n,k}$ is increasing together with the node trust value. As soon as $r_{o,n,k_1} = t_{o,n,k_1}$ at time k_1, the confidence approximates also to its maximum and acknowledges the consent with a high value $c_{o,n,k_1} \approx 1$. However, when the message rating suddenly drops at time k_2, for example due to an attack, the confidence drops below the threshold as well. A low confidence value indicates a large difference between the message rating and the node trust. If the message rating remains at a low value then the node trust follows. Consequently, the trust confidence value increases with converging values of r and t at times k_3 and k_4.

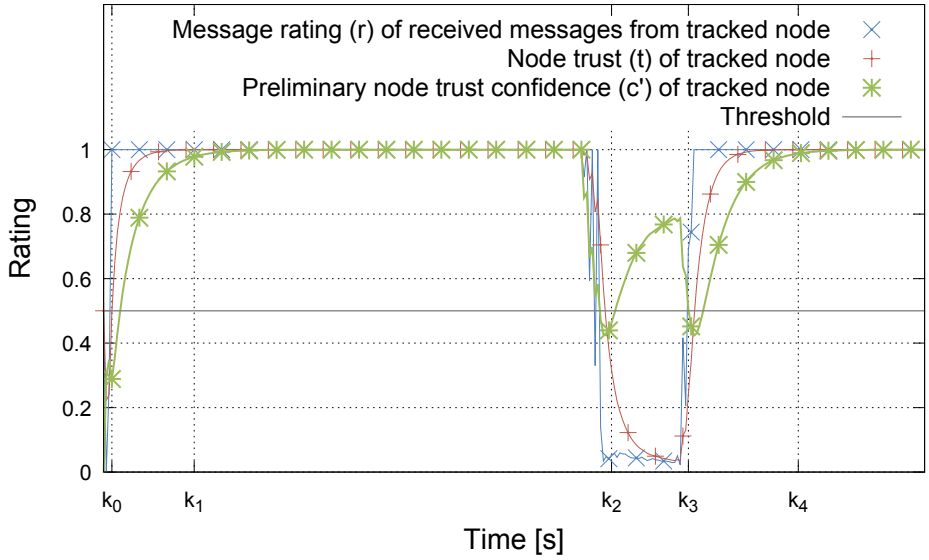


Figure 4.7.: Node trustworthiness under attacks based on message rating, node trust, and confidence

In a second step the preliminary node trust confidence $c'_{o,n,k}$ is extended by context information. Schmidt et al. [SLH09] describe an approach to consider the observed movement distance of neighbor nodes in order to detect potential stationary roadside attackers. For this verification at least twice the transmission radius of a common radio device is used to define the value for the minimum distance moved (MDM) attribute. If the observed travel distance of an adjacent nodes is larger than the MDM distance, then a stationary sender at the roadside can be excluded. Based on this concept, the node trust confidence $c_{o,n,k}$ grows linear with the distance and duration two nodes are in common single-hop communication range. The connection time and the observed driven distance of neighbors is used to calculate the final value for node trust confidence as shown in Equation 4.10. We propose to apply a simple multiplication of the preliminary node trust confidence $c'_{o,n,k}$ value to linear decrease the confidence until the required values for travel distance and contact time are reached. As soon as the values are reached the node trust confidence $c'_{o,n,k}$ is multiplied by 1 and therefore not further manipulated.

$$c_{o,n,k} = c'_{o,n,k} \cdot min\left(1 \quad , \quad \frac{\frac{1}{\gamma} \cdot duration(n) + \frac{1}{\delta} \cdot distance(n)}{2}\right) \tag{4.10}$$

In order to use this context information the security subsystem must be able to provide information how long both stations have been in common communication range and which distance the nodes have been driven in this time. The contact time between the local station and the neighbor n is given by the function $duration(n)$ and the moved distance with $distance(n)$. The variables γ and δ determine the required values for minimum contact time and minimum traveled distance to multiply $c'_{o,n,k}$ with a maximum factor.

In Figure 4.8 the effect of increasing confidence is shown when a new node is discovered at time k_0 and subsequently reaches the minimum required distance and duration at time k_1. In this dissertation a maximum communication range of $\delta = 1000$ meters and an average vehicle speed of 25 m/s is considered. The minimum required duration is consequently reached at $k_1 = 40s = \gamma$ as shown in Figure 4.8.

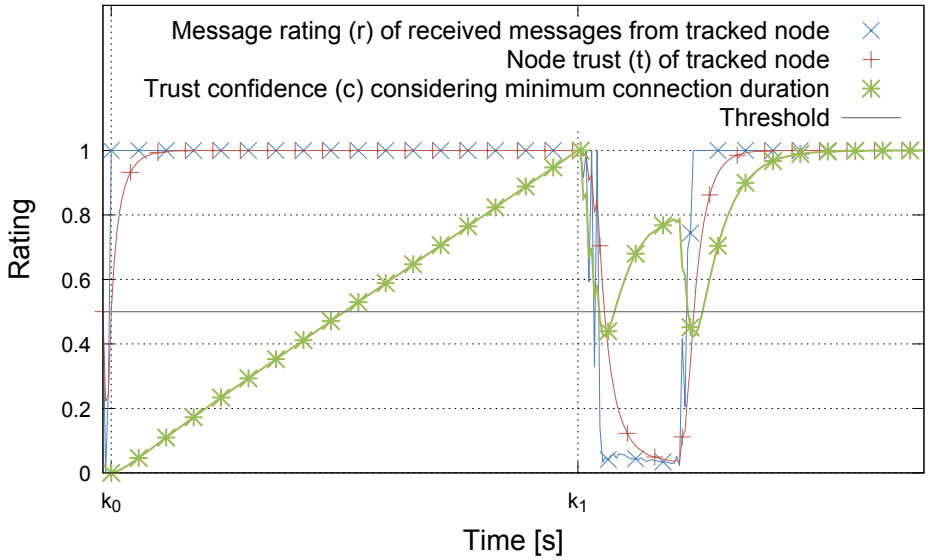


Figure 4.8.: Node trustworthiness with linear increasing confidence

4.4. Local vs. Central Misbehavior Evaluation

In order to locally identify and exclude an attacker from V2X communications two requirements have to be fulfilled. First, the autonomous detection of misbehavior has to be done by the node and second, attacker nodes must be identified by their pseudonymous ID as long as they are in communication range of the detector. The following analysis is based on Bißmeyer et al. [BNPB12] and aims to evaluate possibilities and limitations of local attacker identification. It is assumed that pseudonymous identifiers are changed regularly so that the used IDs cannot be linked or resolved by the nodes of the VANET. After the introduction of general notations in Section 4.4.1, two attack scenarios are discussed in Section 4.4.2 involving local attacker identification. Both scenarios are based on Bißmeyer et al. [BSB10]. Subsequently, the general possibilities of a central attacker identification is analyzed in Section 4.4.3.

4.4.1. Notations

The VANET is modeled as a graph $G = (V, E)$ where V is the set of vertices (nodes) and E denotes the set of edges (communication links between the nodes).

- K: The ordered set K of timestamp elements is related to vehicle trips and contains elements $\{k_0, ..., k_n\}$ with $n \in \mathbb{N}$ and $k_0 < k_i < k_n, \forall\ 1 < i < n$.
- $N_v(k)$: The set $N_v(k)$ contains neighbor nodes that are located within the single-hop communication range of node $v \in V$ at time $k \in K$, where $v \notin N_v(k)$.
- $N_v^*(k) = \{v\} \cup N_v(k)$: The set $N_v^*(k)$ contains node v and all neighbors of node v at time $k \in K$.
- $P_v(k)$: The set $P_v(k)$ contains the pseudonymous unique identifiers of node $v \in V$ that are derived from valid pseudonym certificates[1] owned by this node at time $k \in K$.
- $I_{ov'}(k)$: The set $I_{ov'}(k)$ contains misbehavior events (inconsistencies) detected by observer node $o \in V$ at time $k \in K$ concerning node $v \in V$ that appears with the pseudonym $v' \in P_v(k)$.

4.4.2. Attack Scenario with Local Attacker Identification

A set $V' \subseteq V$ of nodes is passing an area where a ghost node $a \in V$ is simulated within the time frame $K = \{k_0, ..., k_n\}$ as depicted in Figure 4.9. In this example, an attacker creates a stationary ghost vehicle that claims to be broken down on a road. The attacker is able to change the pseudonymous ID of the ghost node arbitrarily as mentioned in Section 4.2. Therefore, node a appears with the identifiers $a', a'', a'''... \in P_a$. A local misbehavior detection system running on the observer nodes $o \in N_a(k)$ is able to detect inconsistencies $I_{oa'}(k)$ that are caused by a ghost vehicle a' when a vehicle is overlapping the stated position. In general, if the attacker $a \in N_o(k)$ is in communication range of observer $o \in V$ and the attacker uses different pseudonyms $a', a'', ...$ at different times k for the ghost vehicle then different detections cannot be assigned by observer.

Location-Based Attacker Fakes a Non-Existing Hazard on the Road Due to the local ID change detection, discussed in Section 4.2, nodes o_2 and o_3, illustrated in Figure 4.9, can assign the overlap detections at time k_0 and time k_1 to a causer set $P_a^* = \{a', a''\}$. If the attacker changes the ID of the ghost node while node o_2 is not in its communication range, an overlap detection at a later time k_n cannot be assigned to the set of previous causers P_a^*. The latter event is depicted in the outer right part of Figure 4.9. In this simple scenario, the stationary position of the ghost vehicle might allow for the linking of the different vehicle overlaps caused by the same ghost vehicle. However, in a more complex and dynamic scenario the detection rate of ID linkings might be lower compared to the test results presented in Section 4.2.

The maximum number of linkable local detections made by the different observers o is discussed in the following. The inconsistencies that are autonomously detected by the nodes $o \in N_a(k)$ over time $k_0...k_n$, are combined in a subset $I_{oa'}$. For the sake of simplicity we focus in this discussion on the detection of vehicle position overlaps. Related to every ghost node a' only one overlap can be observed at time k by another node. However, a detection is only possible if both nodes, the observer o and the

[1] Functions to derive an ID from a certificate are further detailed in related IEEE and ETSI standards [IEE13, ETS13b].

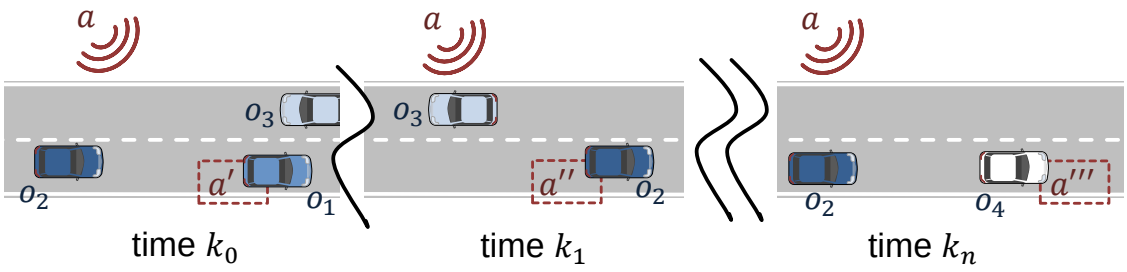


Figure 4.9.: Location-based attacker fakes a non-existing hazard on the road

affected node a, are in common communication range at time k. Node $a \in V$ owning the pseudonymous identifier $a' \in P_a(k)$ must be in range of the observer $a \in N_o(k)$ and, vice versa, the observer must be in range of the affected node: $o \in N_a(k)$. Consequently, the maximum number of elements in the set of detections is $0 \leq |I_{oa'}| \leq |K|$.

The exemplary situation depicted in Figure 4.9 shows that node o_1 is only in communication range of attacker a at time k_0, and therefore o_1 is able to detect only its own overlap with a'. Node o_2 and o_3, however, are element of $N_a(k)$ at time k_0 and k_1, and therefore able to detect autonomously overlaps of o_1 with a' at time k_0 and o_2 with a'' at time k_1. At a point in time when $N_a(k) = \emptyset$ the attacker changes the ID of the ghost vehicle from a'' to a'''. As a result, node o_2, which is element of $N_a(k)$ with $k \in \{k_0, k_1, k_n\}$ can only create a set $|I_{o_2,a'}| \leq 2$ with $a' \in P_a^* \subseteq P_a(k)$.

If observers share their local detections as proposed in related publications [DOJ+10,DFM05,MP12] the detection and temporary exclusion of attacker a might be possible. However, the local exchange of misbehavior detections enables new vulnerabilities, e. g. the discrediting of benign real nodes.

Location-Based Attacker is Denying the Existence of a Real Vehicle Figure 4.10 shows an attack scenario where a real vehicle's position is overlapped by several ghost vehicles created by attacker a. The real vehicle r is blocking the road but as long as its hazard lights are activated, a DENM is period-

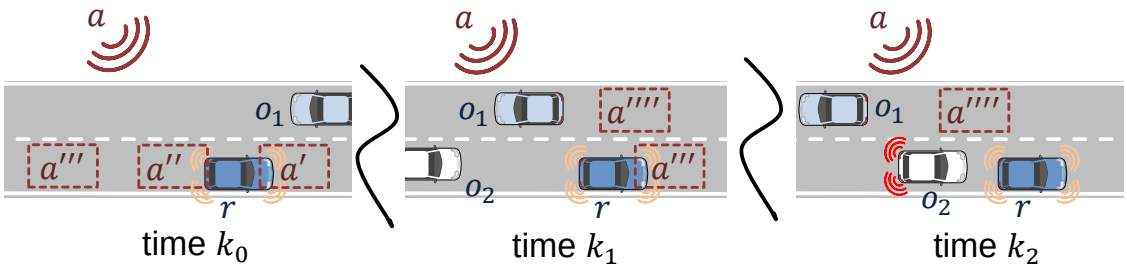


Figure 4.10.: Location-based attacker is denying the existence of a real vehicle

ically distributed by the responsible V2X application of r that aims at warning approaching nodes, e. g. o_2 at time k_1. A stationary attacker, however, is creating several ghost vehicles a', a'', a''' that virtually overlap the position of node r. Such an attack is assumed to be possible since an attacker can change its pseudonymous ID frequently in order to create different vehicles that approach the scene.

It is assumed that node r appears with the same pseudonymous identifier $r' \in P_r(k)$ in the critical time $k \in \{k_0, k_1, k_2\}$. With the vehicle overlap detection mechanism the benign observers $o_1, o_2 \in N_a(k) \cap N_r(k)$ detect the overlaps of the ghost vehicles a', a'', a''' with the real vehicle r autonomously. The corresponding numbers of observed overlaps with $K = \{k_0, k_1, k_2\}$, are as summarized in Table 4.2.

In Table 4.2 it is shown that node r produces three events in this exemplary attack scenario. However, each ghost vehicle creates only one event from the view point of node o_1 and o_2. The reliable local identification of the attacker is therefore not possible. By only considering the number of overlaps per node, the observers o_1 and o_2 may deem node r to be the attacker. Consequently, node o_2 would possibly ignore the hazard warnings that are sent by r, which in turn could cause a dangerous situation since vehicle o_2 has to brake suddenly assuming vehicle r is not in direct line of sight. Even when practicing the local exchange of misbehavior detections or node reputations, the identification of the attacker is not reliably possible for node o_2 because the statement of r would probably contradict with the statements of $o_1, a', a'', a''', a''''$. The latter set of nodes would declare that node r is overlapped three times, and that nodes a', a'', a''' are overlapped only once. As a result, the reputation of node r would possibly be three times lower than the reputation of the remaining nodes in the scenario. Another aspect that has not been considered in both attacker scenarios is the implausible behavior of vehicles that might be shown in critical situations having involved tossing or crashing vehicles. The temporary exclusion of suspicious nodes may hinder the V2X applications to warn the driver about dangerous situations since safety-related messages would be dropped.

Table 4.2.: Observed overlaps of o_1 and o_2 in the ghost vehicle attack

Node / Node	o_1	o_2	r	a'	a''	a'''	a''''	Σ
r	0	0	-	1	1	1	0	3
a'	0	0	1	-	0	0	0	1
a''	0	0	1	0	-	0	0	1
a'''	0	0	1	0	0	-	0	1

Equation 4.11 shows the collection of misbehavior detections exchanged between VANET neighbors. In this equation a collector node $c \in V$ receives misbehavior detections from its neighbors $o \in N_c$. The set of collected misbehavior detections $I_{oa'}(k)$ accusing one specific node a' may comprise only detections from those neighbors $o \in N_a(k)$ that were situated in the communication range of the attacker a at time k. Furthermore, at either the same time $j = k$ or a later time $j > k$, the observer node o must be a single-hop neighbor of the collector node c, cf. $o \in N_c(j)$ in Equation 4.11.

$$I_{a'} = \bigcup_{o \in N_c(j)} I_{oa'}, \forall o \in N_a(k), \exists a' \in P_a(k) \wedge k, j \in K \wedge j \geq k \tag{4.11}$$

As a consequence, the local attacker identification is not sufficient if nodes are using pseudonymous identifiers that can be changed arbitrarily. In the following section, the local attacker identification is compared with a central attacker identification.

4.4.3. Attack Scenario with Central Attacker Identification

In contrast to a local evaluation of misbehavior detections, a central solution is able to use additional possibilities but at the same time also has to deal with limitations. The goal of the central evaluation is the reliable detection of attackers in order to exclude them from V2X communications. For this task, a central misbehavior evaluation authority (MEA) is introduced.

The MEA is able to collect misbehavior detections $I_{oa'}(k)$ from different observer nodes $o \in N_a(k)$ that have been in the communication range of attacker $a \in V$ at time k. It is further assumed that the attacker is using different pseudonymous identifiers $a' \in P_a(k)$ for the location-based attacks. In contrast to the local collection of detections as specified in Equation 4.11 the MEA has two further possibilities that may increase the accuracy of attacker identifications.

- The central entity is not limited to single-hop V2X communications based on ITS-G5 [ETS10b] in order to collect misbehavior detections from observers. Considering the ITS architecture introduced in Section 2.1 the observer is able to transmit its local detections to the central infrastructure via field-vehicle communications with (RSUs) or wide area wireless mobile communications. Further it is assumed that the nodes are able to temporarily store misbehavior detections and transmit them at a later point in time when a RSU is in communication range.
- In contrast to local nodes, the MEA is able to get linking information of pseudonymous identifiers that are related to detected misbehavior. The MEA, however, must not be able to misuse this pseudonym linking function to breach the privacy concept of V2X communications. Having for example two detections $I_{oa'}(k)$ and $I_{oa''}(k)$, the MEA is able to check whether $\{a', a''\} \subseteq P_a(k)$.

Due to these additional possibilities the central collection of misbehavior detections as shown in Equation 4.12 is less restricted compared to the local collection of related events as shown in Equation 4.11.

$$I_{a'} = \bigcup_{o \in V, a' \in P_a(k)} I_{oa'}, \forall o \in N_a(k) \wedge k \in K \tag{4.12}$$

Only if the following three conditions are fulfilled the union set $\bigcup_{o \in V} I_{oa'}$ is equal to the union set $\bigcup_{o \in N_c(j)} I_{oa'}$ with $j, k \in K$ and $j \geq k$. First, all observed misbehavior detections are transmitted to the central MEA. Second, the local collector node c has connection to all VANET nodes $V = N_c(j)$ and third, the attacker has only one pseudonymous ID $P_a(k) = \{a'\}$. In this constructed scenario, the set of locally collected misbehavior detections comprises the same elements as the set of centrally collected misbehavior detections as shown by Equation 4.13.

$$\left(\bigcup_{o \in N_c(j)} I_{oa'} \quad = \quad \bigcup_{o \in V} I_{oa'} \right), \forall o \in N_a(k) \wedge k, j \in K \wedge j \geq k \tag{4.13}$$

Assuming attacker a is able to use more than one pseudonymous identifier $a', a'', a''', \ldots \in P_a(k)$ and node a changes the IDs of its ghost nodes while a local observer $o \in V$ is not in its communication range $o \notin N_a(k)$, then the observer o is not able to identify that different misbehavior events are induced by the same attacker. If additionally the set of nodes in the VANET comprises more elements than the

neighbor set of node c at time $j \in K$ (i. e. $|V| \gg |\bigcup_{j \in K} N_c(j)|$) the relation in Equation 4.14 holds.

$$\left(\bigcup_{o \in N_c(j)} I_{oa'}, \exists a' \in P_a(k) \quad \ll \quad \bigcup_{o \in V, a' \in P_a(k)} I_{oa'} \right), \forall o \in N_a(k) \wedge k, j \in K \wedge j \geq k \tag{4.14}$$

Even if only a subset of local detections are transmitted to the central MEA, it is assumed that the statement of Equation 4.14 is true. In this dissertation it is assumed that in the majority of all cases the set of VANET nodes that are able to report to the central MEA comprises considerably more elements than the set of neighbors of a local collector.

Under the assumptions that, first, the MEA receives sufficient misbehavior reports and second, that the MEA is able to conditionally check the likability of different pseudonymous IDs contained in the reports, the following two attacker identifications are possible. The detailed description of the related concrete concept is given in Chapter 5.

- In the attack scenario with a faked non-existing hazard (cf. Figure 4.9), the central MEA is able to identify that the IDs a', a'', a''' are elements of P_a and that different independent nodes $o_1, o_2, o_4 \in V$ overlapped the stated position of the ghost vehicle. This knowledge allows the MEA to identify node a to be the attacker.
- In the second attack scenario (cf. Figure 4.10), the MEA is likewise able to identify that a', a'', a''', and a'''' are elements of P_a and that no other node $o \in N_r$ has overlapped the position of node r (assuming sufficient high position accuracy). Therefore, the central MEA can conclude that node r is real and that the claimed overlaps are faked.

In summary, it can be stated that a central misbehavior evaluation authority is able to identify attackers and faulty nodes more reliably than local VANET nodes.

4.5. Summary

As analyzed in this chapter the local detection of misbehavior, based on mobility data plausibility checks, can be used to identify the causing node (i. e. an attacker or a faulty station). The majority of related publications has proposed to do this attacker identification locally on the nodes without support of a central entity. Even the exclusion of attackers is proposed to be done locally by sharing information about both detected misbehavior and neighbor reputations. However, most of the related proposals do not consider the application of changing pseudonymous identities. Therefore, most related work is not in line with the privacy design of international standardization (i. e. ETSI [ETS12a, ETS12b] and IEEE [IEE13]) as well as latest V2X field operational tests [BSM+09, Fun13, Sch13].

With the evaluation of the outdoor tests it has been shown that pseudonymous IDs can be changed regularly without negatively effecting traffic safety and efficiency applications. The results show further that a detection of an ID change is possible by neighbors in the single-hop communication range. Based on these findings, an evaluation of the neighbor node's trustworthiness is proposed that can be maintained locally as long as both nodes are in common communication range.

The trustworthiness of a node consists of two measures namely trust and confidence. The node trust value is based on results of local consistency and plausibility checks related to mobility data. The node

trust confidence value could be considered as the weight of the related trust value. If a low message rating value is caused by message-based plausibility checks, the affected single V2X message can be dropped locally on the node. In contrast, an exclusion of neighbors as consequence of a low node trust value should not be performed. As analyzed in this chapter local nodes are not able to reliably identify the attacker who is causing several inconsistencies. Due to the use of different pseudonymous IDs, the attacker can hide its malicious behavior while local observers are not able to decide which IDs belong to the respective attacker. Consequently, a central misbehavior evaluation authority is required to identify the causer of detected misbehavior. In the Chapter 5 we propose a framework to centrally identify attackers in order to permanently exclude them from active VANET participation.

5. Central Long-term Identification of Attackers

The reliable identification of attackers and faulty stations in V2X communications is challenging for local misbehavior detection systems deployed on the network nodes, as discussed in Chapter 4. Moreover, local nodes cannot exclude attackers from the VANET for long periods of time, and the short-term eviction of misbehaving nodes is prone to false-positive detections. There are three main reasons why a central mechanism for long-term exclusion of attackers is indispensable.

a) VANET nodes cannot necessarily distinguish between valid and expected anomalies such as a traffic accident and maliciously created anomalies such as an attack. This issue is discussed in more detail in Section 3.8.

b) As analyzed in Section 4.2, nodes cannot locally recognize an attacker over a long period of time if the attacker performs an ID change after every attack with a silence period in between.

c) In some cases network nodes can only detect a misbehavior event where multiple nodes are involved but the identification of the responsible node is not possible autonomously. In Section 4.4.2 related cases are described in more detail.

As a result, we propose in this dissertation the application of a central misbehavior evaluation authority that identifies attackers and faulty nodes and that excludes them from the VANET to ensure the network's long-term reliability. Based on reported misbehavior detections, a central misbehavior evaluation authority (MEA) aims to identify the causer of location-based attacks and observed implausibilities. The MEA can execute this task more reliably than local network nodes since the MEA is able to collect information from independent observers. However, the central evaluation authority also has to consider attacks such as discrediting and has to consider specific requirements such as scalability and flexibility in order to efficiently identify attackers in the VANET.

In Section 5.1, related work is analyzed that considers both the central identification and exclusion of attackers or faulty nodes. General requirements for a central misbehavior evaluation are discussed in Section 5.2. Subsequently, in Section 5.3 a proposal for misbehavior reporting is described. In Section 5.4 a concept is presented that allows to conditionally link pseudonymous IDs in cooperation with the PKI. Based on these mechanisms, a central MEA is able to assess reported suspicious nodes to identify attackers. The mechanisms for central node evaluation with attacker identification, and final attacker exclusion are detailed in Sections 5.5 and 5.6, respectively.

5.1. Related Work

The central exclusion of VANET attackers is not well considered in related publications due to the general decentralized character of VANETs. However, the analysis in Chapter 4 shows that a reliable identification and permanent exclusion of attackers is not possible for local network nodes. In Sec-

tion 5.1.1, proposals are presented that consider the reporting of misbehavior to central infrastructures, followed by work in the context of central pseudonym resolution in Section 5.1.2. In Section 5.1.3 work in the field of fault diagnosis and attacker identification is presented and in Section 5.1.4 work about the exclusion of VANET nodes.

5.1.1. Misbehavior Reporting to Central Infrastructures

The reporting of misbehavior to a central infrastructure is designated by ETSI in their technical specification of the security services and architecture [ETS10c, ETS12a]. According to this specification a report may contain only the pseudonymous identifier of suspects and information that is not further specified in this related work. The receiving entity within the infrastructure subsequently has to respond with an acknowledgment or a cause in case of report rejection. In a similar way, in the draft version of the security credential management system design of the American VSC3 consortium [oTRA12] a structure for misbehavior reporting is proposed. According to the VSC3, every report contains additionally to the reporter's temporary identifier, the location and time of a suspicious event as well as categorized information about the detected misbehavior. Moreover, a list of multiple recorded V2X messages can be attached.

5.1.2. Pseudonym Resolution

In order to identify attackers based on reported misbehavior, a central MEA may need linking information for pseudonym credentials, which is provided by a credential provider such as a PKI. Different approaches are published that consider the resolution of pseudonymous identifiers. These protocols allow to request information whether different pseudonymous identifiers belong to the same node or alternatively the respective long-term identifier of the owner of a pseudonymous ID.

The *secure revocable anonymous authenticated communication* protocol (SRAAC) [FAEV06] uses magic-ink signatures with shared secret schemes in order to provide blindly signed pseudonym certificates. Using this protocol, the pseudonymous node identifier can only be resolved if a defined number of CAs cooperate to first map a pseudonym certificate to a resolution tag and, subsequently, to the node's identity. In [SKMW10], the authors propose a similar protocol that also blindly signs pseudonym certificates. However, in contrast to SRAAC, the resolution information (called V-token) is stored inside the certificate instead of the CA's database. Both protocols, SRAAC [FAEV06] and V-Token [SKMW10], require extensive message exchange in the pseudonym acquisition phase caused by the blind signature scheme.

The security credential management system of the American VSC3 consortium [oTRA12,WWKH13] also applies a method for pseudonym resolution. Their proposed framework is based on the imprint of linked identifiers in pseudonym certificates. The linking information is managed by at least two linkage authorities that both have to cooperate in order to get long-term information or pseudonym linking information. Similar to this solution, both Pietrowicz et al. [PZS10] and the European Car-to-Car Communication Consortium [BSS+11] propose a simplified split of duties within the PKI to protect the drivers' privacy. This strategy prevents a single instantiation from storing resolution information for pseudonymous data. However, the conditional resolution of pseudonymous identifiers

is not considered by the authors of latter mentioned publications [BSS+11, PZS10]. Similarly, ETSI specifies a PKI architecture with different entities [ETS10c], but a protocol for pseudonym resolution is not included.

5.1.3. Fault Diagnosis and Attacker Identification

The detection of Byzantine attack behavior is a common problem in different wireless networks such as MANETs [EB09,SPC11] or WSNs [SONP12]. The general Byzantine problem has been first described by Lamport et al. [LSP82] in the year 1982. The principles of the Byzantine problem are later applied in computer networks, primarily in the field of fault tolerance [CL99] and fault detection [SA14]. Fault detection is recognizing that a problem has occurred, even if the root cause is not known. In addition fault diagnosis and fault isolation is applied to pinpoint one or more root causes of a problem. This diagnosis may therefore be used for attacker identification in VANETs. A central misbehavior evaluation authority has to equally trust in general the senders of authorized reports but it is not required that all the non-Byzantine nodes come to a common agreement regarding the content of their reports. This trust association reflects essentially the problem of the Byzantine generals [LSP82].

Fault Management The process of attacker identification is in general similar to fault management. As a consequence related mechanisms are discussed in this section. The term *fault management* describes the overall process and infrastructure associated with detecting, diagnosing, and fixing faults as well as returning to normal operations. In context of misbehavior detection in VANETs the local nodes are responsible for detecting the anomalies. The central infrastructure is responsible in the VANET context for the diagnosis and mitigation actions. However, mechanisms related to fixing of problems and returning to normal operation are not discussed in this dissertation because these are tasks that are handled individually by vehicle and RSU manufacturers for specific use cases. In fault diagnosis different models are used to identify the "root cause". According to Stanley et al. [SA14] a root cause is an underlying problem leading to other problems and observable symptoms. In the context of fault detection and fault diagnosis different models are defined.

- **Abnormal vs. normal operation**: Models of normal operation observe the behavior of system components in order to detect deviations from the model. This allows a sensitive detection of problems but the observation of normal operation might also be prone to false positive detections if the detectors are not configured appropriately.

  According to Stanley et al. [SA14] models of abnormal behavior are generally qualitative and need to capture more extreme changes in behavior. However, the transition between abnormal and normal operation modes could be ambiguous.
- **Static vs. dynamic models**: In dynamic models the behavior of system components is modeled over time. These models consider the order of events as well as time delays included. The synchronization of inputs can help to process data with static models that are much easier to handle in most cases.
- **Quantitative vs. qualitative models**: Quantitative models process numerical data in algebraic equations and differential equations. On the contrary, qualitative models do not include information on the magnitude of misbehavior detection. In qualitative model often terminologies are

used such as "large deviation in time" instead of numerical expressions. There are techniques, e. g. based on fuzzy logic, that translate between quantitative and qualitative models.

- **Compiled vs. first principle models**: The term "first principle" is used by Stanley et al. [SA14] to express the detection of faults based on fundamental models using physical laws or device implementations. Compiled models, however, are based primarily on the processing of empirical data involving "training" with measured data. The compile models are considered sometimes as blackbox because they process the same knowledge as first principle models but are generally not explicit, and hence cannot be easily inspected for accuracy and completeness.
- **Probabilistic vs. deterministic models**: Deterministic models do not consider the uncertainty of faults or misbehavior events. However, in real systems it is mostly reasonable to include a representation of uncertainty in order to consider inaccuracy and imperfection of system components, sensors, detection models, and diagnosis models. In related work different probabilistic approaches are described that base on the evidence theory of Dempster-Schafer, Bayesian Models or neural networks.

Fault Diagnosis Based on Causal Models An important piece of information in fault management is the relation between cause and effect. Causal models are a way to process this information. A causal model can be used to *predict* on the one hand events based on sensor measurements and to *infer* on the other hand a faulty sensor that is based on measured events. Figure 5.1 shows an example for the diagnosis using causal models. In this example it is assumed that C1 can be a possible cause of the (symptom) event E1 and E2 and C2 can be a possible cause of E2. That is, if E2 is true than at least one, C1 *or* C2 must be true. In addition only C1 can be a cause of the event E1.

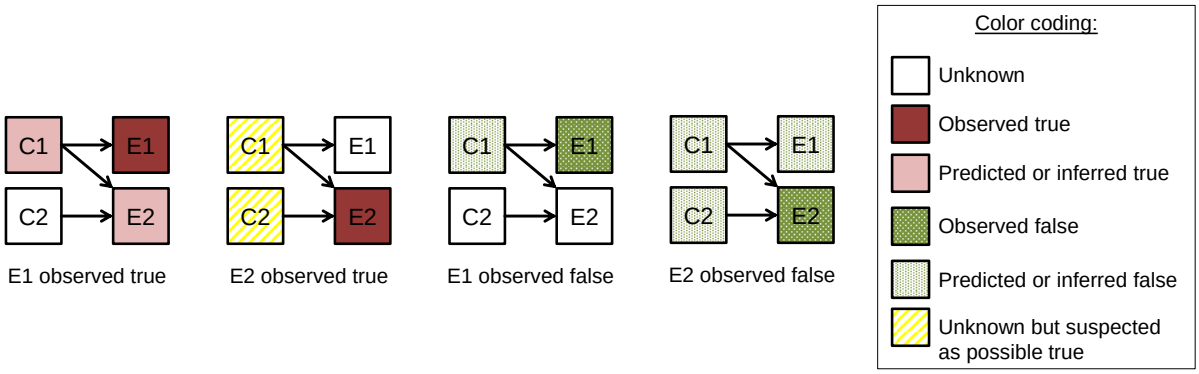


Figure 5.1.: Example of fault diagnosis using causal models according to Stanley et al. [SA14]

In the first case on the left hand side of Figure 5.1 the event E1 is observed to be true. Due to the OR connections between the cause and the event elements C1 is inferred to be also true. Knowing that C1 is true, it can be further predict that E2 is also true. A conclusion about C2 is not possible unless a single-fault assumption is taken for the causal model. In the second diagnosis example of Figure 5.1 event E2 is observed true. In this case no concrete conclusion can be made about C1 and C2. However, since one of them must be false, both are added to a group of suspects. In the third example E1 is observed false. Consequently, C1 can be inferred false but no further prediction about E2 can be made

due to the OR connections between the cause and the event. In the fourth example, E2 is observed false. Due to the OR connection to C1 and C2, both causes must be false. Therefore, if C1 is assumed to be false then E1 can be predicted to be false.

Fault Diagnosis Based on Probabilistic Models In addition to simple causal models more complex probabilistic models are used in the fault management to consider uncertainty [SA14,LWR03]. The uncertainty can be caused by imperfect observations, imperfect models, or missing observations. Dealing with uncertainty is essential for real world systems but could lead to undetected events (false-negative) and false events (false-positive). Defining the appropriate threshold is one of the most challenging tasks. A Bayesian network is a tool that can be applied to process cause-effect information if uncertainty is included. These systems start with prior estimates of failure probabilities for the root causes and determine the probability of each possible root cause, given the observed symptoms. In a Bayesian network every fault and symptom is modeled as a random variable with a probability distribution. When an observed symptom Y is input to the network, probabilities of every fault X are computed according to the Bayes rule shown in equation 5.1. The term $P(X|Y)$ denotes the posterior probability of fault X that can be computed when the likelihood $P(Y|X)$ and prior probability $P(X)$ is known.

$$P(X|Y) = \frac{P(Y|X) \cdot P(X)}{P(Y)} \tag{5.1}$$

In most related proposals in the context of VANET security, trust or reputation profiles are constructed that contain information about accused nodes based on measurements provided by local observer modules. Gerlach [Ger10] applies an Bayesian network to process observations locally on the node. The result of this local processing is a temporary database with trust information that can be used to identify misbehaving nodes. The beta distribution which is also based on Bayesian rules and introduced in Section 4.1.2.1, is commonly used to probabilistically calculate whether a node can be considered as benign or malicious [BB04, EB09, Ger10, SPC11]. However, this approach works best with periodic information updates that attest benign behavior (called *positive evidence*) or prove malicious behavior (called *negative evidence*). These periodic updates may be locally available but usually not at a central entity.

Mármol et al. [MP12] propose TRIP, a trust and reputation infrastructure-based framework that centrally collects reported reputation information for all nodes of the VANET. It has to be considered that the central infrastructure requires both positive and negative reputations in order to prevent the discrediting of benign network nodes. The central reputation database can be accessed on demand by vehicles via RSU connections to obtain reputation information from the infrastructure in order to support the local calculation of neighbor reputation. However, a specific proposal for the central processing of reported reputation is not given by Mármol et al. [MP12] since they focus on the local calculation of reputations.

5.1.4. Attacker Exclusion

A revocation of VANET nodes is described in related work that is based on the detection of irregular behavior. If a node should be excluded from the network then information about the nodes' credential has to be quickly distributed to every node in the network, for example as certificate revocation

list (CRL). According to Laberteaux et al. [LHH08] and Raya et al. [RMFH08] the exclusive distribution of CRLs by RSUs is in particular not suitable during the initial deployment phase when a dense network of infrastructure access points is probably not available. An alternative is the exclusion of vehicles by rejecting the request of new pseudonyms as first mentioned in technical project reports of NOW [Ger07b] and SEVECOM [Kun08]. This approach has been adopted and further substantiated by the C2C-CC in their PKI concept [BSS+11]. In both solutions the revocation or deactivation of vehicles has to be triggered by the identification of misbehavior.

5.1.5. Evaluation of Related Work

A collection of disadvantages and open problems in the context of global revocation in VANETs is provided by Lui et al. [LCH10]. Under the assumption that local misbehavior detection is not free of false positives and false negatives, the central attacker identification must also consider false accusations of benign nodes and undetected attackers. Consequently, an appropriate reporting of attackers is required but currently not specified or proposed (cf. Section 5.1.1). Mármol et al. [MP12] propose with their TRIP protocol the report of misbehavior to create a central database containing long-term node reputations. However, they did not consider the periodical change of pseudonymous identifiers in V2X communications. In this dissertation the detection and exclusion of attackers is addressed under consideration of drivers' privacy. However, approaches for privacy preserving pseudonym resolution are discussed in related work but these approaches burden the ad hoc communication by increasing packet sizes and complex infrastructure communication links. The author of this dissertation proposes an alternative lightweight protocol for conditional pseudonym resolution.

Even if the pseudonym resolution can be regarded as being solved, the proposal of Mármol et al. [MP12] does not consider the scalability of the central framework sufficiently. Their solution requires the periodic report of both positive and negative observations. Especially, the amount of reported positive data regarding node behavior dramatically increases with an increasing number of network nodes. Our proposed solution aims for central misbehavior evaluation and attacker identification considering scalability, changing pseudonyms and the report of false accusations. As far we know there is no related work that fulfill all these requirements.

5.2. Requirements for Central Misbehavior Evaluation

Based on the analysis in Section 4.4.3 requirements are listed in the following that have to be considered for the evaluation of detected misbehavior in order to identify the causer (i. e. attacker or faulty station).

- **Time between misbehavior detection and attacker identification**: Since most vehicles are probably not provided with wide area wireless mobile communications to arbitrarily establish a connection to the central infrastructure, the observed misbehavior has to be stored in the station's security subsystem until the data can be transmitted via RSUs. Moreover, the storage on the nodes may be limited so that the data of old detections might be overwritten by data of new detections and consequently some detections cannot be reported. When the central MEA receives a specific misbehavior detection event it should wait until other observers or involved nodes report

their related detections. Consequently, the central MEA has to be provided with information regarding how many reports can be expected for a known misbehavior event.

The goal of local misbehavior evaluation also differs from the goal of the central MEA. A local observer of misbehavior o has to rapidly decide which node is probably the attacker in order to ignore further messages from this suspect. A long-term collection of detections regarding a specific suspect is not reasonable and also may not be possible since the attacker can change the ID of the affected node as soon as o is out of the attacker's communication range. On the contrary, the central MEA aims for a long-term exclusion of attackers. As a result, the central MEA can collect sufficient evidence from independent reporters until a substantiated attacker identification can be performed.

- **Accuracy:** A reliable identification of an attacker is not possible by VANET nodes under the assumption that ghost vehicles are created by using different pseudonymous identifiers of the same node. Although the nodes can detect the misbehavior itself, reliable identification of the attacker is not possible because the different IDs of the attacker cannot be linked by a local misbehavior evaluation. A central entity, however, has the possibility to check whether different pseudonymous IDs belong to the same node. The main goal of the MEA is to generally reduce the number of false detections, be it false-positives or false-negatives.
- **Discrediting:** The false accusation of benign nodes has to be considered by the central misbehavior evaluation with high priority. If for example a node b is accused to misbehave by a node o, then it is necessary that this accusation is confirmed by other independent neighbors of b. Further, it is required to obtain the information from independent nodes that the observer o is a physically existing station and not a faked sender of reports created by an attacker. Colluding attackers $a_1, a_2, ..., a_n \in V$ are another threat that has to be considered by the central MEA.
- **Availability and Scalability:** Compared to the local misbehavior evaluation, a central MEA has to process the detections from all nodes of the VANET. As a result, the central evaluation has to be either scalable or dividable in order to consider a growing number of nodes in the network. The more nodes are on the road, the more misbehavior events are probably detected and transmitted.
- **Privacy:** Although the central MEA requires the ability to check whether different pseudonymous IDs belong to the same physical station, the privacy of all unconcerned nodes should not be affected. Especially the privacy of drivers must be preserved due to the partial resolution of pseudonymous IDs. The MEA requires only the information whether IDs a' and a'', contained in detected misbehaviors, e. g. $I_{oa'}(k)$ and $I_{oa''}(k)$, belong to the same owner. For the misbehavior evaluation it is not necessary to check the link of IDs from different misbehavior events that has been observed at different times and locations.

5.3. Misbehavior Reporting

Autonomously observed anomalies caused by attacks or critical traffic situations such as accidents are reported to a central MEA. Node-based plausibility checks are the basis for misbehavior detection reports that possibly accuse different nodes. The report structure has to be designed in a way that

accusations with low confidence are possible. For example, a plausibility check that is based on received second hand information (e. g. vehicle overlap checks) is not necessarily able to decide which of the involved nodes is causing the implausibility. Additionally, discrediting of benign nodes has to be considered in the misbehavior reporting strategy in order to satisfy the requirements of central misbehavior evaluation as listed in Section 5.2. In order to consider these requirements, a specific approach for misbehavior reporting is proposed by the author of this dissertation [BNPB12]. The novelty of this proposal is that some environment information of the attack scene can be stored in the report and signed evidence can corroborate the reported misbehavior detection. Misbehavior reporting is also a topic of international harmonization and standardization involving the ETSI (cf. TS 102 941 [ETS12b]), VSC3 CAMP [oTRA12], and IEEE [IEE13] in which the author of this dissertation is involved.

In the following, first the required elements of the report structure are discussed in Section 5.3.1. Subsequently, a description of related security aspects is provided in Section 5.3.2.

5.3.1. Structure of Misbehavior Reports

A misbehavior report (MR) is used to send information regarding potential misbehavior from distributed network nodes to a central MEA. In order to avoid that nodes are constantly sending MRs it is required that the detection mechanisms on the nodes are able to handle most false-positive detections locally. Only relevant detections should be sent to the MEA.

Generally, a report contains the type of detected misbehavior such as vehicle overlap, implausible movement or suddenly appearing station. In addition, the pseudonymous ID of the reporter node, a list of suspected nodes, and a list of neighbors surrounding the reporter can be included. The neighbors may be able to witness or refute an event as autonomous observers. Figure 5.2 shows the proposed MR structure.

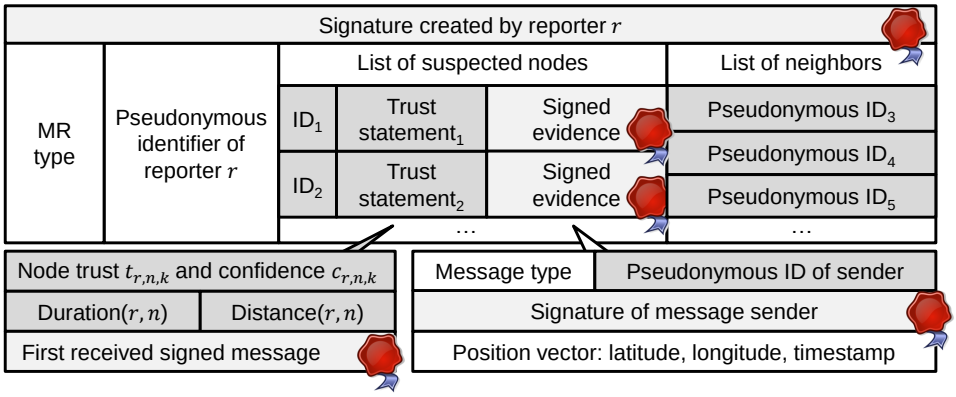


Figure 5.2.: Structure of misbehavior report (MR)

Every report contains an evidence of the observed event. For example, in the case of an observed relevant position overlap two signed CAMs are added proving the overlap of vehicle polygons as detailed in Section 3.5. The list of suspected nodes, e. g. the two overlapping nodes, and a list of relevant

one-hop neighbors are reported to the MEA by providing the respective pseudonymous IDs being used by the nodes at event time. Additionally, suspected nodes are evaluated by a trust statement.

This statement contains one pair of trust-confidence information per suspected node. The trust-confidence values are calculated by the local misbehavior detection system of the reporter. The node trust is the first element of a trust statement and models the subjective probability that a neighbor behaves as expected from the reporter's point of view. The *trust* that reporter $r \in V$ specifies regarding node $n \in V$ at time k is denoted as $t_{r,n,k} \in \mathbb{R}$ (cf. Section 4.3.2). The *trust* value in the MR is defined for the range $[0,1]$, where 0 denotes maximal distrust and 1 denotes maximal trustworthiness. The second element of a trust statement is the node trust confidence. It models the confidence regarding the node trust as specified in Section 4.3.3. The confidence value that node r assigns to the trust value of node n at time k is denoted as $c_{r,n,k} \in \mathbb{R}$ and comes within a value range of $[0,1]$.

Moreover, every trust statement of a suspected node is extended by a contact duration and the distance that a reporter and a suspect have been in common communication range. In order to confirm these distance and duration values a signed message such as a CAM has to be appended to the trust statement. Later on, the MEA can compare the position of this message with the position of the messages that evidence the observed event in order to verify the plausibility of given distance and duration values.

After the complete report is signed and encrypted by applying connectionless security mechanisms such as the elliptic curve integrated encryption scheme (ECIES) [IEE04] the report is sent to the central MEA. Consequently, the sender's and receiver's authentication is ensued as well as the integrity and confidentiality of the MR. If connection to the infrastructure is temporarily not available, the reporter can store the MR and postpone its transmission. The local MR storage on the stations should be sufficiently persistent and specific requirements regarding security or tamper protection should be specified in a real deployment. If a misbehavior is detected in a dense traffic scenario involving a large number of VANET nodes, the size of a MR can be limited by adding only relevant neighbors that can probably witness the observed misbehavior. Only selected one-hop neighbors should be added, prioritized by the distance between the respective neighbor and the location of the misbehavior. The probability that nearby neighbors have also detected the inconsistency autonomously is higher than for distant neighbors. This list of neighbors is relevant for the central MEA in order to decide whether a misbehavior event has really happened or an attacker is just using received messages from benign nodes to discredit them. In order to calculate the probability of a misbehavior event, the entropy can be reduced with more information regarding a same event from independent sources.

Due to the signed evidence that proves the misbehavior (e. g. a vehicle overlap), an attacker cannot create arbitrary events accusing benign nodes. Cooperative attacks with several malicious reporters are consequently spatially and temporarily limited.

5.3.2. Certification of Misbehavior Reports

When the central MEA receives a MR, the contained signatures are first verified by using the public keys of the related pseudonym certificates. If the certificates with the required public keys are contained in the MR, the verification can immediately be done. Alternatively, it is assumed that the MEA is permitted to request missing certificates from the PKI. In a second step, the evidence of the reported

misbehavior is checked by verifying the signature of contained V2X messages (cf. Figure 5.2). If for example an overlap scenario is reported, the misbehavior can be verified by comparing the position vectors of the appended messages with the algorithm proposed in Section 3.5.

Subsequently, all information of the appended neighbor list is verified by comparing the position vector of the first received signed message with the given duration and distance values. If the MEA detects a noteworthy difference the report is discarded and not used in the further evaluation process.

Additionally, the confidence $c_{r,n,k}$ of the trust statement is compared with the plausibility checked duration and distance. As a reminder, these duration and distance values indicate how long the two nodes has been located in common communication range. Assuming a linear increase of confidence with increasing duration and distance, Equation 5.2 is used to calculate a reference confidence value that should be consistent with the given confidence of the trust statement. This reference confidence value is calculated by the central MEA in accordance to the local calculation of confidence as described in Section 4.3.3. In contrast to Equation 4.10 that is used by the local nodes the central MEA can calculate only an estimated value for the distance based on the provided first received signed messages. The functions $duration(r,n)$ and $distance(r,n)$ in Equation 5.2 provide the contact time and the estimated commonly driven distance of node n and node r. The variables γ and δ determine the required values for minimum contact time and minimum traveled distance to get a maximum node trust confidence value. In order to be conform to the configuration of the local station's security subsystem (cf. Section 4.3.3), the following values are applied: $\gamma = 40$ seconds and $\delta = 1000$ meters.

$$c_{r,n,k} = min\left(1 \quad , \quad \frac{\frac{1}{\gamma} \cdot duration(r,n) + \frac{1}{\delta} \cdot distance(r,n)}{2}\right) \tag{5.2}$$

If the confidence in the trust statement of node n, reported by node r, is considerably larger than the calculated reference value of $c_{r,n,k}$, the misbehavior report should be discarded.

Duplicated reports from the same node are discarded as well even if different pseudonymous IDs are used. In order to check the independence of reporters, the MEA requires linking information of pseudonymous IDs. A protocol to request this information is described in Section 5.4 that considers relevant privacy protection requirements. After the verification of all signatures contained in the MR, a reduced report structure can be used for subsequent internal operations. This reduces the storage capacity required at the MEA.

The verified MRs are stored in order to collect enough reports from independent nodes that are involved or have observed an inconsistency related to the same event such as a specific overlap of vehicle positions. Having collected enough reports for an evaluation, a session object is created for every misbehavior scenario. The session maintains a list of suspected nodes and a list of reported neighbors that have witnessed the misbehavior events. Based on a policy, the number of required witnesses can be defined before starting further evaluation as detailed in Section 5.5.

5.4. Conditional Pseudonym Resolution for Misbehavior Detection

Protecting the location privacy of drivers is a major requirement in VANETs as defined in Section 2.2. As a solution, frequently changing pseudonymous IDs are applied in V2X packets to complicate the

long-term tracking of VANET nodes. In general, it should not be possible to link a pseudonymous identifier to its long-term identifier, neither by the nodes of the VANET nor by a single entity of the security infrastructure such as a CA of the PKI. However, in specific situations, conditional pseudonym resolution is required, for example in the case for central attacker identification. In this case, a MEA only needs to know whether messages with different pseudonymous IDs belong to the same physical station. In order to fulfill the requirements regarding pseudonym resolution, the *conditional pseudonym resolution algorithm* (CoPRA) is developed by the author of this dissertation [BPB13]. An implementation of CoPRA was integrated into a PKI implementation that follows the specifications of C2C-CC [BSS+11] and ETSI [ETS10c] in order to evaluate its applicability and performance. As far we know, CoPRA is the only protocol that has shown to be compatible with the European V2X PKI solution.

Using this protocol, pseudonym resolution information can be requested based on defined conditions, i. e. permissions and policies. Depending on the desired resolution information type, several independent authorities are involved in the process in order to avoid misuse. In addition, CoPRA does not decrease the performance and the security data overhead in wireless ad hoc communications as the size of certificates and therefore the message size remains untouched. The evaluation in Section 5.4.4 shows further that complexity and workload for pseudonym certificate issuance is not increased. Since the communication links between the vehicles and the PKI might be temporary and instable, the process of requesting pseudonym certificates should be realized connectionless oriented rather than based on complex sessions.

5.4.1. Privacy Preserving Pseudonym Resolution Protocol

The following protocol for pseudonym resolution aims to be applicable in different PKI environments to provide privacy preserving acquisition of pseudonym certificates and to enable conditional resolution of pseudonyms in specific situations. The protocol is divided into two processes: During acquisition of pseudonym certificates, resolution information is created and distributed as shown in Figure 5.3. Subsequently, authorized authorities are allowed to request pseudonym resolution information as depicted in Figure 5.5 and detailed in the related text. In this resolution process it is differentiated between identity resolution and resolution of pseudonym linkability.

In case of **identity resolution**, an authority A requests the vehicle identity id (e. g. the vehicle's long-term certificate identifier id_{LTC}, its license plate number, or the vehicle's identification number) that is related to a given pseudonym certificate PC. This identity resolution should be possible only in well defined cases, for example, if a law enforcement agency needs to know the identity of a vehicle after a hit-and-run accident. For this purpose, CoPRA can be used with a defined number of privacy protection authorities $PPA_1, ..., PPA_n$ or juridical institutions $J_1, ..., J_n$ that have to be involved in the process to request id_{LTC_v} and id_v with $v \in V$. For simplicity, only one instance of a PPA is considered in the following protocol.

In case of **linking resolution**, an authority A requires only the information whether pseudonymous IDs $id_{PC_{v'}}$ and $id_{PC_{v''}}$ with $v', v'' \in PI_v(k)$ belong to the same station $v \in V$ at arbitrary time k. We propose for this linkability resolution a Pseudonymous Long-Term identifier PLT that can be used by a misbehavior evaluation authority to identify stations that fake misbehavior events and misbehavior

reports. This kind of resolution may have lower privacy protection requirements since the long-term identifier id_V is not disclosed and PLT can change regularly. Nevertheless, privacy protection authorities $PPA_1, ..., PPA_n$ can also be integrated in the pseudonym linkability resolution process.

5.4.1.1. Pseudonym Certificate Acquisition

Basic protocols for requesting PCs from the PKI are described in the PKI design of the C2C-CC [BSS+11]. However, this published basic PKI design has not considered mechanisms for pseudonym resolution for misbehavior detection and active revocation. The authors of the C2C-CC PKI design [BSS+11] propose a split of powers between the enrollment authority (LTCA) and the pseudonym certificate provider (PCA) due to privacy protection requirements within the PKI. The ETSI [ETS12b] and IEEE [IEE13] protocols are extended in CoPRA to enable conditional and temporal restricted pseudonym resolution. An overview of the protocol is provided in Figure 5.3 and is further detailed in Figure 5.4. The numbers in both figures are related to each other. With this protocol the enrollment of vehicles as well as the acquisition of pseudonym certificates is realized. CoPRA applies the well-known idea of separation of duties [oTRA12, ETS10c] in order to ensure unlinkability of pseudonym certificates and, therefore, protect the identity of vehicles and the privacy of drivers.

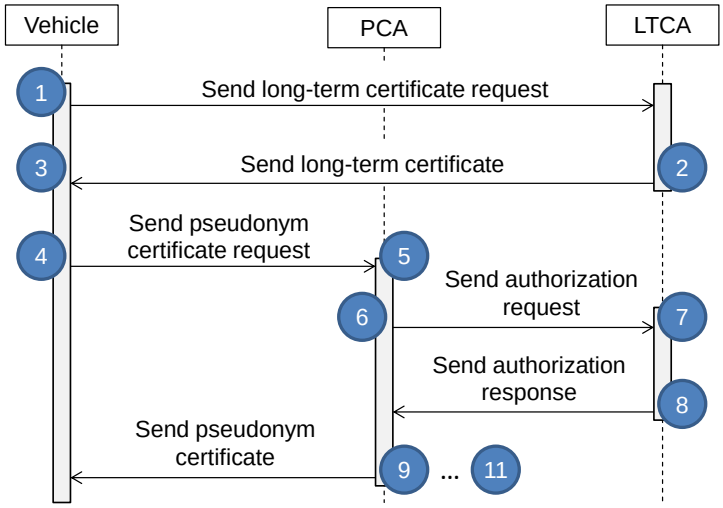


Figure 5.3.: Sequence of successful certificate acquisition

Enrollment phase Every vehicle of the VANET $v \in V$ has to be equipped with valid certificates in order to securely communicate with other ITS stations. Therefore, vehicle $v \in V$ has to be enrolled at a LTCA in order to get a valid long-term certificate LTC_v. Details of the enrollment should be left unspecified in this protocol as vehicle manufacturers may have specific solutions to register their ITS station in a secure manner.

(1) Nevertheless, in the first step the enrollment process should consider authentication, authorization, integrity, and non-repudiation of the requesting ITS station (i. e. vehicle or RSU) in order to prevent enrollment of malicious stations.

(2) If this is ensured the LTCA generates and issues in the second step a new long-term certificate LTC_v based on the given public key PK_{LTC_v}. A signature over a whole content with the private key SK_{LTCA} is indicated with $\sigma_{LTCA}(\circ)$. The resulting certificate is sent to v and can be used subsequently to request pseudonym certificates.

Enrollment phase:

$$Vehicle \rightarrow LTCA \quad : \quad (id_v, PK_{LTC_v}) \tag{1}$$
$$Vehicle \leftarrow LTCA \quad : \quad LTC_v = (PK_{LTC_v}, id_{LTCA}, \sigma_{LTCA}(\circ)) \tag{2}$$

Pseudonym acquisition phase:

$$Vehicle \quad : \quad req = (PK_{PC_v}, E_{PK_{LTCA}}(id_{LTC_v})) \tag{3}$$
$$Vehicle \rightarrow PCA \quad : \quad (req, \sigma_{LTC_v}(req)) \tag{4}$$
$$PCA \quad : \quad RId_{PC_v} = (\delta(PK_{PC_v}) \,||\, rand) \tag{5}$$
$$PCA \rightarrow LTCA \quad : \quad (\sigma_{LTC_v}(req), \delta(req), RId_{PC_v}, E_{PK_{LTCA}}(id_{LTC_v}), \sigma_{PCA}(\circ)) \tag{6}$$
$$LTCA \quad : \quad store(RId_{PC_v}, id_{LTC_v}, id_{PCA}) \tag{7}$$
$$PCA \leftarrow LTCA \quad : \quad (\delta(req), exp_{PC_v}, \sigma_{LTCA}(\circ)) \tag{8}$$
$$PCA \quad : \quad PC_v = (PK_{PC_v}, id_{PCA}, \sigma_{PCA}(\circ)) \tag{9}$$
$$PCA \quad : \quad store(id_{PC_v}, RId_{PC_v}, id_{LTCA}) \tag{10}$$
$$Vehicle \leftarrow PCA \quad : \quad PC_v \tag{11}$$

Figure 5.4.: Protocol showing successful issuing of long-term and pseudonym certificates

Pseudonym acquisition phase The protocol for pseudonym certificate acquisition has to consider the split of duties between enrollment authority (LTCA) and short-term pseudonym certificate provider (PCA).

(3) In the third step vehicle v creates a pseudonym certificate request that contains the public key of a securely generated asymmetric key pair (PK_{PC_v}, SK_{PC_v}) and the long-term ID id_{LTC_v} that is encrypted with the public key PK_{LTCA} of the LTCA using an Integrated Encryption Scheme (IES). The private key SK_{PC_v} is stored securely in the ITS station and must never leave it. In order to proof the knowledge of SK_{PC_v} and that the key pair is generated within a security device additional signatures are required according to the basic system standards profile of the C2C-CC [WBF+13]. For the sake of complexity these additional signatures are not considered in this protocol description.

(4) This request is signed with the long-term certificate proving identity id_{LTC_v} and, subsequently, sent to a PCA.

(5) The PCA generates a resolution identifier RId_{PC_v} related to the requested pseudonym PC_v by composing the hashed digest $\delta(PK_{PC_v})$ of the given public key PK_{PC_v} and a random *rand*. Inside the PCA domain, *RId* and PC_v has to be unique which is ensured by a database lookup. If a conflict is detected, the PCA recreate *RId* or PC_v with a different random value *rand* or a new generation timestamp, respectively. As the PCA is not able to verify the signature $\sigma_{LTC_v}(req)$ of the pseudonym request, due to the encrypted long-term ID id_{LTC_v}, the request is forwarded to the appropriate LTCA.

(6) This authentication request consists of the request signature $\sigma_{LTC_v}(req)$ created by v, a hash digest of the request $\delta(req)$ created by the PCA, the resolution ID RId_{PC_v}, and the encrypted long-term ID $E_{PK_{LTCA}}(id_{LTC_v})$. The PCA signs the authentication request with SK_{PCA} to prove its ownership. A signature over the whole message is indicated with $\sigma(\circ)$. The LTCA decrypts id_{LTC_v} using SK_{LTCA} and verifies $\sigma_{LTC_v}(req)$ with the appropriate public key PK_{LTC_v} to check the correctness of the pseudonym certificate request. Furthermore, the desired pseudonym certificate information such as expiration time and permissions of the station are checked by the LTCA.

(7) In case of positive verification, the resolution ID RId_{PC_v} is stored in a database of the LTCA linked to the respective long-term ID id_{LTC_v} and PCA identifier id_{PCA}. The verification result is further used to generate an appropriate response for the PCA.

(8) In case of successful verification, this response contains a hashed digest of the original pseudonym request $\delta(req)$ as well as expiration information exp_{PC_v} of the new pseudonym certificate. The whole response message is signed by the LTCA using SK_{LTCA} to prove the possession of the secret key.

(9) After verification of the returned authentication request, the PCA creates a new pseudonym certificate *PC*.

(10) The previously generated resolution ID RId_{PC_v} is stored in a database together with the related id_{PC_v} and id_{LTCA}.

(11) Finally, the pseudonym certificate PC_v is transmitted to the vehicle.

In order to protect the communication against manipulation and eavesdropping, all data transmitted between the entities are encrypted with an IES such as ECIES [IEE04] in the proposed protocol. In this encryption protocol, the sender of a message generates an asymmetric key pair $(PK_{s,r}, SK_{s,r})$ and a symmetric key $K_{s,r}$. This set of keys is only used to protect the message transport between a specific sender s and a receiver r in context of a distinct session. According to the IEEE 1363 standard [IEE04] the transmitted message is first encrypted with the symmetric key $K_{s,r}$, and subsequently $K_{s,r}$ is encrypted with the public key of the receiver PK_r. This strategy allows for connectionless oriented communication between the entities (i. e. vehicle, PCA, and LTCA in Figure 5.4) without establishing complex sessions with an exchange of several packets.

5.4.1.2. Conditional Pseudonym Resolution

Vehicles equipped with valid pseudonym certifi cates are able to use them in VANET communications. In case of misbehavior detection or critical traffic situations (e. g. car accidents) the resolution of the pseudonymous short-term identifier may be necessary. The protocol shown in Figure 5.5 and detailed

in Figure 5.6 allows either for the linking of different pseudonyms or for providing the respective long-term ID of a pseudonym.

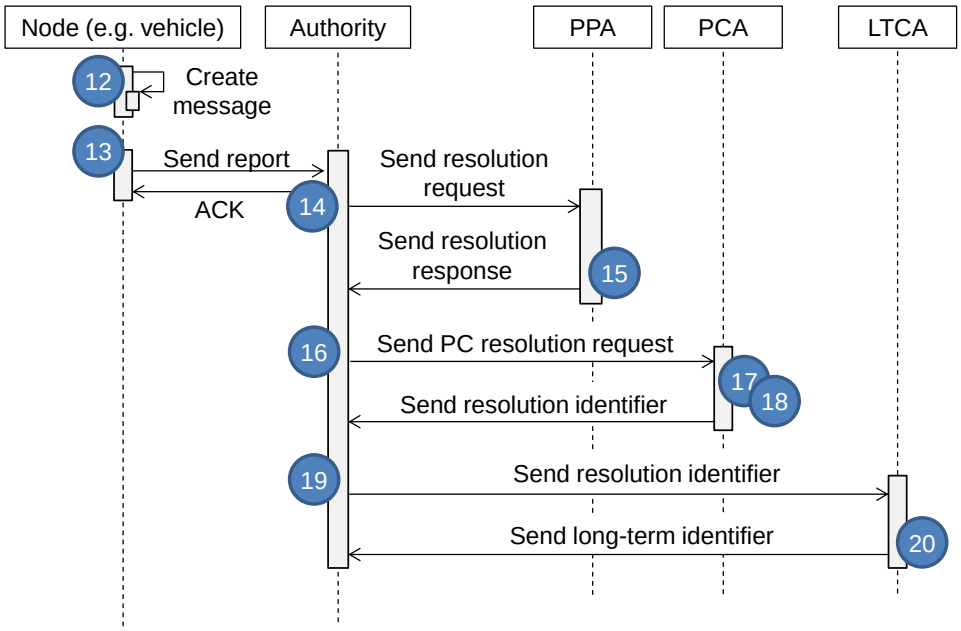


Figure 5.5.: Generic sequence of successful pseudonym certificate resolution

Based on policies, the LTCA is able to provide different resolution information to an authorized authority. A misbehavior evaluation authority *MEA* may need only temporary linking information of pseudonyms $PC_1, ..., PC_n$ in form of a pseudonymous long-term ID id_{PLT}. On the contrary, a law enforcement agency may need to know the non-pseudonymous long-term ID id_{LTC_v} of PC_v in order to request additional information id_v regarding $v \in V$. For the protocol shown in Figure 5.6, the request of the long-term ID id_{LTC_b} by an authority is assumed in which a PPA must be involved as attesting notary. During communication in the VANET, node a is able to record short-term IDs id_{PC_b} from received messages, whereby $a, b \in V$.

(12) If an event occurs, e. g. relevant misbehavior is detected, a message *msg* is created by node a in this step that contains the short-term ID id_{PC_b} of a node b which is involved in the related event. Additionally, a signed record of node b is appended to *msg* that motivates the pseudonym resolution. This could be for example a broadcasted message containing a position vector proving the location of b at the specific time. For simplicity, only one pseudonym is added in this step to the message that should be resolved. Depending on the purpose, additional short-term IDs with related records can be added to the message *msg*.

(13) Before the message is provided to the authorized authority, the whole message content is signed with the private key of a *PC* of node a as indicated by $\sigma_{PC_a}(\circ)$ in the protocol. The authority acknowledges the receipt of the report with a signed answer.

(14) Based on regulations defined in a policy the pseudonym resolution request must optionally be supported by other entities such as privacy protection agencies. If this support is needed, the

$$Node\ a \quad : \quad msg = (list(id_{PC_b}, record_b, \sigma_{PC_b}(record_b)), \sigma_{PC_a}(\circ)) \tag{12}$$

$$Node\ a \rightarrow Authority \quad : \quad msg \tag{13}$$

$$Authority \rightarrow PPA \quad : \quad (msg, id_{PC_b}, rt, \sigma_{Authority}(\circ)) \tag{14}$$

$$Authority \leftarrow PPA \quad : \quad res_{PPA} = (\delta(msg, id_{PC_b}), t_c, rt, \sigma_{PPA}(\circ)) \tag{15}$$

$$Authority \rightarrow PCA \quad : \quad (msg, id_{PC_b}, res_{PPA}, rt, \sigma_{Authority}(\circ)) \tag{16}$$

$$PCA \quad : \quad eRId = E_{PK_{LTCA}}(RId_{PC_b}, \delta(msg, id_{PC_b}), t_e) \tag{17}$$

$$Authority \leftarrow PCA \quad : \quad res_{PCA} = (\delta(msg, id_{PC_b}), eRId, rt, res_{PPA}, \sigma_{PCA}(\circ)) \tag{18}$$

$$Authority \rightarrow LTCA \quad : \quad (res_{PCA}, \sigma_{Authority}(\circ)) \tag{19}$$

$$Authority \leftarrow LTCA \quad : \quad (\delta(msg, id_{PC_b}), id_{LTC_b}, t_{exp}, \sigma_{LTCA}(\circ)) \tag{20}$$

Figure 5.6.: Protocol showing the successful conditional pseudonym resolution

authority extracts the pseudonym PC_b to be resolved and forwards the original message along with id_{PC_b} to the respective PPA. Furthermore, the desired resolution type rt (e. g. full identity resolution or pseudonym linking information) is appended. The whole request is signed with the private key $SK_{Authority}$ of the authority. Subsequently, the PPA verifies the signature with the public key $PK_{Authority}$ and checks whether the authority is authorized to request pseudonym resolution information from the PKI.

(15) If the PPA supports the resolution request, a digest δ of the request data is generated by using a hash function. Subsequently, the digest, the current time t_c, and the confirmed resolution type rt are signed and sent to the authority.

(16) After receiving the response from the supporting PPA, the authority signs msg, id_{PC_b}, and the confirmation from PPA with its private key $SK_{Authority}$. Subsequently, this signed data is sent to the PCA.

(17) If the PCA can successfully verify the signatures and permissions of the authority and the PPA, the appropriate resolution ID RId_{PC_b} is read from its database. In order to prevent misuse of RId_{PC_b}, it is encrypted with the public key of the related LTCA.

(18) Subsequently, the PCA generates a response with the digest of message msg and the pseudonym ID id_{PC_b} that should be resolved, the encrypted resolution ID RId_{PC_b}, and the confirmation of PPA. The whole response is signed and sent to the authority.

(19) When the authority receives the data from the PCA, the response res_{PCA} is signed by the authority and sent to the appropriate LTCA. The ID of the responsible LTCA can be extracted from the encryption header of $eRId$.

(20) First, the LTCA verifies all signatures and certificates from the authority, PPA, and PCA as well as their permissions included in the respective certificates. Afterwards, the LTCA checks that all contained digests $\delta(msg, id_{PC_b})$ are equal. The kind of pseudonym resolution is based on the type rt that must be confirmed by the PPA and the PCA. In the presented protocol a request for the long-term identity is assumed. Therefore, the LTCA provides the identifier id_{LTC_b} that

is linked to the given resolution ID RId_{PC_b}. The timestamp t_{exp} denotes the expiry date of the provided long-term identifier. In order to guarantee authenticity and integrity of this information a signature is created by the LTCA over the whole responded data, indicated by $\sigma_{LTCA}(\circ)$.

5.4.2. Security and Privacy Analysis of CoPRA

The following attacker analysis considers both a single attacker and multiple cooperating attackers that have access to pseudonymous information (e. g. PC_v, id_{PC_v} or RId_{PC_v}) but aim for obtaining uncontrolled access to the long-term information of a specific vehicle $v \in V$. Alternatively, attackers may aim to get only pseudonym linking information in order to track a specific vehicle within the VANET. We analyze the properties of privacy with respect to unlinkability of PCs and disclosure of long-term information. The privacy protection is mainly related to the cooperation level of involved entities.

CoPRA provides a flexible mechanism to conditionally resolve pseudonyms without affecting the privacy of other pseudonyms. Due to the split of duties, one entity alone cannot break privacy by linking arbitrary pseudonyms to the long-term certificate. Since PCA and LTCA can independently verify the correctness of requests according to local policies, malicious authorities cannot arbitrarily obtain resolution information. The following sets of authorities would have to cooperate in order to create an unauthorized request.

- PCA and LTCA are compromised and maliciously cooperate. If both CA types are compromised, an attacker could create a database in which both CAs collect linking information between issued PCs and related long-term certificates. In this case, both PCA and LTCA violate the PKI policy by not following the acquisition protocol shown in Figure 5.4. Security mechanisms have to ensure that PKI operators are not able to manipulate certified software implementations or install malware.
- The authority (e. g. MEA), the PPA, and the PCA are compromised and maliciously cooperate. Assuming that the PCA is compromised, arbitrary resolution IDs could be requested by a malicious MEA implementation. Security mechanisms have to be applied that ensure the integrity of MEA and PCA software implementations. In addition, the application of several independent monitoring instances is proposed, i. e. $PPA_1, ..., PPA_n$.
- A vehicle $v \in V$, the authority, and the PPAs are compromised and maliciously cooperate. The report of fake events created by node v is considered, since resolution information is provided based on the event type. Only misbehavior reports *msg* containing a signed record should be usable to request pseudonym linking information. If a resolution to the long-term ID is requested, for example in the case of a hit-and-run offense, additional support by external authorities such as $PPA_1, ..., PPA_n$ as well as manual interaction should be dictated by the MEA policy. The latter case is not further considered in this dissertation.

The central PKI entities must further be resistant against relevant threats such as replay attacks and denial of service (DoS) attacks. In addition, the general protective goals of security, i. e. confidentiality, integrity, authenticity, authorization, non-repudiation, availability, and revocation have to be considered.

- **Confidentiality** We recommend to encrypt all data while it is transmitted between the entities in order to ensure its confidentiality. For infrastructure entities and vehicles with cellular network

connection it is reasonable to apply transport layer security such as SSL to establish a secure channel that is used to transmit all data. If the vehicles have to transmit their misbehavior reports via RSUs it is reasonable to encrypt single reports with the asymmetric pseudonym keys applying an integrated encryption scheme such as ECIES [IEE04]. In this case the previously encrypted packets can be directly transmitted as soon as a RSU comes into communication range of the vehicle.

- **Data Integrity** The integrity of transmitted data between all entities has to be protected. In both cases, if transport layer security or an integrated encryption scheme is applied, a message authentication code is used to protect the message integrity.
- **Authenticity** The authenticity of all entities is ensured with digital certificates. The entities of the PKI and the misbehavior evaluation infrastructure are equipped with certificates issued by the root CA. The vehicles and roadside stations are equipped with pseudonym certificates issued by a PCA. Both, the classical certificate formats such as X.509v3 and the VANET specific formats such as ETSI TS 103 097 [ETS13b] or IEEE 1609.2 [IEE13] allow to include application specific permissions. Based on a certification policy and permissions included in the certificate a specific role is assigned to the certificate holder. In the secure connection establishment or in the decryption process of received reports the authentication and authorization of the communication endpoints is verified.
- **Non-repudiation** The non-repudiation of an origin is ensured by digital certificates. As long as the messages are signed and the related private key is not compromised or maliciously excluded the messages can be assigned unambiguously to a single entity. The non-repudiation of the receipt of a message is ensured between a VANET node and the MEA by a signed acknowledgment of received misbehavior reports. If the node do not receive the acknowledgment it must assume that the report is not transmitted successfully. The communication between the infrastructure entities is secured by transport layer security that ensures the non-repudiation of message receipt.
- **Revocation** The revocation of certificates is applied to exclude attackers or compromised entities. According to the PKI design of the C2C-CC [BSS+11] entities of the security infrastructure such as LTCA, PCA, MEA, or PPA are actively revoked by utilizing CRLs. Nodes of the VANET, however, are passively excluded by issuing certificates with a short lifetime.
- **Availability** The availability ensures that legitimate users of the service have in general access to that service. DoS attacks should be limited in order to increase the availability of CoPRA. In our proposal digital signatures are used in combination with the revocation of certificates to limit DoS attacks. In particular, requests and responses are only accepted and processed if the message signature and the sender's certificate is valid and not revoked. Therefore, an attacker must spend cryptographic effort in signing operations to mount a DoS attack. Indeed, an attacker could flood the authorities with invalid signed messages. As a result, sender certificates are handled first and untrusted senders are processed with low priority.
- **Replay Protection** The replay of resolution requests sent by external attackers is detected and directly filtered out at all entities. A digest $\delta(msg, id_{PC_b})$ is used in this case as unique identifier of a resolution task, having involved vehicle $b \in V$. It has to be further considered that the $record_b$, which is part of a message msg, contains variable location data and timestamps. Finally, the

integrity and confidentiality of transmitted data between vehicles, authorities, PPAs, PCA, and LTCA is ensured.

5.4.3. Comparison of Pseudonym Resolution Protocols

In this section we provide a comparison of related schemes considering most relevant aspects such as the enlargement of pseudonym certificates and overhead in PC acquisition and PC resolution by means of computation and data size. Table 5.1 subsumes the comparison of CoPRA with related schemes that are proposed for pseudonym resolution in the context of misbehavior detection in ITS communications. An overview and introduction of the related protocols V-Token, SRAAC, and CAMP is provided in Section 5.1.2.

In the first row, the effect of pseudonym resolution is compared by means of overhead in pseudonym certificates. Since PCs are appended to messages in the wireless communication, the overhead should be optimized to a minimum. This parameter is most relevant from communication architecture perspective. The second row shows the amount of data that needs to be stored at the CAs in order to support

Table 5.1.: Comparison of Pseudonym Resolution Schemes for VANETs

Topic of comparison	**V-Token** [SKMW10]	**SRAAC** [FAEV06]	**CAMP** [WWKH13]	**CoPRA** [BPB13]
Overhead in PCs	$\geq$ 61 Bytes	0 Bytes	8 Bytes	0 Bytes
Certificate acquisition overhead at CA	0 Bytes per cert.	$\geq$ 64 Bytes per cert.	$\geq$ 44 Bytes per cert.	$\geq$ 8 Bytes per cert.
Performance relevant algorithms in the cert. acquisition process	DSS encryption operation	shared secret interpolations (e. g. [Sha79])	no additional overhead	no additional overhead
Certificate acquisition connection type (vehicle $\leftrightarrow$ PCA)	connection oriented (blind signature) [Cha88, JJM07]	connection oriented (MI-DSS*)[1]	connectionless oriented	connectionless oriented
Resolution overhead within the PKI	$\geq$ 61 Bytes	$\geq$ 64 Bytes	$\geq$ 32 Bytes	$\geq$ 1 KB
Performance relevant algorithms in the cert. resolution process	shared secret interpolations (e. g. [Sha79])	shared secret interpolations (e. g. [Sha79])	DSS sign and verify operations	DSS sign and verify operations

pseudonym resolution. In contrast to the V-Token protocol, SRAAC, CAMP, and CoPRA manage the resolution information centrally by storing data in a database. In the third row, the performance relevant algorithms are compared that are applied in the certificate acquisition process. In this comparison, only operations are considered that are necessary to add resolution information in form of a *V-Token* in [SKMW10], a *Tag* in SRAAC [FAEV06], a *Linkage Value* in CAMP [WWKH13, oTRA12] or a *Resolution-Id* in CoPRA. The V-Token concept applies cryptographic operations based on the digital

[1] Jakobson's magic-ink signatures with DSS are described in [Jak97]

signature standard (DSS), and SRAAC uses cryptographic shared secret interpolations. Consequently, these concepts create significant overhead in the acquisition phase. However, both concepts provide protection against colluding PCAs and LTCAs. This protection can not be cryptographically achieved with CoPRA since no cryptographic operations are entailed for the generation and storage of resolution information. The CAMP solution proposed by the U.S. Department of Transportation is comparable with CoPRA. In this approach resolution information is stored at dedicated linkage authorities (LAs). The LAs, however, have no information about the long-term information of the vehicles and the LTCA gets the *Linkage Value* only in encrypted form. The CAMP approach is designed to revoke pseudonyms in case of misbehavior detection. According to Whyte et al. [WWKH13] a long-term ID of a misbehaving station can only be set to an internal black list but is not provided to a MEA. The type of connection required between vehicle and pseudonym certificate provider (PCA) is compared in the fourth row. According to Section 5.4 the request of pseudonym certificates from the PKI should be connectionless oriented. This allows interruption of pseudonym acquisition with later continuation. In the last two rows, the communication overhead and performance-relevant cryptographic protocols in the resolution process are compared.

As shown in Table 5.1 the application of CoPRA does not affect wireless vehicular communication performance since no additional data is added to pseudonym certificates. Also no additional cryptographic operations are introduced in the pseudonym acquisition phase. For evaluations of CoPRA a testbed PKI implementation based on IEEE 1609.2 [IEE13] was used with LTCA - PCA server separation, running on a quad core CPU with 2.7 GHz. Using this environment, the processing of one pseudonym certificate request takes 179 ms at the CAs, and a request with 50 public keys can be processed within one second.

Avoiding additional delay in the pseudonym acquisition phase is important since every vehicle in the network requires at minimum 1500 pseudonym certificates per year [BSS+11]. The storage of resolution information is in the magnitude of megabytes and, therefore, not critical for PKI operation. In case of pseudonym resolution several bytes of data have to be transmitted between involved entities and several signing and verification processes are required when CoPRA is applied, cf. rows 5 and 6 of Table 5.1. However, it is assumed that the conditional resolution of pseudonyms is rarely performed compared to the pseudonym acquisition process. Consequently, CoPRA is the optimal choice if resolution information inside certificates must be omitted due to low overhead requirements, connectionless certificate acquisition is required and resolution operations are rarely performed. The CAMP approach described by Whyte et al. [WWKH13] is comparable with CoPRA but it only fits in with the specific public key architecture of the American CAMP project [oTRA12]. Our proposal is designed to be compatible with the European PKI approach published by ETSI [ETS12a, ETS12b] and the C2C-CC [BSS+11].

5.4.4. Performance Analysis of Pseudonym Resolution

Applying a testbed implementation, the performance of pseudonym resolution with CoPRA is analyzed in the following. Figure 5.7 shows the latency in milliseconds of pseudonym resolution processes. On the x-axis, the number of pseudonyms to be resolved, contained in a single request, is increased. According to Section 5.3.1 a misbehavior report typically contains several pseudonymous identifiers id_{PC}

from different stations, i. e. reporter, suspected nodes, witnesses. In this evaluation the performance of linkability resolution of involved pseudonyms is analyzed.

In Figure 5.7, the measured latency at involved PKI entities is shown. According to the protocol described in Section 5.4.1.2 the MEA assembles the pseudonym resolution request and subsequently sends it to the PCA. In a next step the PCA checks the content of the request by verifying the contained misbehavior report with included CAMs. This step mainly causes the increase of latency at the PCA with increasing number of desired PC resolutions. We analyzed that the increase of latency is linear. Every additional PC in the resolution process adds approximately 45 ms. The remaining operations at the MEA and LTCA are relatively constant. General overhead for every pseudonym resolution is introduced by DSS operations in the protocol. Every message between MEA, PCA, and LTCA is signed and encrypted at the sender and decrypted and verified at the receiver using ECC-256 and ECIES according to IEEE 1609.2 [IEE13].

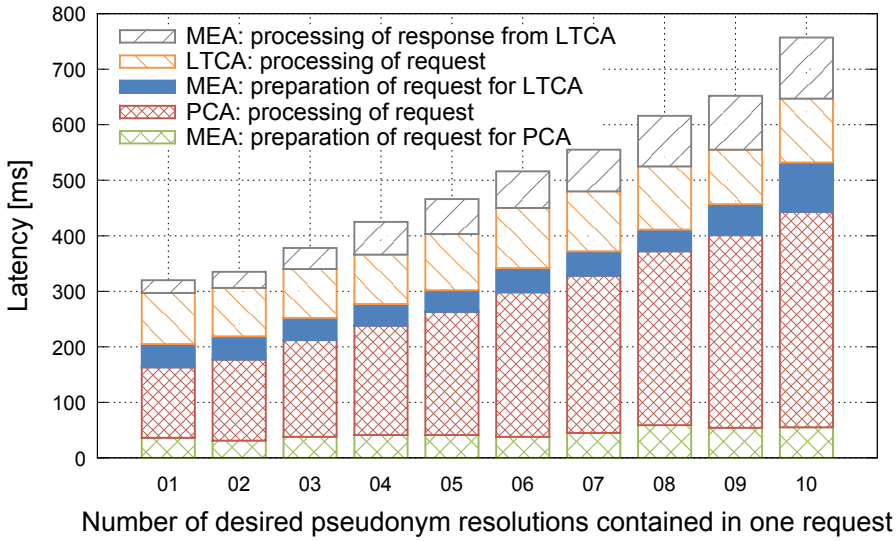


Figure 5.7.: Latency in the pseudonym resolution process using CoPRA

In summary, CoPRA avoids additional data overhead in pseudonym certificates and does not create significant latency in the pseudonym certificate acquisition process. As discussed in Section 5.4.2 the privacy of vehicles that are not involved in misbehavior events is not affected and for involved vehicles only the linkability of pseudonymous certificates is resolved temporarily. Furthermore, the proposed solution is resistant against relevant security attacks such as discrediting of benign nodes and replay attacks. A performance analysis based on a prototypical implementation shows finally that a conditional pseudonym resolutions can be done in acceptable time. Since MRs of different observers may be received at different times in the magnitude of minutes or hours the performance requirements for pseudonym resolution are relaxed.

5.5. Evaluation of Suspected Nodes

Based on reported misbehavior and the conditional pseudonym resolution protocol a central identification of attackers is proposed by the author of this dissertation. We propose a three step mechanism to evaluate misbehavior reports and suspected nodes with a central MEA.

a) Verification of received evidence (cf. Section 5.5.2)

b) Aggregation of syndromes (cf. Section 5.5.3)

c) Assessment of suspects (cf. Section 5.5.4)

These mechanisms were developed by the author of this dissertation [BNPB12]. Joël Njeukam has implemented and evaluated the concept of suspect assessment by simulating benign and malicious misbehavior reporting vehicles as part of his Master thesis [NSKB11] which was supervised by the author of this dissertation. Based on the software, developed in this Master thesis, the concept was refined and further evaluated within this dissertation.

The novelty and benefit of our approach is that we focus on the long-term perspective to permanently exclude attackers and faulty nodes from active V2X communications. Most related work focus on the local short-term exclusion of misbehaving nodes. Together with our approaches for misbehavior reporting (cf. Section 5.3) and conditional pseudonym resolution (cf. Section 5.4) the mechanism discussed in this section aims to identify the responsible nodes, based on the fundamentals of fault diagnosis.

The central evaluation of suspects benefits from misbehavior observations sent by different independent nodes. In contrast to the local attacker identification, the central MEA can collect misbehavior reports over a long period of time and is furthermore able to access pseudonym resolution information.

In the following subsections notations are used as defined in Section 5.5.1. In Section 5.5.2 the evidence provided by misbehavior reports is analyzed as described and processed with mechanisms based on fault diagnosis as detailed in Section 5.5.3. In addition, reported trust statements of suspects are analyzed in order to assess the involved nodes as explained in Sections 5.5.4 and 5.5.5. The evaluation of our concept is discussed in Section 5.5.6 and a security and vulnerability analysis is provided in Section 5.5.7.

5.5.1. Notations

Nodes of a VANET are elements of a set V according to the notations defined in Section 4.4.1. In addition to these notations the following donations are used in this chapter.

- S: Denotes a set holding reported information regarding a misbehavior scenario. A session can consider different types of misbehavior that are reported for a similar time and location.
- S_{MR}: Set containing MRs according to the description given in Section 5.5.2
- V_S: Set of nodes that are involved in S_{MR} as reporters, suspects or witnesses
- $V_{S_S} \subseteq V_S$: Set of nodes that are involved as suspects in S_{MR}
- $V_{S_R} \subseteq V_S$: Set of nodes that are involved as reporters in S_{MR}

5.5.2. Verification of received evidence

Due to limitations of the communication range in VANETs, shadowing effects or missing possibilities of sending reports to the infrastructure, the central MEA may not be able to obtain all misbehavior reports from nodes that are involved in a session. Furthermore, attackers who aim to discredit benign nodes by sending fake MRs should be detected. The following considerations are checked before starting the evaluation of a session as discussed in Sections 5.5.3 and 5.5.4.

a) **Satisfying independent reporters:** Either all suspected nodes have reported respective MRs or sufficient independent witness reports must be gathered by the MEA. If for example a witness node w_1 detects and reports a position overlap of its neighbors a and b at time k, it is necessary that respective reports from nodes a and b concerning the same overlap at time k are obtained by the MEA. This scheme aims to avoid blacklisting of benign nodes and, as a consequence, force colluding attackers to spatially and temporarily synchronize their attacks. As a result, the effort for colluding attacks increases with every additional cooperating malicious node required for a successful attack.

b) **Confirmation of misbehavior by witnesses:** A received MR, stating a misbehavior that suspects nodes a and b at time k (e. g. to overlap each other), has to be confirmed by witness nodes w_i with $i = 1, ..., n$ with $n \in \mathbb{N}$. Determining the value of n is further discussed in Section 5.5.6 and is addressed by Petit et al. [PFK11].

We propose that syndromes reflecting different kinds of detectable misbehavior should have different weights. For example, the violation of the maximum communication range (MCR) or the observation of violations of plausible movement (PM) provide probably higher evidence for misbehavior than a violation of a map related position (MRP) or a vehicle overlap (VO) detection. We propose to assign a weight to every kind of reported syndrome. If a node reports an observed misbehavior as witness then the weight should be lower compared to a misbehavior where a reporter is actively involved. This is relevant in particular for vehicle overlap detections. In a next step, the conditional pseudonym resolution is utilized to filter multiple reports sent by the same node. Subsequently, the received reports are assigned to a session under consideration of location and time of the observed misbehavior. The nodes are extracted from the MRs and are assigned to the sets V_S, V_{S_S}, and V_{S_R}.

In order to check if sufficient reports were gathered for one of the suspects $s \in V_{S_S}$ the weights of syndromes related to the MRs of the session are added up per suspect. If the sum is larger than a threshold it is assumed that satisfying independent reporters are involved to allow an identification of the attacker or faulty node. The configuration of the syndrome weight and the threshold is related to assumptions and experiences about having cooperating attackers that aim for discrediting benign nodes.

In Figure 5.8 an example is shown concerning the verification of received evidence. There are four MRs sent by different reporters that are related to observed misbehavior of a node a. MR_1 reports a vehicle overlap of node a and b whereby either a or b is the reporter. MR_2 and MR_3 consider the same overlap of node a and b but these reports are sent by witness nodes that are not actively involved in the overlap. As already mentioned, reports that contain the reporter as suspect should be weighted higher than reports sent by witnesses. The fourth report MR_4 shows an implausible movement of node a. Whenever another report is received and added to the session the sum of weights for the affected

suspects are updated. If the sum is larger than the predefined threshold, the processing of the session is continued with the aggregation of syndromes.

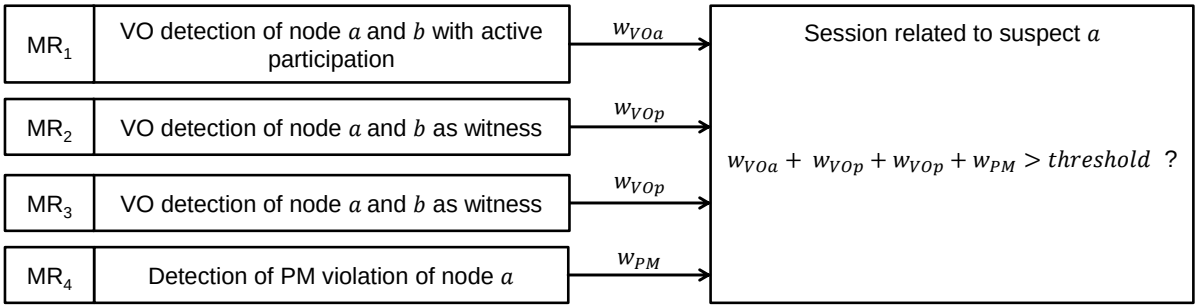


Figure 5.8.: Example of received evidence associated to one suspect of a session

5.5.3. Aggregation of Syndromes

In the aggregation process of syndromes we propose to apply a causal model. The reports contain evidence about a misbehavior event which should result in a binary decision whether the misbehavior has happened or is bogus. As introduced in Section 5.1.3 fault diagnosis models have different properties. Our causal model for syndrome aggregation is a static model since all misbehavior reports related to similar time and location are combined in a session having a set S_{MR}. The reports of each session are processed subsequently in a static way. It is, for example, not relevant if first an implausible movement is detected and subsequently a vehicle overlap or vise versa. In addition, time delays and lags in the reporting of misbehavior are not relevant for the diagnosis as long as the time synchronization is ensured in the local detection process on the VANET nodes. The syndrome aggregation method applies further a quantitative model to process first principle observations of abnormal behavior. A qualitative model is not necessarily needed as long as a representation for humans is not required. For the aggregation of syndromes we propose to apply a deterministic causal model. The nodes of the network process the location-related information and filter observed events with high uncertainty. Nevertheless, the uncertainty concerning observed misbehavior is considered by trust statements provided for every suspected node. After the aggregation of syndromes the assessment of suspects is computed based on these trust statements as further detailed in Section 5.5.4. The proposed concept for central misbehavior evaluation is utilizing a hybrid approach considering deterministic and probabilistic models.

After the MEA has verified that sufficient reports from independent observes are received a causal model is applied to aggregate the syndromes (detected and reported misbehavior). In the optimal case, this process confirms that one suspect node in the set V_{S_S} is inferred to be the cause of the syndrome. However, it might happen that not a single node of the set V_S is inferred to be the potential cause.

If, for example, a vehicle overlap is observed two signed messages with corresponding position vectors should prove the overlap. In the same way, a PM violation should be attested by two signed messages that show the position jump based on location and time. Considering the example used in Section 5.5.2 and illustrated in Figure 5.8 the report of vehicle overlaps create an *ambiguity group* containing both nodes. A diagnosis of this syndrome, shown on the left hand side of Figure 5.9, creates

such an scenario. In this example the nodes *a* and *b* are part of the *ambiguity group*. If there is another report in the session S_{MR} that proves a PM violation of suspect *a* then this node is inferred to be the responsible node as long as only a single cause is assumed. However, in the context of misbehavior detection in VANETs multiple causes must be assumed to be possible. If cooperating physical attackers create ghost vehicles in a session then all attackers should be identified. As a result, the status of the suspect is not changed from suspected to unknown as shown in the lower part of Figure 5.9. It has to be considered that only nodes are suspected and therefore element of V_{S_S} if sufficient independent reports are received as discussed in Section 5.5.2.

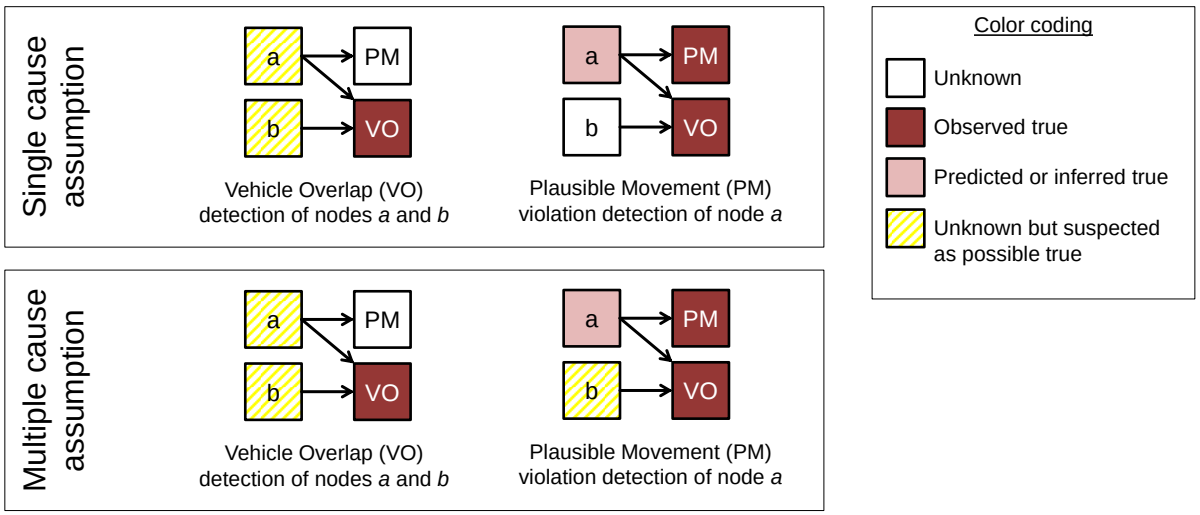


Figure 5.9.: Fault diagnosis using causal models for misbehavior detection in VANETs

5.5.4. Assessment of Suspected Nodes

As soon as sufficient evidence is collected from independent observers and the syndromes are aggregated an assessment of the suspected nodes is performed. If there is only one suspect which means that the responsible node can be unambiguously inferred from the misbehavior reports it is expected that the assessment confirms the inference. Otherwise, the suspect should not be considered as attacker or faulty node. If there are multiple suspects this assessment process is required to identify the responsible node assuming a majority of benign reporters. In the central suspect evaluation process the reported trust values $t_{r,n,k}$ with the associated and verified node trust confidence $c_{r,n,k}$ values gained from misbehavior reports of a session set S_{MR} are processed.

When the nodes are extracted from received reports and assigned to a session S_{MR}, then the time information k can be ignored in subsequent aggregation operations, cf. Section 5.5.2. Within a session S_{MR}, all misbehavior reported by the nodes relate to the same event with respect to time and location. Based on the tuple of $(t_{r,n}, c_{r,n})$ the assessment of suspected nodes is performed with two equations. The applied Equations 5.3 and 5.4 are based on strategies for trust and confidence value aggregation, defined by Ebinger and Bißmeyer [EB09].

Trust Value Aggregation The aggregated trust t_n and confidence c_n values related to a suspected node $n \in V_{S_S}$ are calculated using the reports of node $r \in V_{S_R}, r \neq n$. The aggregation of multiple trust estimations must have the following properties.

- The trust values should be weighted in the aggregation process according to its related node trust confidence value. If the confidence is close to 1 the associated trust value should be considered much. Otherwise, if the confidence is close to 0 the trust value should be considered less. If the confidence is equal to 0 then the trust value should be ignored.
- The values provided by the reports should be handled equally. A pair of trust and confidence provided by a reporter $r1$ should not be handled differently than a pair provided by a reporter $r2$.
- The resulting value for trust must be in the range $[0,1]$.
- If all node trust confidence values are 0 then the aggregated trust t_n should be considered to be irrelevant.

In Equation 5.3 different trust values considering the same suspected node $n \in V_{S_S}$ are combined. The numerator ensures the weighting of trust values with the associated confidence value by multiplying each trust value with its associated confidence value. Subsequently, the sum of these values is divided by a sum of confidence values that is provided by the session reporters. This sum of confidence in the denominator is used for normalization in order to ensure that the results of the function are in the range $[0,1]$. Equation 5.3 can only be applied if the sum of confidence values in the denominator is larger than 0. If this is not the case, we define $t_n = 0$ irrespective of the trust values in the nominator.

$$t_n = \frac{\sum_{r,r\neq n}^{V_{S_R}} t_{r,n} \cdot c_{r,n}}{\sum_{r,r\neq n}^{V_{S_R}} c_{r,n}}, \quad n \in V_{S_S} \tag{5.3}$$

Trust Confidence Value Aggregation Equation 5.4 shows the aggregated confidence of a node $n \in V_{S_S}$ calculated from a combination of values from all reporters of a session. The aggregation of multiple node trust confidence estimations must have the following properties.

- The resulting node trust confidence should be high if the associated trust values from all reporters agree on each other. If, for example, one reporter provides high trust close to 1 in node $n \in V_{S_S}$ and another reporter provides low trust close to 0 then the resulting confidence should reflect this disagreement. On the contrary, if the trust values confirm each other than the confidence should increase accordingly.
- The values provided by the reports should be handled equally. A pair of trust and confidence provided by a reporter $r1$ should not be handled differently than a pair provided by a reporter $r2$.
- The resulting node trust confidence must have values in the range $[0,1]$.

The formula shown in Equation 5.4 ensures that the confidence increases if the different nodes agree on similar trust levels (i. e. the gap between trust values is small) and the reverse if the opinions differ a lot (i. e. trust value differentials are high). The cardinality $|V_S|$ in the denominator defines the number of different reporters r of a session that have evaluated node n. The fraction in the first bracket expresses the mean value of differences between all trust values. A small mean difference in the trust values should result in a large factor. As a consequence, this mean difference is subtracted from 1 in order to get the final factor. This factor is then multiplied by the sum of confidence values $\sum_r^{V_S} c_{r,n}$. The

resulting factor on the right hand side is limited to the maximum node trust confidence 1 in order to ensure normalization of the result.

$$c_n = \left(1 - \frac{\sum_{r,r' \in V_{S_R}, r \neq r' \neq n}^{V_{S_R}} |t_{r,n} - t_{r',n}|}{|V_{S_R}| \cdot (|V_{S_R}| - 1)}\right) \cdot min\left(1 \ , \sum_{r,r \neq n}^{V_{S_R}} c_{r,n}\right), \quad n \in V_{S_S} \tag{5.4}$$

Since all required properties are fulfilled by Equations 5.3 and 5.4 the formulas, proposed by Ebinger and Bißmeyer [EB09,Ebi13], are appropriate for the aggregation of trust confidence pairs in the context of attacker identification.

In the final assessment process of suspected nodes, the MEA combines the previously calculated values for trust and confidence. Suspects with an assessment value below a defined threshold are considered as attacker or faulty node and are consequently excluded from the VANET. The assessment function, shown in Equation 5.5, multiplies the trust and confidence values using Equations 5.3 and 5.4 as input. The higher the confidence value c_n the more the trust value t_n is considered for a suspect $n \in V_{S_S}$. Suspicious nodes with low confidence values around 0 result in neutral assessments $a \approx 0$.

$$a_n = t_n \cdot c_n \tag{5.5}$$

Assuming a benign majority of reporters perform well specified and accurate local misbehavior detections, a ghost vehicle is rated with a negative trust value and a real vehicle is rated with a positive trust value.

5.5.5. Discussion of Node Assessment for Misbehavior Evaluation based on an Example

Based on an example the node assessment for misbehavior evaluation is discussed in this section. The adversary scenario at time frame $K = \{k_0, k_1\}$ depicted in Figure 5.10 is used to discuss the node assessment process. According to this scenario the nodes $o_1, o_2, o_3, o_4, o_5 \in N_a(k), k \in K$ are in communication range of node a. Node o_1 and o_2 are actively involved in a vehicle overlap event with the ghost vehicle $a', a'' \in PI_a(k), k \in K$. Nodes o_3, o_4, o_5 passively and autonomously observe the vehicle overlap events. It is assumed in this example that the central MEA has received misbehavior reports from $o_1, o_2, o_3, o_4, o_5, a', a'' \in V_S$ whereby o_1 and o_2 are also suspects $o_1, o_2 \in (V_{S_R} \cap V_{S_S})$ and the other vehicles are only reporter, i. e. $o_3, o_4, o_5 \in (V_{S_R} \setminus V_{S_S})$. The reports contain the two overlapping nodes and the remaining nodes are attached as witnesses to the list of relevant neighbors. If a sufficient

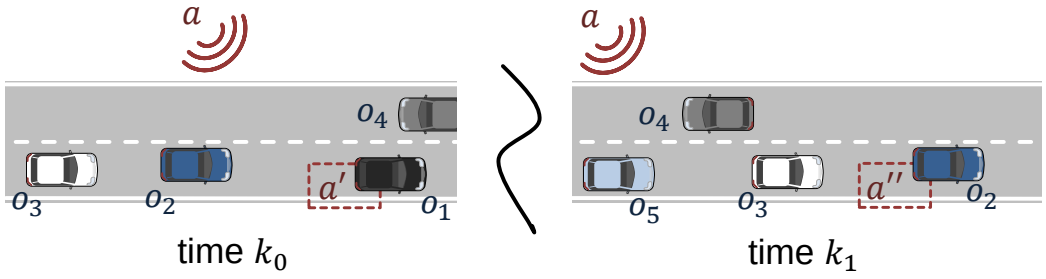


Figure 5.10.: Example of location-based attack with vehicle-overlap detection

number of reports are collected (cf. Section 5.5.2), the certificates of the MRs are verified and the plausibility of the given confidence is checked, applying Equation 5.2. Subsequently, the conditional pseudonym resolution detects that a' and a'' belong to the same station ($a', a'' \in PI_a(k)$ with $k \in K$). Consequently, the IDs a' and a'' are linked to a pseudonymous long-term ID a^* that is chosen by the LTCA (cf. Section 5.4.1.2).

At this stage, a trust value t_{o,a^*} and a confidence value c_{o,a^*} exist for every combination of $o \in V_{S_R}$ and $a^* \in V_{S_S}$ with $o \neq a^*$. In order to assess the suspects, only $o_1, o_2, a^* \in V_{S_S}$ are considered in the aggregation process (cf. Equation 5.3 and 5.4) that outputs t_{a^*}, c_{a^*} for all $o \in V_{S_R}$ that accused a^* in their reports. In Figure 5.11, the assessment of node a^* is illustrated exemplarily. The resulting tuple (t_{a^*}, c_{a^*}) for the suspect $a^* \in V_{S_S}$ is combined to a final assessment value using the function $a(t_{a^*}, c_{a^*})$. After also calculating the final values for o_1 and o_2, the MEA can decide depending on policies and defined thresholds which nodes should be excluded.

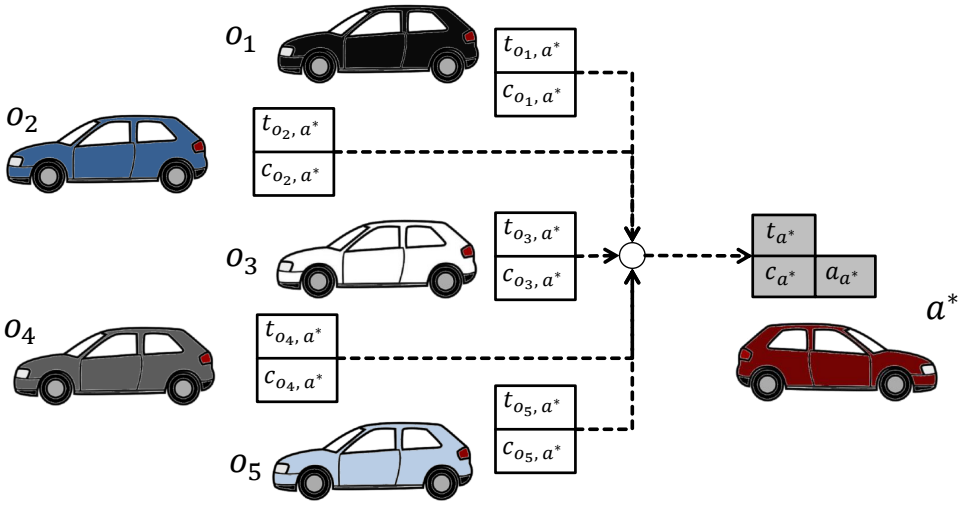


Figure 5.11.: Example for central node assessment for misbehavior evaluation

5.5.6. Evaluation of Attacker Node Identification

The goal of the central misbehavior evaluation is the identification of attackers from a given set of suspected nodes that are actively involved in a misbehavior scenario. We aim to verify the hypothesis that a central MEA is able to identify multiple attackers based on a majority of benign reporters that observed abnormal behavior according to Section 1.2. A simulation study is conducted to evaluate the central node assessment as detailed in the following paragraph.

Evaluation Setup A simulation allows a statistical evaluation of the proposed solution under consideration of realistic assumptions and limitations as derived from the long-term FOT described in Section 3.4.4. For the central evaluation of misbehavior reports it is not relevant to have a detailed traffic flow simulation and detailed communication simulations for the nodes of a VANET. The reporting

can be considered as interface between the local misbehavior detection, analyzed in Chapter 3, and the central evaluation of detections. As shown in Figure 5.12 a misbehavior report generator is used to create a set of MRs that are handed over to the MEA where the reports are processed.

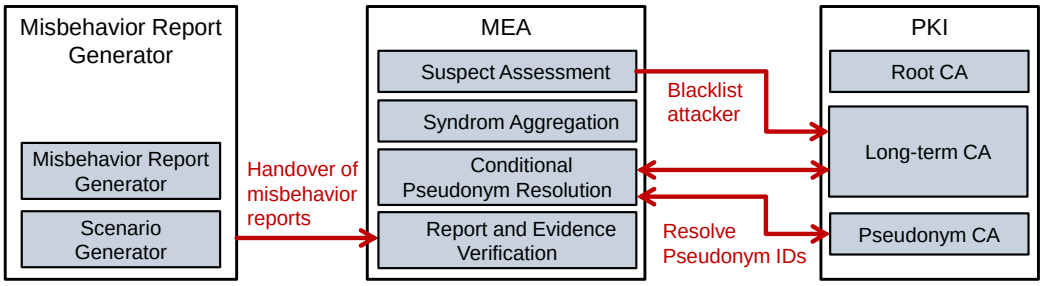


Figure 5.12.: Evaluation setup of central misbehavior report processing and attacker identification

Relevant information for the central evaluation of reports are the number of involved independent attackers, the number of involved benign nodes and the number of benign witnesses. Based on these parameters the content of the different misbehavior reports is calculated by a report generator implementation which provides a set of reports to the MEA implementation. Both the report generator and the MEA implementation are realized with Java. The software was executed in our experiments on common commercial off-the-shelf personal computer hardware. Due to the simulation of report generation different setups with varying parameter were tested in order to evaluate the proposed mechanism. Furthermore, the simulation allows to replicate and repeat the experiments.

For the verification of received evidence (cf. Section 5.5.2) configuration parameters shown in Table 5.2 were applied. If a vehicle overlap is reported than either both suspects and three witnesses have to report this event or one suspect and five witnesses have to send a report in order to overstep the configured threshold. In the following description of experiment results, we consider the first case in which both involved nodes and at least three witnesses that passively observed the overlap send a report.

Table 5.2.: Configuration of experiments related to report collection of central MEA

Parameter	Value
Weighting of vehicle overlap detection with active participation as suspect	1
Weighting of vehicle overlap detection with passive participation as witness	0.4
Weighting threshold for satisfying independent reporters. According to Section 5.5.2 the sum of weights must be larger than this threshold.	3
Node assessment threshold a_{thld} used to distinguish benign and malicious nodes.	0.5

In the simulations the report generator allocated randomly trust and confidence values between benign nodes and ghost nodes according to Table 5.3. In the following description an attacker is assumed who is causing ghost vehicle overlaps as depicted in Figure 5.10. Using different types of detected misbehavior according to the Section 3.2 would allow a simple evaluation of the attacker node by applying the causal model. We focused in the following evaluation on the most complex scenario in which only

vehicle overlaps are reported. As a consequence, in every test case several nodes are suspected. Nevertheless, the evaluation results are transferable to other kinds of location-related misbehavior where only one suspect is available in the session set V_{S_S}.

According to Table 5.3 the benign nodes provide positive trust values to other benign nodes and negative values for detected ghost vehicles. On the contrary, attackers assign a maximal positive trust value to other attackers and minimum values for benign nodes. Since the confidence depends on the together traveled distance and duration of two nodes, the confidence value cannot be arbitrarily faked by an attacker.

Table 5.3.: Value ranges for trust and confidence used for central MEA evaluation

Direction of rating (provider → target)	Trust as range	Confidence as range
benign node → benign node	[0.75, 1]	[0, 1]
benign node → faked node	[0, 0.5]	[0, 1]
faked node → benign node	0	[0.1, 0.7]
faked node → faked node	1	[0.1, 0.7]

Based on the simulation setup evaluations of the two most relevant attack scenes are presented in the following. Each simulation scenario were repeated 10 times. According to the requirements for central misbehavior evaluation listed in Section 5.2, the simulator generates an incomplete set of misbehavior reports S_{MR} that is provided to the MEA. In order to consider limited communication links between reporters and the infrastructure, 30 percent of the simulated observers $o \in V_{S_R}$ are not able to transmit their MR to the MEA in the conducted tests.

(1) Attack Scenario with Single Physical Attacker Node In the first configuration the optimal misbehavior scenario under consideration of the above mentioned constraints is analyzed. In this case a single physical attacker node creates one ghost vehicle that causes vehicle overlaps that are detected by benign nodes in the single-hop communication range of the attacker. Reports that contain several pseudonymous IDs related to the same physical station are filtered by the MEA. The report generator of the simulator creates for every involved node one report with random trust and confidence values according to the ranges defined in Table 5.3 for all nodes in the scene. In order to gain the information on how many witness nodes are needed for reliable detection of an attacker, the number of benign witnesses is increased (cf. x-axis of Figure 5.13). This experiment was used to configure the VO weighting parameters listed in Table 5.2. The two graphs illustrate the assessment value of the benign nodes and the ghost vehicle. The second graph shows that the decrease of the faked node's assessment value attenuates with four benign witnesses.

(2) Attack Scenario with Increasing Number of Cooperating Physical Attacker Nodes In the second configuration the limitations of the proposed concept are analyzed. In Figure 5.14 the respective results are shown evaluated with the report generator and the MEA implementation. In this scene several benign nodes generate misbehavior reports stating that 50 percent of these benign nodes are actively overlapping a single ghost vehicle. The other 50 percent of the benign nodes are acting as witnesses. In this simulation the number of malicious reporters is increased in order to measure the impact of several cooperating attackers. By assigning trust and confidence

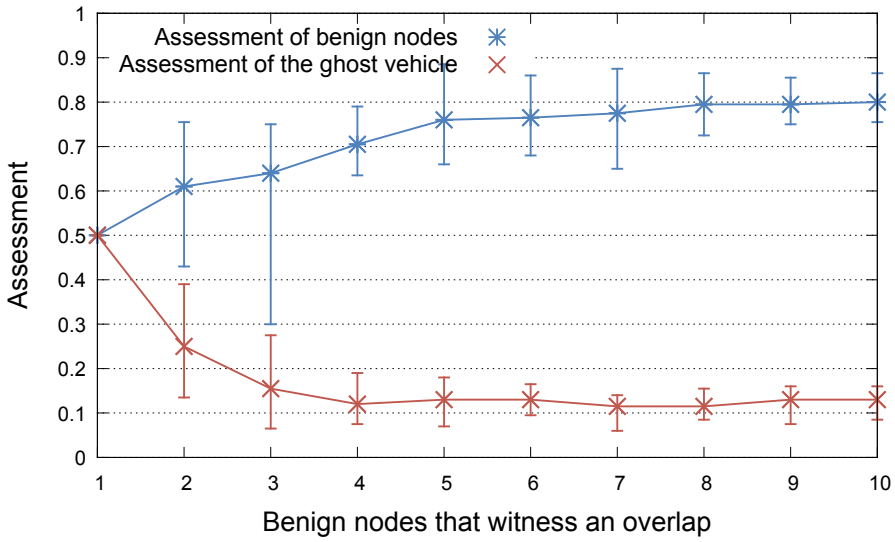


Figure 5.13.: Attack with increasing number of benign witnesses observing a misbehavior event

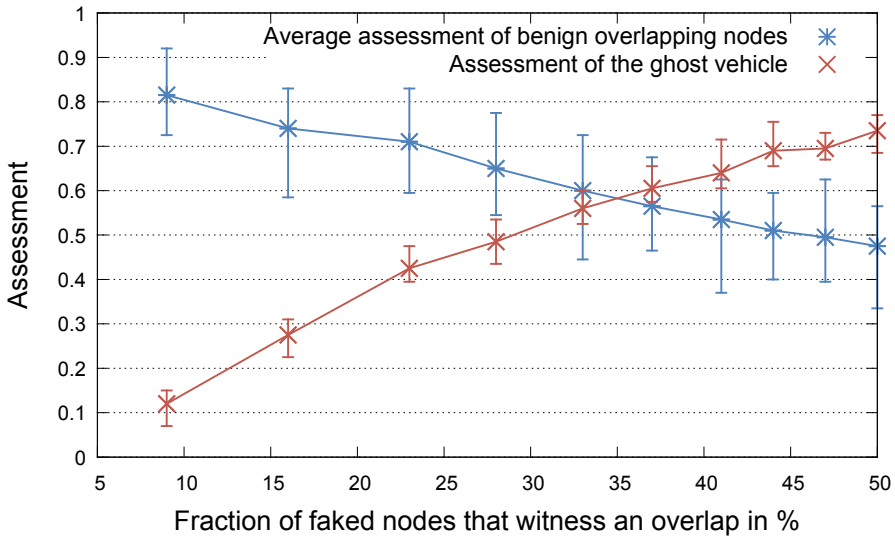


Figure 5.14.: Attack with increasing number of maliciously cooperating witnesses providing MRs

values for suspects according to the configuration listed in Table 5.3, it is sufficient if 35 percent of the involved nodes belong to independent cooperating attackers in order to hide a real attack. This result complies with the Byzantines generals problem [LSP82] that states that no solution involving less than $3m+1$ nodes can cope with m attackers. However, the effort for an attacker is relatively high to mount an attack where several manipulated vehicles are at the same location at specific time. Using only one manipulated station for this cooperative attack is not possible since the MEA is able to link different pseudonymous identifiers that belong to the same physical station.

Based on a threshold value a_{thld} as defined in Table 5.2, the attackers can finally be distinguished from benign nodes. All suspects V_{S_S} of a session S that are rated with a value below a_{thld} can be considered to be identified as attacker or faulty node.

Our evaluations based on simulated reports are an appropriate basis for future FOTs since the central MEA is using the MR as well-defined interface between VANET nodes and the central MEA. Additionally, we evaluated the most complex case of misbehavior evaluation with several suspects per misbehavior session. Based on the scenario with several cooperating attackers and multiple suspects we have confirmed the hypothesis that a majority of approximately two-thirds benign nodes is required to identify the attackers. In this complex scenario, the evaluation is based on trust-confidence information in addition to a causal model. Finally, realistic configurations of the report generator were considered as listed in Table 5.3. We considered beside others the loss of MRs and fake reports of involved attackers.

5.5.7. Security and Vulnerability Analysis of Central Attacker Node Identification

The MEA has to consider strong security and privacy characteristics in order to prevent attacks and misuse. In this analysis the generic security protective goals such as confidentiality, integrity, authenticity, authorization, non-repudiation, revocation, and availability are discussed. Moreover, specific attacks such as replay of data, discrediting of benign nodes and cooperative attacks are considered. Finally, the effects on privacy are discussed. Within the infrastructure, the MEA has to establish connections to the PKI with respect to conditional pseudonym resolution and to revoke identified attackers and faulty nodes. As a consequence this security and privacy analysis is closely related to the security and privacy analysis of CoPRA in Section 5.4.2.

- **Confidentiality of MR** The MRs provided by nodes of the VANET has to be encrypted. For this purpose, we propose to apply transport layer security such as SSL or packet based encryption based on an integrated encryption scheme such as ECIES. Within the infrastructure all communication between the MEA and the PKI must also be encrypted. In addition the MEA must be operated in a trusted environment. This implies that data stored by the MEA is not accessible by outsiders and sensitive information such as private keys are not readable.
- **Integrity Protection of MR** The data integrity of transmitted data has to be ensured. As discussed in Section 5.4.2, both the transport layer security and integrated encryption schemes support this function. In addition, we propose to sign every MR with the reporter's private key of the pseudonym certificate as further detailed in Section 5.3.2. In order to prevent manipulation of data that is stored in the database of the MEA we propose to apply trusted platform modules

to ensure software and database integrity of the MEA. Outsiders must not be able to insert, alter or drop information without authorization.

- **Authenticity of MEA and Reporters** The MEA, the VANET nodes and all entities of the PKI are equipped with certificates issued by the root CA or a pseudonym CA. According to the PKI concept, presented in Section 2.2.1, VANET nodes use pseudonymous certificates to ensure authenticity according to privacy protection requirements. These PCs are used to sign and encrypt locally generated MRs. The MEA uses a certificate issued by the root CA in order to authenticate itself against other entities of the security infrastructure. These certificates authenticate the respective stations in the security negotiation procedure when a symmetric key is exchanged in transport layer security (e. g. SSL) or the integrated encryption scheme (e. g. ECIES).
- **Authorization of MEA and Reporters** The certificates contain information about authorization of the stations. We propose that every trustworthy node of the VANET is authorized to provide a MR. The permission should be associated to the trust and assurance level (TAL) that is part of the pseudonym certificate. The TAL concept is developed by the C2C-CC [WBF+13]. With respect to misbehavior reporting vehicles and RSUs should be permitted to generate and provide MRs to the MEA as long as the used PC contains the minimum TAL required for V2X communications.

  The MEA is equipped with a certificate that contains required permissions to request conditional pseudonym resolution and to revoke attacker nodes. The root CA is responsible to ensure that the MEA considers and follows the rules described in the certificate policy of the PKI. Based on a regular audit which confirms that the MEA follows the policy the certificate of the MEA is renewed by the root CA.
- **Non-repudiation of an Origin (Reporter of MR)** Since every MR is signed with a private key related to a PC the MEA can verify that the report is generated by an authenticated and authorized VANET node. The conditional pseudonym resolution is applied to identify duplicate reports generated by the same physical station that is using different pseudonymous certificates in different MRs. A sender can consequently not repudiate the sending of a MR. The communication between the MEA and the PKI entities is secured by transport layer security that ensures the non-repudiation of message receipt.
- **Non-repudiation of the Receipt of MR** As discussed in Section 5.4.2 the receipt of a MR is acknowledged by the MEA with a signed message.
- **Revocation of MEA and Reporters** The revocation of a compromised MEA is manually done by adding the certificate ID on a CRL. According to the C2C-CC PKI concept [BSS+11] this CRL lists only entities of the security infrastructure. Updates of the CRL are distributed to all nodes of the VANET and to all entities of the security infrastructure. As soon as a MEA is revoked the PCA and LTCA reject for example the request for conditional pseudonym resolution as well as requests for node revocations.

  We propose to perform the revocation and exclusion of reporters by two measures. Since all nodes of the VANET are registered with a LTCA the respective LTCA is also responsible to reject PC acquisition requests of the blacklisted node. However, as long as the node is equipped with valid pseudonym certificates it can actively participate in V2X communications. In order to prevent blacklisted nodes to possibly send fake MRs, we propose to use the online certificate status protocol (OCSP) to exchange the revocation status between entities of the security infras-

tructure. By using OSCP the MEA is able to request the status of misbehavior reporters before their provided report is processed.

- **Availability of MEA** In order to limit the impact of DoS attacks against the central MEA, every MR is signed with the pseudonym private key of the respective sender. The MEA checks in the first step the validity of the sender by verifying its pseudonym certificate and in a second step the message signature is verified. Reports signed with an invalid signature or involving invalid certificates are discarded after reception as described in Section 5.3.2. This strategy ensures that attackers must invest in cryptographic signing operations in order to flood the MEA with invalid reports. However, the system performing the verification of incoming reports should be equipped with enough processing power to be able to process a large number of incoming reports.
- **Replay of MR** As discussed in Section 5.3.1 the observed misbehavior is proven by one or more signed messages containing location information and corresponding timestamps. The combination of position and time allows the MEA to assign the report to a misbehavior session. Duplicates and replayed reports are detected and discarded. It has to be considered for both, the DoS attack and the replay attack, that the MEA is able to check whether different pseudonyms belong to the same node. Reports from the same node using different pseudonyms are discarded as well.
- **Discrediting of Benign Nodes** The arbitrary generation of faked misbehavior reports is limited as discussed in Section 5.3.1. Depending on the type of observed misbehavior the reporter has to prove the event by adding appropriate signed messages that cannot be faked by an attacker. Therefore, attackers are not able to blacklist nodes of the VANET arbitrarily.
- **Cooperation and Level of Attacker** The level of cooperating attackers with respect to the misuse of the conditional pseudonym resolution is discussed in 5.4.2. In our concept only the MEA is responsible to decide whether sufficient evidence was collected to exclude a node from active participation in a VANET. A compromised MEA is in general able to request the LTCA to exclude and blacklist specific nodes of the VANET as long the MEA knows the long-term ID of the nodes. As a consequence, the MEA implementation must be operated in a trusted environment. In order to reconstruct a decision of the MEA we propose to perform a detailed logging at the MEA with respect to misbehavior report processing.
- **Regulatory Compliance** The proposed concept for misbehavior detection and evaluation bases on regulatory compliance. It is required that a large set of nodes of a VANET are equipped with mechanisms to locally detection misbehavior. The nodes have to perform the misbehavior detection according to a defined concept that is implemented in the same way at all nodes. If, for example, vehicles of different manufacturers implement the detection mechanisms differently then the central evaluation of MRs might not be possible. The MEA should be able to process reports from vehicles and RSUs of different manufacturers in order to increase the number of possible reporters. The higher the number of independent reporters the higher the possibility to identify attackers reliably. As a result, it is important that the MEA is accepted by all stakeholders of a VANET.
- **Privacy** The privacy of reports is affected due to the conditional pseudonym resolution as discussed in the security and privacy analysis of CoPRA in Section 5.4.2. We propose in Section 5.4.1.2 to use a pseudonymous long-term ID id_{PLT} that links pseudonymous IDs. This id_{PLT}

changed over time in order to protect the privacy of drivers. Consequently, the MEA is not able to gather the real long-term ID of VANET nodes.

5.5.8. Performance Analysis of Central Misbehavior Evaluation

In general, the scalability of a central entity has to be particularly considered since several hundred million vehicles can be assumed to be part of a future VANET referencing to the mandate of the European commission [Com09] and the memorandum of understanding of automobile manufacturers [Con11]. However, the number of processed misbehavior reports is not directly related to the number of nodes in the network. For example, the network might consist of several million vehicles but only a handful of attackers are producing inconsistencies on the road that are detected by a handful of vehicles passing this area. In a first step, the nodes can filter the detected misbehavior. Only reliable detections are sent to the MEA. In a second step, the impact of a ghost vehicle attack is spatially restricted and therefore, only a relative small subset of nodes is able to send related misbehavior reports. Reports are created only if misbehavior is autonomously detected. In contrast to other related schemes (i. e. [CKL+08, MP12, ODS07]), the permanent report of node position and their system state is not needed. Indeed, by reporting event-based, the dimensions of the infrastructure entities can be realized smaller and a constant communication link to the infrastructure is not required. The dimensions of the MEA is therefore only directly related to the number of mounted attacks and false positive detections.

5.6. Exclusion of Attackers and Faulty Nodes

The exclusion of attackers and faulty nodes can only be done in cooperation with the LTCA of the PKI. In the process of misbehavior evaluation, the MEA needs to conditionally resolve the pseudonymous IDs of the involved nodes. Consequently, the MEA is in possession of a pseudonymous long-term ID id_{PLT} that can be linked by the LTCA to the corresponding long-term ID id_{LTC_v} of the enrolled vehicle or RSU $v \in V$. If subsequently new pseudonym certificates are requested by affected stations the LTCA can reject these requests. According to the pseudonym certificate acquisition process discussed in Section 5.4.1.1, the PCA queries the LTCA in every PC request for permission. As proposed by the author of this dissertation [BSS+11] the lifetime of pseudonym certificates is limited by the following three parameters.

- **Parallel pseudonym number (PPN):** The PPN determines the maximal number of valid PCs that an ITS station may possess for a given time period, e. g. PPN = 10.
- **Pseudonym lifetime period (PLP):** The PLP determines the maximal lifetime of a pseudonym certificate, e. g. PLP = 1 day.
- **Pseudonym preloading period (PPP):** The PPP determines the maximum time period for which new pseudonym certificates may be requested, e. g. PPP = 1 month.

Using the example values for PPN, PLP, and PPP, an ITS station is permitted to request at maximum 300 different PCs that are valid in a sequencing order. The 10 PCs created last expire also last, at least one month after the request time. A revocation of PCs by distributing CRLs is not considered in

the European PKI design [BSS+11, ETS10c] due to its complexity. The main reasons are listed in the following.

- CRLs in the VANET context may contain a large number of entries resulting in big CRLs.
- The disconnection of vehicles from the infrastructure may delay periodic updates of the CRL. If vehicles have the most times no connection to the infrastructure, the latest CRL cannot be loaded from the PKI and consequently the vehicle cannot check whether the certificate of a neighbor is revoked.
- The application of CRLs increases the latency of the certificate verification process. In a worst case all entries of a revocation list have to be compared with the certificate that is verified.

The PPP parameter finally determines the amount of time in which VANET nodes can be equipped with valid certificates. As a consequence, also attackers or faulty nodes might be in the possession of valid credentials for a relatively long period of time. Even if the MEA has already identified the attacker and the LTCA has deactivated the corresponding id_{LTC_v}, the attacker may still be equipped with valid PCs. Only after all certificates of the attacker's PC pool are expired, the attacker is excluded from the VANET by rejecting its PC request in the acquisition process. As a result, the pseudonym preloading period should be kept as small as possible to minimize the amount of time in which attackers can continue with their malicious activities until their exclusion. However, the PPP has to be large enough to ensure that benign, but isolated ITS stations are constantly equipped with valid PCs.

5.7. Summary

In this chapter a proposal for the central long-term identification of misbehaving stations and their exclusion from V2X communications is presented. The proposed framework aims to ensure the VANET's long-term reliability. The analysis of related work has shown that other solutions have not considered pseudonymous identifiers appropriately and do not sufficiently address scalability and low-overhead requirements. Our approach is the only concept in the context of misbehavior detection in VANETs that considers the report of locally detected misbehavior events, the central conditional pseudonym resolution and the central identification of responsible nodes. Even if the nodes are able to detect the misbehavior the related node can only be recognized as long as the node is in single-hop communication range or if its pseudonymous ID is not changed. The long-term recognition of attackers is not possible by the nodes. In addition, the local nodes might not be able to distinct between abnormalities created due to an attack or abnormalities created by vehicles in exceptional situations such as an accident. Our proposal for central evaluation of misbehavior reports is able to collect detections from a large set of independent observers over a longer period of time.

The proposed framework is based on plausibility checks and the local evaluation of the neighbor nodes' trustworthiness by VANET nodes. In case of local detection of misbehavior, the stations send reports to the central MEA. The reports contain at least the type of detected misbehavior including related evidence and the pseudonymous IDs of suspected neighbors. Moreover, other neighbors of the reporter are included as potential witnesses that may also have observed the same misbehavior event. All contents of the reports are digitally signed, and V2X messages are added to the reports aiming for attesting the observed misbehavior event. Consequently, cooperating attackers who aim to discredit

benign nodes have to spatially and temporarily synchronize each other. This requirement drastically increases the effort for attackers since, by the time of the attack, they all have to be situated in single-hop communication range of a specific discredited victim. As soon as the central MEA has received the reports it verifies the contents and signatures, and subsequently allocates the reports to a misbehavior session. A causal model is applied to aggregate the reported syndromes. However, since multiple causes must be assumed in misbehavior detection the causal model returns multiple suspects in complex misbehavior scenarios. If not a single causer of a misbehavior event (e. g. two unknown neighbors overlap their vehicle positions) can be uniquely identified trust-confidence pairs provided by the reporters are processed. Based on this information, the central MEA starts the evaluation of received reports as soon as sufficient evidence in form independent misbehavior reports is available. In order to check whether different pseudonymous IDs, e. g. $id_{PC_{v'}}, id_{PC_{v''}}, id_{PC_{v'''}}, \ldots$ stated in the reports belong to the same ITS station, the MEA is permitted to request pseudonym linking information in form of a pseudonymous long-term ID id_{PLT}. In the node assessment process the MEA is able to identify attackers and faulty nodes, based on the majority of benign reporters. As shown by a simulation study a single attacker can be detected reliably if at least four witnesses are available (cf. Figure 5.13 in Section 5.5.6) and less than one-third cooperating attackers are involved (cf. Figure 5.14 in Section 5.5.6). In cooperation with the PKI, the identified attackers and faulty nodes can finally be excluded from the VANET by rejecting pseudonym certificate acquisition requests.

Part IV.

Summary, Conclusion, Outlook, and Appendices

6. Summary, Outlook and Conclusion

In 2011, by signing a memorandum of understanding (MoU) [Con11], European automobile OEMs have jointly agreed on the implementation and deployment of cooperative ITS in Europe from the year 2015. In the same way, the Ministries of Infrastructure and Environment of the Netherlands, Germany, and Austria have agreed to deploy ITS at the highway corridor among Rotterdam, Frankfurt/M. and Vienna, also scheduled from 2015. Both MoUs focus on the application of wireless V2X ad hoc communication as discussed in this thesis rather than merely utilizing cellular networks. As a consequence, security and privacy protection mechanisms have to be available for vehicles and RSUs that will be delivered in the near future. However, the mitigation of internal attacks is not sufficiently addressed by the security solutions currently specified in European standardization groups such as ETSI [Ins13], ISO [fSI10], and industrial consortia such as the C2C-CC [CC13]. It is therefore required to implement, even for the day-one deployment, reactive security mechanisms that are able to detect attackers and faulty stations and exclude them from VANET communication if required. The solution discussed in this dissertation is compatible with the ITS security design being in the process of standardization at the time of writing this dissertation. Moreover, the proposed solution has already been partially tested in FOTs. In order to consider novel attack variants that might arise in future the design for misbehavior detection and attacker identification is easily adaptable.

In Chapter 1 on page 5 (*Problem Statement*) we discussed the main problems as well as the goals that are addressed within this dissertation.

In Chapter 2 the VANET architecture is introduced including its characteristics, participants, and communication technologies. Since security and privacy protection play an important role for reliable and trustworthy V2X communication, related mechanisms are also introduced in this chapter. Furthermore, a detailed discussion of the adversary model is included in Chapter 2, as well as test results gained from location-related attacks. The results were obtained through performing simulations and tests with real vehicles on a test track.

The core contributions were presented in Chapter 3, 4, and 5. They were summarized in Section 1.5 and are reflected in this conclusion in Section 6.1.

In the following, these main contributions of this dissertation are summarized (cf. Section 6.1). In Section 6.2 an outlook is provided, and potential future work is discussed.

6.1. Summary of Contributions

The following summary is related to the four scientific questions introduced in Chapter 1. The respective answers refer to our approaches described in Chapter 3 (*Local Misbehavior Detection on VANET*

Nodes), Chapter 4 (*Local Short-term Identification of Potential Attackers*), and Chapter 5 (*Central Long-term Identification of Attackers*).

(1) How is it possible to detect internal misbehaving network nodes?

In Chapter 3 data consistency checks and data plausibility checks were described that can be applied in vehicles and RSUs in order to detect suspicious behavior of single-hop neighbor vehicles. At first several known message-based and node-based checks were analyzed and classified. In addition to the known approaches a new consistency check was proposed that detects vehicles showing position overlaps in their provided location data [BSB10]. The most promising misbehavior detection algorithms were implemented and evaluated with prototypical frameworks to perform the local misbehavior detection on VANET nodes [BB11], [BMBK12], [JBSH11], and [SJB+10].

A module-based approach was elaborated that is able to utilize different consistency and plausibility tests. In this approach every test module is responsible to verify a specific mobility data related policy. The results of the modules are aggregated in order to evaluate the plausibility of received V2X messages and the trustworthiness of the related sender node [SJB+10]. This module-based plausibility test framework was utilized in a large outdoor field operational test in order to evaluate its applicability. On the one hand, these tests have shown that location-based attacks were reliably detected by the use of several specialized data consistency and plausibility checks [BSP+13]. On the other hand, long-term measurements have proven that the false-positive rate can be kept in an acceptable range (i. e. $\approx 1.6‰$) [SES+13, BSS13] by focusing on neighbor nodes' movement verifications. These false detections, however, do not result in false reactions on the node, e. g. by discarding driver warnings. It is proposed that detected misbehavior is reported to a central evaluation entity after a filtering is performed on the nodes. The central entity collects independent reports from different nodes regarding the same event. Only if the detected misbehavior is confirmed by a specific number of independent reporters a reaction is initiated. Consequently, the false-positive rate at the nodes is only partly relevant for the final exclusion of attackers and faulty nodes.

We have further extended the module-based approach by a radar sensor that is able to verify the indicated location of neighbor nodes [JBSH11]. Most environment sensors, however, can verify objects only in line of sight. With regard to this limitation we proposed to additionally check stated vehicle locations based on received second hand location information. The proposed consistency test detects vehicle position overlaps of single-hop neighbors. In this test it is verified that only one vehicle is located at a specific position on the road at the same time [BSB10].

Prototypical implementations of the module-based approach, however, pointed out that with an increasing number of information sources and plausibility modules the performance decreases. Additionally, the complexity increases dramatically since dependencies between the modules have to be considered. As a result, the application of particle filters for misbehavior detection was elaborated [BMBK12]. The particle filter provides a sophisticated way to combine information sources and allows for the direct plausibility evaluation of location-related data.

Within this dissertation we confirmed the hypothesis that mobility data contained in received V2X messages can be used to detect misbehavior as defined in Section 1.2. Even sophisticated attacks can be detected that are caused by internal attackers who send messages with faked loca-

tion data aiming to create non-existing ghost vehicles.

(2) Are VANET nodes able to identify attackers under consideration of privacy protection mechanisms?

As analyzed in Chapter 4 local detection of misbehaving VANET nodes is possible. However, the long-term identification of the responsible causer is challenging. The results of a study performed by the author of this dissertation on ID changes in VANETs [BSS13, SES+13] within a large outdoor test show that ID changes were not reliably detected. In the majority of all cases, nodes were not able to recognize each other after a period of a few minutes. This circumstance limits the possibilities of local misbehavior detection, since attackers can be identified by their pseudonymous ID only for a short period of time. Furthermore, VANET nodes are not able to exchange large amounts of data that is related to misbehavior detection via ad hoc communication due to the limited bandwidth. Therefore the local attacker detection mechanism suffers from the lack of information that would increase the time of identifying attacker nodes. However, we proposed to determine the trustworthiness of neighbors in the single-hop communication range [BMBK12, EB09], even if processed on a local basis, the trust profile may only be valid until the next ID change of the neighbor. In summary, a long-term identification of nodes is locally not sufficiently possible.

(3) Is a central identification of attackers feasible in order to support the long-term operation of the VANET?

In Chapter 5 of this dissertation, a central misbehavior evaluation authority (MEA) was proposed for more reliable and long-term identification of attacker nodes. The concept is based on misbehavior reports sent by VANET nodes, that have independently observed inconsistencies in location-related information and implausible node behavior [BNPB12]. The report structure is provided in a way that VANET nodes must add information proving the observed misbehavior. This approach prevents attackers to arbitrarily blackmail benign nodes of the VANET. As discussed in Chapter 4, the central MEA is able to collect several reports from different observers that have autonomously detected the same misbehavior. Furthermore, the central MEA is able to check whether different pseudonymous identifiers, reported in context with a specific attack scene, belong to the same node. Based on reports provided by independent misbehavior observers, and a conditional pseudonym resolution, the MEA is able to identify attacker nodes and exclude them from active VANET participation. Even if a reported location-based attack is constructed by cooperating attackers the responsible nodes can be identified having a majority of two-thirds benign observers that provide misbehavior reports.

(4) Is it possible to apply a central attacker identification scheme that meets relevant privacy protection requirements?

Protecting the drivers' privacy in VANETs is an essential requirement for the network's future deployment and acceptance. Vehicles must not be trackable over long periods of time by monitoring their V2X communication. Furthermore, VANET infrastructure entities such as traffic management centers, the PKI or the MEA must not be able to link the pseudonymous identifiers to the vehicle's long-term ID. Moreover, it should not be possible to obtain information

whether two pseudonymous IDs belong to the same network node without providing evidence for misbehavior.

Within this dissertation a conditional pseudonym resolution protocol was proposed that allows the MEA to merely identify whether particular pseudonyms were used by the same physical node [BPB13]. However, the MEA is only permitted to request this information for nodes that are involved in detected misbehavior attested by a reporter through signed data. Consequently, the hypothesis was confirmed that long-term privacy of a driver can be preserved, and especially the privacy of uninvolved nodes is not affected by the proposed central attacker identification solution. Moreover, the resolution is spatio-temporally related to a specific misbehavior situation. A resolution linking among different misbehavior scenarios is excluded.

The proposed concept for misbehavior detection and attacker identification might be relevant for other ICT domains as discussed in Section 1.5. In general, misbehavior detection in cyber-physical systems could be related to our proposals and attacker identification in communication networks applying short-term pseudonymous identifiers. As a consequence, our proposals might be interesting for enterprise networks that handle physical input and output and systems that have to consider frequently changing identifiers.

6.2. Outlook

In this section, both future research topics and potential extensions are outlined with respect to misbehavior detection and attacker identification in VANETs.

Within this dissertation a generic location-based attack was analyzed by using an exemplary V2X malicious software. However, other location-based attack variants and application-specific attacks might require additional misbehavior detection mechanisms. Additional sensors and information sources could be considered in future work to further increase the misbehavior detection accuracy, and to minimize the false-positive rate on the VANET nodes. In particular, since the number of vehicles equipped with cameras (be it for traffic signage recognition, weather condition detection, or parking assistance) is growing, these systems could be additionally used to optically verify the position claimed by adjacent V2X nodes. Furthermore, the proposed misbehavior detection solutions were evaluated over a long period of time under real-world conditions without attackers. The results show that the message-based false-positive rate exceeded the expectations. The main reason for this was the unreliable transmission of mobility data and its inaccuracy. Assuming further advancement and optimization of V2X communication systems in the future, a significantly improved level of accuracy of mobility data can be expected to be available for misbehavior detection.

A large-scale integration of misbehavior detection frameworks on vehicles and RSUs and the operation of a central misbehavior evaluation authority in a real pre-productive environment is necessary to identify potential deployment issues. Even if the local misbehavior detection solution was already deployed on several test vehicles within the research related to this dissertation, the transmission of misbehavior reports and their evaluation at the central MEA has only been evaluated in a proof-of-concept manner. At least for the central misbehavior report evaluation and conditional pseudonym resolution the development of policies is required that need to be accepted by the responsible VANET

stakeholders. For instance, a threshold has to be specified by which misbehaving ITS station are considered to be attackers, and consequently become excluded from active VANET communications. The conditional pseudonym resolution is likewise based on policies that specify which type of misbehavior report content justifies the request of temporary pseudonym linking information.

Furthermore, in future work the mechanism for attacker node exclusion could be elaborated in more detail. In this dissertation, the approach is followed as discussed within the European context (i. e. ETSI [ETS10c, ETS12a, ETS12b] and C2C-CC [BSS+11]) to reject new certificate requests of identified attackers. However, this passive approach may allow the attacker to continue his or her malicious activities until the certificates are expired. A more active solution could be applied to promptly exclude identified attackers from active network participation. Additionally, remote diagnosis and remote update mechanisms could be elaborated in future work that would allow the reactivation of faulty ITS stations after repair and reset of manipulated software.

6.3. Conclusion

The approaches discussed in this dissertation aim on the extension of the existing VANET security solution by two important building blocks: *misbehavior detection* and *attacker identification*. For the large-scale and long-term operation of a VANET in a productive environment it is required to apply an extended security framework as proposed in this dissertation in order to permanently exclude attackers. Within this dissertation new concepts and mechanisms for misbehavior detection in VANETs were developed based on results gained in a large field operational test involving authentic attacking scenarios. We are the first who propose the reporting of misbehavior and the central long-term identification and exclusion of attackers. The proposed concepts were tested and evaluated further with close-to-market VANET security infrastructures. By making attacks on VANETs unattractive it is the goal of this research to make V2X communications more reliable and trustworthy for drivers on the long-term perspective.

Appendices

A. Author's Publications

A.1. Journal Articles

[JBSH11] Attila Jaeger, Norbert Bißmeyer, Hagen Stübing, and Sorin A. Huss. A novel framework for efficient mobility data verification in vehicular ad-hoc networks. International Journal of ITS Research, ITS Japan, 9(3), September 2011.

A.2. Conference Contributions

[BSP+13] Norbert Bißmeyer, Henrik Schröder, Jonathan Petit, Sebastian Mauthofer, and Kpatcha Bayarou. Short paper: Experimental analysis of misbehavior detection and prevention in VANETs. In IEEE Vehicular Networking Conference (VNC). IEEE, December 2013.

[BPB13] Norbert Bißmeyer, Jonathan Petit, and Kpatcha M. Bayarou. CoPRA: Conditional pseudonym resolution algorithm in VANETs. In The 10th Annual Conference on Wireless On-Demand Network Systems and Services (WONS). IEEE, March 2013.

[BMBK12] Norbert Bißmeyer, Sebastian Mauthofer, Kpatcha M. Bayarou, and Frank Kargl. Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters. In IEEE Vehicular Networking Conference (VNC). IEEE, November 2012.

[BNPB12] Norbert Bißmeyer, Joel Njeukam, Jonathan Petit, and Kpatcha Bayarou. Central misbehavior evaluation for VANETs based on mobility data plausibility. In VANET '12: International workshop on Vehicular inter-networking. ACM, April 2012.

[BSS+11] Norbert Bißmeyer, Jan Peter Stotz, Hagen Stübing, Elmar Schoch, Stefan Götz, and Brigitte Lonc. A generic public key infrastructure for securing car-to-x communication. In 18th World Congress on Intelligent Transportation Systems. ITS America, October 2011.

[BB11] Norbert Bißmeyer and Kpatcha M. Bayarou. Angriffserkennung in der Car-to-X Kommunikation basierend auf Bewegungsinformationen. In 27. VDI / VW-Gemeinschaftstagung Automotive Security. Verein Deutscher Ingenieure (VDI), Oktober 2011.

[BSRS11] Norbert Bißmeyer, Björn Schünemann, Ilja Radusch, and Christian Schmidt. Simulation of attacks and corresponding driver behavior in vehicular ad hoc networks with VSim-RTI. In SIMUTools 2011, 4th International ICST Conference on Simulation Tools and Techniques, March 2011.

[SJB+10] Hagen Stübing, Attila Jaeger, Norbert Bißmeyer, Christian Schmidt, and Sorin A. Huss. Verifying mobility data under privacy considerations in car-to-x communication. In 17th ITS World Congress. ITS Asia, October 2010.

[BSB10] Norbert Bißmeyer, Christian Stresing, and Kpatcha Bayarou. Intrusion detection in VANETs through verification of vehicle movement data. In IEEE Vehicular Networking Conference (VNC). IEEE, December 2010.

[BSM+09] Norbert Bißmeyer, Hagen Stübing, Manuel Mattheß, Jan Peter Stotz, Julian Schütte, Matthias Gerlach, and Florian Friederici. simTD security architecture: Deployment of a security and privacy architecture in field operational tests. In 7th Conference: escar - Embedded Security in Cars. isits International School of IT Security, November 2009.

[EB09] Peter Ebinger and Norbert Bißmeyer. TEREC: Trust evaluation and reputation exchange for cooperative intrusion detection in MANETs. In Communication Networks and Services Research Conference, CNSR'09. ACM, May 2009.

A.3. Technical Reports / Miscellaneous

[BMP+14] Norbert Bißmeyer, Sebastian Mauthofer, Jonathan Petit, Mirko Lange, Martin Moser, Daniel Estor, Michel Sall, Michael Feiri, Rim Moalla, Marcello Lagana, and Frank Kargl. PRESERVE d1.3 v2x security architecture v2. Deliverable, PREparing SEcuRe VEhicle to-X Communication Systems Consortium, January 2014.

[SES+13] Jens Schmidt, Kurt Eckert, Gunther Schaaf, Stefan Gläser, Ralf Grigutsch, Ingo Totzke, Madeline Volk, Norbert Bißmeyer, Carsten Kühne, Gert Stahnke, and Markus Bauer. Safe and Intelligent Mobility Test Field Germany: Deliverable D5.5 Part B-2; Nutzerakzeptanz, IT-Sicherheit, Datenschutz und Schutz der Privatsphäre. Technical Report D5.5 - Part B-2, simTD Consortium, July 2013.

[SBK+11] Jan Peter Stotz, Norbert Bißmeyer, Frank Kargl, Stefan Dietzel, Panos Papadimitratos, and Christian Schleiffer. PRESERVE d1.1 security requirements of vehicle security architecture. Deliverable, PRESERVE consortium, July 2011.

[MBS+09] Manuel Mattheß, Norbert Bißmeyer, Julian Schütte, Jan Peter Stotz, Matthias Gerlach, Florian Friederici, Christoph Sommer, Hervé Seudié, Winfried Stephan, Eric Hildebrandt, Jonas Vogt, Bechir Allani, Tobias Gansen, Anke Jentzsch, Hagen Stübing, and Attila Jaeger. Safe and Intelligent Mobility Test Field Germany; Deliverable D21.5; Specification of IT Security Solution. Technical report, simTD Consortium, Germany, October 2009.

B. Glossary

Definition	Synonyms	Description	Details
API		Application Programming Interface	An API is a particular set of specifications that software programs can follow to communicate with each other.
Assessment			An *assessment* value is used to express a combination of trust and confidence that node b assigns to node a. It is denoted as $a_{b,a}(k) \in \mathbb{R}$ with values in the range $[-1,1]$.
AU		Application Unit	Hardware unit in an ITS station running the ITS applications
CA		Certificate Authority	A certificate authority is an entity that issues digital certificates.
CAM		Cooperative Awareness Message	CAMs are sent by vehicles and roadside units multiple times a second (typically up to 10 Hz), they are broadcasted unencrypted over a single-hop and thus receivable by any receiver within range. They contain the vehicle's current position and speed, along with information such as steering wheel orientation, brake state, and vehicle length and width.
CAN		Controller Area Network	A CAN is a vehicle bus standard designed to allow microcontrollers and on-board devices to communicate with each other.
CCU		Communication & Control Unit	Hardware unit in an ITS station running the communication stack
Confidence	Certainty		The *confidence* value is always related to an opinion (i.e. a trust value). According to [Rie07], modeling the confidence of an opinion provides information on how much evidence an opinion is based, or to state that there is no evidence available. In this work, opinions are denoted as trust values and the confidence value is used as respective weighting factor.

Definition	Synonyms	Description	Details
DoS		Denial of Service	A DoS is a form of attack on a computer system or networks.
DENM	DNM	Decentralized Environmental Notification Message	A DENM transmission is triggered by a cooperative road hazard warning application, providing information to other ITS stations about a specific driving environment event or traffic event. The ITS station that receives the DENM is able to provide appropriate HMI information to the end user, who makes use of these information or takes actions in its driving and traveling.
DSS		Digital Signature Standard	
FOT		Field Operational Test	FOTs are large-scale testing programs aiming at a comprehensive assessment of the efficiency, quality, robustness and acceptance of solutions.
G5A		ITS road safety communication (802.11p)	Frequency band between 5.875 GHz and 5.905 GHz - reserved for ITS road safety communication
G5B		ITS non-safety communication (802.11p)	Frequency band between 5.855 GHz and 5.875 GHz - reserved for ITS road non-safety communication
G5C	C-WLAN	5GHz WLAN communication (802.11a)	
GNSS	GPS	Global Navigation Satellite System	Generic term for an Global navigation satellite system (GPS, GLONAS, Galileo)
HMI		Human-Machine Interface	The HMI is the interface where interaction between humans and machines occurs.
HSM		Hardware Security Module	A HSM is targeted at managing digital keys, accelerating cryptographic processes and for providing strong authentication to access critical keys.
I2V	I2C, I2V	Infrastructure-to-Vehicle	Communication between infrastructure components like roadside units and vehicles
I2I		Infrastructure-to-Infrastructure	Communication between multiple infrastructure components like roadside units

Definition	Synonyms	Description	Details
ITS		Intelligent Transportation Systems	Intelligent transport systems (ITS) are systems to support transportation of goods and humans with information and communication technologies in order to efficiently and safely use the transport infrastructure and transport means (cars, trains, planes, ships).
IVC	ITSC, ITS Communications	Inter-Vehicle Communication	Combination of V2V and V2I
LTC		Long-Term Certificate	Realization of an ETSI Enrolment Credential. The long-term certificate authenticates a station within the PKI, e. g.e. g., for PC refill and may contain identification data and properties. In ETSI standards the LTC is named *enrollment certificate* [ETS10c].
LTCA		Long-Term Certificate Authority	Realization of an ETSI Enrollment Credential Authority that is part of the PKI and responsible for issuing long-term certificates.
MCR		Maximum Communication Range	Is a specific plausibility check that compares a stated position with local specifications of the maximum reception range.
MEA		Misbehavior Evaluation Authority	System that collects misbehavior reports in order to identify the causer of observed inconsistencies that may disturb regular V2X communications.
MR		Misbehavior Report	Message structure that contains information about observed inconsistencies that may disturb regular V2X communications.
MRP		Map Related Position	Is a specific plausibility check that compares a stated position with local map data.
MBF		Maximum Beacon Frequency	Is a specific plausibility check that checks the beacon transmission frequency with local specifications of the maximum allowed frequency.
MTD		Maximum Transmission Delay	Is a specific plausibility check that checks the single-hop transmission delay of V2X messages with local specifications of the maximum allowed delay.
OEM		Original Equipment Manufacturer	Refers to a generic car manufacturer

Definition	Synonyms	Description	Details
OBU		On-Board Unit	An OBU is part of the V2X communication system at an ITS station. In different implementations different devices are used such as a CCU and a AU
PC	Short Term Certificate	Pseudonym Certificate	A short term certificate authenticates stations in ITS-G5A communication and contains data reduced to a minimum. In ETSI standards the PC is named *authorization ticket* [ETS10c].
PCA		Pseudonym Certificate Authority	Certificate authority entity in the PKI that issues pseudonym certificates
PKI		Public Key Infrastructure	A PKI is a set of hardware, software, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
PM		Plausible Movement	Is a specific plausibility check that verifies that adjacent nodes are following a locally specified mobility model.
PPA		Privacy Protection Authority	A PPA controls and monitors other authorities in order to ensure the adherence of privacy protection rules.
Pseudonymity			According to Pfitzmann et al. [PH10] a subject is pseudonymous if a pseudonym is used as identifier instead of one of its real names. Pseudonym comes from Greek "pseudonumon" meaning *falsely named* (pseudo: false; onuma: name). Thus, it means a name other than the "real name".
PV	Mobility Data	Position Vector	The position vector is periodically broadcasted by all VANET nodes and specified current absolute position of this node. Details about the position vector can be found in Section 2.2.2 on page 18
RSU	IRS, ITS Roadside Station	Roadside Unit	A RSU is a stationary or mobile ITS station at the roadside acting as access point to the infrastructure.
SAS		Suddenly Appearing Station	Is a specific plausibility check that detects nodes which appear suddenly in a not plausible vicinity to the receiver.

Definition	Synonyms	Description	Details
Trust		Trust is modeled as the subjective probability that an entity behaves as expected.	The *trust* that node $b \in V$ has regarding node $a \in V$ at time k is denoted as $t_{b,a,k} \in \mathbb{R}$. Trust has values in the range $[0,1]$, where 0 denotes maximal distrust and 1 denotes maximal benignity. New nodes start with a balanced trust value of 0.5.
UTC		Coordinated Universal Time	UTC is the primary time standard by which the world regulates clocks and time.
V2I	C2I	Vehicle-to-Infrastructure	Ad hoc vehicle to roadside infrastructure communication using a wireless local area network
V2V	C2C	Vehicle-to-Vehicle	Ad hoc vehicle(s) to vehicle(s) communication using a wireless local area network
V2X	C2X	Vehicle-to-Vehicle (V2V) and/or Vehicle-to-Infrastructure (V2I)	Ad hoc vehicle(s) to vehicle(s) or vehicle(s) to infrastructure communication using a wireless local area network
VIN		Vehicle Identification Number	Unique serial number of a vehicle

C. Curriculum Vitae

C.1. Personal Details

Name:	Norbert Bißmeyer
Telephone:	+49 6151 869 324
Email:	norbert.bissmeyer@sit.fraunhofer.de
Date of birth:	25.09.1981 in Osnabrück, Germany
Nationality:	German

C.2. Academic History

03/2009 - 06/2012	Supervision of student works in the seminar “Security in Ad hoc, Sensor, and Mesh Networks” at the Darmstadt University of Technology, Department of Computer Science.
10/2006 - 10/2008	Technical College FH Joanneum in Kapfenberg, Austria Course of studies: Advanced Security Engineering Master thesis at the Fraunhofer Institute IGD in Darmstadt, Germany ”Distributed Data Collection and Analysis for Attack Detection in Mobile Ad hoc Networks”. Creating a concept for data collection and intrusion detection in mobile ad hoc networks and implementation in a simulation environment in order to evaluate the concept. Completion in October 2008 with total mark: excellent (1.4).
10/2003 - 09/2006	Technical College FH Münster, Germany Curse of studies: Applied Computer Science Bachelor thesis at the insurance company LVM in Münster, Germany

	”Realtime observation of OpenNMS”. Analysis of the possibilities to apply the software into the infrastructure of the company. Developing an real time observation module as enhancement for OpenNMS. Completion in September 2006 with total mark: good (1.8).

C.3. Professional Education

08/1998 - 08/2001	Bosch Telecom / Tenovis GmbH & Co. KG in Dortmund, Germany IT Service Engineer at the customer and in the online service. Responsible for the installation of telephone systems at the customer and 2nd level support tasks in the online service. Completion in August 2001 as IT-Service Engineer with total mark: good

C.4. Professional Experience

11/2008 -	Scientific employee at Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt, Germany in the department Mobile Networks (MNE). The primary work area are vehicular ad hoc networks with focus on security and privacy concepts. Misbehavior detection with appropriate response mechanisms in decentralized ITS commutation is the primary research topic.
10/2007 - 12/2007	Internship at the Letterkenny Institute of Technology in Letterkenny, Ireland Developing of an application in Microsoft .NET for the management and helpdesk of the college.
01/2003 - 12/2009	Self-employed in the field of web application development. Primary active in creating dynamic web applications and product management systems for national and international customers.
08/2001 - 08/2003	Tenovis Service GmbH & Co. KG in Dortmund, Germany Helpdesk and online service for telephone systems. IT Service Engineer in the 2nd level support.

C.5. Supervision of Diploma-, Master- and Bachelor-Theses

10/2012 - 04/2013
Master thesis of Henrik Schröder
Supervised by Prof. Dr. Michael Waidner from Darmstadt University of Technology, Germany, Security in Information Technology
Analysis of Attack Methods on Car-to-X Communication Using Practical Tests

06/2012 - 09/2012
Bachelor thesis of Tobias Gundlach
Supervised by Prof. Dr.-Ing. Horst Wieker, Hochschule für Technik und Wirtschaft, Germany
Implementation of the Automated Evaluation of Security Related Log Data for simTD

11/2011 - 5/2012
Master thesis of Sebastian Mauthofer
Supervised by Prof. Dr.-Ing. Matthias Hollick from Darmstadt University of Technology, Germany, Secure Mobile Networking (Department of Computer Science)
Security in VANETs: Assessment of Vehicle Trustworthiness using Particle Filters

03/2011 - 09/2011
Master thesis of Joël Njeukam
Supervised by Prof. Dr.-Ing. Ralf Steinmetz and Dr.-Ing. André König from the Darmstadt University of Technology, Germany, Multimedia Communications Lab (Department of Electrical Engineering and Information Technology)
Development of an Automated Revocation Mechanism based on Misbehavior Detection in a Car-to-X PKI

08/2010 - 01/2011
Bachelor thesis of Daniel Quanz
Supervised by Prof. Dr.-Ing. Sorin A. Huss from the Darmstadt University of Technology, Germany, Integrated Circuits and Systems (Department of Computer Science)
Implementation of a Vehicle Plausibility Check based on Communication Data and Sensor Data

04/2010 - 10/2010
Bachelor thesis of Christian Schmidt
Supervised by Prof. Dr. Ulf Schemmert from the University of Applied Sciences Leipzig (HfTL), Germany

	Implementierung und Evaluierung von Angriffen in der VANET Simulationsumgebung VSimRTI
02/2010 - 8/2010	Master thesis of Christian Stresing Supervised by Prof. Dr.-Ing. Matthias Hollick from Darmstadt University of Technology, Germany, Secure Mobile Networking (Department of Computer Science) Intrusion Detection in VANETs through Verification of Vehicle Movement Data Applying a Plausibility Model
10/2009 - 04/2010	Diploma thesis of Mohammed Douiri from Koblenz-Landau University, Germany Supervised by Prof. Dr. Rüdiger Grimm from the Koblenz-Landau University, Germany Analyse und Evaluierung der Angriffserkennung in Car-to-Car Netzwerken

C.6. Review Work

- International Conference on Advances in Vehicular Systems (VEHICULAR), Technologies and Applications 2013 and 2014
- IEEE Transactions on Vehicular Technology (TVT) 2013
- IEEE Vehicular Technology Conference (VTC) 2013-Spring
- International Conference on Computer and Communication Technology (ICCCT) 2011, 2012 and 2013
- IEEE Vehicular Networking Conference (VNC) 2012
- IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) 2011 and 2012
- European Symposium on Research in Computer Security (ESORICS) 2012
- IEEE Wireless Communications and Networking Conference (WCNC) 2011

Bibliography

[All13] OSGi Alliance. Open services gateway initiative, October 2013.

[Bar04] Rimon Barr. JiST - java in simulation time. Technical report, Cornell University, USA, barr@cs.cornell.edu, 2004.

[Bar06] Rimon Barr. *SWANS - Scalable Wireless Ad hoc Network Simulator: User Guide*. Cornell Research Foundation, Inc., January 2006.

[BB04] Sonja Buchegger and Jean-Yves Le Boudec. A robust reputation system for p2p and mobile ad-hoc networks. In *P2PEcon*, 2004.

[BB11] Norbert Bißmeyer and Kpatcha M. Bayarou. Angriffserkennung in der Car-to-X Kommunikation basierend auf Bewegungsinformationen. In *27. VDI / VW-Gemeinschaftstagung Automotive Security*. Verein Deutscher Ingenieure (VDI), Oktober 2011.

[BLB11] Chaminda Basnayake, Gérard Lachapelle, and Jared Bancroft. Relative positioning for vehicle-to-vehicle communications-enabled vehicle safety applications. In *18th ITS World Congress*. ITS America, October 2011.

[BMBK12] Norbert Bißmeyer, Sebastian Mauthofer, Kpatcha M. Bayarou, and Frank Kargl. Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters. In *IEEE Vehicular Networking Conference (VNC)*. IEEE, November 2012.

[BMP+14] Norbert Bißmeyer, Sebastian Mauthofer, Jonathan Petit, Mirko Lange, Martin Moser, Daniel Estor, Michel Sall, Michael Feiri, Rim Moalla, Marcello Lagana, and Frank Kargl. PRESERVE d1.3 v2x security architecture v2. Deliverable, PREparing SEcuRe VEhicle-to-X Communication Systems Consortium, January 2014.

[BNPB12] Norbert Bißmeyer, Joel Njeukam, Jonathan Petit, and Kpatcha Bayarou. Central misbehavior evaluation for VANETs based on mobility data plausibility. In *VANET '12: International workshop on Vehicular inter-networking*. ACM, April 2012.

[BP99] Samuel S. Blackman and Robert Popoli. *Design and Analysis of Modern Tracking Systems*. Artech House Publishers, 1999.

[BPB13] Norbert Bißmeyer, Jonathan Petit, and Kpatcha M. Bayarou. CoPRA: Conditional pseudonym resolution algorithm in VANETs. In *The 10th Annual Conference on Wireless On-Demand Network Systems and Services (WONS)*. IEEE, March 2013.

[BS02] Yaakov Bar-Shalom. Update with out-of-sequence measurements in tracking: exact solution. *IEEE Transactions on Aerospace and Electronic Systems*, 38(3):769–777, July 2002.

[BSB10] Norbert Bißmeyer, Christian Stresing, and Kpatcha Bayarou. Intrusion detection in VANETs through verification of vehicle movement data. In *IEEE Vehicular Network-*

ing Conference (VNC). IEEE, December 2010.

[BSM+09] Norbert Bißmeyer, Hagen Stübing, Manuel Mattheß, Jan Peter Stotz, Julian Schütte, Matthias Gerlach, and Florian Friederici. simTD security architecture: Deployment of a security and privacy architecture in field operational tests. In *7th Conference: escar - Embedded Security in Cars*. isits International School of IT Security, November 2009.

[BSP+13] Norbert Bißmeyer, Henrik Schröder, Jonathan Petit, Sebastian Mauthofer, and Kpatcha Bayarou. Short paper: Experimental analysis of misbehavior detection and prevention in VANETs. In *IEEE Vehicular Networking Conference (VNC)*. IEEE, December 2013.

[BSRS11] Norbert Bißmeyer, Björn Schünemann, Ilja Radusch, and Christian Schmidt. Simulation of attacks and corresponding driver behavior in vehicular ad hoc networks with VSimRTI. In *SIMUTools 2011, 4th International ICST Conference on Simulation Tools and Techniques*, March 2011.

[BSS+11] Norbert Bißmeyer, Jan Peter Stotz, Hagen Stübing, Elmar Schoch, Stefan Götz, and Brigitte Lonc. A generic public key infrastructure for securing car-to-x communication. In *18th World Congress on Intelligent Transportation Systems*. ITS America, October 2011.

[BSS13] Norbert Bißmeyer, Florian Schimandl, and Jens Schmidt. Safe and Intelligent Mobility Test Field Germany: Working Document W43.2; Technische Auswertung, IT-Sicherheit. Working Document W43.2, simTD Consortium, September 2013.

[Buc04] Sonja Buchegger. *Coping with Misbehavior in Mobile Ad-hoc Networks*. Phd thesis, École Polytechnique Fédérale de Lausanne, February 2004.

[CC13] C2C-CC. Car 2 car communication consortium. online, November 2013. http://www.car-to-car.org.

[Cha88] David Chaum. Blind siganture systems, July 1988. Patent.

[CKL+08] Zhen Cao, Jiejun Kong, U. Lee, M. Gerla, and Zhong Chen. Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks. In *INFOCOM Workshops 2008*, pages 1 – 6. IEEE, April 2008.

[CL99] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the third symposium on Operating systems design and implementation*, OSDI '99, pages 173–186. USENIX Association, February 1999.

[CLPZ10] Giovanni Di Crescenzo, Yibei Ling, Stanley Pietrowicz, and Tao Zhang. Non-interactive malicious behavior detection in vehicular networks. In *IEEE Vehicular Networking Conference (VNC)*. IEEE, December 2010.

[CNW11] Liqun Chen, Siaw-Lynn Ng, and Guilin Wang. Threshold anonymous announcement in VANETs. *IEEE Journal on Selected Areas in Communications*, 29(3):605–615, March 2011.

[Com09] European Commission. Standardisation mandate addressed to CEN, CENELEC and ETSI in the field of information and communication technologies to support the interoperability of co-operative systems for intelligent transport in the european community, October 2009. http://ec.europa.eu/enterprise/sectors/ict/files/

standardisation_mandate_en.pdf.

[Con11] Car 2 Car Communication Consortium. Memorandum of understanding for OEMs within the car 2 car communication consortium on deployment strategy for cooperative ITS in europe. online, June 2011. http://www.car-to-car.org.

[CWHZ09] Chen Chen, Xin Wang, Weili Han, and Binyu Zang. A robust detection of the sybil attack in urban VANETs. In *29th IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW '09*. IEEE Computer Society, June 2009.

[DFM05] Florian Dötzer, Lars Fischer, and Przemyslaw Magiera. VARS: a vehicle ad-hoc network reputation system. In *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM)*, pages 454 – 456. IEEE, June 2005.

[DGB08] Anurag D, Srideep Ghosh, and Somprakash Bandyopadhyay. GPS based vehicular collision warning system using IEEE 802.15.4 MAC/PHY standard. In *8th International Conference on ITS Telecommunications (ITST)*, pages 154 –159, October 2008.

[DLJZ10] Qing Ding, Xi Li, Ming Jiang, and Xuehai Zhou. Reputation management in vehicular ad hoc networks. In *International Conference on Multimedia Technology (ICMT)*, pages 1–5. IEEE, October 2010.

[DOJ+10] Sanjay K. Dhurandher, Mohammad S. Obaidat, Amrit Jaiswal, Akanksha Tiwari, and Ankur Tyagi. Securing vehicular networks: A reputation and plausibility checks-based approach. In *GLOBECOM Workshop on Web and Pervasive Security*, pages 1550–1554. IEEE, December 2010.

[Dou02] John R. Douceur. The sybil attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, IPTPS '01, pages 251–260. Springer-Verlag, 2002.

[DS06] Murat Demirbas and Youngwhan Song. An rssi-based scheme for sybil attack detection in wireless sensor networks. In *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks*, WOWMOM '06, pages 564–570. IEEE Computer Society, 2006.

[EB09] Peter Ebinger and Norbert Bißmeyer. TEREC: Trust evaluation and reputation exchange for cooperative intrusion detection in MANETs. In *Communication Networks and Services Research Conference, CNSR'09*. ACM, May 2009.

[Ebi13] Peter Ebinger. *Robust Situation Awareness in Tactical Mobile Ad Hoc Networks*. PhD thesis, Technische Universität Darmstadt, 2013.

[ESG+10] David Eckhoff, Christoph Sommer, Tobias Gansen, Reinhard German, and Falko Dressler. Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping. In *IEEE Vehicular Networking Conference (VNC)*, pages 174–181. IEEE, December 2010.

[ETS09] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions. Technical Report TR 102 638, ETSI, June 2009. v1.1.1.

[ETS10a] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); communications architecture. European Norm EN 302 665, ETSI, September

2010. v1.1.1.

[ETS10b] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); european profile standard for the physical and medium access control layer of intelligent transport systems operating in the 5 ghz frequency band. European Standard ES 202 663, ETSI, January 2010. v1.1.0.

[ETS10c] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); security; security services and architecture. Technical Standard TS 102 731, ETSI, September 2010. v1.1.1.

[ETS10d] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. Technical Standard TS 102 637-2, ETSI, April 2010. v1.1.1.

[ETS10e] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service. Technical Standard TS 102 637-3, ETSI, September 2010. v1.1.1.

[ETS11] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); vehicular communications; geonetworking; part 3: Network architecture. European Norm EN 302 636-3, ETSI, 2011. v1.1.1.

[ETS12a] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); security; its communications security architecture and security management. Technical Standard TS 102 940, ETSI, July 2012. v1.1.1.

[ETS12b] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); security; trust and privacy management. Technical Standard TS 102 941, ETSI, June 2012. v1.1.1.

[ETS13a] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); osi cross-layer topics; part 8: Interface between security entity and network and transport layers. Technical Standard TS 102 723-8, ETSI, April 2013. v0.1.0.

[ETS13b] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (its); security; security header and certificate formats. Technical Standard TS 103 097, ETSI, April 2013. v1.1.1.

[ETS13c] ETSI - European Telecommunications Standards Institute. Intelligent transport systems (ITS); security; threat, vulnerability and risk analysis (TVRA). Technical Report TR 102 893, ETSI, January 2013. v1.1.3.

[FAEV06] Lars Fischer, Amer Aijaz, Claudia Eckert, and David Vogt. Secure revocable anonymous authenticated inter-vehicle communication (SRAAC). In *4th Conference: escar - Embedded Security in Cars*. isits International School of IT Security, November 2006.

[fAITI13] Daimler Center for Automotive Information Technology Innovations. VSimRTI - Smart Mobility Simulation. online, October 2013. http://www.dcaiti.tu-berlin.de/research/simulation/.

[FCCP13] Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, and Panagiotis Papadimitratos. Discovery and verification of neighbor positions in mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 12(2):289–303, 2013.

[FGJ+10] Andreas Festag, Maria Goleva, Armin Jahanpanah, Hugo Santos, Christoph Sorge, and Wenhui Zhang. Safe and intelligent mobility test field germany - functional description and basic sim-net specification. Deliverable NEC-M1, NEC Europe Ltd., December 2010.

[fSI10] International Organization for Standardization (ISO). Intelligent transport systems – communications access for land mobiles (CALM) – architecture. Technical Report 21217, International Organization for Standardization (ISO), 2010.

[Fun13] Dillon Funkhouser. Safety pilot model deployment. Internet, March 2013. `http://safetypilot.umtri.umich.edu`.

[Gam88] Diego Gambetta. *Trust: Making and breaking cooperative relations*. Basil Blackwell, 1988.

[Ger07a] Matthias Gerlach. Trust for vehicular applications. In *Eighth International Symposium on Autonomous Decentralized Systems (ISADS)*, pages 295–304. IEEE, March 2007.

[Ger07b] Matthias Gerlach. Use cases for a vehicular network security system. Project Report 2.4, NOW: Network on Wheels, May 2007.

[Ger10] Matthias Gerlach. *Trusted Ad Hoc Communications for Intelligent Transportation Systems*. PhD thesis, Technische Universität Berlin, 2010.

[GFL+05] Matthias Gerlach, Andreas Festag, Tim Leinmüller, Gabriele Goldacker, and Charles Harsch. Security architecture for vehicular communication. In *International Workshop on Intelligent Transportation (WIT)*, 2005.

[GG07] Matthias Gerlach and Felix Güttler. Privacy in VANETs using changing pseudonyms - ideal and real. *IEEE 65th Vehicular Technology Conference (VTC-Spring)*, pages 2521 –2525, April 2007.

[GGS04] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks (VANET)*, pages 29–37. ACM, September 2004.

[GP09] Philippe Golle and Kurt Partridge. On the anonymity of home/work location pairs. In *Proceedings of the 7th International Conference on Pervasive Computing*, Pervasive '09, pages 390–397. Springer-Verlag, 2009.

[GT96] E. G. Golshtein and N. V. Tretyakov. *Modified Lagrangians and Monotone Maps in Optimization*. Wiley, April 1996.

[GVKG09] Mainak Ghosh, Anitha Varghese, Arzad A. Kherani, and Arobinda Gupta. Distributed misbehavior detection in VANETs. In *Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, April 2009.

[GWB12] Tobias Gundlach, Horst Wieker, and Norbert Bißmeyer. Implementation of the automated evaluation of security related log data for simtd. Bachelor thesis, Hochschule für Technik und Wirtschaft des Saarlandes, September 2012.

[HAF+09] Olaf Henniger, Ludovic Apvrille, Andreas Fuchs, Yves Roudier, Alastair Ruddle, and Benjamin Weyl. Security requirements for automotive on-board networks. In *9th International Conference on Intelligent Transport Systems Telecommunications (ITST)*, pages 641–646. IEEE, October 2009.

[HCL04] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *Security Privacy, IEEE*, 2(3):49–55, May 2004.

[HMdPS05] Kaijen Hsiao, Jason Miller, and Henry de Plinval-Salgues. Particle filters and their applications. *Cognitive Robotics*, April 2005.

[HMYS05] Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki. Enhancing wireless location privacy using silent period. In *Wireless Communications and Networking Conference*, volume 2, pages 1187–1192. IEEE, March 2005.

[HPJ06] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, February 2006.

[HRM10] Jorge Hortelano, Juan Carlos Ruiz, and Pietro Manzoni. Evaluating the usefulness of watchdogs for intrusion detection in VANETs. In *IEEE International Conference on Communications Workshops (ICC)*, pages 1–5. IEEE, May 2010.

[IEE04] IEEE Computer Society. IEEE standard specifications for public-key cryptography-amendment 1: Additional techniques. *IEEE Std 1363a-2004 (Amendment to IEEE Std 1363-2000)*, pages 1 –159, 2004. ECIES.

[IEE10] IEEE Computer Society. IEEE standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – Part II: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. Technical report, IEEE Std 802.11p, 2010.

[IEE13] IEEE Computer Society. Ieee standard for wireless access in vehicular environments - security services for applications and management messages. IEEE Standard IEEE P1609.2-2013, Institute of Electrical and Electronics Engineers, April 2013. (Revision of IEEE Std 1609.2-2006).

[Ins13] European Telecommunications Standards Institute. ETSI - Cooperative ITS. online, July 2013. http://www.etsi.org/index.php/technologies-clusters/technologies/intelligent-transport/cooperative-its.

[Jak97] Markus Jakobsson. *Privacy vs. Authenticity*. Phd thesis, University of California, San Diego, 1997.

[JBSH11] Attila Jaeger, Norbert Bißmeyer, Hagen Stübing, and Sorin A. Huss. A novel framework for efficient mobility data verification in vehicular ad-hoc networks. *International Journal of ITS Research, ITS Japan*, 9(3), September 2011.

[JI02] Audun Jøsang and Roslan Ismail. The beta reputation system. In *In Proceedings of the 15th Bled Electronic Commerce Conference*, 2002.

[JJM07] Debasish Jena, Sanjay Kumar Jena, and Banshidhar Majhi. A novel untraceable blind signature based on elliptic curve discrete logarithm problem. *IJCSNS*, 7(6):269–275,

June 2007.

[Jøs01] Audun Jøsang. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3):279–311, June 2001.

[Kal60] Rudolph Emil Kalman. A new approach to linear filtering and prediction problems. In *Transactions of the ASME - Journal of Basic Engineering*, 1960.

[KCD+09] Ram Kandarpa, Mujib Chenzaie, Matthew Dorfman, Justin Anderson, Jim Marousek, Ian Schworer, Joe Beal, Chris Anderson, Tim Weil, and Frank Perry. Final report: Vehicle infrastructure integration (vii) proof of concept (poc) test – executive summary. Technical Report FHWA-JPO-09-038, Booz Allen Hamilton, February 2009.

[KHRW02] Daniel Krajzewicz, Georg Hertkorn, Christian Rössel, and Peter Wagner. SUMO (Simulation of Urban MObility); an open-source traffic simulation. In *Proceedings of the 4th Middle East Symposium on Simulation and Modelling (MESM2002)*, pages 183–187, September 2002.

[KL08] William Kozma and Loukas Lazos. Reactive identification of misbehavior in ad hoc networks based on random audits. In *5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pages 612–614. IEEE, June 2008.

[Kun08] Antonio Kung. Deliverable 2.1 security architecture and mechanisms for V2V / V2I. Deliverable Projectnumber: IST-027795, SeVeCom, February 2008.

[LB09] Christine Laurendeau and Michel Barbeau. Probabilistic localization and tracking of malicious insiders using hyperbolic position bounding in vehicular networks. *EURASIP Journal on Wireless Communications and Networking*, pages 1–13, 2009.

[LCH10] Bisheng Liu, Jerry T. Chiang, and Yih-Chun Hu. Limits on revocation in VANETs. In *8th International Conference on Applied Cryptography and Network Security*. ACNS, June 2010.

[LHH08] Kenneth P. Laberteaux, Jason J. Haas, and Yih-Chun Hu. Security certificate revocation list distribution for VANET. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking (VANET)*, pages 88–89. ACM, September 2008.

[LHSW04] Tim Leinmüller, Albert Held, Günter Schäfer, and Adam Wolisz. Intrusion detection in VANETs. In *12th IEEE International Conference on Network Protocols(ICNP)*, 2004.

[LMSK06] Tim Leinmüller, Christian Maihöfer, Elmar Schoch, and Frank Kargl. Improved security in geographic ad hoc routing through autonomous position verification. In *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 57–66, New York, NY, USA, 2006. ACM.

[LS06] Tim Leinmüller and Elmar Schoch. Greedy routing in highway scenarios: The impact of position faking nodes. In *Workshop on Intelligent Transportation (WIT)*, 2006.

[LSK06] Tim Leinmüller, Elmar Schoch, and Frank Kargl. Position verifcation approaches for vehicular ad hoc networks. *Wireless Communications, IEEE*, 13(5):16 –21, October 2006.

[LSKM05] Tim Leinmüller, Elmar Schoch, Frank Kargl, and Christian Maihöfer. Influence of falsified position data on geographical ad-hoc routing. In *ACM Workshop on Security and*

Privacy in Ah hoc and Sensor Networks (ESAS), pages 102–112. ACM, 2005.

[LSM07] Tim Leinmüller, Elmar Schoch, and Christian Maihofer. Security requirements and solution concepts in vehicular ad hoc networks. *Fourth Annual Conference on Wireless on Demand Network Systems and Services (WONS)*, pages 84 –91, January 2007.

[LSP82] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, July 1982.

[LSS+08] Tim Leinmüller, Robert Schmidt, Elmar Schoch, Albert Held, and Christian Schafer. Modeling roadside attacker behavior in VANETs. *IEEE GLOBECOM Workshops*, pages 1 –10, December 2008.

[LWR03] CH Lo, YK Wong, and AB Rad. Bayesian network for fault diagnosis. In *European Control Conference*. IEEE, September 2003.

[MAG14] M2M MAGAZINE. Nokia HERE, continental team up on connected car. online, January 2014. http://www.machinetomachinemagazine.com/2014/01/20/nokia-here-continental-team-up-on-connected-car.

[Mai04] Christain Maihöfer. A survey of geocast routing protocols. *IEEE Communications Surveys Tutorials*, 6(2):32–42, 2004.

[MBH12] Sebastian Mauthofer, Norbert Bißmeyer, and Matthias Hollick. Security in VANETs: Assessment of vehicle trustworthiness using particle filters. Master thesis, Technical University Darmstadt, Department of Computer Science, Secure Mobile Networking Lab, May 2012.

[MBS+09] Manuel Mattheß, Norbert Bißmeyer, Julian Schütte, Jan Peter Stotz, Matthias Gerlach, Florian Friederici, Christoph Sommer, Hervé Seudié, Winfried Stephan, Eric Hildebrandt, Jonas Vogt, Bechir Allani, Tobias Gansen, Anke Jentzsch, Hagen Stübing, and Attila Jaeger. Safe and Intelligent Mobility Test Field Germany; Deliverable D21.5; Specification of IT Security Solution. Technical report, simTD Consortium, October 2009.

[MBZ+12] Charles Miller, Dion Blazakis, Dino Dai Zovi, Stefan Esser, Vincenzo Iozzo, and Ralf-Phillipp Weinmann. *IOS Hacker's Handbook*. Wiley, 2012.

[MGLB00] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 255–265, New York, NY, USA, 2000. ACM.

[MP12] Félix Gómez Mármol and Gregorio Martínez Pérez. TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, 35:934–941, May 2012.

[MRC+08] Tyler Moore, Maxim Raya, Jolyon Clulow, Panagiotis (Panos) Papadimitratos, Ross Anderson, and Jean-Pierre Hubaux. Fast exclusion of errant devices from vehicular networks. In *IEEE SECON*. IEEE, June 2008.

[NSKB11] Joël Njeukam, Ralf Steinmetz, André König, and Norbert Bißmeyer. Development of an automated revocation mechanism based on misbehavior detection in a car-to-x PKI.

Master thesis, Technische Universität Darmstadt, Fachbereich Elektrotechnik und Informationstechnik, September 2011.

[ODS07] Benedikt Ostermaier, Florian Dötzer, and Markus Strassberger. Enhancing the security of local danger warnings in VANETs - a simulative analysis of voting schemes. In *Second International Conference on Availability, Reliability and Security (ARES)*, 2007.

[oEE00] Institute of Electrical and Electronics Engineers. *IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)–Federate Interface Specification. IEEE Standard 1516.1*. IEEE, 2000.

[oTRA12] U.S. Department of Transportation Research and Innovative Technology Administration. Security credential management system design security system design for cooperative vehicle-to-vehicle crash avoidance applications using 5.9 ghz dedicated short range communications (DSRC) wireless communications. Draft report, CAMP, VSC3, www.its.dot.gov, April 2012.

[OYN+08] Hisashi Oguma, Akira Yoshioka, Makoto Nishikaw, Rie Shigetomi, Akira Otsuka, and Hideki Imai. New attestation based security architecture for in-vehicle communication. In *IEEE Global Telecommunications Conference*, pages 1–6. IEEE, December 2008.

[Pap08] Panagiotis Papadimitratos. "On the Road" - reflections on the security of vehicular communication systems. *IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, pages 359–363, sept. 2008.

[PATZ09] Soyoung Park, Baber Aslam, Damla Turgut, and Cliff C. Zou. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In *Military Communications Conference (MILCOM)*, pages 1–7. IEEE, October 2009.

[PB11] Zeljko Popovic and Sue Bai. Automotive lane-level positioning: 2010 status and 2020 forecast. In *18th ITS World Congress*. ITS America, October 2011.

[PBH+08] Panagiotis Papadimitratos, Levente Buttyán, Támas Holczer, Elmar Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, and Jean-Pierre Hubaux. Secure vehicular communication systems: Design and architecture. *IEEE Communications Magazine*, 0163-6804/08:100–109, November 2008.

[PFK11] Jonathan Petit, Michael Feiri, and Frank Kargl. Spoofed data detection in VANETs using dynamic thresholds. In *IEEE Vehicular Networking Conference (VNC)*. IEEE, November 2011.

[PH10] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, August 2010. v0.34.

[PZS10] Stan Pietrowicz, Tao Zhang, and Hyong Shim. Short-lived, unlinked certificates for privacy-preserving secure vehicular communications. In *17th ITS World Congress*, number 01345263. ITS America, October 2010.

[QBa11] Daniel Quanz, Norbert Bißmeyer, and Attila Jaeger and. Implementation of a vehicle plausibility check based on communication data and sensor data. Bachelor thesis, Technical University Darmstadt, January 2011.

[QSR08] Tobias Queck, Björn Schünemann, and Ilja Radusch. Runtime infrastructure for simulating vehicle-2-x communication scenarios. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, VANET '08. ACM, 2008.

[RA12] Research and Innovative Technology Administration. The national its architecture 7.0. Technical Report 7.0, U.S. Department of Transportation, Research and Innovative Technology Administration (RITA), January 2012.

[Rie07] Sebastian Ries. Certain trust: A trust model for users and agents. In *Proceedings of the 2007 ACM Symposium on Applied Computing (SAC)*, pages 1599–1604. ACM, 2007.

[Rie09] Sebastian Ries. *Trust in Ubiquitous Computing*. PhD thesis, Technische Universität Darmstadt, 2009.

[RLY+09] Ziwei Ren, Wenfan Li, Qing Yang, Shaoen Wu, and Lei Chen. Location security in geographic ad hoc routing for VANETs. In *International Conference on Ultra Modern Telecommunications Workshops (ICUMT)*, pages 1–6. IEEE, October 2009.

[RMFH08] Maxim Raya, Mohammad Hossein Manshaei, Márk Félegyhazi, and Jean-Pierre Hubaux. Revocation games in ephemeral networks. In *Proceedings of the 15th ACM conference on Computer and communications security*, CCS '08, pages 199–210, New York, NY, USA, 2008. ACM.

[RPA+07] Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, and Jean-Pierre Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, 25(8):1557–1568, October 2007.

[SA14] Greg Stanley and Associates. A guide to fault detection and diagnosis. Online, Febraury 2014. http://gregstanleyandassociates.com/whitepapers/FaultDiagnosis/faultdiagnosis.htm.

[SBH+10] Hagen Stuebing, Marc Bechler, Dieter Heussner, Thomas May, Ilja Radusch, Horst Rechner, and Peter Vogel. simTD: A Car-To-X System Architecture for Field Operational Tests. *IEEE Communications Magazine*, May 2010.

[SBK+11] Jan Peter Stotz, Norbert Bißmeyer, Frank Kargl, Stefan Dietzel, Panos Papadimitratos, and Christian Schleiffer. PRESERVE d1.1 security requirements of vehicle security architecture. Deliverable, PRESERVE consortium, July 2011.

[Sch09] Elmar Schoch. *Secure Communication in Inter-Vehicle Networks*. PhD thesis, Ulm university, October 2009.

[Sch13] Matthias Schulze. DRIVE C2X - accelerate cooperative mobility, March 2013. http://www.drive-c2x.eu.

[SES+13] Jens Schmidt, Kurt Eckert, Gunther Schaaf, Stefan Gläser, Ralf Grigutsch, Ingo Totzke, Madeline Volk, Norbert Bißmeyer, Carsten Kühne, Gert Stahnke, and Markus Bauer. Safe and Intelligent Mobility Test Field Germany: Deliverable D5.5 Part B-2; Nutzerakzeptanz, IT-Sicherheit, Datenschutz und Schutz der Privatsphäre. Technical Report D5.5 - Part B-2, simTD Consortium, July 2013.

[SFH11] H. Stubing, J. Firl, and S.A. Huss. A two-stage verification process for car-to-x mobility data based on path prediction and probabilistic maneuver recognition. In *Vehicular*

Networking Conference (VNC), 2011 IEEE, pages 17 –24, nov. 2011.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.

[SHB10] Christian Stresing, Matthias Hollick, and Norbert Bißmeyer. Intrusion detection in VANETs through verifcation of vehicle movement data applying a plausibility model. Master thesis, Technische Universität Darmstadt, Department of Computer Science, Secure Mobile Networking (SEEMOO), 2010.

[SIF97] Kiyotaka Shimizu, Yo Ishizuka, and Jonathan F.Bard. *Nondifferentiable and Two-Level Mathematical Programming*. Kluwer Academic Publishers, 1997.

[SJB+10] Hagen Stübing, Attila Jaeger, Norbert Bißmeyer, Christian Schmidt, and Sorin A. Huss. Verifying mobility data under privacy considerations in car-to-x communication. In *17th ITS World Congress*. ITS Asia, October 2010.

[SJWH11] Hagen Stübing, Attila Jaeger, Nikolas Wagner, and Sorin A. Huss. Integrating secure beamforming into car-to-x architectures. *SAE International Journal of Passenger Cars-Electronic and Electrical Systems*, 4:88–96, June 2011.

[SKMW10] Florian Schaub, Frank Kargl, Zhendong Ma, and Michael Weber. V-tokens for conditional pseudonymity in VANETs. In *IEEE Wireless Communications and Networking Conference (WCNS)*. IEEE, April 2010.

[SLH09] Robert K. Schmidt, Tim Leinmüller, and Albert Held. Defending against roadside attackers. In *16th World Congress on Intelligent Transport Systems*. ITS Europe, September 2009.

[SLS+08] Robert K. Schmidt, Tim Leinmüller, Elmar Schoch, Albert Held, and Günter Schäfer. Vehicle behavior analysis to enhance security in VANETs. In *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM)*. IEEE, June 2008.

[SMR08] Björn Schünemann, Kay Massow, and Iljia Radusch. A novel approach for realistic emulation of vehicle-2-x communication applications. In *Vehicular Technology Conference (VTC Spring)*, volume 7, pages 2709–2713. IEEE, May 2008.

[SONP12] Erfan Soltanmohammadi, Mahdi Orooji, and Mort Naraghi-Pour. Distributed detection in wireless sensor networks in the presence of misbehaving nodes. In *Military communications conference (MILCOM)*, pages 1–6. IEEE, November 2012.

[SPC11] Xueyuan Su, Gang Peng, and Sammy Chan. Forbid: Cope with byzantine behaviors in wireless multi-path routing and forwarding. In *Global Telecommunications Conference (GLOBECOM)*, pages 1–6. IEEE, 2011.

[SSB10] Christian Schmidt, Ulf Schemmert, and Norbert Bißmeyer. Implementierung und evaluierung von angriffen in der VANET simulationsumgebung VSimRTI. Bachelor thesis, Hochschule für Telekommunikation Leipzig, Fachbereich Nachrichtentechnik, Institut für Telekommunikationsinformatik, September 2010.

[Stü12] Hagen Stübing. *Multi-Layered Security and Privacy Protection in Cooperative Vehicular Networks*. PhD thesis, Technische Universität Darmstadt, 2012.

[SWB13] Henrik Schröder, Michael Waidner, and Norbert Bißmeyer. Analysis of attack methods on car-to-x communication using practical tests. Master thesis, Technische Universität

Darmstadt, Department of Computer Science, 2013.

[SWS+12] Ankit Singh, Matthias Wagner, Jörg Schäfer, Hervais Simo-Fhom, and Norbert Bißmeyer. Restricted usage of anonymous credential in VANET for misbehavior detection. Master thesis, University of Applied Sciences Frankfurt am Main, Germany, 2012.

[Tan03] Andrew S. Tanenbaum. *Computer Networks*, volume 5. Pearson Educations, 2003.

[Tar10] Christopher Tarnovsky. Hacking the smartcard chip. In *Blackhat Decipher Security 2010*, February 2010.

[TBF05] Sebastian Thrun, Wolfram Burgard, and Dieter Fox. *Probabilistic Robotics*. MIT Press, Cambridge, 2005.

[TWLY10] Daxin Tian, Yunpeng Wang, Guangquan Lu, and Guizhen Yu. A vehicular ad hoc networks intrusion detection system based on busnet. In *2nd International Conference on Future Computer and Communication (ICFCC)*, volume 1, pages 225–229, May 2010.

[WBB+12] Christian Weiß, Harald Berninger, Norbert Bißmeyer, Kurt Eckert, Wilfried Enkelmann, Jörg Freudenstein, Stefan Gläser, Dieter Heussner, Arno Hinsberger, Attila Jaeger, Volker Kanngießer, Stefan Karl, Carsten Kemper, Benjamin Kentsch, Sascha Kilb, Carsten Kühnel, Andreas Lotz, Robert Mänz, Manuel Matteß, Gerhard Nöcker, Robert Protzmann, Hongjun Pu, Thomas Riedel, Gunther Schaaf, Manuel Schoch, Burak Simsek, Jonas Vogt, Andreas von Eichhorn, Martin Wiecker, and Peter Zahn. Safe and Intelligent Mobility Test Field Germany; Working Document W41.2c Technical Evaluation Concept. (Access restricted to consotium members), April 2012.

[WBF+13] Christian Wewetzer, Thomas Biehle, Andreas Festag, Tim Leinmueller, Teodor Buburuzan, Nikoletta Sofra, Elmar Schoch, Bernhard Jungk, Lan LIN, Katrin Sjöberg, and Achim Brakemaier. C2C-CC basic system standards profile. Draft 0.4, CAR 2 CAR Communication Consortium, March 2013.

[Wei09] Christian Weiß. Safe and Intelligent Mobility Test Field Germany, Project Profile. online, September 2009. Eight pages with the most important facts on the project. http://www.simtd.de.

[Wei12] Christian Weiß. Safe and Intelligent Mobility Test Field Germany; Field Operational Test Brochure. online, October 2012. http://www.simtd.de.

[WKMP10] Björn Wiedersheim, Frank Kargl, Zhendong Ma, and Panos Papadimitratos. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In *7th International Conference on Wireless On-demand Network Systems and Services (WONS)*, pages 176–183, February 2010.

[WWKH13] William Whyte, André Weimerskirch, Virendra Kumar, and Thorsten Hehn. A security credential management system for v2v communications. In *IEEE Vehicular Networking Conference (VNC)*. IEEE, December 2013.

[WWZ+11] Benjamin Weyl, Marko Wolf, Frank Zweers, Timo Gendrullis, Muhammad Sabir Idrees, Yves Roudier, Hendrik Schweppe, Hagen Platzdasch, Rachid El Khayari, Olaf Henniger, Dirk Scheuermann, Andreas Fuchs, Ludovic Apvrille, Gabriel Pedroza, Hervé Seudié, Jamshid Shokrollahi, and Anselm Keil. EVITA Deliverable D3.2: Secure On-board Architecture Specification. Technical report, EVITA Consortium, August 2011.

[XYG06] Bin Xiao, Bo Yu, and Chuanshan Gao. Detection and localization of sybil nodes in vanets. In *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks (DIWANS)*, pages 1–8. ACM, 2006.

[YCO09] Gongjun Yan, Xingwang Chen, and Stepharl Olariu. Providing VANET position integrity through filtering. *Intelligent Transportation Systems, 2009. ITSC '09. 12th International IEEE Conference on Intelligent Transportation Systems Communication*, pages 1–6, October 2009.

[YOW08] Gongjun Yan, Stephan Olariu, and Michele C. Weigle. Providing VANET security through active position detection. *Computer Communications*, 31(12):2883–2897, July 2008.

[Zad75] Lotfi A. Zadeh. Fuzzy logic and approximate reasoning. *Synthese*, 30(3-4):407–428, 1975.

[ZBS12a] Shuo Zhang and Yaakov Bar-Shalom. Optimal update with multiple out-of-sequence measurements with arbitrary arriving order. *IEEE Transactions on Aerospace and Electronic Systems*, 48(4):3116–3132, October 2012.

[ZBS12b] Shuo Zhang and Yaakov Bar-Shalom. Out-of-sequence measurement processing for particle filter: Exact bayesian solution. *IEEE Transactions on Aerospace and Electronic Systems*, 48(4):2818–2831, October 2012.

[ZCNC07] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty. Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. In *Proceedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous)*, pages 1–8. IEEE, 2007.

[Zha11] Jie Zhang. A survey on trust management for VANETs. In *IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pages 105–112, March 2011.

[ZMHT05] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo, and Roshan K. Thomas. A quantitative trust establishment framework for reliable data packet delivery in MANETs. In *ACM workshop on Security of ad hoc and sensor networks*. ACM, 2005.

[ZMHT06] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo, and Roshan K. Thomas. Robust cooperative trust establishment for MANETs. In *ACM workshop on Security of ad hoc and sensor networks*. ACM, October 2006.