

11-2015

Using Similarity to Achieve Trust to Enhance Decision Making in Vehicular Safety Applications

Hind Obaid Hamad Saeed Al Falasi

Follow this and additional works at: https://scholarworks.uaeu.ac.ae/all_dissertations

Part of the [Architecture Commons](#)

Recommended Citation

Saeed Al Falasi, Hind Obaid Hamad, "Using Similarity to Achieve Trust to Enhance Decision Making in Vehicular Safety Applications" (2015). *Dissertations*. 50.

https://scholarworks.uaeu.ac.ae/all_dissertations/50

This Dissertation is brought to you for free and open access by the Electronic Theses and Dissertations at Scholarworks@UAEU. It has been accepted for inclusion in Dissertations by an authorized administrator of Scholarworks@UAEU. For more information, please contact fadl.musa@uaeu.ac.ae.



جامعة الإمارات العربية المتحدة
United Arab Emirates University

United Arab Emirates University

College of Information Technology

USING SIMILARITY TO ACHIEVE TRUST TO ENHANCE
DECISION MAKING IN VEHICULAR SAFETY APPLICATIONS

Hind Obaid Hamad Saeed Al Falasi

This dissertation is submitted in partial fulfilment of the requirements for the degree
of Doctor of Philosophy

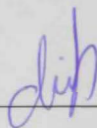
Under the Supervision of Dr. Hesham El-Sayed

November 2015

Declaration of Original Work

I, Hind Obaid Hamad Saeed Al Falasi, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this dissertation entitled "*Using Similarity to Achieve Trust to Enhance Decision Making in Vehicular Safety Applications*", hereby, solemnly declare that this dissertation is my own original research work that has been done and prepared by me under the supervision of Dr. Hesham El-Sayed, in the College Of Information Technology at UAEU. This work has not previously been presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my dissertation have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this dissertation.

Student's Signature _____



Date 21-Jan-2016

Copyright © 2015 Hind Obaid Hamad Saeed Al Falasi
All Rights Reserved

Advisory Committee

1) Advisor: Dr. Hesham El-Sayed

Title: Associate Professor

Networking Track

College of Information Technology

2) Co-advisor: Dr. Nader Mohamed

Title: Associate Professor

Networking Track

College of Information Technology

3) Member: Dr. Mohammad Mehedy Masud

Title: Assistant Professor

Enterprise Systems Track

College of Information Technology

Approval of the Doctorate Dissertation

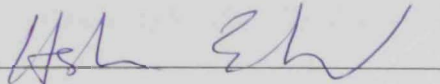
This Doctorate Dissertation is approved by the following Examining Committee Members:

- 1) Advisor (Committee Chair): Dr. Hesham El-Syed

Title: Associate Professor

Department of Networking

College of Information Technology

Signature 

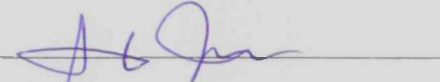
Date Nov. 24, 2015

- 2) Member: Dr. Imad Jawhar

Title: Associate Professor

Department of Networking

College of Information Technology

Signature 

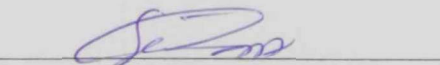
Date Nov. 24, 2015

- 3) Member: Dr. Mohamed Adel Serhani

Title: Associate Professor

Department of E-Commerce

College of Information Technology

Signature 

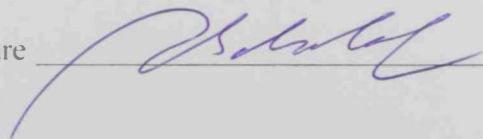
Date 24/11/2015

- 4) Member (External Examiner): Prof. Abdelsalam Helal

Title: Professor

Department of Computer and Information Science & Engineering

Institution: University of Florida

Signature 

Date 11/24/2015

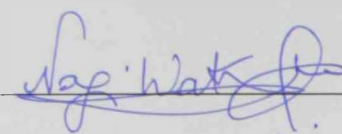
This Doctorate Dissertation is accepted by:

Dean of the College of Information Technology: Professor Omar El-Gayar

Signature  _____

Date Jan 21, 2016

Dean of the College of the Graduate Studies: Professor Nagi T. Wakim

Signature  _____

Date 24/1/2016

Copy 11 of 13

Abstract

Vehicles exchange different types of messages either periodically or as needed for different types of applications. The data in the network of vehicles can be used to extract valuable knowledge to support various applications in vehicular ad hoc networks (VANETs). Knowledge gained from the gathered data can be used to create local views of the network for individual vehicles; for instance, a vehicle can form a view of a subset of the network using neighboring vehicles' directions of travel, speeds, and the types of applications they run. In the network, vehicles that have common attributes and requirements facilitate the establishment of trust between them as these shared features make up the foundation for trust. Trust relations between vehicles can be utilized for enhancing the performance and reliability of some applications. This dissertation is concerned with trust establishment in VANETs, and how it can be utilized to enhance efficiency and decision making in the network. We provide solutions to this question: How to utilize trust relationship between vehicles to improve decision-making and efficiency in VANET safety applications. In our research, we aim to establish trust relationships through similarity to assist vehicles in identifying false safety messages in the network. We start by designing and implementing a trust management system to generate and process trust values and to establish a set of trusted relationships for vehicles running vehicular safety applications. Next, we explore the possibility of enhancing the decision-making process using trust. First, we develop an analytical model that associates trust with the performance of the decision-making process and the accuracy, and then we study the effectiveness of similarity-based trust in identifying false safety event messages in VANETs. Finally, we show that similarity-based trust has a positive impact on the time needed to make a decision and on the accuracy of that decision.

Keywords: VANETs, trust, similarity, system, architecture, model, safety applications, protocol.

Title and Abstract (in Arabic)

استخدام التشابه في تحقيق الثقة لتعزيز عملية صنع القرار في تطبيقات السلامة في المركبات

المخلص

تتبادل السيارات لطريق أنواعاً مختلفة من الرسائل إما دورياً أو عند الحاجة لأنواع مختلفة من التطبيقات. البيانات المرسله في شبكة من السيارات يمكن استخدامها لاستخراج معلومات قيمة لدعم تطبيقات مختلفة في VANETs. المعرفة المكتسبة من البيانات يمكن استخدامها لتشكيل مجموعات من المركبات، حيث أن المركبات يمكن جمعها معاً على أساس اتجاههم، وسرعتهم، وأنواع التطبيقات التي يستخدمونها. تسهل إقامة علاقات مبنية على الثقة بين المركبات التي تحتوي على سمات ومصالح واحتياجات مشتركة، كما تشكل هذه الميزات المشتركة الأساس للثقة. يمكن استخدام العلاقات المبنية على الثقة بين المركبات في رفع مستوى الأداء لبعض التطبيقات.

الهدف من هذه الأطروحة هو دراسة كيفية إنشاء نظام مبني على الثقة بين المركبات، من ثم كيفية استخدام علاقات الثقة في تحسين الكفاءة وعملية اتخاذ القرار في الشبكة. نهدف في بحثنا إلى بناء علاقات بين المركبات باستخدام الثقة. بالإضافة إلى ذلك، نقوم بتصميم وتنفيذ نظام لحساب الثقة المستخدمة في بناء هذه العلاقات بين المركبات. وعلاوة على ذلك، نحن ندرس تأثير الثقة على الوقت المتطلب لاتخاذ قرار سليم في تطبيقات السلامة للمركبات.

في هذه الأطروحة نقوم بتطوير نموذج تحليلي حتى ندرس العلاقة بين الثقة وعملية صنع القرار من حيث الأداء ومعدل الدقة، وبعد ذلك نقوم بدراسة مدى فعالية بناء الثقة على أساس التشابه لاستخدامها في تحديد صدق الرسائل في تطبيقات السلامة في VANETs. وأخيراً، يتبين لنا أن الثقة القائمة على التشابه لها تأثير إيجابي على الوقت اللازم لاتخاذ القرار وعلى دقة هذا القرار.

مفاهيم البحث الرئيسية: الشبكات المخصصة للمركبات، الثقة، التشابه، نظام، بنية، نظام، الأمان، تطبيقات، بروتوكول.

Acknowledgements

This work would not have been complete without the blessings of Allah. I am thankful to Allah for granting me strength and patience, and for providing great social and technical support systems. I would like to express my heartfelt gratitude to my family and friends for their love and support.

I am indebted to Dr. Nader Mohamed first as advisor and later as co-advisor; he has given me the opportunity to see this work become a reality by taking me on as a student with a ridiculous idea and has provided continuing support and guidance.

I would like to extend my appreciation to my dissertation committee members for their time and effort spent reviewing this document.

Finally, and most importantly, I would like to thank Dr. Hesham El-Sayed, my advisor, for extending his support when needed the most.

Dedication

*To my beloved parents and family: Obaid, Kaltham, Alia, Asma, Rauda, Fatima,
Mariam, Ahmed, Shaikha, Hamad and Abdulla.*

Table of Contents

Title	i
Declaration of Original Work	ii
Copyright	iii
Advisory Committee	iv
Approval of the Doctorate Dissertation	v
Abstract	vii
Title and Abstract (in Arabic)	viii
Acknowledgements	ix
Dedication	x
Table of Contents	xi
List of Tables.....	xiv
List of Figures	xv
List of Abbreviations.....	xvi
List of Definitions	xvii
Chapter 1: Introduction	1
1.1 Background	1
1.2 Research Motivation	3
1.3 Dissertation Structure.....	5
Chapter 2: Problem Statement, Research Scope, and Methodology.....	7
2.1 Introduction	7
2.2 Problem Statement	7
2.3 Contribution	8
2.4 Research Scope and Assumptions.....	9
2.5 Research Methodology.....	11
Chapter 3: Literature Review	13
3.1 Introduction	13
3.2 Trust	13
3.3 Trust and Similarity	17
3.4 Safety Applications	22
3.5 Data Mining in VANETs	23
3.6 Summary	26
Chapter 4: Using Similarity to Establish Trust between Vehicles	28
4.1 Introduction	28
4.2 Motivation	29
4.3 Trust Applications in VANETs.....	30

4.4 System Description	31
4.4.1 System Modules	32
4.4.2 System Components	33
4.4.3 Similarity	34
4.4.4 Trust	37
4.5 Simulation and Results.....	38
4.6 Discussion	40
4.6.1 Maximum Meeting Time	40
4.6.2 Average Trust Rating	41
4.6.3 Identifying Abnormal Vehicles	44
4.6.4 Scalability	44
4.7 Summary	45
Chapter 5: The Impact of Trust on Vehicular Applications.....	46
5.1 Introduction	46
5.2 Motivation	46
5.3 The Model	47
5.3.1 Expected Number of Messages	50
5.3.2 Expected Error Rate	50
5.4 Evaluation and Discussion	51
5.4.1 Discussion	54
5.5 Summary	55
Chapter 6: Similarity-based Trust Management System for Detecting Fake Safety Messages in VANETs	56
6.1 Introduction	56
6.2 Data Validation Approaches	57
6.3 Goals	59
6.4 Background	60
6.4.1 Collaborative Vehicles	60
6.4.2 Adversary Model.....	61
6.4.3 Trust	61
6.5 Scheme Overview	62
6.5.1 Echo Protocol	64
6.6 Simulation and Results.....	65
6.7 Discussion	68
6.8 Summary	69
Chapter 7: Conclusion.....	70
7.1 Conclusions	70
7.2 Directions for Future Work.....	71
Bibliography.....	75
List of Publications	82
Appendix	83
SUMO Networks.....	83

Percentage of abnormal vehicles = 0%	83
Percentage of abnormal vehicles = 20%	85
Percentage of abnormal vehicles = 50%	87
Percentage of abnormal vehicles = 80%	90

List of Tables

Table 3-1: Summary of Trust in VANETs related work	16
Table 3-2: A qualitative comparison of Trust Management Systems in VANETs....	18
Table 3-3: Summary of Data Mining in VANETs related work.....	24
Table 4-1: System Modules	33
Table 4-2: Sample Similarity Matrix in Vehicle V_2	35

List of Figures

Figure 4-1: System Architecture	33
Figure 4-2: Average trust rating in the network between vehicles	37
Figure 4-3: Sample Highway Segment	39
Figure 4-4: Average Meeting Time	41
Figure 4-5: Average trust rating in the network between normal vehicles	42
Figure 4-6: Average trust rating in the network between normal vehicles and abnormal vehicles.....	42
Figure 4-7: Average trust rating between normal vehicles, and between normal and abnormal vehicles in different size networks.....	44
Figure 5-1: The depth of the tree is $\left\lfloor \frac{N}{2} \right\rfloor + 1$	49
Figure 5-2: The depth of the tree is $u + 1$	49
Figure 5-3: Expected Number of Messages.....	52
Figure 5-4: Expected Error Rate	53
Figure 6-1: State transition diagram of the onboard unit (OBU) in a vehicle.....	60
Figure 6-2: The Echo Protocol.....	66
Figure 6-3: Average percentage of vehicles that accepted true safety event report...	67
Figure 6-4: Average percentage of vehicles that accepted false safety event report .	68

List of Abbreviations

BSM	Basic Safety Message
CF	Collaborative Filtering
DSRC	Dedicated Short Range Communication
IOV	Internet of Vehicles
ITS	Intelligent Transportation System
MANET	Mobile Ad hoc NETWORK
MQTT	MQ Telemetry Transport
OBU	Onboard Unit
SbTMS	Similarity-based Trust Management System
SEE	Safety Event Evaluator
SER	Safety Event Reporter
SUMO	Simulation of Urban MObility
VANET	Vehicular Ad hoc NETWORK
VARS	Vehicle Ad hoc Reputation System

List of Definitions

Abnormal Vehicles	Vehicles that exhibit unpredictable behaviors, such as irregular rates of acceleration and deceleration and failure to maintain safety distance.
Beaconing	The periodic transmission of information to all neighbors within radio range
Echo Protocol	A protocol used to discover false safety event messages sent by a selfish adversary

Chapter 1: Introduction

A close examination of collaborative networks led to our research on how we can simulate human interactions in collaborative networks in an environment of autonomous vehicles. In these networks vehicles use wireless communication infrastructure making up VANETs. On social network sites, we are provided recommendations on adding, following, or befriending new people. As humans we use our judgment to evaluate the recommendations and either accept or reject them. Moreover, we use our judgment to accept or reject any information we receive from our acquaintances on social networks. The question is how can we extend the same to VANETs?

In this chapter, we start with providing a brief background on VANETs: their characteristics and applications. Next, we discuss the motivation that drives our work. Finally, we conclude this chapter with an overview of the structure of this dissertation.

1.1 Background

VANETs are networks of vehicles where the members of the network communicate using a wireless communication infrastructure. They are a special class of mobile ad hoc networks (MANETs) (Hadim, Al-Jaroodi, & Mohamed, 2006), which comprise moving nodes. However, the mobility pattern is much faster, and the available resources are much greater. The topology of the network is dynamic; changes in the networks are frequent due to the speed with which the vehicles travel and the changes in the underlying road infrastructure. They consist of vehicles that communicate with each other to send, receive or relay messages willingly thereby

creating an Ad-Hoc network. Apart from MANET properties, VANET possesses a few distinguishing characteristics, presenting itself as a particular challenging class of MANETs:

- **Highly dynamic topology:** Since vehicles are moving at high speeds, the topology formed by vehicles in VANETs is always changing.
- **Frequently disconnected network:** The highly dynamic topology results in frequently disconnected network; a link between two vehicles can quickly disappear while the two vehicles are transmitting information.
- **Patterned Mobility:** Vehicles follow a certain mobility pattern that is a function of the underlying roads, the traffic lights, the speed limit, traffic condition, and drivers' driving behaviors.
- **Unlimited Battery Power and Storage:** Nodes in VANETs are not subject to power and storage limitation as in sensor networks.

Researchers have investigated many aspects of VANETs (El Zarki, Mehrotra, Tsudik, & Venkatasubramanian, 2002; Enkelmann, 2003; Golle, Greene, & Staddon, 2004; Xu, Mak, Ko, & Sengupta, 2004; X. Yang, Liu, Vaidya, & Zhao, 2004). There are different methods for information transport in VANETs, one of which is beaconing. Beaconing is defined by (Hartenstein & Laberteaux, 2009) as: "The periodic transmission of information to all neighbors within radio range". The packet sent using beaconing is called a beacon. A beacon contains time varying data, such as: speed and coordinates. The size of the beacon differs depending on the application that uses it i.e. varies depending on the information inside it (Na Nakorn, Yusheng, & Rojviboonchai, 2014). For example, the Basic Safety Message (BSM) defined by the SAE J2735 standard (SAE-International, 2009) consists of two parts: part one includes: position, motion, time and general status of the vehicle. Part two of

the message includes varying connect, and is sent when needed; therefore, it is optional. The Dedicated Short Range Communication (DSRC) standard defines the operating parameters required for communication between vehicles and road side units as well as vehicles themselves (ASTM, 2003).

VANETs have a variety of applications, ranging from critical to entertainment. Applications in VANETs typically fall under one of the following categories (Hartenstein & Laberteaux, 2008):

1. Safety applications.
2. Information/entertainment applications, and
3. Transport efficiency applications.

Safety applications include emergency breaking, lane change warning messages, and collision avoidance applications (Jawhar, Mohamed, & Zhang, 2010). These are the most critical applications in VANETs because of the severity of loss associated with them.

These applications must be carried out in an environment where the data exchange is secure. Depending on the application, the security requirements can be anything from confidentiality to integrity and availability. Trust is another element to consider. Vehicles need to trust that the information they receive, no matter how secure, is authentic. Vehicles need to ensure trust either by trusting the entity that generates the data or trusting the data itself.

1.2 Research Motivation

The ability to trust messages from similar vehicles is key: trust is vital for maintaining order in the network. A vehicle must be able to accept such messages in order to take the best action. We argue that trust exists in VANETs either implicitly

or explicitly. Vehicles form trust relationships with other vehicles due to many factors, such as the role of a vehicle in the network, its activities, and the context of a vehicle. Therefore, trust can be used to support vehicles in the decision-making process. The challenges with trust management in VANETs are the following:

1. How to overcome the limitations of reputation schemes? Reputation schemes rely on voting, and due to continuously changing topology of VANETs, a voting threshold may never be reached to make a decision.
2. How to establish trust relationships?
3. How to illustrate the impact of trust on the decision making process?
4. The networks are highly dynamic, and connections are short lived. Any trust management scheme should account for this.
5. How to handle vehicles that may not be malicious but selfish? They are not always good and not always bad.

Our goal in this research is to form trust relationships between vehicles through similarity and to study the impact of trust in VANETs. We study the effect of trust on the time needed for a vehicle to make a decision and on the accuracy of that decision. We show that trust has a positive effect on the number messages needed for a vehicle to make a decision. Additionally, we show that the error rate decreases.

Using trust to group vehicles can be utilized by many VANETs applications; for example, if a vehicle traveling on the highway is grouped with vehicles in which the passengers share the same taste in food, messages from vehicles recommending a food outlet are more likely to be accepted. Another example is recommendations for tourist sites or alternate routes. These are only a few examples where trust can be

utilized. In this research, we focus on VANETs safety applications because of their criticality and the challenge they present.

1.3 Dissertation Structure

In Chapter 2, we present our problem statement. We define the scope of our research and present our contribution. In addition, we outline the steps of our research methodology. We use a methodology proposed by Vaishnavi and Kuechler (Vaishnavi & Kuechler, 2004) to collect and verify the data needed to support our work.

In Chapter 3, we present the research done in the area of data mining in relation to VANETs. In addition, we discuss the importance of safety applications and review their different categories. Moreover, we present the state of the art in the area of trust management in VANETs. Finally, we highlight some research work that we believe is relative to our research.

In Chapter 4, we lay the foundations for the remainder of the dissertation by describing the system architecture for trust management in VANETs. We design the framework of a system that continuously calculates trust ratings for all the neighbors of a vehicle. These trust ratings will then be used to assist a vehicle in making a decision about an event in the network, like the saying: "Forewarned is forearmed". The trust rating of a vehicle coupled with any report it sends out about an event in the network will be used by the receiving vehicle as an endorsement or corroboration of the reported event.

In Chapter 5, we develop an analytical model that associates trust with the performance of the decision-making process and the accuracy. We provide some analyses and discussions in that regard. We find that trust has a constructive impact

on the number of messages needed for a vehicle to make a decision about a safety event in the network and on the accuracy of that decision. However, validation for our approach is still required, which led us to the next investigation.

In Chapter 6, we present a scheme that uses similarity-based trust relationships to detect false safety event messages from abnormal vehicles in VANETs. Our scheme reacts to safety events claims made by a vehicle. The scheme predicts that the source vehicle will react to a truthful safety event report. We perform simulations to study the effectiveness of the proposed scheme in uncovering false safety event messages sent by abnormal vehicles. We design and evaluate an adversary model in order to study the effect of trust on the accuracy of the decision made in the presence of false data in the network. The simulation results show that our proposed system for using similarity to achieve trust is proof against a false data injection attack.

Finally, in Chapter 7, we conclude our dissertation and present further research opportunities in the area of trust management in VANETs.

Chapter 2: Problem Statement, Research Scope, and Methodology

2.1 Introduction

In this chapter we begin by stating the problem we aim to solve. Next, we present our contributions: we outline our suggestions for solving the identified problem. In addition, we define a scope for our research where we describe all that we address with our solution. Finally, we outline the steps we follow in order to achieve the objectives of this research.

2.2 Problem Statement

VANET applications must be carried out in an environment where the data exchange is secure. Depending on the application, the security requirements could be anything from confidentiality to integrity and availability. Trust is another element to consider. Vehicles need to trust that the information they receive, no matter how secure, is genuine and real. Vehicles should be able to form relationships based on trust. These relationships are used to facilitate the provision of VANET services where trust is guaranteed or when trust is a given. The goal is to enhance the performance of VANET applications through trust. This notion of using trust as a basis for accepting information from other vehicles in the network is highly dependent on a vehicle's own preferences, its degree of readiness to accept the actions or messages of other vehicles. Later, these preference settings can be promoted from reflecting an individual vehicle to reflecting a group of vehicles using the similarity between vehicles to calculate trust. Golbeck (Golbeck, 2009) argued that trust must reflect user similarity: recommendations are more likely to be accepted if they are from people with similar tastes. Therefore, a vehicle is more

willing to depend on or believe in an event reported by a similar vehicle because they share similar attributes and preference settings.

The problem we aim to solve is: **How to achieve trust through similarity in order to enhance efficiency and the decision-making process i.e. reduce the time needed to make a decision, and increase the accuracy of the decision.** This can be mapped to reduce the number of messages and the error rate in vehicular safety applications. We are faced with a number of questions: How to establish trust relationships between the vehicles in the network? How to utilize trust in the decision making process? How to illustrate the impact of trust on the decision making process?

2.3 Contribution

We take a closer look at the components of the above mentioned problem statement: How to identify and utilize trust relationships to enhance the decision making process and efficiency in VANETs safety applications. In addition, we provide solutions to the problem's components.

In this dissertation, our contributions are as follows:

- a. We design and implement a system architecture to generate and process trust ratings of vehicles in the network. The rating is based on the similarity between a vehicle and any of its one-hop neighbors. We use association rules to discover relations between the different vehicles and to calculate the similarity degree between every vehicle and its one-hop neighbors.
- b. We build a mathematical model to study the effect of trust on the number of messages needed to make a decision, and on the error rate

of that decision. We show that we could enhance the performance of vehicular safety applications using a smaller number of messages with reasonable error rates using trust relationships. This enables vehicles to make better decisions with a smaller number of messages.

- c. We evaluate the performance of our trust management system in a safety application. We study the effectiveness of the system in helping vehicles identify a false data injection attack.

2.4 Research Scope and Assumptions

In this dissertation, we define our scope of work as the following:

- **VANET applications:** VANETs have a variety of applications, ranging from critical to entertainment. Our research focuses on safety applications because of their criticality and the challenge they present. We simulate a safety event and observe the behavior of the vehicles when receiving message reporting in which safety event vehicles need to trust that the information they receive, no matter how secure, is real. Vehicles need to ensure trust either by trusting the entity that generates the data or trusting the data itself. All categories of VANET applications need trust in order to ensure the genuineness of the data in the network.
- **Collaborative vehicles:** AVANET comprises vehicles that cooperate to achieve advantages. The vehicles in a VANET work toward individual goals and other collective goals of the members of the network. For example, an individual goal would be for a vehicle to ensure the security of its communications. On the other hand, an

example of a collective goal would be to reduce the network communications overhead, which in turn helps the vehicles achieve another individual goal of a better quality of service in the network.

Cooperation in VANETs means that vehicles rely on reports generated by other vehicles on the road to react to safety events.

Using similarity, vehicles construct local views of their surroundings, and form opinions about their neighbors. Assuming trust is established, vehicles rely on their calculation of a trust rating of their peers to validate event-generated reports.

We use the following assumptions in VANETs:

- **Network model:** The network is comprised of communicating vehicles. Each vehicle broadcasts beacons periodically; 10 beacons are sent every second. Each beacon will carry information about the current position and speed of a vehicle. The vehicles move at high speeds, up to 120 k/h on a one-way highway. The movements of the vehicles are restricted to the layout of the road. The network is partitioned into cells depending on the transmission range of the vehicles, which in VANETs is 1,000 m (Hartenstein & Laberteaux, 2009). Vehicles within transmission range of each another can be made into groups.
- **Adversary model:** In examining the security of the VANET environment, we take a conservative approach by assuming that an adversary is working alone. We consider a type of attack that is localized; it only affects the immediate neighbors of the adversary. If most of the adversary's neighbors are in collusion with them, then no

scheme running in the network can withstand an attack carried out by the majority of the network's participants.

2.5 Research Methodology

The aim of this research is reduce the number of messages needed for a vehicle to make a correct decision about a safety event in the network. Moreover, this research objective is to reduce the decision error rate by trusting the right vehicles in the right situations. We start our research by identifying the problem, and then suggesting a solution. Next, we develop our solution and evaluate it. Finally, we present our conclusions based on the evaluation. Following the research methodology proposed by Vaishnavi and Kuechler (Vaishnavi & Kuechler, 2004), we divide our research into the following steps:

Step 1: Survey the literature to review existing trust management systems in VANETs. This requires analyzing and comparing the different proposed systems to clearly identify the research gap between existing systems and our proposed system.

Step 2: A proposal of our system architecture is presented to address the issues identified in Step 1. We propose a system architecture that provides trust ratings of vehicles in a network. Additionally, the system generates and processes trust ratings to establish trust relationships.

Step 3: We use mathematical modeling and simulation to analyze the proposed system architecture. We design a mathematical model to study the effect of trust on the expected number of messages and the error rate. We use the mathematical model to study the effect of trust on the number of messages needed by a vehicle to make a decision about a reported safety event. We have the following inputs to the model: N is the number of one-hop neighbors of a vehicle, t is the

number of trusted neighbors, and u is the number of untrusted neighbors. We see how the model reacts to the increase or decrease of trusted vehicles in the network. We use a data mining technique to measure the similarities between the vehicles. Accordingly, we use the measured similarity to calculate trust ratings that reflect the vehicles' preferences. Data mining is used to calculate the degree of similarity between a vehicle and its one-hop neighbors. The rates from the similarities are then used to form relationships based on trust.

Step 4: We evaluate the results produced by our proposed system architecture. We employ simulation to verify the accomplishment of the research objectives. We implement a mathematical model to study the effect of trust on the expected number of messages and the error rate. Furthermore, we implement the mathematical model designed to study the effect of trust on the expected number of messages and on the error rate. We experiment with the model using simulation.

We further validate our proposed trust management system by implementing an adversary model where vehicles inject false reports of safety events in the network. Our verification scheme inspects whether our proposed trust management system assists vehicles in identifying false reports in the network.

Step 5: In this step, we present the results of our research. Based on the identified research gaps, we show how our work has contributed in providing a solution for the identified problem. In addition, we highlight a few points as future direction for this research.

Chapter 3: Literature Review

3.1 Introduction

In this dissertation we aim to reduce the communication overhead of safety event reports in VANETs. However, our efforts to achieve this aim must not compromise the security of safety applications in VANETs. We set out to achieve our goal using trust. To identify the research opportunities in this area, we survey the state of the art.

In this chapter, we begin by exploring the literature in the area of trust and similarity to identify and analyze any gaps in the body of work for our contribution. We then discuss the importance of safety applications in VANETs and present their different categories. Next, we provide an overview of the application of data mining techniques in VANETs to assert the applicability of such techniques in a highly dynamic network. We suggest that there exist data mining techniques that are suitable for use in the highly dynamic environment of VANETs, which we later demonstrate in this dissertation.

3.2 Trust

Trust as a concept has many definitions in computer science. Trust is belief and commitment: belief that an entity will act a certain way in a situation and commitment is acting upon that belief (Golbeck, 2009). Therefore, trust is a subjective term; it involves an entity's personal experience and the effect of trust on an entity in a specific context. A definition of trust was provided by (Avižienis, Laprie, Randell, & Landwehr, 2004); they defined trust as an accepted dependence, such that A depends on B based on a judgment made by A or on behalf of A. The

readiness for A to accept B's faults can be used to measure the level of trust it has in B. A survey of trust management system in MANET is presented in (Cho, Swami, & Chen, 2011). The authors defined trust management as a unified approach for specifying and interpreting relationships. Their definition of trust is based on belief, the belief that an entity will behave in a certain way. The research of (Huang, Ruj, Cavenaghi, & Nayak, 2011) showed that trust management schemes in MANETs cannot be used in VANETs. A survey of trust management in intelligent transportation systems (ITS) was presented by (Ma, Wolfson, & Lin, 2011). The authors described two different types of trust: entity-centric and data-centric. In entity-centric trust, a node in the network assigns the same level of trust to all messages received from another node. On the other hand, in data-centric trust, a node in the network makes trust decisions based on messages received from other nodes. Trust management in VANETs was surveyed in the research of (Jie Zhang, 2011). The author proposed desired properties for trust management in VANETs. Metrics such as location, time, and event type should be used in calculating trust. In addition, each metric should have a confidence measure or weight attached to it.

(Gerlach, 2007) defined trust as the level of acceptable dependency of one entity on another. In this work, the author defined entities of a security system, and the dependencies between them. Every system has a set of applications, such as warning messages, congestion, etc. Trust is calculated using four different measures: dispositional, system, situation, and belief formation process. The last one is the evaluation of available data, which together with an entity's own calculated confidence level about the result of this evaluation form the trusting belief about a trustee in a specific situation. Trust values are calculated and assigned to every entity

that provides information to an application. The application then determines whether to act on the information or not. One of the applications of trust was presented by (C. Chen, Zhang, Cohen, & Ho, 2010a) where the authors utilized trust for message propagation; messages are aggregated from group members and sent to other groups' leaders. The groups' leaders then broadcast the message to their group members. A message is only forwarded to the other groups if it has a trust weight that is over some threshold set by the originator group leader. On the other side, a receiver will only forward the message to group members if the message weight scores a predefined confidence level. In addition, (C. Chen, Zhang, Cohen, & Ho, 2010b) used trust for message propagation in the network as well. A vehicle sends out a message, and every vehicle in a cluster in the network aggregates its opinion with it. The leader of the cluster determines the vote of the cluster and forwards the message to the leaders to the other clusters on the road. The opinions are made of the trust value placed on the entity and the event, so trust is combined. Contrary to the aforementioned approach, every message is forwarded to every leader in the network. (Petit & Mammeri, 2011) used trust to reach a consensus decision about an event in a safety critical application. Other applications for trust include the support of recommendations. A vehicle will accept another vehicle's recommendation if it trusts it. In (Worndl, Brocco, & Eigner, 2008), the system recommends gas stations by predicting the relevance of information to a vehicle. (Kumar & Chilamkurti, 2014) use trust to build an intrusion detection system in VANETs. The system identifies nodes that have unauthorized access to other nodes data to compromise confidentiality, integrity and availability.

Trust in VANETs is calculated using different approaches. For example, (Mazilu, Teler, & Dobre, 2011) calculated trust using the timestamp of the event, the

number of hops of the message, and the number of messages that report the same event. Recommendations are used to calculate trust in the work of (Mármol & Pérez, 2012). The authors used recommendations received from vehicles in the network for calculating trust values. The trust values are maintained through past experiences with vehicles in the network. An interactive approach for trust calculation was presented by (Minhas, Zhang, Tran, & Cohen, 2010). The authors proposed a trust management scheme where a vehicle first sends a query, and, based on the responses; it accepts the one with the majority agreement. If a majority cannot be reached, it refers to a trust matrix and accepts the votes from the vehicle with the authority role and most experience. After a decision is made, it evaluates the responses and, based on them; it updates its trust matrix. The trust matrix is built from the following components: role-based trust and experience-based trust. The priority-based trust is then created from ordering the vehicles based on roles and experience.

Table 3-1: Summary of Trust in VANETs related work

Title	Author	Year	Remarks
Basic concepts and taxonomy of dependable and secure computing	Avizienis et al.	2004	Trust is acceptable dependence
Trust and nuanced profile similarity in online social networks	Golbeck	2009	Trust is belief and commitment
A survey on trust management for mobile ad hoc networks	Cho et al.	2011	Trust management is a unified approach for specifying and interpreting relationships
A survey on trust management for VANETs	Zhang	2011	Desired properties for trust management in VANETs
A survey on trust management for intelligent transportation system	Ma et al.	2011	Two different types of trust: entity-centric and data-centric

3.3 Trust and Similarity

Due to the nature of VANETs, vehicles tend to move as a group. Vehicles are restricted by roads and speed limits (Sampigethaya et al., 2005); therefore, their movement is dependent on each other. Groups are formed from vehicles where every vehicle is within communication range of the other vehicles in the group. (Caballero Gil, Caballero Gil, & Molina Gil, 2010) demonstrated that using groups enhances the performance of the communications link.

In our work, we suggest that each vehicle will maintain a local cluster of its neighbors: any vehicle that is within the communication range of another vehicle is part of that vehicle's cluster. The clusters will be dynamic, and each member of the cluster receives a trust score based on the similarity degree between itself and the owner of each cluster. These groups of vehicles represent communities with individuals of varying and common attributes. We argue that the common attributes between the members of the community will assist them in the decision-making process. Table 3-1 displays related trust management systems with a qualitative comparison of the attributes, applications, and techniques.

Generally, a recommender system matches items to users based on the attributes of the user (Woerndl & Eigner, 2007). In online communities: a collaborative recommender system includes ratings from other users in the decision-making process.

Trust defines how data is handled, with whom it is shared, from whom it is accepted, and how it should be acted upon.

Table 3-2: A qualitative comparison of Trust Management Systems in VANETs

Name	Description	Attributes	Application	Technique	Trust Calculation	Limitations
A Similarity-based Trust Management System	Uses data mining techniques to utilize attribute similarity to assign trust ratings to neighboring vehicles	<ul style="list-style-type: none"> • Time • Speed • Location 	Safety applications	Hybrid	Every vehicle uses association rules to calculate the similarity degree between itself and its neighbors, the similarity degree is then used to compute the pairwise trust.	Considers only misbehaving (selfish) vehicles in its adversary model
A Similarity based Trust and Reputation Management Framework for VANETs(N. Yang, 2013)	Visual confirmation of an event enhances the reputation of the originator vehicle	<ul style="list-style-type: none"> • Time • Location • Event type • Message ID 	Report events in VANETs	Hybrid	Similarity is used to calculate a vehicle's reputation. Trust is the weighted average of direct experienced and recommended reputation.	<ul style="list-style-type: none"> • Uses momentary connections to confirm a safety event. • Doesn't consider trust decay.

Name	Description	Attributes	Application	Technique	Trust Calculation	Limitations
A Model for Detecting and Correcting Malicious Data in VANETs (Golle et al., 2004)	A model is built to explain data gathered by a vehicle	Sensor data	Thwart Sybil attack	Data-centric	The model looks for anomalies that might indicate a possible adversarial behavior in the network.	Doesn't consider the highly dynamic nature of relationships in VANETs.
A social network approach to trust management in VANETs (Huang, Ruj, Cavenaghi, Stojmenovic, & Nayak, 2014)	A voting scheme for decision making in VANETs	Sensor data	Safety applications	Data-centric	Trust in the correctness of the received report is reached through voting.	<ul style="list-style-type: none"> • Forwarding nodes may alter the content of the messages. • The number of reports needed to make a decision is not specified.

Name	Description	Attributes	Application	Technique	Trust Calculation	Limitations
Vehicle Behavior Analysis and Evaluation Scheme (VEBAS) (Schmidt, Leinmüller, Schoch, Held, & Schäfer, 2008)	A behavior analysis system is built to use information contained in beacons to build behavioral modules of the nodes in the network	Sensor data	Thwart Sybil attack	Data-centric	A framework of modules is constructed to analyze the behavior of the vehicles to determine their classifications i.e. trustworthy, untrustworthy, or neutral.	Susceptible to Sybil Attack.

The homophily principle was explained by (Xiang, Neville, & Rogati, 2010) as the tendency of like to associate with like (McPherson, Smith-Lovin, & Cook, 2001). The principle suggests that people tend to form ties with other people who have similar characteristics. (Golbeck, 2009) also illustrated that there is a correlation between trust and similarity. Nevertheless, (Ziegler & Golbeck, 2007) proved that there is a correlation between trust and similarity. (Montaner, López, & de la Rosa, 2002) claimed that trust should be derived from user similarity. Moreover, (J. Wang, Liu, Liu, & Zhang, 2009) presented a trust propagation scheme. In their work, the authors used attribute similarity to achieve routing in VANETs; they defined a pair-wise trust value to determine how to interact with a node. A vehicle determines whether to forward a packet to another vehicle or not based on the degree of similarity between this vehicle and the source of the packet.

(N. Yang, 2013) built a trust management system that generates trust values for messages in VANETs. The system depends on the redundancy of messages to build the vehicle trust values. More messages that are received describing the same event result in better trust values. The disadvantage of this approach is that trust is calculated by the vehicles on the spot as more and more messages are received, which creates an unacceptable delay in VANETs.

(Huang et al., 2014) present a voting scheme for decision making in VANETs. The authors rely on reports about a safety event from first-hand observers and multi-hop reporters where the messages from first hand observers out-weigh the multi-hop messages. The authors show through experiments that considering first-hand information is better than voting the opinions of neighboring nodes.

(Golle et al., 2004) evaluated the validity of VANET data. The approach adopted by the authors builds behavioral models of the vehicles in the network using

recommendations from neighbors under the assumption that they are honest. (Schmidt et al., 2008) built a behavior analysis system to detect misbehaving vehicles through movement analysis. The system then classifies vehicles in VANETs as trustworthy, untrustworthy, or neutral. The behavior analysis system builds modules to analyze movement-related data that focuses on the detection of stationary attackers.

3.4 Safety Applications

The importance of communications between vehicles in safety applications is to allow cooperation and coordination of vehicle movements to prevent collisions and life threatening incidents (Hartenstein & Laberteaux, 2009).

The transmission of safety messages can be preventative or event-driven (R. Chen, Jin, & Regan, 2010): preventative safety messages are transmitted periodically, carrying information about a vehicle's speed, acceleration, deceleration, and direction. Event-driven safety messages are transmitted as a response to an event, such as hard braking and sudden direction change.

Safety applications can be categorized into the following categories (R. Chen et al., 2010):

- **Intersection collision avoidance:** traffic signal violation warning, intersection collision warning, and blind merge warning. In a traffic signal violation warning, the vehicle warns the driver of an imminent violation of a red light. In an intersection collision warning, the vehicle warns the driver of an imminent crash through information about other vehicles' speeds, positions, and directions of driving.

Similarly, the vehicle uses the aforementioned information to warn drivers at road merges.

- **Messages from other vehicles:** cooperative collision warning and blind spot warning. The application running onboard the vehicle uses information about the positions and speeds of other vehicles to warn of imminent collision and assist drivers intending to change lanes by warning them when it is unsafe to do so.
- **Signage extension:** messages from the infrastructure warning of road work or of a curved road ahead.
- **Public safety:** an approaching emergency vehicle warning.

3.5 Data Mining in VANETs

(Al-Khassawneh & Salim, 2012) listed applications of data mining in VANETs. Data mining has been used in identifying malicious vehicles, routing and route prediction, and creating an image of the network. In the work by (Smaldone, Han, Shankar, & Iftode, 2008), people driving on the same road can be added to groups to chat with each other depending on their similarities. Summarizations of the traffic data were constructed using data mining (Jiadong Zhang, Xu, Zhu, Wang, & Liao, 2010). The authors experimented with three sampling techniques, examining the following measures: the mean speed on the road and the rate of information.

(Golbeck, 2009) investigated trust-based recommender systems. These systems capture similarities between user profiles. The author explained that users express trust. They provide more data to find similarities between them and other users in online communities, and data mining is used to match items to users.

Table 3-3: Summary of Data Mining in VANETs related work

Title	Author	Year	Remarks
Association rule mining in peer-to-peer systems	Wolff & Schuster	2004	Algorithms that mine association rules in peer-to-peer networks
Distributed data mining in peer-to-peer networks	Datta et al.	2006	Find associations between attributes in a distributed environment with partitioned databases
RoadSpeak: enabling voice chat on roadways using vehicular social networks	Smaldon et al.	2008	Create chat groups on the road
Constructing summarizations for V2V traffic data based on sampling methods	Zhang et al.	2010	Construct summarizations of the traffic data in VANETs
On the Use of Data Mining Techniques in Vehicular Ad Hoc Network	Al-Khassawneh	2012	Applications of data mining in VANETs: <ul style="list-style-type: none"> • Identify malicious vehicles • Routing • Create an image of the network

Another example of using data mining in online communities is mining for association rules. In some research studies (Wolff & Schuster, 2004)(Datta, Bhaduri, Giannella, Wolff, & Kargupta, 2006), the authors designed algorithms that mine association rules in peer-to-peer networks. The algorithms find associations between attributes in a distributed environment with partitioned databases. In (Al Falasi & Mohamed, 2013) we introduce a system for building trust rules from preferences. Trust rules are statements that describe the preferences of a vehicle. Each statement can be used to express an attribute: its characteristics and relationships with other attributes. The statements are created from monitoring a vehicle's communications, its interactions with other vehicles and from the vehicles itself. Given the nature of the rules, they're influenced by the context of a vehicle. The weight of every attribute

differs as the context differs, allowing for a better expression of trust. Trust is not ultimate, and just as the rules, it's highly influenced by the context of the vehicle. For example, I trust a doctor with my health, but not my car; unless he was a mechanic as well. The trust rules are built from the beacons sent by a vehicle's neighbors. If the frequency of beaconing is 10 beacons per second, a vehicle travelling at speed of 120 km/hr would send 600 beacons per minute, assuming 0% message loss rate. At this speed the vehicle will move 33.33 m per second and receive 300 beacons per km. We suggested the use of data mining algorithms to extract knowledge from these beacons.

In this dissertation, we take advantage of the plethora of information in the network in the form of beacons. Information about other vehicles on the road can be collected through the beacons they send periodically. A beacon includes information about the current state of a car, such as speed and coordinates. This inspired us to look into the use of data mining techniques to discover relationships between vehicles on a road, and then utilize these relationships to reduce the communications overhead in the network. In recommender systems, Collaborative Filtering (CF) techniques are used to derive similarity between two items or two users (Su & Khoshgoftaar, 2009) if two users behave similarly, then they will act similarly on other items. The authors state that Pearson's Correlation Coefficient is used in CF techniques and is dependent on item ratings to provide predictions. We don't have explicit ratings to use to derive similarity in our system. Another technique is Euclidean Distance which requires an assumption of the value of trust to predict the future value of trust using the similarities between the messages that report the same event. The author in (N. Yang, 2013) assumes that messages generating from the same vehicle about the same event usually has the same trust value. We decided to

use association rules because we wanted to discover interesting relations between the vehicles. We focused on identifying item pairs that occur frequently together; counting the number of co-occurrences of the pairs.

Moreover, in this dissertation, we take a hybrid approach in terms of trust sources to verify the authenticity of safety events. We start with an entity-centric metric of trust (i.e., measure of similarity to form the relationships between the vehicles) and then we input data-centric trust metrics to validate safety event reports. For example, a vehicle receiving a warning message about an accident has to make a decision; either act on or ignore the message. The vehicle in question will input the reputation of the source vehicle and the vehicle's own observation of the source vehicle's behavior to evaluate and take an action with respect to the reported accident.

3.6 Summary

The trust management systems proposed by (Huang et al., 2014; N. Yang, 2013) show good potentials for implementation in VANETs; however, they come short when it comes to addressing the challenges of trust management in VANETs highlighted in Chapter 1. In (N. Yang, 2013), the author uses trust to build reputation. Their system doesn't count for the ephemeral nature of VANETs; they don't consider the decay of trust value over time. In addition, they assume that messages generated from the same vehicle about the same event within a similar period of time will have the same trust value; however, they don't say how this value is first calculated.

One of the challenges of trust management in VANETs is reaching a voting threshold on a decision in reputation systems. The authors in (Huang et al., 2014)

don't say how many reports they need before a vehicle can make a decision. In addition, they are using a voting scheme that given the dynamic nature and time criticality of VANETs safety applications may not be applicable. Furthermore, their voting scheme relies on reports about a safety event from first hand observers and multi-hop reporters. The problem with this approach is that they rely on intermediate neighbors forwarding the correct message; they neglect the possibility of having malicious vehicles that may alter the content of the message. In their research the authors show that considering first-hand information is better than voting the opinions of neighboring nodes. We demonstrate the same in this dissertation.

In this dissertation, we address the challenges of trust management in VANETs through the following:

1. We don't rely on voting to assess the correctness of a safety event message. Every vehicle relies on its own observations and uses their subjective view of the network to make their decision. Our system is introduced in Chapter 4.
2. Our trust management system considers the highly dynamic nature of the network; the system collects enough information to support the decision making process in the vehicles. This is demonstrated in Chapter 6.
3. Our adversary model presented in Chapter 6 considers misbehaving or selfish vehicles selfish: they are not always good and not always bad. We aim to investigate the effectiveness of our system in discovering malicious vehicles in the future.

Chapter 4: Using Similarity to Establish Trust between Vehicles

4.1 Introduction

VANETs offer a range of applications; therefore, security has become a major concern. Many researchers targeted the provisioning of security services to ensure the availability of protection measures for the information in the network (Hao, Cheng, Zhou, & Song, 2011; Karim, 2008; Papadimitratos et al., 2008; N. W. Wang, Huang, & Chen, 2008; L. Zhang, Wu, Solanas, & Domingo Ferrer, 2010). The security services in VANETs include: confidentiality, integrity, and availability. Trusting the network's content; content correctness is another service to look for in addition to the previously mentioned security services.

There are many definitions of trust in the literature (Gerlach, 2007; Golbeck, 2009; Montaner et al., 2002). They all have one thing in common, belief. Trusting an entity means that an entity is expected to behave in a certain way; this is because of a subjective view of that entity's attributes. When a vehicle trusts a message, this means that it has a level of belief that the content of the message is true. It is defined by (Gerlach, 2007) as the willingness of an entity to behave in a certain way or to make a certain decision because the entity believes in the other entity given a situation they both encounter. This belief is governed by three aspects (Gerlach, 2007): the trusting entity, which defines a level of dependency on another entity, the availability of certain attributes in the trusted entity, and the context of the interaction between the two entities. The attributes that an entity selects to evaluate trust originate either from needs or preferences. Trust models in VANETs can be categorized into three categories (Jie Zhang, 2011): entity centric, data centric, and

combined. The entity centric model defines trust relationships between the vehicles in the network: if one trusts a vehicle, then one trusts its data, while the data centric model puts the trust on the information exchanged in the network. The more votes a piece of information attains, the more trusted it is. The combined model, as the name suggests, uses a combination of both models.

Our ultimate goal is to enhance the decision-making process using trust: we plan to study the effect of trust on the time needed to make a decision and on the accuracy of that decision. For example, when a vehicle receives a message reporting an event in the network, we want to learn how long it will take the vehicle to react to the event, positively or negatively (i.e., how many reports are needed for the vehicle to make a decision). Moreover, we want to study whether the vehicle's reaction is the right one. Did it accept a false report or did it ignore a genuine report?

In this chapter, we study the effect of attribute similarity on the average trust level in a network of vehicles. We use three attributes to calculate the pair-wise similarity degree: speed, location, and time. We find that these three relate the most to the behavior we seek to study. The similarity degree is then used to derive trust ratings for the vehicles in the network. In addition, we study the time it takes a vehicle to evaluate another vehicle in the network. Our contribution in this chapter addresses the feasibility of using similarity to achieve trust.

4.2 Motivation

Our goal in this research is to form trust relationships between vehicles through similarity and to use the calculated trust ratings to identify abnormal vehicles. Abnormal vehicles are vehicles that exhibit unpredictable behaviors, such as capricious rates of acceleration and deceleration and failure to maintain safety

distance. We expect these vehicles to have low trust ratings, as their actions cannot be counted on (i.e., they are untrustworthy).

Using trust to form relationships between vehicles can be used by many VANET applications; for example, if a vehicle traveling on the highway is grouped with vehicles in which the passengers share the same taste in food, messages from vehicles recommending a food outlet are more likely to be accepted. Vehicles equipped with the same fog detection sensors will accept the readings from these sensors. Other examples include recommendations of tourist sites or alternate routes. These are only a few of the examples where trust can be utilized.

4.3 Trust Applications in VANETs

In the work of (Golbeck, 2009), trust defines how we deal with data, from whom we accept it, and how we act on it. The author explained that trust is belief and commitment: belief that an entity will act a certain way in a situation, and commitment is acting upon that belief. Trust should be derived from user similarity (Montaner et al., 2002). Trust is having faith in other entities, and acting in accordance with that faith without any guarantee of the outcome.

As mentioned in Chapter 3, the relationship between trust and similarity is investigated in recommender systems to understand how similarity relates to the way users determine trust. Researchers studied the influence of similarity in users' choices and selections when presented with recommendations. For instance, trust-based recommender systems capture similarities between user profiles (Golbeck, 2009). Users tend to prefer recommendations from friends or people they trust.

Data mining has many applications in VANETs (Al-Khassawneh & Salim, 2012). As mentioned in Chapter 3, data mining is used to construct an image of the

network. Furthermore, it is then used for routing and route predictions in addition to identifying malicious vehicles. In VANETs, members of the network process streams of data. To ensure efficient performances of the vehicle's resources, the data in the network should be handled in ingenious ways. One approach is to process the stream in chunks and to replace the chunks as more data arrive for processing (Golab & Özsu, 2003). Another approach is to replace the sample data periodically (Domingos & Hulten, 2003). Finally, the incremental learning approach adopts the use of windows (Gama, Medas, & Rodrigues, 2005). (Rezgui & Cherkaoui, 2011) used association rules to identify faulty or malicious vehicles. The association rules are constructed in periods of times that are called episodes. A vehicle listens for reports on an event in the network, and at the end of the episode, it forms association rules based on whether a vehicle reported an event or not. Faulty or malicious vehicles are identified when they fail to report an event. The identification of malicious or faulty vehicles is done at the moment of an event without prior knowledge of past behaviors of the vehicles in the network. (N. Yang, 2013) proposed a similar approach to evaluate the reputation of vehicles in the network. In our approach, we plan to establish relationships between the vehicles in the network and then use these relationships to provision different services to the vehicles, such as identifying abnormal vehicles.

4.4 System Description

Data from the sensors and the other vehicles in the network constitute data streams in VANETs. In our previous work (Al Falasi & Mohamed, 2013) as explained in Chapter 3, we explain how the nature of the data created in vehicular networks dictates the use of data mining techniques that adapt to the continuously

changing streams. We propose the use of data mining techniques to find similarities between the vehicles to achieve the following benefits:

1. Assign a trust rating to each neighbor of a vehicle. Trust ratings are used to identify abnormal vehicles.
2. Understand the vehicles' demographics in a certain area, which can help commercial companies market their products or services to potential customers.
3. Assist the transport authorities to enhance the quality of service for the travelers. For example, if roads are congested because vehicles use similar routes at similar times of the day, the transport authorities can suggest alternate routes to alleviate the congestion.

Our main focus is to use similarity to assign trust ratings to the vehicles in the network and then use the trust ratings to identify abnormal vehicles. Each vehicle will calculate and assign its own ratings to its neighbors; the view of trust is therefore subjective. In addition, trust is a cumulative value, as past interactions affect the value of the new trust rating. If a vehicle behaves normally most of the time, and due to some kind of malfunction it exhibits an abnormal behavior, its trust rating would not be solely calculated based on this abnormality or the normality, but all historical behaviors will be considered. However, more recent trust ratings will be given higher weight than older ratings in the overall trust calculation. Trust will be an amalgamation of a vehicle's behavior where past behavior is not discounted.

4.4.1 System Modules

We design the framework of a system that continuously calculates trust ratings for all the neighbors of a vehicle. These trust ratings will then be used to

assist a vehicle in making a decision about an event in the network. The trust rating of a vehicle along with any report it sends out about an event in the network will be used by the receiving vehicle as an endorsement or corroboration of the reported event.

4.4.2 System Components

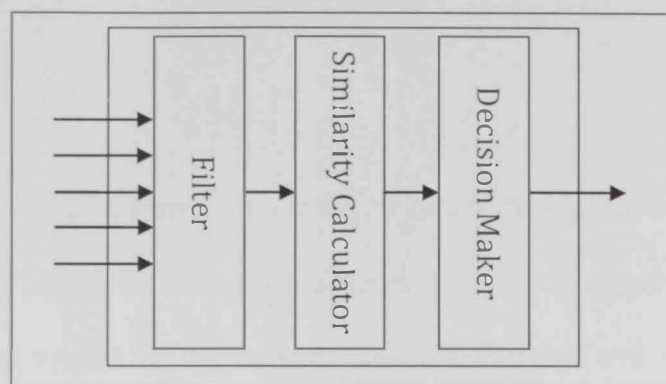


Figure 4-1: System Architecture

As shown in Figure 4-1, our Similarity-based Trust Management System (SbTMS) comprises three modules. The first module filters the data streams from the network in order to prepare them to be processed by the following modules in the system; it extracts the information required by the next modules.

Table 4-1: System Modules

Module	Description		
	Function	Input	Output
Filter	Extract information from received beacons	Beacons from neighboring vehicles	Array of neighboring vehicles speed, location and messagetimestamp
Similarity Calculator	Assign similarity rating to every neighbor of a vehicle	The array from the Filter module	Similarity rating for every neighbor
Decision Maker	Assign trust rating to every neighbor of a vehicle	Similarity ratings from the Similarity Calculator module	Trust ratings of the neighboring vehicles

Vehicles exchange messages for different applications; it is the responsibility of the Filter module to extract speed, position and time information from the received beacons for the Similarity Calculator module. The second module calculates the similarity between the vehicles using a data mining technique (see Section 4.4.3). The final module makes the judgment about a vehicle; it assigns the trust ratings to the information provided by the vehicle. A summary of each module's function is provided in Table 4-1.

4.4.3 Similarity

Throughout the journey of a vehicle, it meets many other vehicles along the way. The vehicle listens for beacons sent from its one-hop neighbors. The beacons carry information related to the source vehicle's location and speed. Additional information might be available in the beacon depending on the applications running onboard. As more attributes are added to calculate the similarity degree, different methods must be used to validate them (N. Yang, 2013). The received information is processed and stored in the receiving vehicle for later handling. During the listening period, V_2 encountered the below vehicles driving at a similar speed:

V_0 : 4 times

V_1 : 1 time

V_5 : 2 times

V_6 : 1 time

V_7 : 4 times

V_8 : 2 times

V_9 : 2 times

Table 4-2 shows the frequency at which the neighbors of V_2 have exhibited similar speeds at similar locations.

Table 4-2: Sample Similarity Matrix in Vehicle V_2

V_0	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8	V_9
1	?	1	?	?	?	?	?	1	?
1	1	1	?	?	?	?	1	1	?
1	?	1	?	?	?	?	1	?	?
1	?	1	?	?	1	?	1	?	?
?	?	1	?	?	1	1	1	?	1

In order to investigate the existence of relationships between the vehicles, we use Apriori, which is a data mining algorithm that is used to mine frequent item sets and develop association rules (Wu et al., 2008). When we feed this dataset to Apriori, the below association rules are derived:

$$V_2=1 \implies V_0=1, \text{ confidence: } (0.8)$$

$$V_2=1 \implies V_1=1, \text{ confidence: } (0.2)$$

$$V_2=1 \implies V_5=1, \text{ confidence: } (0.4)$$

$$V_2=1 \implies V_6=1, \text{ confidence: } (0.2)$$

$$V_2=1 \implies V_7=1, \text{ confidence: } (0.8)$$

$$V_2=1 \implies V_8=1, \text{ confidence: } (0.4)$$

$$V_2=1 \implies V_9=1, \text{ confidence: } (0.2)$$

Where the confidence value of each association rule represents its correctness; for example, the probability that V_2 and V_0 will travel at the same speed during the same time is 80%, and the probability that V_2 and V_5 will travel at the same

speed during the same time is 40%. 20% is the probability that V_2 and V_9 will travel at the same speed during the same time.

We use the association rules to compute the similarity rating. At the end of the listening period, the similarity rating S_{ij} is calculated using the following equation:

$$S_{ij} = \text{Freq}_{ij}/x, \quad x > 0 \quad (1)$$

Where Freq_{ij} is the *met* value for vehicles i and j , and x is the duration (in seconds) of the observation (listening period). Three measures are considered when calculating the pair-wise similarity degree: location, speed, and time. The vehicle continuously listens for beacons from its one-hop neighbors (i.e., when their locations are within the communication range of the vehicle). Only neighbor vehicles traveling at a similar speed as the listening vehicles cause the increment of the *met* value.

Finally, a vehicle V listens for other vehicles that have similar speeds during the listening period. The resulting similarity rating is then used to calculate the trust rating.

The average trust rating between a pair of normal vehicles in the network, and between a pair of normal vehicles and abnormal is displayed in Figure 4-2. The calculated average trust rating represents the current similarity rating calculated using Equation 1. Equation 1 does not provide sufficient information to distinguish between normal and abnormal vehicles in the network. The trust rating is instantaneous; it does not include—to some extent—long-term information about the vehicles in the network (i.e., it does not help vehicles attain clear information regarding their neighbors).

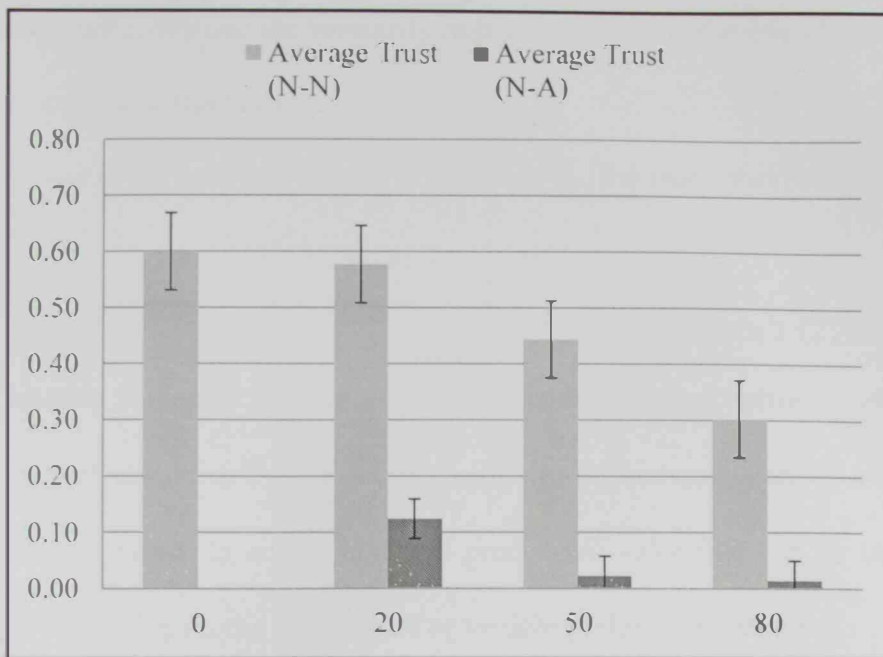


Figure 4-2: Average trust rating in the network between vehicles

In the next section, we introduce the rate of decay α , which we anticipate to assist in distinguishing between normal and abnormal vehicles in the network.

4.4.4 Trust

Each vehicle listens to the beacons sent from its neighbors throughout the journey. The duration of the journey is divided into equal length time intervals (e.g., 10 seconds), which we call *periods*. Calculating similarity and consequently trust ratings is done over these periods of time. Trust is a cumulative value where, at the end of each listening period, the trust rating is updated by adding the current similarity rating to the previous trust rating. Moreover, VANETs are constantly changing, as they comprise highly mobile nodes. In order to capture this characteristic of VANETs, we use an exponential decay function to assign a weight to the old and new values of trust in our calculation. We derive trust from similarity; we look for vehicles that exhibit similar behaviors in terms of acceleration and

deceleration rates. We use the similarity rating calculated at the end of each listening period to compute a trust rating.

Below is the equation we use to calculate T_{ij} , the trust rating between vehicles i and j :

$$T_{ij}^n = (1-\alpha)T_{ij}^{n-1} + \alpha S_{ij}^n, \quad T_{ij}^0 = \varphi, 0 < \alpha < 1 \quad (2)$$

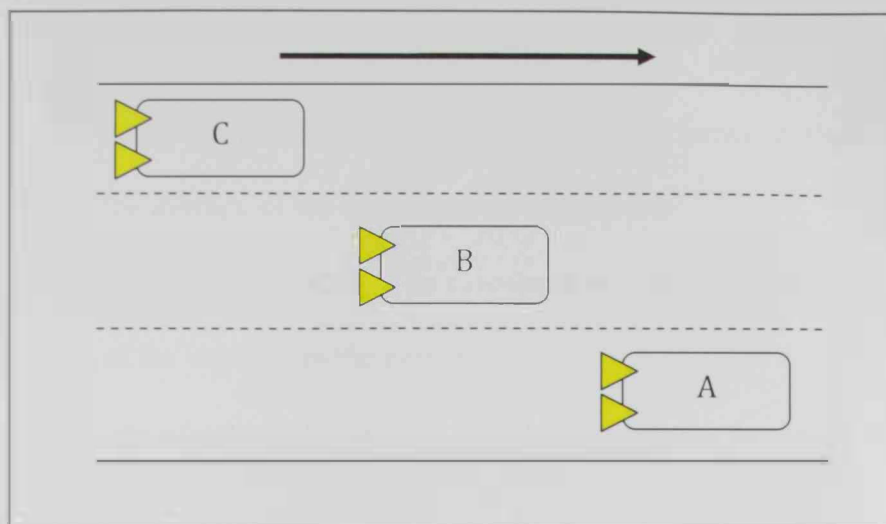
where α is the rate of decay, S_{ij}^n is the similarity rating between vehicles i and j in the current period n , T_{ij}^{n-1} is the trust value in the previous period, $n-1$, and φ is the initial trust value. In addition, α is a predefined value that can be increased or decreased depending on the application or vehicle preference settings.

Similar to recommender systems, we face the problem of meeting new vehicles. In order to address this problem, we implement the following: when a vehicle meets a new neighbor, it assigns the vehicle a predefined trust rating φ . The value of φ in our simulation is set to 0.5; it's the average trust value between untrusted (0) and trusted (1). The trust rating of the new vehicle will then be adjusted using the above formula through the communication between the two vehicles. The more communication a vehicle receives from another vehicle results in more information for computing the similarity rating.

4.5 Simulation and Results

Throughout this dissertation we use Simulation of Urban Mobility (SUMO) (Krajzewicz, Bonert, & Wagner, 2006), which is a microscopic simulator, to simulate the traffic in a network of vehicles. It generates realistic traffic traces of vehicles' movements. The trace files generated from SUMO indicate the speed and location of every vehicle in the network during every step of the simulation. Each step of the simulation represents one second of simulation time. Our simulation is a

simplified highway topology, a one-way highway with three lanes. The length of the



highway segment is 5,000 m as shown in Figure 4-3.

All of the simulation runs use 100 vehicles. We use the built-in Sigma parameter to define the driver imperfection in the simulation regarding the driver's ability to adapt to the desired safe speed. The percentage of vehicles with $\text{Sigma} = P$ is P . We have four simulation runs with different values of P as follows: 0, 20, 50, and 80. The listening period used to calculate similarity and trust ratings is set to 60 seconds in all runs.

On top of the traffic generated from SUMO, we build an application that

Figure 4-3: Sample Highway Segment

assigns trust ratings to all the vehicles in the network. We read the trace file generated by SUMO for further processing. We use the formulas defined earlier to compute the average trust rating between normal vehicles and abnormal vehicles. At the end of the listening period, the similarity rating is used to calculate the pair-wise trust rating between all vehicles in the network. In the simulation runs, α is set to 0.2, 0.5, and 0.9 in order to experiment with different weights of the current trust rating.

4.6 Discussion

We performed a series of experiments to compute the following:

- Maximum meeting time: The longest period of continuous communication between the vehicles in the network. Here, we present the average of the maximum meeting times.
- Average trust rating: The calculated average value of the trust ratings of the vehicles in the network.
- Identification of abnormal vehicles through the use of the trust rating.

4.6.1 Maximum Meeting Time

In order to validate our proposed system, we use the simulation to compute the maximum meeting time for the vehicles in the network, which is the longest period of continuous communication. We want to know if a vehicle will have enough time to make a determination regarding its neighbors and to build a view of its local network. We capture the duration of continuous communication by calculating how long a vehicle was uninterruptedly in another vehicle's communication range. As mentioned earlier, the simulation was run on four values of P : 0, 20, 50, and 80. In the first network, where $P = 0$, the average meeting time of the vehicles is 118seconds. In the fourth network, the average meeting time is 133seconds. On average, the vehicles remain in contact for 124seconds. Figure 4-4 displays the average meeting time in the different networks. Vehicles seem to maintain their speeds, and the more vehicles that travel at the same speed results in a better opportunity for them to learn about each other.

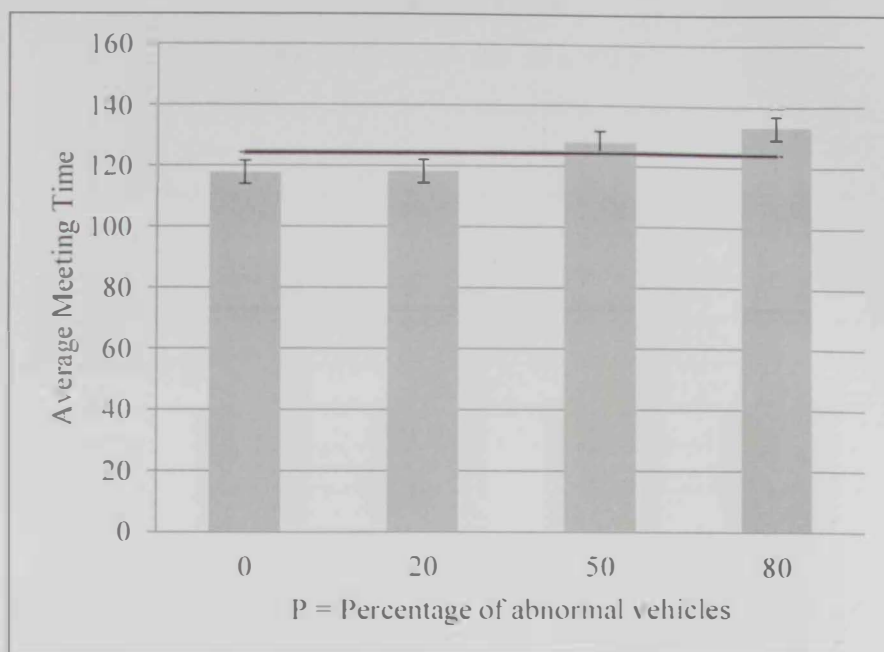


Figure 4-4: Average Meeting Time

4.6.2 Average Trust Rating

The value P in our simulation defines the percentage of vehicles with unpredictable drivers' behaviors. Prior to the start of the simulation, these vehicles are not known. The average trust rating is used to identify these vehicles. During the listening period, every vehicle stores the frequency at which any of its one-hop neighbors has reported a similar traveling speed. The listening vehicle keeps a record that registers all the vehicles that had similar attributes of speed, location, and time.

We experimented with several different values for P to study the effect of similarity on trust. When $\alpha = 0.2$, the average trust rating between normal vehicles is approximately 0.3, and it decreases as the percentage of abnormal vehicles increases in the network to 80% as shown in Figure 4-5. On the other hand, the average trust rating between normal and abnormal vehicles increases as the number of abnormal vehicles increases, as shown in Figure 4-6.

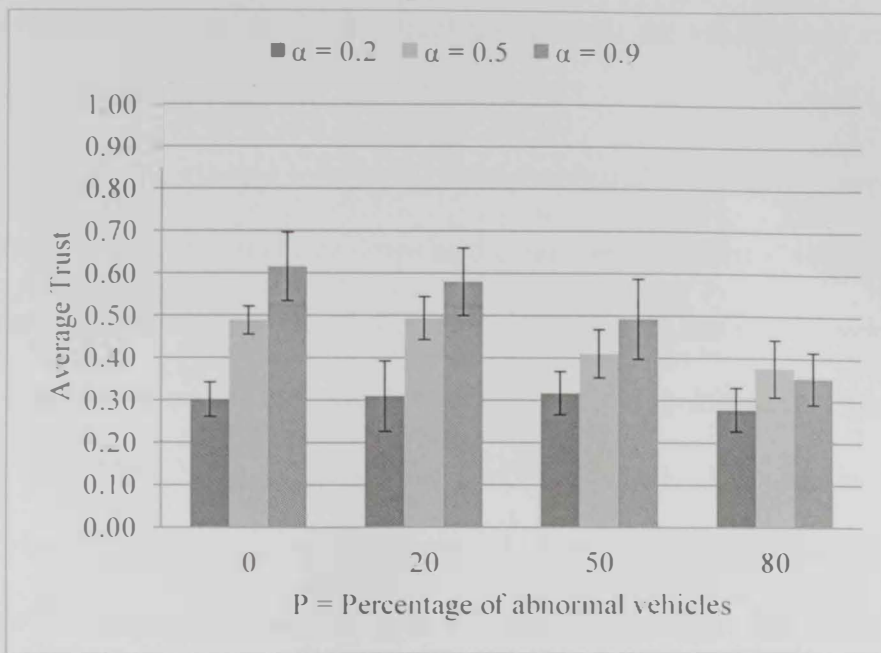


Figure 4-5. Average trust rating in the network between normal vehicles

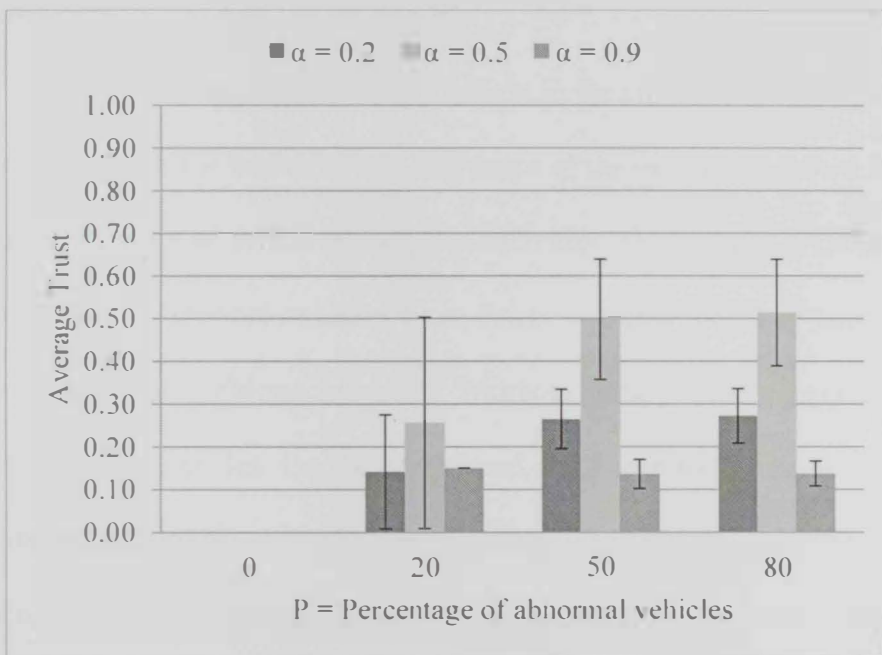


Figure 4-6. Average trust rating in the network between normal vehicles and abnormal vehicles

The average trust rating reaches values almost similar to the average trust rating between normal vehicles. The value of $\alpha = 0.2$ does not provide enough information to distinguish between normal and abnormal vehicles in the network;

more weight is assigned to the old trust rating when the vehicles are still learning about each other.

Initially, the average trust rating between normal vehicles is at approximately 50% when $\alpha = 0.5$. The trust rate drops as the number of abnormal vehicles increases in the network as shown in Figure 4-5. The vehicles meet less normal vehicles along the way, and as a result, the overall average trust rating drops. In Figure 4-6, the average trust rating between normal and abnormal vehicles increases as the number of abnormal vehicles increases in the network. The trust rating of abnormal vehicles increases to reach 50%. Setting α to 0.5 does not support the decision-making process in the network, as the distinction between normal and abnormal vehicles diminishes.

When $\alpha = 0.9$, we assign a larger weight to the current trust rating of a vehicle in order to maintain the freshness and relevance of the rating. As shown in Figure 4-5, when the number of abnormal vehicles increases, the average trust rating in the network decreases. Normal vehicles have fewer vehicles that they can trust as the number of abnormal vehicles increases. Moreover, the vehicles have less time to locate trustworthy vehicles. On the other hand, as shown in Figure 4-6, the average trust rating for abnormal vehicle is approximately 0.15. This is understandable, as the trust rating is based on similarity. If a vehicle cannot find similarities between itself and another vehicle, the trust rating for that vehicle will be low.

Throughout this dissertation, we use a value of $\alpha = 0.9$ to calculate trust. As per the results displayed in Figure 4-6, we have better results identifying abnormal vehicles using $\alpha = 0.9$.

4.6.3 Identifying Abnormal Vehicles

Given the results from our simulations, we can safely assume that a vehicle is abnormal if its trust rating is close to 0.15.

4.6.4 Scalability

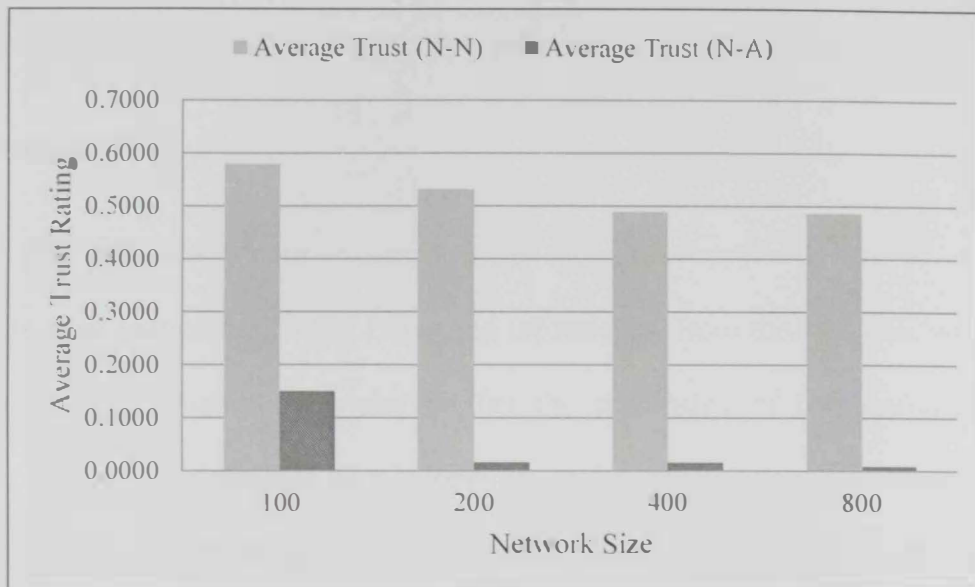


Figure 4-7: Average trust rating between normal vehicles, and between normal and abnormal vehicles in different size networks

In our simulation, the vehicle listens to the beacons sent from its neighbors throughout the journey. If a vehicle stops receiving beacons from a former neighbor for a while, that vehicle is then removed from the neighborhood list; the list of vehicles within communication range. At every given moment, each vehicle has a finite number of neighbors, which allows this model to be implemented in big networks. We analyze this further by examining the scalability of our trust management system in different size networks. We first define what we mean by scalability; scalability is the ability of our trust management system to achieve trust ratings between normal vehicles that are much larger than the trust ratings between normal and abnormal vehicles, both in sparse and highly overloaded networks. Then,

we simulate the average trust rating between normal vehicles, and normal and abnormal vehicles in different network sizes. A representation of the simulation result can be seen in Figure 4-7. We can see that the average trust rating between normal vehicles remains high as the number of vehicles increase. However, the average trust rating between normal and abnormal vehicles decreases as the number of vehicles increase. These results indicate a good performance by our trust management system in different network sizes whether sparse or dense.

4.7 Summary

Our proposed system architecture has shown that similarity can be used to compute trust between vehicles. Using the information from the beacons, we were able to build association rules that predict the probability of correspondence in driving behavior (i.e. the rate of acceleration, rate of deceleration, and preservation of safety distance). Moreover, we calculated the maximum meeting time of vehicles in the network through simulation and demonstrated that there is enough time for the vehicles to gather information about their one-hop neighbors. In addition, we were able to successfully identify abnormal vehicles through the computed trust rating. We proposed a system architecture that filters the data in the network in order to isolate useful information. The isolated bits of information are then used to calculate the similarity degree between a vehicle and all of its one-hop neighbors. Finally, the generated similarity ratings are used to compute the trust ratings of the vehicles. The system is designed to use data mining techniques to find high value information in a highly dynamic network. In the system, similarity between vehicles is mined using association rule mining. Each vehicle looks for other vehicles that frequently exhibit similar speeds in a given location and a specific timeframe.

Chapter 5: The Impact of Trust on Vehicular Applications

5.1 Introduction

Vehicles form trust relationships with other vehicles in a network for many reasons. For example, in safety applications, it's more important to ensure the correctness of the data than to authenticate the vehicles (Huang et al., 2014). Some VANET applications can make use of the formed trust relations to enhance their performance and reliability. In this chapter, we study the impact of vehicular trusted groups on the network. We develop an analytical model that associates trust with the performance of the decision-making process and the accuracy.

5.2 Motivation

Relationships between vehicles on a road exist. They might not be explicit, but they are certainly understood by the members of the network. A trust relationship exists between private vehicles and a police car because of the latter's role in the network. Vehicles trust a police car as an authoritative source of information; therefore, messages sent by a police car are accepted and trusted by all members of the network.

Other types of relationships are created from the behavior of the vehicles. A behavior can be any activity exhibited by a vehicle or the travelers on board, such as vehicles driving in the same direction or passengers playing the same video games on board. Sometimes relationships can be manifested as dependencies. A vehicle or a group of vehicles can be the only source for information. This creates a dependency relationship between them and the other vehicles in the network. For example, there can be two clusters (C1 and C2) of vehicles on a stretch of a road, and vehicle A is

traveling halfway between the two clusters. Due to A's proximity to both clusters, A is the only connection C2 has with C1. Therefore, C2 is dependent on vehicle A to receive messages from C1.

Majority voting has been investigated by (C. Chen et al., 2010b). The authors proposed a protocol where trust is already established between groups of vehicles. The aim of the paper is to reach a consensus about a safety event using trust. In our model, we study the effect trust has on the number of messages needed for a vehicle to make a decision and on the error probability of that decision.

In this chapter, we investigate the effect of trust in the performance of safety applications. Safety applications have strict requirements: most important of them all is a minimum delay. We show the positive impact of trust on the decision-making process in a vehicle; it facilitates better decisions with less information. We compare the performance of our system that utilizes trust with a generic voting system in terms of number of messages needed to reach a decision, and the accuracy of that decision. We assume that trust is already established between some vehicles in a network using the system architecture introduced in Chapter 4. Using trust, we examine vehicle reactions to warning messages from other vehicles.

5.3 The Model

In this section, we present the trust model. In the model, we want to calculate the expected number of warning messages needed for a vehicle to react and for the expected error rate. Every vehicle in the network would have already formulated trust relationships with some of its one-hop neighbors; for example, (J. Wang et al., 2009) proposed a trust building scheme that aims at integrating attribute similarity with ad hoc routing protocols to improve the reliable delivery of packets. The

scheme is built by defining a pair-wise trust value to determine how to interact with a node around the notion that a user is more inclined to trust a node that shares common attributes.

In our model, we want to measure two things: the expected number of messages needed for a vehicle to make a decision and the error rate of that decision. We have the following inputs to the model: N is the number of one-hop neighbors of a vehicle, t is the number of trusted neighbors, and u is the number of untrusted neighbors. For example, a vehicle might have five neighbors ($N = 5$), where three of them are untrusted ($u = 3$) and two vehicles are trusted ($t = 2$). This results in a ratio of 60:40 between the number of untrusted vehicles and trusted vehicles. One message from a trusted vehicle warning of an event is enough to make a vehicle react, while it takes the majority of the neighbors to report the same event in the case of untrusted vehicles. Every received message represents a level in a tree. The ratio of untrusted to trusted vehicles changes from one level to another, as whenever a vehicle receives a message from an untrusted vehicle, they must be removed from the ratio calculation. Therefore, we have $N = 5$, $t = 2$, and $u = 3$, in this case, we have a tree with three levels.

Level 1: The percentage of trusted vehicles is $2/5 = 40\%$, while the percentage of untrusted vehicles is $3/5 = 60\%$.

Level 2: We remove one untrusted vehicle, which leaves a total of four vehicles ($N = 4$). The percentage of trusted vehicles is $2/4=50\%$, while the percentage of untrusted vehicles is $2/4 = 50\%$.

Level 3: We remove one more vehicle and then $N = 3$. The percentage of trusted vehicles is $2/3=66.67\%$, while the percentage of untrusted vehicles is $1/3 = 33.33\%$.

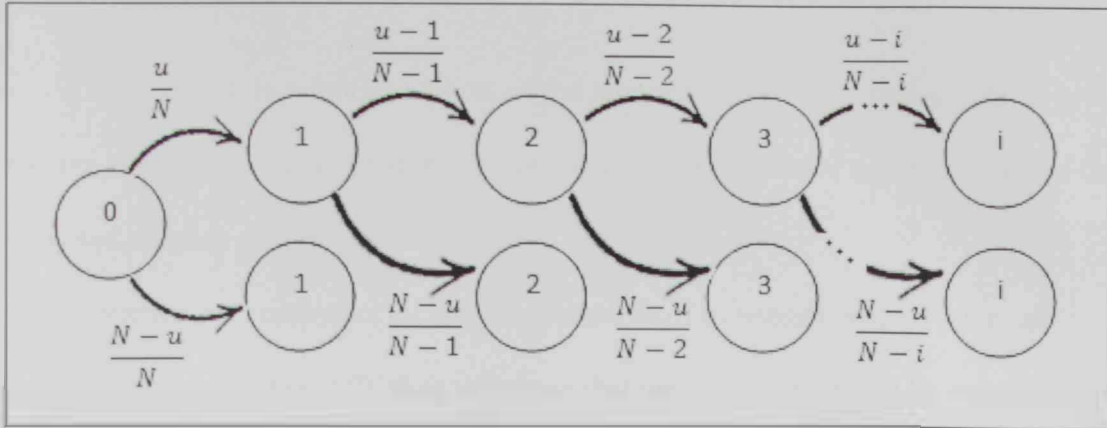


Figure 5-1: The depth of the tree is $\left\lfloor \frac{N}{2} \right\rfloor + 1$

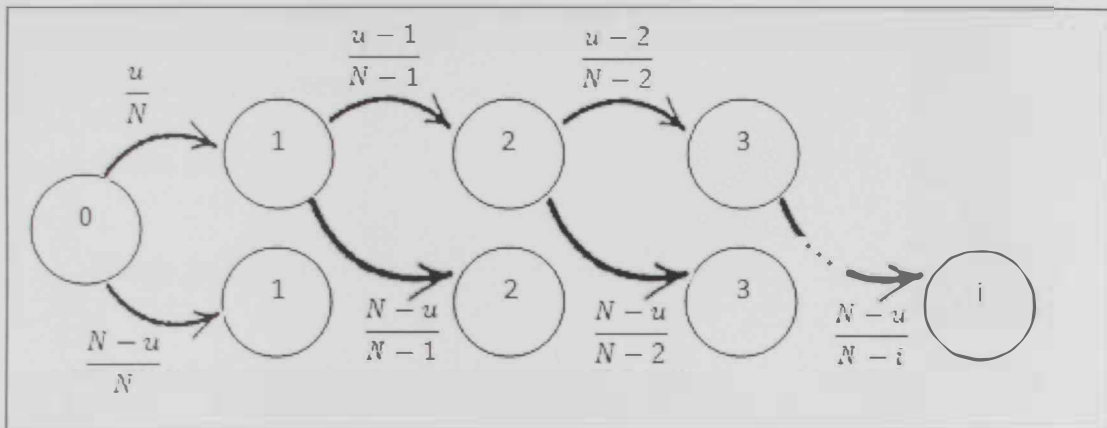


Figure 5-2: The depth of the tree is $u + 1$

We evaluate the trust models using the following two metrics:

1. Expected number of messages and
2. Expected error rate.

Expected number of messages is defined as the number of messages needed for a vehicle to make a decision with respect to an event. Expected error rate is the probability of a vehicle making the wrong decision based on the messages it receives about an event.

5.3.1 Expected Number of Messages

Figure 5-1 is a representation of the number of messages that a vehicle must receive before making a decision. Figure 5-1 provides a general representation of the expected number of messages when $u > t$.

Figure 5-2 represents the expected number of messages when $u \leq t$. If all neighbors are trusted ($u = 0$), then we argue that one message should be enough for a vehicle to make a decision and react.

$$\text{Expected Number of Messages} = 1 \quad (\text{a})$$

Using Figures 5-1 and 5-2 above, we found that the expected number of messages can be calculated using the following expressions:

When $u > t$, we have three terms:

$$\text{Term 1: } \frac{N-u}{N}$$

$$\text{Term 2: } \sum_{i=1}^{\lfloor \frac{N}{2} \rfloor} \left[(i+1) \times \left(\frac{N-u}{N-i} \right) \times \prod_{k=0}^{i-1} \left(\frac{u-k}{N-k} \right) \right]$$

$$\text{Term 3: } \left[\left(\left\lfloor \frac{N}{2} \right\rfloor + 1 \right) \times \prod_{i=0}^{\lfloor \frac{N}{2} \rfloor} \left(\frac{u-i}{N-i} \right) \right]$$

$$\text{Expected Number of Messages} = \text{Term 1} + \text{Term 2} + \text{Term 3} \quad (\text{b})$$

Meanwhile, when $0 < u \leq t$, we have two terms:

$$\text{Term 4: } \frac{N-u}{N}$$

$$\text{Term 5: } \sum_{i=1}^u \left[(i+1) \times \left(\frac{N-u}{N-i} \right) \times \prod_{k=0}^{i-1} \left(\frac{u-k}{N-k} \right) \right]$$

$$\text{Expected Number of Messages} = \text{Term 4} + \text{Term 5} \quad (\text{c})$$

5.3.2 Expected Error Rate

Using Figures 5-1 and 5-2 again, but replacing the number of messages with the probability of receiving false messages from a vehicle's neighbors, using the following:

- e_u = probability of receiving a false message from an untrusted neighbor.
- e_t = probability of receiving a false message from a trusted neighbor.

First, if all neighbors are trusted or when $u = 0$, then we have:

$$\text{Expected Error Rate} = e_t. \quad (d)$$

When $u > t$, we have the following three terms:

$$\text{Term 1: } \frac{N-u}{N} \times e_t$$

$$\text{Term 2: } \sum_{i=1}^{\lfloor \frac{N}{2} \rfloor} \left[\left(\frac{N-u}{N-i} \right) \times e_t \right] \times \left[\prod_{k=0}^{i-1} \left(\frac{u-k}{N-k} \right) \times e_u \right]$$

$$\text{Term 3: } \prod_{i=0}^{\lfloor \frac{N}{2} \rfloor} \left[\left(\frac{u-i}{N-i} \right) \times e_u \right]$$

$$\text{Expected Error Rate} = \text{Term 1} + \text{Term 2} + \text{Term 3} \quad (e)$$

Meanwhile, when $0 < u \leq t$, we have the following two terms:

$$\text{Term 4: } \frac{N-u}{N} \times e_t$$

$$\text{Term 5: } \sum_{i=1}^u \left[\left(\frac{N-u}{N-i} \right) \times e_t \right] \times \prod_{k=0}^{i-1} \left(\frac{u-k}{N-k} \right) \times e_u$$

$$\text{Expected Error Rate} = \text{Term 4} + \text{Term 5} \quad (f)$$

5.4 Evaluation and Discussion

In this chapter, we make use of a simulation tool that we have developed in Java to calculate the expected number of messages and the expected error rate. The tool accepts as parameters the number of one-hop neighbors, the number of untrusted neighbors, and the probability of receiving false messages from either group of neighbors. In the simulator, the vehicles are randomly classified as trusted or untrusted. In addition, they are randomly selected to either be honest or dishonest. For example, an untrusted vehicle might provide an honest report about a safety event despite its classification. On the other hand, a trusted vehicle might provide a dishonest report about a safety event in the network. We calculate the number of

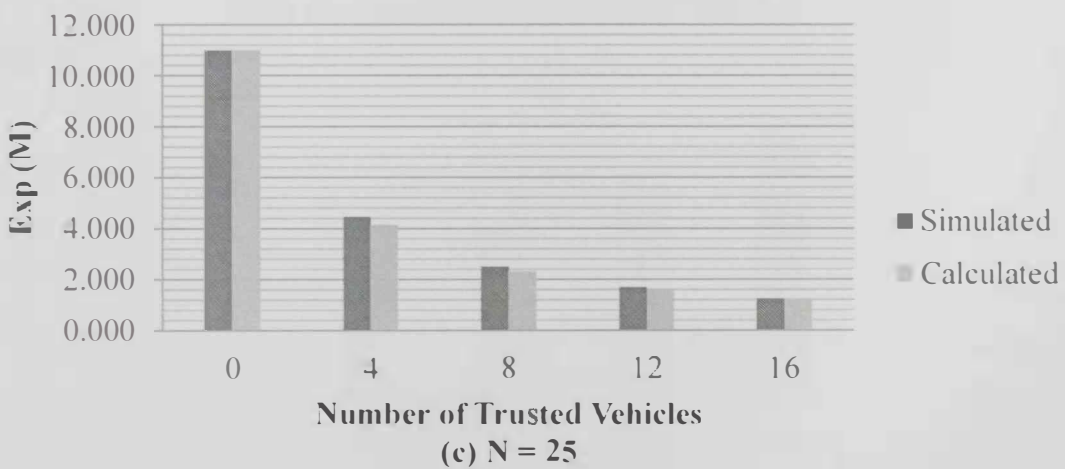
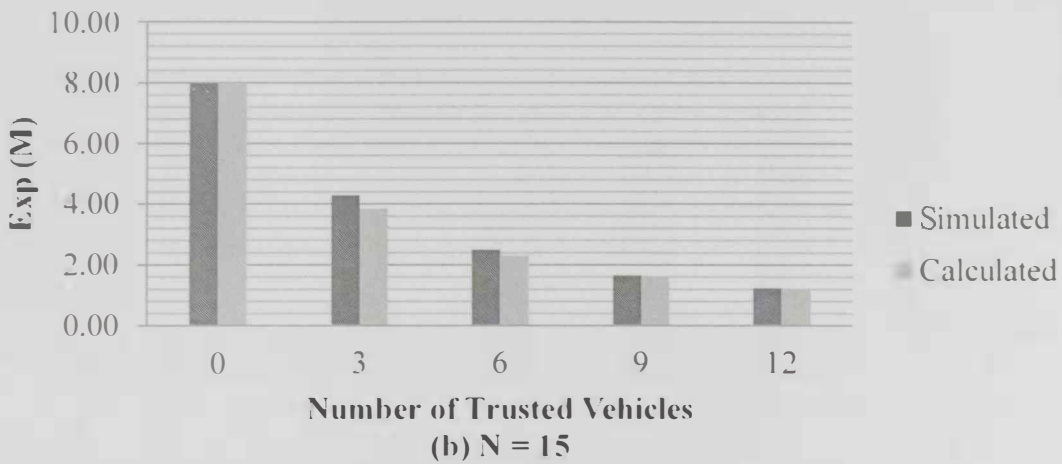
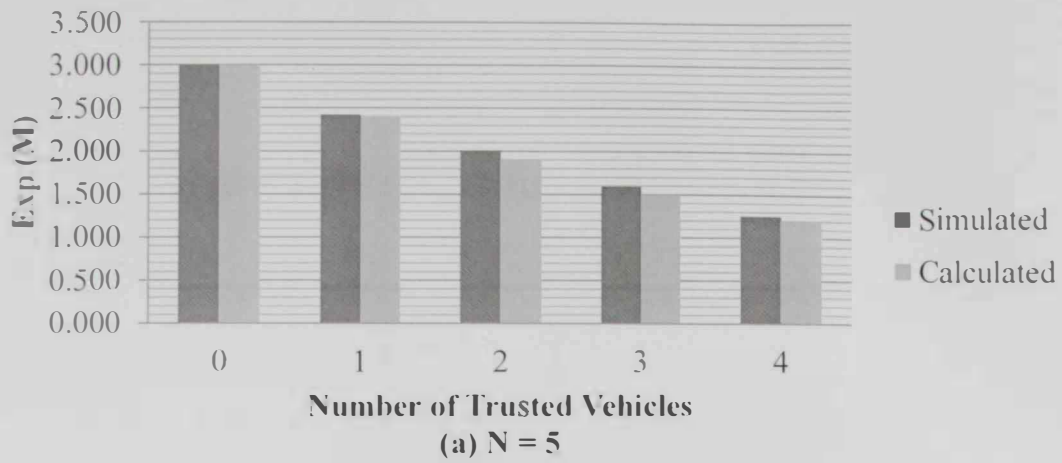


Figure 5-3: Expected Number of Messages

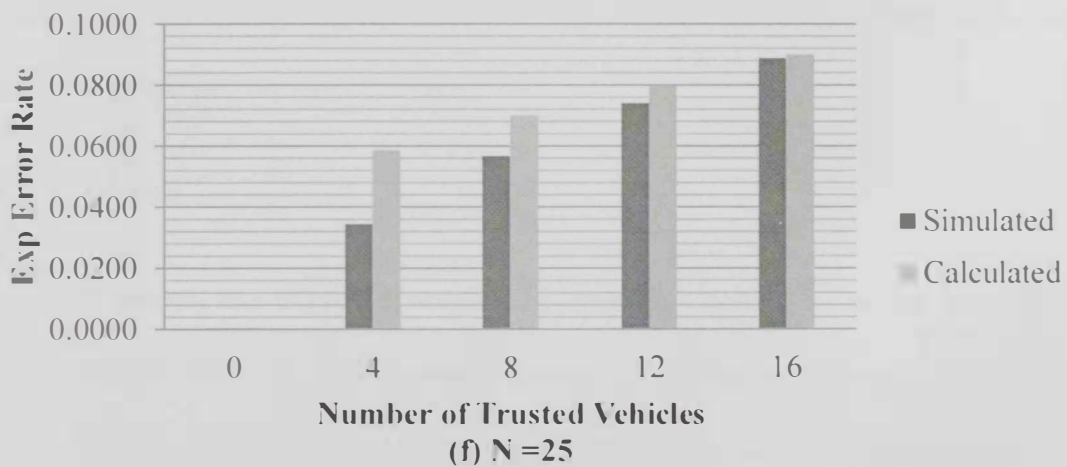
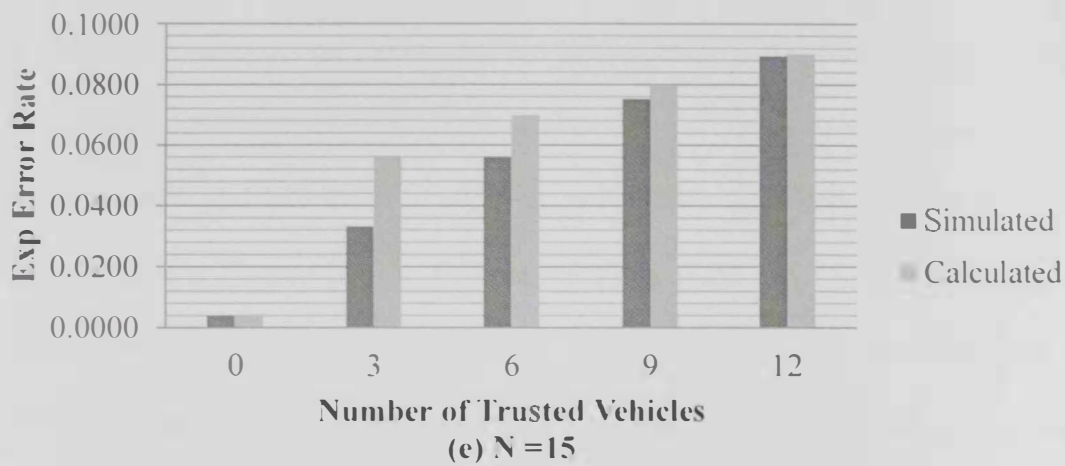
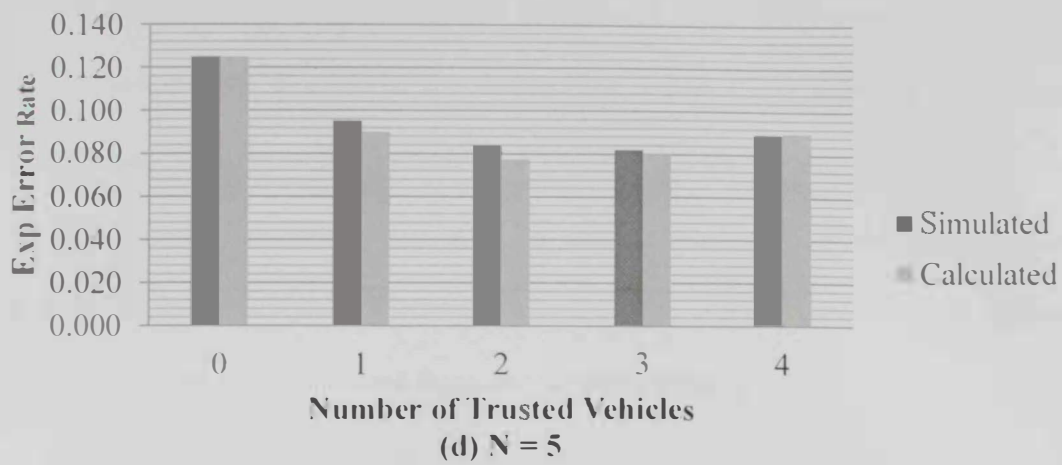


Figure 5-4: Expected Error Rate

messages needed by a vehicle to reach a decision about a safety event, and then we calculate the error rate. For all the simulation runs, we fix the probability of receiving a false message from a trusted vehicle to 0.1 and to 0.5 for an untrusted vehicle. The small false probability reflects the level of confidence a vehicle has in its trusted neighbors, while the 0.5 probability serves as the expected outcome from the gamble of acting on information provided from an untrusted vehicle.

For the other parameters, we experiment with 5, 15, and 25 one-hop neighbors (N) to keep the simulation as real as possible. Our scenario is 5 km-long highway with 3 lanes in one direction (Petit & Mammeri, 2011; Sampigethaya et al., 2005; Zaidi, Milojevic, Rakocevic, & Rajarajan, 2014). The vehicles move at speeds between 80 km/h and 120 km/h. In addition, average distance between two vehicles in the same lane is 77 m as per the recommendations of the Road Safety Authority in UK for minimum stopping distance (RSA, 2012). Given the above parameters, a vehicle can have up to 36 neighbors within communication range. We change the ratio of untrusted vehicles to trusted vehicles for every N . We start with the ratio 1:0 to establish a benchmark to track either the improvement or the degradation that trust introduces to our performance metrics.

5.4.1 Discussion

As shown, the expected number of messages decreases as the number of trusted vehicles increases. The expected number of messages approaches one as the number of trusted vehicles increases in relation to the number of untrusted vehicles. This is consistent with our model where the expected number of messages is equal to one message when all the neighbors are trusted vehicles. From Figure 5-3, we observe that trust can have a positive impact by decreasing the network overhead.

Figure 5-4 shows the expected error rate with the three values of N . As shown, the expected error rate approaches 0.1 as the number of trusted vehicles increases (i.e., the maximum error rate is equal to the error rate of trusted vehicles).

In our calculation of error rate, we use the error rates from both trusted vehicles and untrusted vehicles, and the error rate remains reasonable. When a vehicle receives a warning message from a trusted vehicle, it will take the appropriate action with some risk: a vehicle might have rejected a true safety event warning message. The more trusted vehicles there are in the neighborhood, the less information a vehicle needs before making a decision and taking action.

5.5 Summary

In this chapter, we used both trusted vehicles and untrusted vehicles, and, on average, we acquired good results. With a trusted group, we could enhance the performance of vehicular applications using a smaller number of messages with reasonable error rates. This will enable us to make better decisions with a smaller number of messages. Therefore, we could reduce the average time needed to make such decisions and reduce the overhead on the network.

We demonstrated that trust can reduce the error rate when making a decision about a safety event. In the next chapter, we utilize vehicles behaviors to eliminate the error rate: to ensure that no vehicle accepts a false report of a safety event in the network.

Chapter 6: Similarity-based Trust Management System for Detecting Fake Safety Messages in VANETs

6.1 Introduction

In safety applications, vehicles exchange messages to communicate their current speed and location. In addition, vehicles send safety event messages to warn other vehicles of an incident on the road. The security of the safety event messages is critical, and similarly the accuracy of these messages is as critical. The vehicles in VANETs need to trust safety event messages sent by their neighbors in the network; a few false messages from misbehaving vehicles can disturb the performance of the network. In safety applications, false messages can cause serious accidents. Due to the nature of the applications, any disturbance to the normal operation of the network can threaten the lives of users and incur losses to their properties.

In this chapter, we present an enhancement to the similarity-based trust management system from Chapter 4, which is used to establish trust relationships between vehicles traveling on a road. Vehicles use similarity to assign trust ratings for their one-hop neighbors in the network. The preliminary results of the effectiveness of this similarity-based management system are presented in Chapter 4. In addition, we develop a scheme that utilizes the trust ratings of the vehicles to determine whether the safety event reported by a vehicle is truthful or not. We present the performance of the scheme that is based on trust relationships derived from similarity. Our ultimate goal is to enhance the decision-making process using trust: we want to study whether the vehicle's reaction to a message reporting an event in the network is the right one. Did it accept a false report or did it ignore a genuine report?

6.2 Data Validation Approaches

Data validation is an important element of security in VANETs. In addition to the standard security services, vehicles must ensure that the information they receive is correct and truthful (i.e., trustworthy). Without data validation, an adversary would be able to inject false data into the network to alter the behavior of the participating vehicles. In order to preserve the security of data in VANETs, researchers proposed the use of reputation systems. In reputation systems, the trustworthiness of the data is derived from the trustworthiness of the source of the data (i.e., entity-centric trust). (Mármol & Pérez, 2012) proposed a scheme to assess the reliability of a reported warning message using reputation. The vehicle's decision to accept a warning message or not is determined by considering three sources of information: the reputation of the sender, the recommendation of the neighbors, and the reputation of the sender provided by a central authority if exist. The problem with this scheme is that a vehicle has little time to make a decision about a safety event in the network. It does not have time to query its neighbors about the reliability of the reported safety event.

(Ding, Li, Jiang, & Zhou, 2010) used an event-based reputation model to identify false data. Upon receipt of a safety event message, a vehicle observes the behavior of the sender to determine the truthfulness of the event's report. If the behavior of the sender matches the behavior expected in the presence of such events, then the receiver will conclude that the event is true. Otherwise, the receiver will assign a low reputation value for the reported message. Although this seems like a good solution, it is susceptible to attacks. The malicious vehicle providing false data can modify its behavior during the observation period to deceive the receiver.

Another event-based reputation system, which was presented by (Dötzer, Fischer, & Magiera, 2005), is Vehicle Ad hoc Reputation System (VARs), an event-based reputation system. In the system, the vehicles make the decision to forward an event based on the reputation of the event; when an event is sent, an opinion is attached to it. A vehicle calculates the forwarding probability of an event using three attributes: direct experience of the event, trust value of the reporting vehicle, and aggregated partial opinions. The problem with this system is the use of aggregated opinions; a vehicle will take into account an opinion from a stranger that it never interacted with previously. In (Lo & Tsai, 2009) the authors propose a system to determine if an event occurs in a network and how long it lasts through collecting the observations of vehicles in the network. The vehicles in their proposed system collaborate in terms of either reporting an event in the network, or a misbehaving vehicle using local lists that each vehicle maintains. The problem with this system is that it could fail in delivering a genuine report of a safety event in the network due to the fact that there are no other reports to support it.

In order to prevent false data injection attacks, (Ghaleb, Zainal, & Rassam, 2015) suggested that every vehicle models its neighborhood or the vehicles within its communication range, and then compares the received information from its neighbors to the locally built model. The premise of the research is that a misbehaving vehicle is likely to be an outlier in the local model. Such an approach is hard to implement due to the nature of the neighbor list, as it changes frequently. (Zaidi, Milojevic, Rakocevic, & Rajarajan, 2014) used the speed, density, and flow to build a model to identify malicious vehicles. Flow is calculated from speed and density, and then every vehicle compares the locally calculated flow and density with the flow and density calculated by the sender. If the information does not match, then

the sender is assumed malicious. The model fails to detect a false data injection attack if the data sent by the malicious vehicle conforms to the locally built model. Consensus was used by (Cao, Kong, Lee, Gerla, & Chen, 2008) to prove that a vehicle is relevant to the event it has reported; the burden of proof is on the sender. The reporting vehicle must collect endorsement messages from witnessing vehicles in the area of the detected event to serve as proof. This scheme is prone to failure in areas where there is low traffic density. (Petit & Mammeri, 2011) investigated the consensus problem. The authors investigated the best threshold value needed to react to a warning message.

In this chapter, we use echoing to observe the behavior of the abnormal vehicle. When a vehicle reports a safety event in the network, the receiver of the report will echo that message. If the originator of the safety event message reacts to its own report, then they are assumed truthful; otherwise, they are assumed dishonest, and their trust rating is demoted as a consequence.

6.3 Goals

For a given partition of a VANET, we aim to detect a false data injection attack (i.e., an attempt by an adversary to disseminate false information to disturb the behavior of other vehicles).

We would like to detect this attack using a distributed solution due to the issues inherent in centralized solutions (Dötzer et al., 2005; Raya, 2009).

We evaluate the scheme by examining the probability of detecting an attack given the adversary's trust rating. We also evaluate the efficiency of the scheme. Our aim is to detect the attack using the minimum number of messages and consequently,

minimize the communication overhead on the network as a whole and on the individual vehicles.

6.4 Background

Our scheme is proposed to protect vehicles from a false data injection attack. It reacts to safety event claims made by a vehicle. The scheme predicts that the

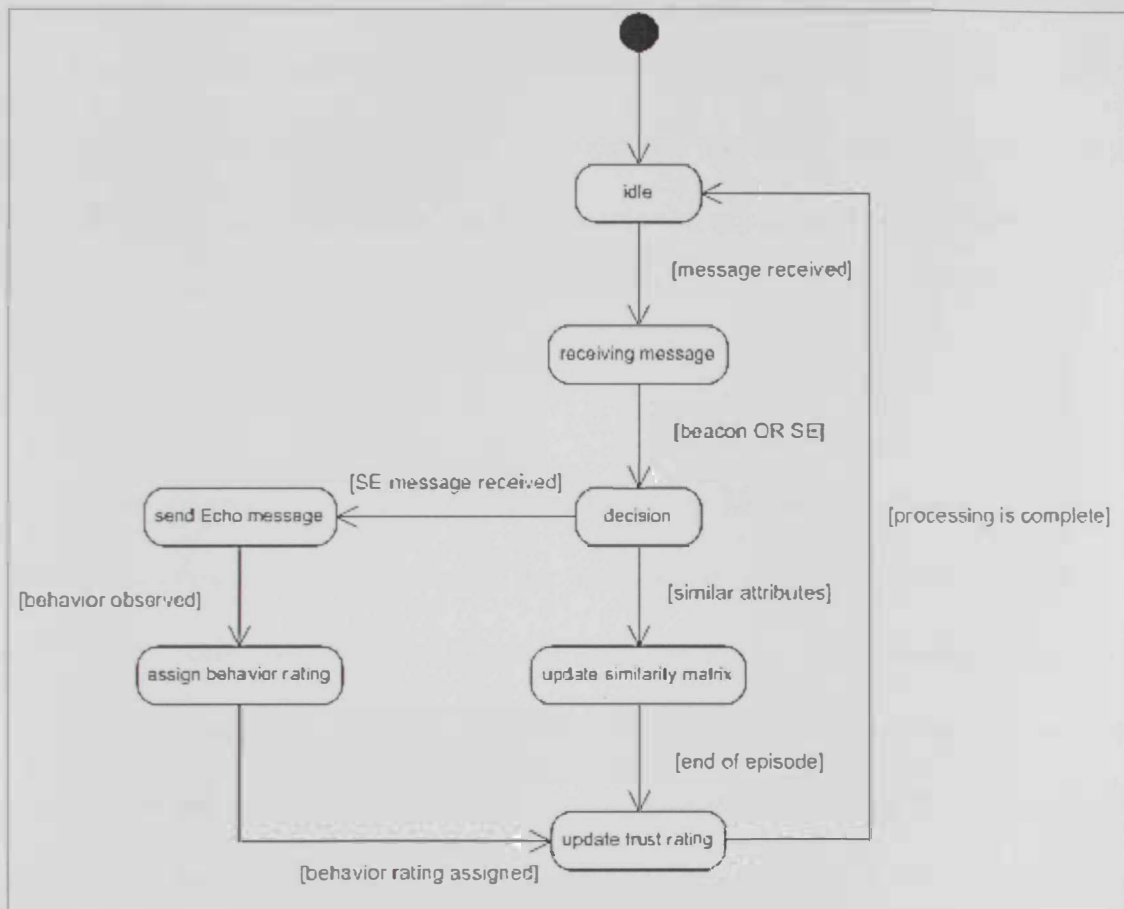


Figure 6-1: State transition diagram of the onboard unit (OBU) in a vehicle source vehicle will react to a truthful safety event report. Figure 6-1 shows the state transition diagram of a vehicle's on-board unit (OBU).

6.4.1 Collaborative Vehicles

VANET comprises vehicles that cooperate to achieve advantages. The vehicles in a VANET work toward individual goals and other collective goals of the

members of the network. For example, an individual goal would be for a vehicle to ensure the security of its communications. On the other hand, an example of a collective goal would be to reduce the network communications overhead, which in turn helps the vehicles achieve other individual goals of better quality of service in the network.

Cooperation in VANETs means that vehicles rely on reports generated by other vehicles on the road to react to safety events. With our proposed trust management system architecture for VANETs using similarity, vehicles construct local views of their surroundings and form opinions about their neighbors. Assuming trust is established, vehicles rely on their calculation of the trust rating of their peers to validate event-generated reports.

6.4.2 Adversary Model

An adversary can send a broadcast to its one-hop neighbors to falsely warn about a safety event in the network for their selfish objectives. The adversary is assumed to exhibit an abnormal behavior (i.e., the vehicle is abnormal). Abnormal vehicles are vehicles that exhibit unpredictable behaviors, such as irregular rates of acceleration and deceleration and failure to maintain safety distance. We expect these vehicles to have low trust ratings, as their actions cannot be counted on (i.e., untrustworthy).

6.4.3 Trust

As explained in Chapter 4, each vehicle listens to the messages sent from its neighbors throughout the journey. The trip duration is divided into equal length time intervals, which we called periods. Similarity and subsequently trust ratings are

calculated at the end of each period. Trust as a cumulative value is updated by adding the current similarity rating to the previous trust rating. In this chapter we introduce a new parameter for calculating trust.

Below is the updated equation we use to calculate T_{ij} , the trust rating between vehicles i and j :

$$T_{ij}^n = [(1 - \alpha)T_{ij}^{n-1} + \alpha S_{ij}^n] B_{ij}^n, \quad T_{ij}^0 = \varphi \quad (3)$$

where α is the rate of decay, S_{ij}^n is the similarity rating between vehicles i and j at the current period n , T_{ij}^{n-1} is the trust value in the previous period, $n-1$, and φ is the initial trust value. In addition, α is a predefined value that can be increased or decreased depending on the application or vehicle preference, and B_{ij}^n is the behavior rating assigned by the receiver to the source of the safety event message, such that:

$$B_{ij}^n = \begin{cases} y, & v_i \text{ is dishonest} \\ 1, & \text{otherwise} \end{cases} \quad (4)$$

As shown in (4), y is the penalty given to the source vehicle for reporting a false safety event. In safety application, this value is subjective and significant as we are dealing with critical applications; there is no room for tolerance. Any report is treated the same way whether it was intentional or not. This value can be relaxed in other types of applications where fault is more tolerable.

6.5 Scheme Overview

In our verification scheme, we have two participants depending on the role they play in the network.

1. **Safety Event Reporter (SER):** A vehicle is designated as SER if it is the originator of the safety event message.

2. **Safety Event Evaluator (SEE):** The one-hop neighbors of the safety event reporter are designated as safety event evaluators.

Our aim is to use the trust rating calculated by every vehicle in the network to validate a safety event reported by a SER. A SEE has the responsibility to identify true from false messages from a SER. When a SEE receives a safety event message from SER, it has t time to verify the event before it must make a decision.

Given the fact that SER and SEE are one-hop neighbors, they have already established a trust relationship between each other following the equations presented in the previous section. The SEE can verify the truthfulness of the received safety event message even though it has not experienced it directly. When a SEE receives a safety event message from a SER, it will react by sending the same message to the SER.

Intuitively, the SER will react to its own message, and the SEE will observe the SER's reaction. If the behavior of the SER matches the typical behavior expected by the SEE, it will consider the message trusted. For example, if a SER sends a safety event message about a road deadlock ahead, the SEE will send the same message back to the SER expecting that the SER's behavior would be to slow down or change the route. If the observed behavior of the SER does not match the behavior the SEE expects, it will conclude that the safety event message is false. The SEE's trust rating of the SER will be updated accordingly to reflect its misbehavior.

We factor the trust rating of the SER calculated by the SEE in the decision-making process. The trust rating is calculated from attribute similarity. Our aim is to improve the precision of the calculated trust ratings by factoring a behavioral element in the calculation.

6.5.1 Echo Protocol

The Echo Protocol is a protocol used to discover false safety event messages sent by a selfish adversary. As presented earlier, we have two participants in the echo protocol, the SER and the SEE. The SER sends the safety event message, and reacts to an echo message. The SER reacts to the echo message in one of the following actions:

- **Brake:** the safety event is a genuine safety event message; therefore, the SER is honest.
- **Do nothing:** The safety event is a fake safety event message; therefore, the SER is a dishonest vehicle.

The receiver of the safety event messages (SEE) sends the echo message to the SER upon receipt of the safety event message. The echo message contains the original safety event message and the hash of the message for authentication. The protocol message exchange is shown in Figure 6-2.

The SEE will continue to receive updates in the form of beacons from the source vehicle and will use these updates to observe which reaction the SER is exhibiting upon receipt of the echo message. The reaction of the SER will help the SEE to draw conclusions about the behavior of the SER and therefore determine the appropriate behavior rating to use in updating the trust rating of the source vehicle. The echo message is intended for the SER only, the original SE message will be broadcast to all the SER neighbors; however, the echo message will only be sent to the source of the SE message. Concerns for viral effects in the network can be addressed as follows: The normal reaction of a vehicle encountering a safety event is to slow down to avoid crashing into the vehicles involved in the safety event. The

purpose of the Echo protocol is to confirm an SE report by simply observing behavior and matching it to the behavior expected in the presence of a safety event.

6.6 Simulation and Results

In this section, we will describe the conducted simulation to demonstrate the validity of the echo protocol using our enhanced similarity-based trust management system. We use SUMO (Krajzewicz et al., 2006) to simulate the traffic in a network of vehicles. Each step of the simulation represents of one second of simulation time. Our simulation is a simplified highway topology, a one-way highway with three lanes. The length of the highway segment is 5,000 m. This is the same setup we used in Chapter 4.

We have 100 vehicles in all of the simulation runs. We use the built-in Sigma parameter to define the driver imperfection in the simulation regarding the driver's ability to adapt to the desired safe speed. Additionally, P is the percentage of vehicles with Sigma = 1.

We have three simulation runs with the following different values of P : 20, 50, and 80. The listening period used to calculate similarity and trust ratings is set to 60 seconds in all the runs. On top of the traffic generated from SUMO, we build an application that assigns trust ratings to all the vehicles in the network.

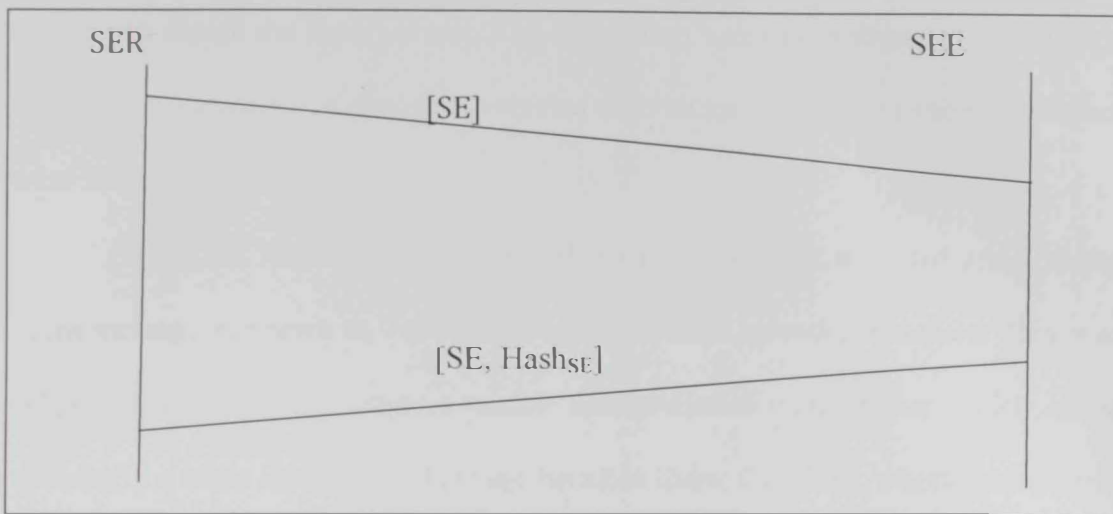


Figure 6-2: The Echo Protocol

We read the trace file generated by SUMO for further processing. In addition, the application is used to validate the echo scheme by incorporating the behavior rate in the calculation of trust. We use Formula (3) to compute the average trust rating between normal vehicles and abnormal vehicles when a vehicle reports a safety event.

The average trust rating is continuously updated throughout the simulation, either through recalculating the similarity or through the behavior rating of the source vehicle.

We simulate a safety event in the network, and then calculate how many vehicles accepted the reporting vehicle's message. The reporting vehicles can either send truthful or dishonest messages. We use the trust rating of the reporting vehicle to assist the receiving vehicles in making their decisions about the safety event message.

We validate the system by calculating the percentage of vehicles that accepted a true report of a safety event in the network vs. the percentage of vehicles that accepted a false report of a safety event. A vehicle that receives a report about a safety event uses the calculated trust rating of the sender to make a decision on

whether to accept the report or not. The simulation was run in three network setups where the percentages of abnormal vehicles or vehicles with unpredictable behaviors were 20%, 50%, and 80%.

Figure 6-3 illustrates that the number of vehicles that accepted a true safety event message increases as the number of observation episodes increases. This is to be expected because the longer a vehicle communicates with another vehicle in the network, the more similarities there are between them; therefore, a better trust rating is calculated.

In the first and second networks, we can see that the average percentage of vehicles that accept a safety event message becomes steady as the number of observation episodes increases.

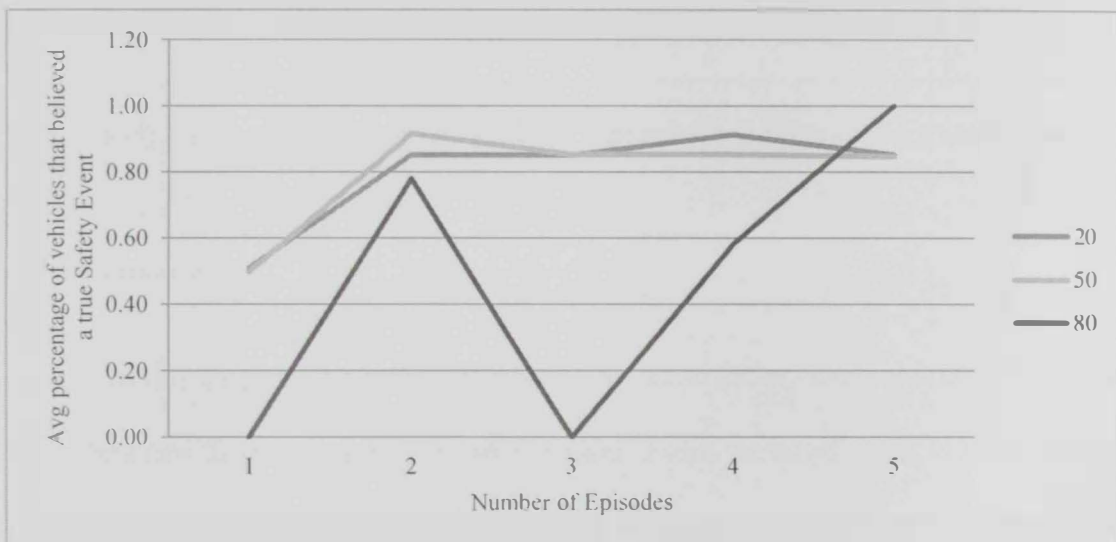


Figure 6-3: Average percentage of vehicles that accepted true safety event report

However, in the third network, the number of vehicles fluctuates. This is understandable given the fact that the majority of the network participants are abnormal vehicles; therefore, it is difficult for the normal vehicles to find similarities with their neighbors to use to establish trust relationships. Therefore, the vehicles cannot use the calculated trust rating to identify truthful safety event messages.

On the other hand, Figure 6-4 shows the number of vehicles that accepted a false safety event message using information collected from a different number of episodes. In all network simulations, the number of vehicles is zero. The simulation results show that our proposed system for using similarity to achieve trust is proof against a false data injection attack.

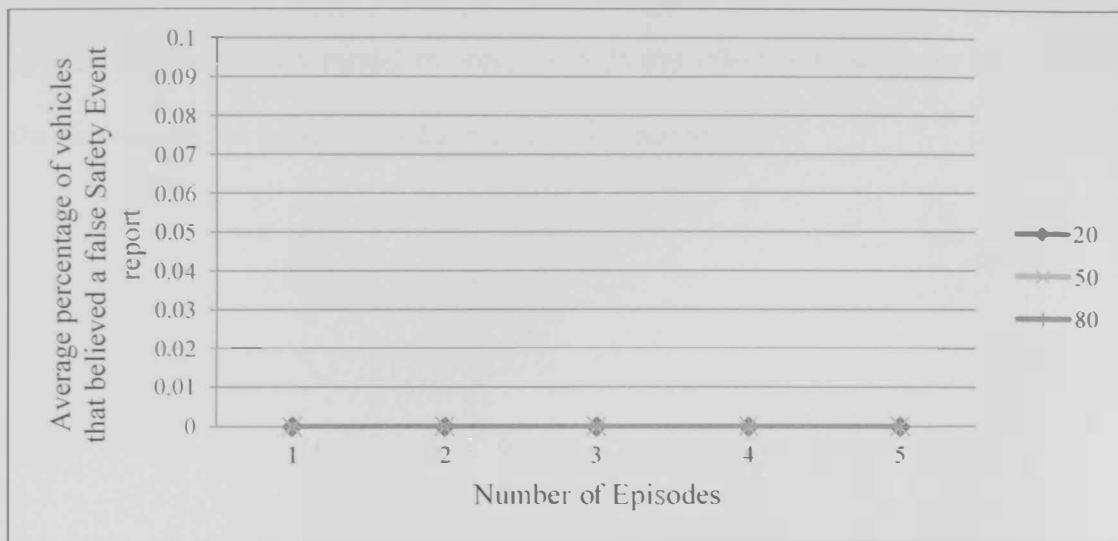


Figure 6-4: Average percentage of vehicles that accepted false safety event report

6.7 Discussion

In this chapter, we discussed penalizing an adversary that intentionally injects false data into the network for selfish purposes. From the simulation, we have shown that our protocol can be used to protect the vehicles in the network of this attack; however, our protocol does not extend the same level of protection to vehicles that are simply faulty; vehicles that unintentionally report a false safety event in the network. The trust rating of these vehicles will be affected negatively using the behavior rating. However, since trust rating is calculated over time, these vehicles will have the chance to improve their trust rating over the next episodes gradually through high similarity rating and good behavior.

6.8 Summary

Our proposed system has shown that similarity can be used to compute trust between vehicles. The generated similarity ratings are used to compute the trust ratings of the vehicles. The trust rating is updated using observations of other vehicles' behaviors in the network. Additionally, in this chapter, we designed and evaluated an adversary model in order to study the effect of trust on the accuracy of the decision in the presence of false data in the network.

Chapter 7: Conclusion

7.1 Conclusions

Every day in growing numbers, we see ubiquitous devices that are interconnected with each other and with human users. These devices collect and process information and cooperate to enhance the quality of experience for their human users. The OBUs of the vehicles are some of these devices. They use the underlying network of communications to exchange messages about the vehicle, road, weather, etc. The way these intelligent devices cooperate constantly changes; therefore, we need to adapt to these changes to conform to the new method of interaction. In this dissertation, we design and implement a trust management system for VANETs that derives trust from similarity. Shelby Foote said (Davies, 1800), "Of all the passions of mankind, the love of novelty most rules the mind." We presented the following novel contributions in this dissertation.

In Chapters 1, 2, and 3, we introduce the objectives of our work. We discuss VANETs and their applications. Next, we illustrate why VANET safety applications require trust, and then we state the problem we aim to solve in this work. We list the contributions of this dissertation and the steps we follow to achieve the listed contributions. Finally, we cover the state of the art in the areas of data mining in VANETs, trust and similarity, and VANETs safety applications requirements and examples.

In Chapter 4, we present our similarity-based trust management system. The main concept of this chapter is the use of attribute similarity as a foundation for trust in the network. We show that past interactions must be factored into the calculations

of trust ratings to achieve a better representation of the relationships between the vehicles in the network.

In Chapter 5, we set up an analytical model for studying the impact of trust on the decision-making process in VANETs. Our model actually showed that trust helps in reducing the number of messages needed for a vehicle to react to an event in the network with a low error rate. This encouraged us to further enhance our trust management system to withstand a false data injection attack.

In Chapter 6, we present our enhanced trust management system. We introduce a new parameter in the calculation of trust, which is the behavior rating. In addition, we introduce the echo protocol. The keystone of the protocol is the behavior rating that the receiving vehicle assigns to the source vehicle. We showed that the protocol is proof against false data injection attacks.

7.2 Directions for Future Work

In this work, we showed that similarity could be used to achieve trust in VANETs. In addition, we provided examples of potential uses of similarity-based trust in various VANET applications; however, we only studied the effect of trust on safety applications. This work can be extended in the following directions, such as the following:

- The attributes we used to calculate trust could be extended to suit different VANET applications. For example, the vehicle's make and model can be factored into the similarity rate calculations. Vehicles running the same brand of collision detection systems will logically assign higher trust ratings in the readings coming from these systems. The use of Estimation Similarity techniques can be explored to discover similarities using the new attributes.

- The Internet of Vehicles (IOV) is comprised of all protocols and services required by autonomous vehicles to operate efficiently and safely (Gerla, Lee, Pau, & Lee, 2014). We see a potential of enhancing the similarity-based trust with a vehicle's accessibility to neighboring vehicles sensor data.
- In our approach, we were inspired by human interactions in social network sites. We took inspiration from the way recommender systems work in these websites and attempted to apply similar approaches into classifying autonomous systems. Our venture was successful, which supports our belief that trust management systems can be enhanced using designs inspired by human behavior.
- So far, we have only studied the impact of one-hop messages on the locally calculated trust value. We have not investigated multi-hop messages or messages endorsed from trusted vehicles. Given the fact that we have adopted a social approach in the design of our trust management system, it would be interesting to study the impact of incorporating feedback from peers on the value of trust. In addition, we plan to calculate a measure for True Trust, and then compare it to Accrued Trust. We aim to estimate a more accurate value for trust.
- In this research, the threat model covered vehicles exhibiting unexpected behaviors. In the future, we would like to extend the threat model to include vehicles that maliciously try to undermine the trust system by injecting false safety messages. In addition, we plan to develop an analytical model to measure how much misbehavior our trust management can tolerate, and how much concurrent misbehavior can be tolerated by the trust management system.

- We plan to implement the trust management system for Android Auto by developing the system architecture and algorithms. Android Auto is a standard compatible with phones running Android 5.0 (Lollipop) or higher. Android Auto is compatible with many vehicles, such as: Audi, Cadillac, Nissan and many more (Google, 2015a). The main functionality of Android Auto is to extend the functionality of the mobile phone to the vehicle's dashboard's head unit. The standard offers driver's control over applications, such as: maps, navigation and web searches. This standard opens the possibility of using mobile apps to offer many functionalities; for instance, safety applications. Following the messaging design standard SAE J2735 (SAE-International, 2009), Material Design, Google's new design language (Google, 2015b) can be used to design and create an app to implement our Trust Management System modules for calculating trust ratings between vehicles, and for discovering a false data injection attack using the Echo Protocol. The motivation behind using Android Auto stems from the high penetration rate of Android devices, which means that we won't need special approvals for dedicated hardware installation in vehicles (Tornell et al., 2012). MQ Telemetry Transport (MQTT) is a lightweight messaging protocol that can be used in sensors (Light, 2015). Using the publish/subscribe model, a topic is defined as vehicle status update for beaconing. The status update will include the following: vehicle speed, vehicle position, and a timestamp. Every vehicle will serve as a server and a client for a beaconing service. The one hop neighbors make up the list of subscribers interested in vehicles' status update notifications in the network. Upon meeting, an Android service running in the vehicles will subscribe to this topic, and watch for changes.

Another topic will be SE reporting. MQTT library can be included in an Android app to allow the vehicles to connect, publish and subscribe.

Bibliography

- Al-Khassawneh, Y. A., & Salim, N. (2012). On the use of data mining techniques in vehicular ad hoc network. *Advanced Machine Learning Technologies and Applications* (pp. 449-462). Berlin Heidelberg: Springer.
- Al Falasi, H. O., & Mohamed, N. (2013). *Preference-Based Trust Rules for Group Formation in VANETs*. In proceedings of the 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation (CIMSIm).
- ASTM, E. (2003). Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Retrieved from <https://www.standards.its.dot.gov/Factsheets/Factsheet/66>
- Avižienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), 11-33.
- Caballero Gil, C., Caballero Gil, P., & Molina Gil, J. (2010). *Using groups to reduce communication overhead in vanets*. In proceedings of the the Second International Conference on Advances in P2P Systems.
- Cao, Z., Kong, J., Lee, U., Gerla, M., & Chen, Z. (2008). *Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks*. In proceedings of the INFOCOM Workshops 2008.
- Chen, C., Zhang, J., Cohen, R., & Ho, P. H. (2010a). *A trust-based message propagation and evaluation framework in vanets*. In proceedings of the Int. Conf. on Information Technology Convergence and Services.
- Chen, C., Zhang, J., Cohen, R., & Ho, P. H. (2010b). *A trust modeling framework for message propagation and evaluation in VANETs*. In proceedings of the 2010 2nd International Conference on Information Technology Convergence and Services (ITCS).
- Chen, R., Jin, W. L., & Regan, A. (2010). Broadcasting safety information in vehicular networks: issues and approaches. *Network, IEEE*, 24(1), 20-25.

- Cho, J. H., Swami, A., & Chen, I. R. (2011). A survey on trust management for mobile ad hoc networks. *Communications Surveys & Tutorials, IEEE*, 13(4), 562-583.
- Datta, S., Bhaduri, K., Giannella, C., Wolff, R., & Kargupta, H. (2006). Distributed data mining in peer-to-peer networks. *Internet Computing, IEEE*, 10(4), 18-26.
- Davies, E. (1800). *Other Men's Minds, Or, Seven Thousand Choice Extracts on History, Science, Philosophy, Religion, Etc: Selected from the Standard Authorship of Ancient and Modern Times, and Classified in Alphabetical Order*: Estes and Lauriat.
- Ding, Q., Li, X., Jiang, M., & Zhou, X. (2010). *Reputation-based trust model in vehicular ad hoc networks*. In proceedings of the 2010 International Conference on Wireless Communications and Signal Processing (WCSP).
- Domingos, P., & Hulten, G. (2003). A general framework for mining massive data streams. *Journal of Computational and Graphical Statistics*, 12(4), 945-949.
- Dötzer, F., Fischer, L., & Magiera, P. (2005). *Vars: A vehicle ad-hoc network reputation system*. In proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks.
- El Zarki, M., Mehrotra, S., Tsudik, G., & Venkatasubramanian, N. (2002). *Security issues in a future vehicular network*. In proceedings of the European Wireless.
- Enkelmann, W. (2003). *Fleetnet-applications for inter-vehicle communication*. In proceedings of IEEE Intelligent Vehicles Symposium.
- Gama, J., Medas, P., & Rodrigues, P. (2005). *Learning decision trees from dynamic data streams*. In proceedings of the 2005 ACM Symposium on Applied Computing.
- Gerla, M., Lee, E. K., Pau, G., & Lee, U. (2014). *Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds*. In proceedings of the 2014 IEEE World Forum on Internet of Things
- Gerlach, M. (2007). *Trust for vehicular applications*. In proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, 2007.

- Ghaleb, F. A., Zainal, A., & Rassam, M. A. (2015). Data Verification and Misbehavior Detection in Vehicular Ad-hoc Networks. *Jurnal Teknologi*, 73(2).
- Golab, L., & Özsu, M. T. (2003). *Data stream management issues—a survey*. Retrieved from Technical Report. Apr. 2003. db. uwaterloo. ca/~ddbms/publications/stream/streamsurvey. pdf
- Golbeck, J. (2009). Trust and nuanced profile similarity in online social networks. *ACM Transactions on the Web (TWEB)*, 3(4), 12.
- Golle, P., Greene, D., & Staddon, J. (2004). *Detecting and correcting malicious data in VANETs*. In proceedings of the 1st ACM International Workshop on Vehicular Ad hoc Networks.
- Google. (2015a). Android Auto: The right information for the road ahead. Retrieved from <https://www.android.com/auto/>
- Google. (2015b). Designing for Auto. Retrieved from <https://developer.android.com/design/auto/index.html>
- Hadim, S., Al-Jaroodi, J., & Mohamed, N. (2006). *Middleware issues and approaches for mobile ad hoc networks*. In proceedings of the IEEE Consumer Communications and Networking Conf. (CCNC 2006).
- Hao, Y., Cheng, Y., Zhou, C., & Song, W. (2011). A distributed key management framework with cooperative message authentication in VANETs. *IEEE Journal on Selected Areas in Communications*, 29(3), 616-629.
- Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE*, 46(6), 164-171.
- Hartenstein, H., & Laberteaux, K. P. (2009). *VANET vehicular applications and inter-networking technologies* (Vol. 1): John Wiley & Sons.
- Huang, Z., Ruj, S., Cavenaghi, M., & Nayak, A. (2011). *Limitations of trust management schemes in VANET and countermeasures*. In proceedings of the 2011 IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC).
- Huang, Z., Ruj, S., Cavenaghi, M. A., Stojmenovic, M., & Nayak, A. (2014). A social network approach to trust management in VANETs. *Peer-to-Peer Networking and Applications*, 7(3), 229-242.

- Jawhar, I., Mohamed, N., & Zhang, L. (2010). *Inter-vehicular communication systems, protocols and middleware* In proceedings of the 2010 IEEE Fifth International Conference on Networking, Architecture and Storage (NAS).
- Karim, R. (2008). VANET: Superior system for content distribution in vehicular network applications. *Rutgers University, Department of Computer Science, Tech Rep.*
- Krajzewicz, D., Bonert, M., & Wagner, P. (2006). The open source traffic simulation package SUMO. *RoboCup 2006 Infrastructure Simulation Competition, 1*, 1-5.
- Kumar, N., & Chilamkurti, N. (2014). Collaborative trust aware intelligent intrusion detection in VANETs. *Computers & Electrical Engineering, 40*(6), 1981-1996.
- Light, R. (2015). MQ Telemetry Transport. Retrieved from <http://mosquitto.org/man/mqtt-7.html>
- Lo, N. W., & Tsai, H. C. (2009). A reputation system for traffic safety event on vehicular ad hoc networks. *EURASIP Journal on Wireless Communications and Networking, 2009*, 9.
- Ma, S., Wolfson, O., & Lin, J. (2011). *A survey on trust management for intelligent transportation system*. In proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science.
- Mármol, F. G., & Pérez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications, 35*(3), 934-941.
- Mazilu, S., Teler, M., & Dobre, C. (2011). *Securing vehicular networks based on data-trust computation*. In proceedings of the 2011 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.
- McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual review of sociology, 415-444*.
- Minhas, U. F., Zhang, J., Tran, T., & Cohen, R. (2010). Towards expanded trust management for agents in vehicular ad-hoc networks. *International Journal of Computational Intelligence Theory and Practice, 5*(1).

- Montaner, M., López, B., & de la Rosa, J. L. (2002). Opinion-based filtering through trust. *Cooperative Information Agents VI* (pp. 164-178). Berlin Heidelberg: Springer.
- Na Nakorn, K., Yusheng, J., & Rojviboonchai, K. (2014, 18-21 May 2014). *Bloom Filter for Fixed-Size Beacon in VANET*. In proceedings of the IEEE 79th Vehicular Technology Conference (VTC Spring), 2014.
- Papadimitratos, P., Buttyan, L., Holczer, T. S., Schoch, E., Freudiger, J., Raya, M., . . . Hubaux, J. P. (2008). Secure vehicular communication systems: design and architecture. *Communications Magazine, IEEE*, 46(11), 100-109.
- Petit, J., & Mammeri, Z. (2011). *Dynamic consensus for secured vehicular ad hoc networks*. In proceedings of the 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).
- Raya, M. (2009). *Data-centric trust in ephemeral networks*. École Polytechnique Federale De Lausanne.
- Rezgui, J., & Cherkaoui, S. (2011). *Detecting faulty and malicious vehicles using rule-based communications data mining*. In proceedings of the 2011 IEEE 36th Conference on Local Computer Networks (LCN).
- RSA. (2012). Stopping distance for cars. Retrieved from http://www.rulesoftheroad.ie/rules-for-driving/speed-limits/speed-limits_stopping-distances-cars.html
- SAE-International. (2009). Dedicated Short Range Communications (DSRC) Message Set Dictionary. SAE International.
- Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2005). *CARAVAN: Providing location privacy for VANET*. Retrieved from <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA459198>
- Schmidt, R. K., Leinmüller, T., Schoch, E., Held, A., & Schäfer, G. (2008). *Vehicle behavior analysis to enhance security in vanets*. In proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008).
- Smaldone, S., Han, L., Shankar, P., & Iftode, L. (2008). *RoadSpeak: enabling voice chat on roadways using vehicular social networks*. In proceedings of the 1st Workshop on Social Network Systems.

- Su, X., & Khoshgoftaar, T. M. (2009). A survey of collaborative filtering techniques. *Advances in artificial intelligence*, 2009, 4.
- Tornell, S., Calafate, C. T., Cano, J. C., Manzoni, P., Fogue, M., & Martinez, F. J. (2012). *Implementing and testing a driving safety application for smartphones based on the eMDR protocol*. In proceedings of the IFIP Wireless Days (WD), 2012.
- Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems.
- Wang, J., Liu, Y., Liu, X., & Zhang, J. (2009). *A trust propagation scheme in VANETs*. In proceedings of the Intelligent Vehicles Symposium.
- Wang, N. W., Huang, Y. M., & Chen, W. M. (2008). A novel secure communication scheme in vehicular ad hoc networks. *Computer communications*, 31(12), 2827-2837.
- Woerndl, W., & Eigner, R. (2007). *Collaborative, context-aware applications for inter-networked cars*. In proceedings of the 16th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2007.
- Wolff, R., & Schuster, A. (2004). Association rule mining in peer-to-peer systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 34(6), 2426-2438.
- Worndl, W., Brocco, M., & Eigner, R. (2008). *A Context-Aware Gas Station Recommender System for Vehicular Ad-Hoc Networks*. In proceedings of the Conference on Wireless Applications and Computing Conference, Amsterdam, Netherlands.
- Wu, X., Kumar, V., Quinlan, J. R., Ghosh, J., Yang, Q., Motoda, H., . . . Philip, S. Y. (2008). Top 10 algorithms in data mining. *Knowledge and Information Systems*, 14(1), 1-37.
- Xiang, R., Neville, J., & Rogati, M. (2010). *Modeling relationship strength in online social networks*. In proceedings of the 19th International Conference on World Wide Web.
- Xu, Q., Mak, T., Ko, J., & Sengupta, R. (2004). *Vehicle-to-vehicle safety messaging in DSRC*. In proceedings of the 1st ACM international workshop on Vehicular ad hoc networks.

- Yang, N. (2013). A Similarity based Trust and Reputation Management Framework for VANETs. *International Journal of Future Generation Communication and Networking*, 6(2), 25-34.
- Yang, X., Liu, J., Vaidya, N. H., & Zhao, F. (2004). *A vehicle-to-vehicle communication protocol for cooperative collision warning*. In proceedings of the Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on.
- Zaidi, K., Milojevic, M., Rakocevic, V., & Rajarajan, M. (2014). *Data-centric Rogue Node Detection in VANETs*. In proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).
- Zhang, J. (2011). *A survey on trust management for vanets*. In proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA).
- Zhang, J., Xu, J., Zhu, C., Wang, W., & Liao, S. S. (2010). *Constructing summarizations for V2V traffic data based on sampling methods*. In proceedings of the Vehicular Networking Conference (VNC).
- Zhang, L., Wu, Q., Solanas, A., & Domingo Ferrer, J. (2010). A scalable robust authentication protocol for secure vehicular communications. *IEEE Transactions on vehicular Technology*, 59(4), 1606-1617.
- Ziegler, C. N., & Golbeck, J. (2007). Investigating interactions of trust and interest similarity. *Decision support systems*, 43(2), 460-475.

List of Publications

- Al Falasi, H., & Zhang, L. (2011, March). Modeling and Justification of the Store and Forward Protocol: Covert Channel Analysis. In the Proceedings of the 6th International Conference on Information Warfare and Security (p. 8).
- Al Falasi, H., & Barka, E. (2011, April). Revocation in VANETs: A survey. In 2011 International Conference on Innovations in Information Technology (IIT), (pp. 214-219).
- Al Falasi, H., & Mohamed, N. (2013, April). The impact of trust on vehicular applications. In 2013 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), (pp. 1-4).
- Al Falasi, H., & Mohamed, N. (2013, September). Preference-Based Trust Rules for Group Formation in VANETs. In 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation (CIMSIm), (pp. 333-338).
- Al Falasi, H., Masud, M. M., & Mohamed, N. (2015, June). Trusting the same: Using similarity to establish trust among vehicles. In International Conference on Collaboration Technologies and Systems (CTS), 2015 (pp. 64-69).
- Al Falasi, H., El-Syed, H., & Mohamed, N. (2015, November). Similarity-based Trust Management System: Data Validation Scheme. In Hybrid Intelligent Systems (HIS), 2015.
- Al Falasi, H., & Mohamed, N. (2015, December). Similarity-based Trust Management System for Detecting Fake Safety Messages in VANETs. In the International Conference on Internet of Vehicles (IOV), 2015.

Appendix

SUMO Networks

Percentage of abnormal vehicles = 0%

Nodes

```
<nodes>
<nodeid="1"x="-1000.0"y="+1000.0"/>
<nodeid="2"x="+1000.0"y="+1000.0"/>
<nodeid="3"x="+4000.0"y="+1000.0"/>
</nodes>
```

Edges

```
<edges>
<edgefrom="1" id="12"to="2" type="a"/>
<edgefrom="2" id="23"to="3" type="a"/>
</edges>
```

Routes

```
<routes>
<vTypeDistributionid="typedist">
<vTypeid="type1" accel="1.0" decel="3.0" length="5.0" maxspeed="33.3" probability="1.0" color="0,1,0" sigma="0"/>
<vTypeid="type2" accel="9.0" decel="7.0" length="5.0" maxspeed="66.6" probability="0.0" color="1,0,0" sigma="1"/>
</vTypeDistribution>
<routeDistributionid="routedist1">
<routeid="route0" edges="12 23" probability="1"/>
</routeDistribution>
<vehicledespart="0" id="0" route="routedist1" type="typedist"/>
<vehicledespart="0" id="1" route="routedist1" type="typedist"/>
<vehicledespart="0" id="2" route="routedist1" type="typedist"/>
<vehicledespart="0" id="3" route="routedist1" type="typedist"/>
<vehicledespart="0" id="4" route="routedist1" type="typedist"/>
<vehicledespart="0" id="5" route="routedist1" type="typedist"/>
<vehicledespart="0" id="6" route="routedist1" type="typedist"/>
<vehicledespart="0" id="7" route="routedist1" type="typedist"/>
<vehicledespart="0" id="8" route="routedist1" type="typedist"/>
<vehicledespart="0" id="9" route="routedist1" type="typedist"/>
<vehicledespart="0" id="10" route="routedist1" type="typedist"/>
<vehicledespart="0" id="11" route="routedist1" type="typedist"/>
<vehicledespart="0" id="12" route="routedist1" type="typedist"/>
<vehicledespart="0" id="13" route="routedist1" type="typedist"/>
<vehicledespart="0" id="14" route="routedist1" type="typedist"/>
<vehicledespart="0" id="15" route="routedist1" type="typedist"/>
<vehicledespart="0" id="16" route="routedist1" type="typedist"/>
```



```

<vehicleddepart="0" id="77" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="78" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="79" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="80" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="81" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="82" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="83" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="84" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="85" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="86" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="87" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="88" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="89" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="90" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="91" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="92" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="93" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="94" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="95" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="96" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="97" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="98" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="99" route="routedist1" type="typedist"/>
</routes>

```

Percentage of abnormal vehicles = 20%

Nodes

```

<nodes>
<nodeid="1"x="-1000.0"y="+1000.0"/>
<nodeid="2"x="+1000.0"y="+1000.0"/>
<nodeid="3"x="+4000.0"y="+1000.0"/>
</nodes>

```

Edges

```

<edges>
<edgefrom="1" id="12" to="2" type="a"/>
<edgefrom="2" id="23" to="3" type="a"/>
</edges>

```

Routes

```

<routes>
<vTypeDistributionid="typedist">
<vTypeid="type1" accel="1.0" decel="3.0" length="5.0" maxspeed="33.3" probability="0.8" color="0,1,0" sigma="0"/>
<vTypeid="type2" accel="9.0" decel="7.0" length="5.0" maxspeed="66.6" probability="0.2" color="1,0,0" sigma="1"/>
</vTypeDistribution>
<routeDistributionid="routedist1">

```


Edges

```
<edges>
<edgefrom="1" id="12" to="2" type="a"/>
<edgefrom="2" id="23" to="3" type="a"/>
</edges>
```

Routes

```
<routes>
<vTypeDistribution id="typedist">
<vTypeid="type1" accel="1.0" decel="3.0" length="5.0" maxspeed="33.3" probability="0.5" color="0,1,0" sigma="0"/>
<vTypeid="type2" accel="9.0" decel="7.0" length="5.0" maxspeed="66.6" probability="0.5" color="1,0,0" sigma="1"/>
</vTypeDistribution>
<routeDistribution id="routedist1">
<routeid="route0" edges="12 23" probability="1"/>
</routeDistribution>
<vehicledespart="0" id="0" route="routedist1" type="typedist"/>
<vehicledespart="0" id="1" route="routedist1" type="typedist"/>
<vehicledespart="0" id="2" route="routedist1" type="typedist"/>
<vehicledespart="0" id="3" route="routedist1" type="typedist"/>
<vehicledespart="0" id="4" route="routedist1" type="typedist"/>
<vehicledespart="0" id="5" route="routedist1" type="typedist"/>
<vehicledespart="0" id="6" route="routedist1" type="typedist"/>
<vehicledespart="0" id="7" route="routedist1" type="typedist"/>
<vehicledespart="0" id="8" route="routedist1" type="typedist"/>
<vehicledespart="0" id="9" route="routedist1" type="typedist"/>
<vehicledespart="0" id="10" route="routedist1" type="typedist"/>
<vehicledespart="0" id="11" route="routedist1" type="typedist"/>
<vehicledespart="0" id="12" route="routedist1" type="typedist"/>
<vehicledespart="0" id="13" route="routedist1" type="typedist"/>
<vehicledespart="0" id="14" route="routedist1" type="typedist"/>
<vehicledespart="0" id="15" route="routedist1" type="typedist"/>
<vehicledespart="0" id="16" route="routedist1" type="typedist"/>
<vehicledespart="0" id="17" route="routedist1" type="typedist"/>
<vehicledespart="0" id="18" route="routedist1" type="typedist"/>
<vehicledespart="0" id="19" route="routedist1" type="typedist"/>
<vehicledespart="0" id="20" route="routedist1" type="typedist"/>
<vehicledespart="0" id="21" route="routedist1" type="typedist"/>
<vehicledespart="0" id="22" route="routedist1" type="typedist"/>
<vehicledespart="0" id="23" route="routedist1" type="typedist"/>
<vehicledespart="0" id="24" route="routedist1" type="typedist"/>
<vehicledespart="0" id="25" route="routedist1" type="typedist"/>
<vehicledespart="0" id="26" route="routedist1" type="typedist"/>
<vehicledespart="0" id="27" route="routedist1" type="typedist"/>
<vehicledespart="0" id="28" route="routedist1" type="typedist"/>
<vehicledespart="0" id="29" route="routedist1" type="typedist"/>
<vehicledespart="0" id="30" route="routedist1" type="typedist"/>
<vehicledespart="0" id="31" route="routedist1" type="typedist"/>
<vehicledespart="0" id="32" route="routedist1" type="typedist"/>
<vehicledespart="0" id="33" route="routedist1" type="typedist"/>
<vehicledespart="0" id="34" route="routedist1" type="typedist"/>
<vehicledespart="0" id="35" route="routedist1" type="typedist"/>
<vehicledespart="0" id="36" route="routedist1" type="typedist"/>
<vehicledespart="0" id="37" route="routedist1" type="typedist"/>
<vehicledespart="0" id="38" route="routedist1" type="typedist"/>
```



```
<vehicleddepart="0" id="99" route="routedist1" type="typedist"/>
</routes>
```

Percentage of abnormal vehicles = 80%

Nodes

```
<nodes>
<nodeid="1"x="-1000.0"y="+1000.0"/>
<nodeid="2"x="+1000.0"y="+1000.0"/>
<nodeid="3"x="+4000.0"y="+1000.0"/>
</nodes>
```

Edges

```
<edges>
<edgefrom="1" id="12" to="2" type="a"/>
<edgefrom="2" id="23" to="3" type="a"/>
</edges>
```

Routes

```
<routes>
<vTypeDistributionid="typedist">
<vTypeid="type1" accel="1.0" decel="3.0" length="5.0" maxspeed="33.3" probability="0.2" color="0,1,0" sigma="0"/>
<vTypeid="type2" accel="9.0" decel="7.0" length="5.0" maxspeed="66.6" probability="0.8" color="1,0,0" sigma="1"/>
</vTypeDistribution>
<routeDistributionid="routedist1">
<routeid="route0" edges="12 23" probability="1"/>
</routeDistribution>
<vehicleddepart="0" id="0" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="1" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="2" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="3" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="4" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="5" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="6" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="7" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="8" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="9" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="10" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="11" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="12" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="13" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="14" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="15" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="16" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="17" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="18" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="19" route="routedist1" type="typedist"/>
```



```
<vehicleddepart="0" id="80" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="81" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="82" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="83" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="84" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="85" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="86" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="87" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="88" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="89" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="90" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="91" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="92" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="93" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="94" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="95" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="96" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="97" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="98" route="routedist1" type="typedist"/>
<vehicleddepart="0" id="99" route="routedist1" type="typedist"/>
</routes>
```