Analysis of Cyber Risk and Associated Concentration of Research (ACR)^2 in the Security of Vehicular Edge Clouds

Y. Lu[1], C. Maple[1], T. Sheik[1], H. Alhagagi[1], T. Watson[1], M.Dianati[1], A. Mouzakitis[2]
WMG, University of Warwick, Coventry, UK.
[2]Jaguar Land Rover
{y.lu.16, cm, t.sheik, h.alhagagi.1, tm, m.dianati}@warwick.ac.uk, amouzak1@jaguarlandrover.com

Keywords: Intelligent Transportation Systems, cyber security, cyber risks, threat analysis, Vehicular Edge Cloud computing, vehicular ad-hoc networks

Abstract

Intelligent Transportation Systems (ITS) is a rapidly growing research space with many issues and challenges. One of the major concerns is to successfully integrate connected technologies, such as cloud infrastructure and edge cloud, into ITS. Security has been identified as one of the greatest challenges for the ITS and security measures require consideration from design to implementation. This work focuses on the cyber risk analysis and associated concentration of research (ACR^2). The introduction of ACR^2 approach can be used to consider research challenges in VEC and open up further investigation into those threats that are important but under-researched (e.g. very high/high risk level but less research concentration). In this way, this research can lay the foundations for the development of appropriate countermeasures for the future of ITS.

1 Introduction

Intelligent Transportation Systems (ITS) can be defined as systems that aim to apply intelligent technologies in the field of road transport [1]. Such systems can provide an effective way to manage traffic and reduce the number of accidents. Many techniques have been developed to serve ITS, often taking advantage of cloud computing [2]. However, cloud computing is known to suffer from a variety of communication performance issues, particularly with mobile systems, which can affect the efficacy of vehicular networks. For this reason, edge computing, as a new emerging technology, is being widely considered for ITS. The authors in [3] provide a three-tier distributed computing architecture for a vehicular system which includes vehicles, the edge cloud, and the core cloud. This is an architecture that combines various types of network, such as vehicular ad-hoc networks (VANETs), mobile ad-hoc networks (MANETs) and wireless sensor networks, utilising cloud and edge cloud computing techniques. Due to the high complexity and multi-level connectivity of such a hybrid architecture, a wide range of security issues may be introduced.

To date, there have been lots of research focused on security standards and analysis of ITS to improve the road safety. In the United States, IEEE proposed several protocol and standards for enabling future ITS applications and addressing security issues, for example [4]. In Europe, the Europe Telecommunications Standards Institute (ETSI) focus on a global standard for cooperative ITS systems, including defines the overall communication architectures [5], like vehicle-to-vehicle (V2V) communication, vehicle-to-infrastructure (V2I) communication and vehicle-to-anything (V2X) communication, specifies mechanism for secure communications in ITS [6], threat and risk analysis [7], security services and architectures [8], and so on. In addition, the research on cyber threats analysis, issues, challenges for VANETs, cloud computing and in-vehicles networks have been discussed in detail in various research papers [9], [10], [11]. However, the related work in edge cloud is limited. For this reason, this work will concentrate effort on the vehicular edge cloud (VEC).

This paper will contribute the following: Firstly, the threats in VEC will be analysed from three aspects: the communication between the vehicle and edge cloud, including vehicle-to-edge (V2E) communication and edge-to-vehicle (E2V) communication; the communication between vehicles (V2V); and the in-vehicle network. Secondly, a VEC threat matrix, the Analysis of Cyber Risk and Associated Concentration of Research (ACR^2), is proposed which includes five characteristics:

- Attack Name: a descriptive name identifying the threat.
- Asset: the description of assets of the system impacted (e.g. components, data, services).
- Impact on security requirement: the related security conditions it compromises.
- A list of work addressing the issue: providing the related references.
- Research Concentration (indicating the volume of research to importance): identification of which attacks need further investigation.

Identification of research on the attacks has been undertaken by searching for, and reviewing, peer-reviewed journal and conference papers and project reports, as well as soliciting expert opinion. As far as we are aware, there is only small amount of work in the area of investigating the threats in VEC and no existing threat analysis work has considered ACR[2].

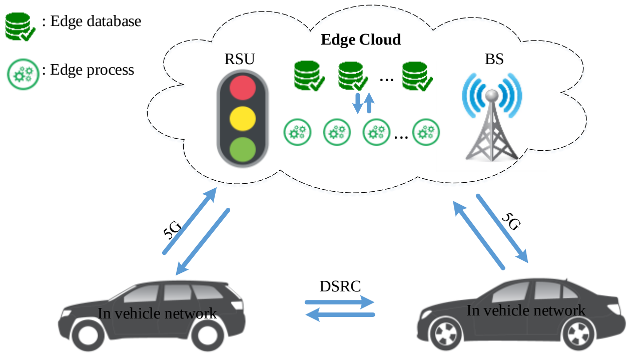
The remainder of this paper is organized as follows. The main architecture of the VEC framework and the subsystems is given in Section 2. The attack surfaces are identified for the VEC system in Section 3 In Section 4, the detailed attack analysis for the proposed VEC system is presented. Finally, the paper is concluded in Section 5.

2 Vehicular Edge Cloud Framework Architecture

Figure 1 illustrates the basic architecture of VEC. as mentioned in cloud computing, the high latency is one of the important issues exists in the cloud computing. To overcome this, one of the potential solutions is mobile edge computing, also known as fog computing. Here the edge cloud used in the ITS system is considered as VEC. It used to complement the core cloud's capacity for decentralising the concentration of computing resources in data centres, provide more local data and resources. It also provides storage and application services to the road users such as the core cloud, but stands out by achieving low latency delay, fast response time, mobility support, location awareness, high availability and scalability and improves quality of service for streaming real-time applications. VEC allows applications to run as close as possible to the end users in a mobile environment, it also helps the autonomous vehicle offload resource-consuming operations and runs applications on multiple platforms. VEC can be located physically close or within an RSU or can be located as mobile edge computing within the 4G/LTE-A/5G base stations.

The security of this system can be considered from the following aspects: the communication between the vehicle and the edge cloud, including vehicle-to-edge (V2E) and edge-to-vehicle (E2V), the communication between vehicles (V2V), and the in-vehicle network, each will be described in detail:

Communication between vehicles and edge cloud (V2E and E2V): V-E interface allows the communications between vehicles and edge cloud. It used to generate a reliable and low-latency communication between vehicle and edge could. Here we consider that the communication between vehicles and edge is over 5G.
V2V: This is a communication designed to transmit information (speed, location, the direction of travel, braking etc.) between vehicles in real-time. V2V technology uses dedicated short-range communications (DSRC). When considering V2V communication, there are three main devices must be mentioned: On Board Units (OBUs) which helps in V2V communication; Sensor network which checks the conditions around; Finally, the Trusted Platform Module (TPM) which is used to generate cryptographic keys to strong sensitive information. An attacker can damage or destroy this system by attacking any of these devices.



DSRC: Dedicated Short Range Communications
RSU: Road Side Unit
BS: Base Station

Figure 1: The architecture of the VEC.

Table 1: Safety Model

Security Aspect	Description
Confidentiality	VEC system should ensure that only authorized users can access information.
Integrity	VEC system should ensure data is accurate and avoid unauthorized modification.
Authenticity	VEC system should be able to verify identity to ensure that a message, transaction or exchange of information is from the source it claims to be from.
Availability	VEC system should ensure that resources are readily accessible to the authorized reviewer at all times.
Privacy	All sensitive message in the VEC should be protected. For example, identities of the drivers, vehicle locations, etc.

In-vehicle network: The in-vehicle network can be divided into four sub-systems which are Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented System Transport (MOST), Byteflight, and FlexPay. These subsystems can be connected via Electronic Control Unit (ECU). The security in this area face lots of challenges, such as ECU has limited processing power and memory; new countermeasures should be more cost effective and so on.

For such a hybrid framework, security and safety must be considered. CIA is a simple but widely-applicable model designed to guide policies for information security within most organizations. CIA standing for Confidentiality, Integrity and Availability. Later, Donn B. Parker proposed a new model for information security called Parkerian Hexad. It adds three additional attributes to the CIA trial which are

Possession/ Control, Authenticity and Utility. These attributes are applicable across the whole subject of security analysis, if anyone has been breached, it will result in a serious safety concern.

To identify a complete, currently relevant list of security requirements, an analysis of the ITS with regard to essential foundation security attributes has been conducted and this analysis is summarized in Table1.

3 ACR^2

VEC system and its applications are susceptible to several kinds of threats, as the system heavily relies on wireless communications and the threats can affect its functioning which leads to safety concern (accident/collision). The main VEC system attacks are related to the security requirements mentioned in Table 1. This section explores in detail about the main attacks, their security attributes, and the impact to the system by reviewing and analysing most of the related attacks in ITS, VANET, modern vehicle, RSU, edge/fog cloud and core cloud. The research reviewed many academic publications and industry project reports such as ETSI-TVRA [12], EVITA[13], SeVeCom [14], PRESERVE [15]. Most of attacks were reviewed and validated by previous industry and academic projects, which helps to join all these attacks and subsume to a joined risk situation for such a system. In addition, more VEC related attacks can be explored while developing the real VEC system.

To foster discussion of the ACR^2, the risk from the attack's hazard should be determined by estimating the potential severity of the attack, and the likelihood that attack will occur.
In this work, three levels have been used, which are: Low (L), Medium (M) and High (H). Table 2-4 give the likelihood, the consequence and the risk level definitions. Moreover, the total number of related references has been divided into three level: 0 ~ 5, Low Concentration, 6 ~ 15, Medium Concentration, above 15, High Concentration. The probability assigned for each risk and concentration level is 1 for High, 0.5 for Medium, 0.1 for Low. Then the ACR^2 is defined as:

$$\text{ACR}^2 = \frac{\text{Probability of Risk Level (PRL)}}{\text{Probability of Concentration of Research (PCR)}}.$$

Table 5 gives the all possible values of ACR^2. Firstly, when ACR^2 = 1, the risk of the attack and associated concentration of research is considered as balanced. For example, a high risk level attack also gains more research of concentration. Secondly, when PRL > PCR, ACR^2 > 1, the attacks which are under this case is considered as under-researched. The larger the value of ACR^2, more research concentration needed. Finally, PRL < PCR, ACR^2 < 1, in this case, the attack is considered as well-researched.

Table 2: Definition of Likelihood

High	Attack is easy to perform, with highly motivated and sufficiently capable
Medium	Attack is feasible with motivated and capable
Low	Attack lacks motivation or capability

Table 3: Definition of Consequence

High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Table 4: Risk Level Definition

Consequence Likelihood	Low	Medium	High
Low	Low	Low	Low
Medium	Low	Medium	Medium
High	Low	Medium	High

Table 5: ACR^2

PRL PCR	0.1	0.5	1
0.1	1	5	10
0.5	0.2	1	2
1	0.1	0.5	1

By searching, reviewing peer-reviewed journal and conference papers and project reports since 2000 including both reviewed and mitigation technique papers, as well as soliciting expert opinion, Table 6 is established. Here, Table 6 is not considered as exhaustive, but it can raising awareness of the security issues in the further VEC.

Table 6 shows the full attack matrix for VEC, includes V2E, E2V and V2V communication networks, in- vehicles, and in edge cloud. The selected attacks will be described below.

A. V2E, E2V and V2V communication networks

Man-in-the-middle: As its name implies, the attacker is inserted between the transmitter and the receiver, for example, as an OBU or RSU inserts between two communicating vehicles to introduces or inject false message or modified the original message.

Table 5: Attack matrix for VEC.

Asset		ID	Attack Name	Security Requirement	Likelihood	Consequence	Risk	Related Work	Research Concentration
V2E, E2V and V2V Communications Networks (DSRC LTE/5G)		C1	Man-in-the-Middle	Integrity Authenticity	M	H	M	[16] , [17], [18], [19], [20], [21] [22], [23]	M
		C2	Sybil	Availbility Authenticity	M	M	M	[24], [25], [26], [27], [28], [29], [18], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40]	H
		C3	Jamming	Availbility	H	H	H	[41, 42] [43], [13], [44], [12], [45], [46], [47], [22], [38]	M
		C4	Flooding	Availbility	H	H	H	[48], [49], [50], [51], [52], [53]	M
		C5	Timing attack	Availbility Authenticity	H	H	H	[54], [55], [56]	L
		C6	Black hole	Availbility	H	M	M	[57], [58], [59], [60], [61], [62], [63], [64], [65], [18], [66, 67], [46] , [68], [69], [70, 71], [72], [22], [73], [74], [75], [76], [77]	H
		C7	GPS Spoofing	Authenticity	H	H	H	[78], [79], [80, 81], [82], [83, 84], [18], [85], [86]	M
		C8	Replay attack	Authenticity Integrity	M	M	M	[87], [88], [89], [90]	L
		C9	Illusion attack	Integrity	M	H	M	[91], [18], [92], [93], [94], [56], [95], [96]	M
In-vehicle networks	OBU	D1	Inject malware	Availability	M	H	M	[18], [97], [46], [98],	L
	ECM	D2	Spoofing	Authenticity	L	H	M	[99]	L
	EBCM	D3	Privilege escalation	Integrity	M	H	M	[99]	L
	Key Fob	D4	Spoofing	Authenticity	H	M	M	[100], [101], [99]	L

	Keyless entry system	D5	Relay attack	Authenticity Integrity	M	M	M	[102], [103], [104], [99]	L
	In-vehicle sensors	D6	Eavesdropping CAN bus	Confidentiality	M	M	M	[105], [106], [85], [107], [108]	L
		D7	Inject CAN message	Integrity	M	M	M	[109], [110], [111], [85]	L
Edge Clod	Edge Data Centre	E1	Physical damage	Integrity	M	L	L	[23], [112]	L
		E2	Rogue component (data centre)	Integrity	M	H	M	[113], [114], [23], [115]	L
		E3	Privacy leakage	Privacy	M	H	M	[116], [117], [118], [114], [115], [23]	M
		E4	Privilege escalation	Integrity	M	H	M	[119], [120], [121], [23]	L

Table Notes: H: High; M: Medium; L: Low; ECM: Engine Control Module; EBCM: Electronic Brake Control Module.

Sybil attack: This kind of attack aims to jam the networks by introducing false nodes identities. Thus, the legitimate vehicles determine that the false message is sent from other legitimate vehicles and cannot detect the real identities of the attacker.

Jamming attack: This attack is realized at the physical layer, the attacker inserts noisy signal with a high frequency in order to disrupt the communication channel.

Flooding attack: The attacker aims to flood the network with a huge volume of dummy messages which can be generated by malicious nodes.

Timing attack: For the ITS, time plays an important role, since the delay in safety message transmission may cause major accidents. In this attack, the attacker does not need to intercept or modify the message instead adds some time slots to delay the message transmission.

Black hole attack: The black hole attack is widely existing in any kind of as hoc network. In this kind of attack, the malicious node indicates that it is part of the networks which leads to redirecting the message to the node which does not exist cause a data loss.

GPS spoofing: Position information is crucial importance in the ITS system. GPS spoofing aims to provide the false location information to neighbour vehicles. It can be achieved using a transmitter to generate localization signals stronger than those real signals generated by.GPS satellites.
Replay attack: This kind of attack aims to replay a previously transmitted message. For example, to manipulate the vehicle locations.

Illusion attack: The adversary broadcasts the traffic warning message which produces illusion to vehicles at their neighborhood.

B. In-vehicle Devices

Inject malware on OBU: viruses can cause serious disruption in the normal vehicle’s operations. It can be executed by an adversary on OBU via physical access.

EBCM, elevation of privileges: A person with physical access to the vehicle installs a custom device to the on board diagnostics II port. The device can run a program which can monitor vehicle parameters and execute the control service to EBCM. It can prevent the use of brakes.

ECM spoofing: ECM can be spoofed results in erratic behaviour outside of normal parameters.

C. Edge Cloud (Edge Data Centre)

Physical damage: For examples fog nodes that are managed by small businesses and user devices forming clusters. In this case, the attacker to be in the vicinity of the device in order to destroy it. However, there is a very high probability that this kind of attack will be witnessed by various observers. Moreover, the impact of this particular attack is limited to a local scope: only the services associated with a particular geographical location will be disabled.

Privacy leakage: The flow of information that traverses the edge data center can be accessed by both internal adversaries and someone who is honest but curious. The edge cloud data centre normally used to stores and processes information from the entities that are located at its vicinity. However, this also provides an opportunity to extract more sensitive user information.

Privilege escalation: The considerable attack surface of these edge data centers allows external adversaries to try to take control of its services. The edge data centers can be managed by professionals with limited security training, or even

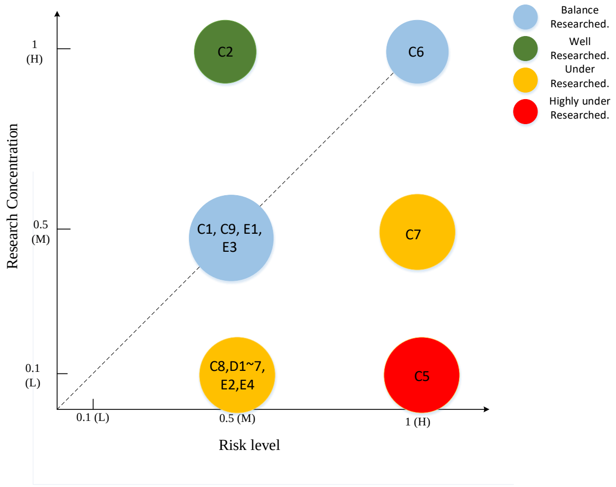


Figure 2: Research concentration versus risk level.

hobbyists. These infrastructures might be misconfigured, or lack proper maintenance.

Figure 2 illustrates the research concentration versus the risk level. It indicates that the potential attacks in communication networks have been balanced researched or well researched except GPS spoofing attack, replay attack and the timing attack. Especially for the timing attack, it has a high risk level but highly under researched. The potential in-vehicle networks attacks we considered in this work are all under researched. In addition, the potential attacks in edge cloud also under researched except privacy leakage which is balanced researched.

4 Conclusions

Security is one of the greatest challenges for any systems, especially for the ITS. Thus, for this rapidly developing area, respective security measures need consideration in advance. In this paper, an attack matrix has been proposed which used to analysis the cyber risks and associated concentration of research. The authors believe that this paper would provide a threat landscape for such hybrid vehicular system.

The results indicated that the selected in-vehicle networks attacks are all under researched. With the development of the VEC, the edge cloud plays an important role, and should be given more research concentration in the future investigation.

Acknowledgements

This work is done as a part of the Cloud Assisted Real-Time Methods for Autonomy (CARMA) project sponsored by EPSRC and Jaguar Land Rover.

References

[1] "DIRECTIVE 2010/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 July 2010," *Official Journal of the European Union*, 2010.

[2] S. Bitam and A. Mellouk, "Its-cloud: Cloud computing for intelligent transportation system," in *Global Communications Conference (GLOBECOM), 2012 IEEE*, 2012, pp. 2054-2059.

[3] K. Katsaros, A. Stevens, M. Dianati, C. Han, McCullough, A. Mouzakitis, *et al.*, *Cooperative automation through the cloud: The CARMA project*, 2017.

[4] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," *IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006)*, pp. 1-203, 2007.

[5] ETSI, "Intelligent Transport Systems (ITS); Communications Architecture," 2010.

[6] ETSI, "Intelligent Transport Systems (ITS); Security; Security Services and Architecture," 2010.

[7] ETSI, "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)," 2010.

[8] ETSI, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," 2012.

[9] D. Shukla, A. Vaibhav, S. Das, and P. Johri, "Security and attack analysis for vehicular ad hoc network—A survey," in *Computing, Communication and Automation (ICCCA), 2016 International Conference on*, 2016, pp. 625-630.

[10] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, 2011, pp. 528-533.

[11] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy*, vol. 2, pp. 155-184, 2017.

[12] ETSI, "INTELLIGENT TRANSPORT SYSTEMS (ITS); SECURITY, THREAT, VULNERABILITY AND RISK ANALYSIS (TVRA)," ed, 2010.

[13] D. W. Alastair Ruddle, etc, "Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios," Technique Report2009.

[14] A. K. Rainer Kroh, Frank Kargl, "SEVECOM, Deliverable 1.1: VANETS Security Requirements Final Version," Technique Report2006.

[15] F. K. Jan Peter Stotz, etc, "PREparing SEcuRe VEhicle-to-X Communication Systems, Deliverable 1.1:Security Requirements of Vehicle Security Architecture," Technique Report2011.

[16] P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Transactions on Software Engineering*, vol. 37, pp. 371-386, 2011.

[17] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, 2011, pp. 1110-1115.

[18] M. S. Al-Kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," in *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, 2012, pp. 1-9.

[19] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, pp. 284-294, 2013.

[20] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Network*, vol. 27, pp. 48-55, 2013.

[21] N. Varshney, T. Roy, and N. Chaudhary, "Security protocol for VANET by using digital certification to provide security with low bandwidth," in *2014 International Conference on Communication and Signal Processing*, 2014, pp. 768-772.

[22] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, pp. 380-423, 2015.

[23] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680-698, 2018.

[24] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006, pp. 1-8.

[25] M. Wolf and P. Daly, *Security engineering for vehicular IT systems*: Springer, 2009.

[26] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support," in *MILCOM 2009 - 2009 IEEE Military Communications Conference*, 2009, pp. 1-7.

[27] Q. Wu, J. Domingo-Ferrer, and G.-N. Ú, "Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 559-573, 2010.

[28] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP : Sybil Attacks Detection in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 582-594, 2011.

[29] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 616-629, 2011.

[30] B. Triki, S. Rekhis, M. Chammem, and N. Boudriga, "A privacy preserving solution for the protection against sybil attacks in vehicular ad hoc networks," in *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*, 2013, pp. 1-8.

[31] J. Grover, V. Laxmi, and M. S. Gaur, "Sybil attack detection in VANET using neighbouring vehicles," *International Journal of Security and Networks*, vol. 9, pp. 222-233, 2014.

[32] R. Hussain and H. Oh, "On secure and privacy-aware sybil attack detection in vehicular communications," *Wireless personal communications*, vol. 77, pp. 2649-2673, 2014.

[33] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1-13, 2014.

[34] P. V. Kumar and M. Maheshwari, "Prevention of Sybil attack and priority batch verification in VANETs," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, 2014, pp. 1-5.

[35] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, pp. 1103-1114, 2012.

[36] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in manets," *IEEE systems journal*, vol. 7, pp. 236-248, 2013.

[37] D. Shrivastava and A. Pandey, "A Study of Sybil and Temporal Attacks in Vehicular Ad Hoc Networks: Types, Challenges, and Impacts," *International Journal of Computer Applications Technology and Research*, vol. 3, pp. 284-291, 2014.

[38] A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, "A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)," in *Computing, Communication & Automation (ICCCA), 2015 International Conference on*, 2015, pp. 414-419.

[39] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325-344, 2014.

[40] M. T. Garip, P. H. Kim, P. Reiher, and M. Gerla, "INTERLOC: An interference-aware RSSI-based localization and sybil attack detection mechanism for vehicular ad hoc networks," in *Consumer Communications & Networking Conference (CCNC), 2017 14th IEEE Annual*, 2017, pp. 1-6.

[41] J. J. Blum, A. Eskandarian, and L. J. Hoffman, "Challenges of intervehicle ad hoc networks," *IEEE transactions on intelligent transportation systems*, vol. 5, pp. 347-351, 2004.

[42] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications,* vol. 13, 2006.

[43] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEE Wireless Commun.,* vol. 14, pp. 84-94, 2007.

[44] A. Hamieh, J. Ben-Othman, and L. Mokdad, "Detection of radio interference attacks in VANET," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1-5.

[45] I. A. Sumra, I. Ahmad, and H. Hasbullah, "Classes of attacks in VANET," in *Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International*, 2011, pp. 1-5.

[46] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems,* vol. 50, pp. 217-241, 2012.

[47] S. O. Tengstrand, K. Fors, P. Stenumgaard, and K. Wiklundh, "Jamming and interference vulnerability of IEEE 802.11 p," in *Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, 2014, pp. 533-538.

[48] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet computing,* vol. 10, pp. 82-89, 2006.

[49] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," *IEEE Transactions on Wireless Communications,* vol. 8, pp. 1974-1983, 2009.

[50] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)," in *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*, 2013, pp. 237-240.

[51] K. Verma, H. Hasbullah, and A. Kumar, "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," in *2013 3rd IEEE International Advance Computing Conference (IACC)*, 2013, pp. 550-555.

[52] K. Verma, H. Hasbullah, and A. Kumar, "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," in *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, 2013, pp. 550-555.

[53] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks," *IEEE Communications letters,* vol. 18, pp. 110-113, 2014.

[54] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Communications,* vol. 4, pp. 894-903, 2010.

[55] I. A. Sumra, J.-L. Ab Manan, and H. Hasbullah, "Timing attack in vehicular network," in *Proceedings of the 15th WSEAS International Conference on Computers, World Scientific and Engineering Academy and Society (WSEAS), Corfu Island, Greece*, 2011, pp. 151-155.

[56] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications,* vol. 1, pp. 53-66, 2014/04/01/ 2014.

[57] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 255-265.

[58] L. Tamilselvan and V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET," in *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)*, 2007, pp. 21-21.

[59] J. Luo, M. Fan, and D. Ye, "Black hole attack prevention based on authentication mechanism," in *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, 2008, pp. 173-177.

[60] P. N. Raj and P. B. Swadas, "DPRAODV: A Dynamic Learning System Against Blackhole Attack In AODV Based MANET," *International Journal of Computer Science Issues, IJCSI,* vol. 2, pp. pp54-59, 2009.

[61] I. Ullah and S. U. Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols," Independent thesis Advanced level (degree of Master (Two Years)) Student thesis, 2010.

[62] S. Misra, K. Bhattarai, and G. Xue, "BAMBi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks," in *Communications (ICC), 2011 IEEE International Conference on*, 2011, pp. 1-5.

[63] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," *Computer Communications,* vol. 34, pp. 107-117, 2011/01/15/ 2011.

[64] J.-W. Huang, I. Woungang, H.-C. Chao, M. S. Obaidat, T.-Y. Chi, and S. K. Dhurandher, "Multi-path trust-based secure AOMDV routing in ad hoc networks," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, 2011, pp. 1-5.

[65] J. Sen, S. Koilakonda, and A. Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks," in *Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on*, 2011, pp. 338-343.

[66] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems,* vol. 50, pp. 217-241, August 01 2012.

[67] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "A novel approach for grayhole and blackhole attacks in mobile ad hoc networks," in *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, 2012, pp. 556-560.

[68] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, 2012, pp. 535-541.

[69] Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in *Communication Systems and Networks (COMSNETS), 2013 Fifth International Conference on*, 2013, pp. 1-7.

[70] H. Almutairi, S. Chelloug, H. Alqarni, R. Aljaber, A. Alshehri, and D. Alotaish, "A New Black Hole Detection Scheme for Vanets," presented at the Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems, Buraidah, Al Qassim, Saudi Arabia, 2014.

[71] J. Rani and N. Kumar, "Improving AOMDV protocol for black hole detection in Mobile Ad hoc Network," in *2013 International Conference on Control, Computing, Communication and Materials (ICCCCM)*, 2013, pp. 1-8.

[72] A. A. Aware and K. Bhandari, "Prevention of black hole attack on AODV in MANET using hash function," in *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*, 2014, pp. 1-6.

[73] I. Dhyani, N. Goel, G. Sharma, and B. Mallick, "A Reliable Tactic for Detecting Black Hole Attack in Vehicular Ad Hoc Networks," in *Advances in Computer and Computational Sciences: Proceedings of ICCCCS 2016, Volume 1*, S. K. Bhatia, K. K. Mishra, S. Tiwari, and V. K. Singh, Eds., ed Singapore: Springer Singapore, 2017, pp. 333-343.

[74] J. Tobin, C. Thorpe, and L. Murphy, "An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks," in *IEEE 85th Vehicular Technology Conference: VTC2017-Spring*, 2017.

[75] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "Using discriminant analysis to detect intrusions in external communication for self-driving vehicles," *Digital Communications and Networks,* vol. 3, pp. 180-187, 2017/08/01/ 2017.

[76] S. S. Albouq and E. M. Fredericks, "Lightweight Detection and Isolation of Black Hole Attacks in Connected Vehicles," in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2017, pp. 97-104.

[77] A. Dorri, "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET," *Wireless Networks,* vol. 23, pp. 1767-1778, August 01 2017.

[78] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal,* vol. 25, pp. 19-27, 2003.

[79] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy,* vol. 2, pp. 49-55, 2004.

[80] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl, "Security requirements for automotive on-board networks," in *Intelligent Transport Systems Telecommunications,(ITST), 2009 9th International Conference on*, 2009, pp. 641-646.

[81] P. Papadimitratos and A. Jovanovic, "GNSS-based positioning: Attacks and countermeasures," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2008, pp. 1-7.

[82] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, pp. 75-86.

[83] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection,* vol. 5, pp. 146-153, 2012.

[84] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation,* vol. 2012, 2012.

[85] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems,* vol. 16, pp. 546-556, 2015.

[86] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Transactions on Intelligent Transportation Systems,* vol. 16, pp. 1794-1805, 2015.

[87] M. Patel and S. Sharma, "Detection of malicious attack in manet a behavioral approach," in *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, 2013, pp. 388-393.

[88] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE systems journal,* vol. 8, pp. 749-758, 2014.

[89] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Systems with Applications,* vol. 41, pp. 1411-1418, 2014.

[90] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad

hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 2681-2691, 2015.

[91] N. W. Lo and H. C. Tsai, "Illusion Attack on VANET Applications - A Message Plausibility Problem," in *2007 IEEE Globecom Workshops*, 2007, pp. 1-8.

[92] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular Security Through Reputation and Plausibility Checks," *IEEE Systems Journal*, vol. 8, pp. 384-394, 2014.

[93] P. Tyagi and D. Dembla, "Investigating the security threats in Vehicular ad hoc Networks (VANETs): Towards security engineering for safer on-road transportation," in *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*, 2014, pp. 2084-2090.

[94] P. Sirola, A. Joshi, and K. C. Purohit, "An analytical study of routing attacks in Vehicular Ad-Hoc Networks (VANETs)," *International Journal of Computer Science Engineering (IJCSE)*, vol. 3, pp. 210-218, 2014.

[95] A. S. K. Pathan, "Chapter 6: Securing Transportation Cyber-Phusical Systems," in *Securing Cyber-Physical Systems*, ed: CRC Press, 2015.

[96] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, pp. 960-969, 2016.

[97] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET 1," 2013.

[98] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet of Things Journal*, vol. 1, pp. 10-21, 2014.

[99] C. McCarthy, K. Harnett, and A. Carter, "Characterization of potential security threats in modern automobiles: A composite modeling approach," 2014.

[100] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *USENIX Security Symposium*, 2011.

[101] H. Schweppe and Y. Roudier, "Security and privacy for in-vehicle networks," in *Vehicular Communications, Sensing, and Computing (VCSC), 2012 IEEE 1st International Workshop on*, 2012, pp. 12-17.

[102] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *IN PROCEEDINGS OF THE 18TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM. THE INTERNET SOCIETY*, 2011.

[103] A. Wright, "Hacking cars," *Communications of the ACM*, vol. 54, pp. 18-19, 2011.

[104] T. Yang, L. Kong, W. Xin, J. Hu, and Z. Chen, "Resisting relay attacks on vehicular passive keyless entry and start systems," in *Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on*, 2012, pp. 2232-2236.

[105] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, *et al.*, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *19th USENIX Security Symposium, Washington DC*, 2010, pp. 11-13.

[106] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, "A method of preventing unauthorized data transmission in controller area network," in *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*, 2012, pp. 1-5.

[107] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, pp. 993-1006, 2015.

[108] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in *Information Networking (ICOIN), 2016 International Conference on*, 2016, pp. 63-68.

[109] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, 2006, pp. 8 pp.-381.

[110] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, 2007.

[111] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in *Communications, 2008. ICC'08. IEEE International Conference on*, 2008, pp. 1436-1440.

[112] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, pp. 2991-3005, 2016.

[113] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Transactions on parallel and distributed Systems*, vol. 22, pp. 1912-1925, 2011.

[114] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *International Conference on Wireless Algorithms, Systems, and Applications*, 2015, pp. 685-695.

[115] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. K. R. Choo, and M. Dlodlo, "From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework," *IEEE Access*, vol. 5, pp. 8284-8300, 2017.

[116] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Infocom, 2010 proceedings ieee*, 2010, pp. 1-9.

[117] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems,* vol. 23, pp. 1621-1631, 2012.

[118] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on parallel and distributed systems,* vol. 25, pp. 222-233, 2014.

[119] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," *Journal of Network and Computer Applications,* vol. 34, pp. 1113-1122, 2011.

[120] N. Penning, M. Hoffman, J. Nikolai, and Y. Wang, "Mobile malware security challeges and cloud-based detection," in *Collaboration Technologies and Systems (CTS), 2014 International Conference on*, 2014, pp. 181-188.

[121] Y. Xiao, X. Zhang, Y. Zhang, and R. Teodorescu, "One Bit Flips, One Cloud Flops: Cross-VM Row Hammer Attacks and Privilege Escalation," in *USENIX Security Symposium*, 2016, pp. 19-35.