UNIVERSITI PUTRA MALAYSIA

SECURE COMMUNICATION IN VEHICULAR AD HOC NETWORK USING MODIFIED AD HOC ON DEMAND DISTANCE VECTOR

ZAID A. ABDULKADER

FSKTM 2018 15

SECURE COMMUNICATION IN VEHICULAR AD HOC NETWORK USING MODIFIED AD HOC ON DEMAND DISTANCE VECTOR

By

ZAID A. ABDULKADER

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirement for the Degree of Doctor of Philosophy

January 2018

DEDICATION

Dedicated this work to my father, my mother and my brother, to my beloved wife and my daughter for their supplication, patience and understanding.

Also, I dedicate this work to everyone who helped me in my life and gave me advice.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of philosophy

SECURE COMMUNICATION IN VEHICULAR AD HOC NETWORK USING MODIFIED AD HOC ON DEMAND DISTANCE VECTOR

By

ZAID A. ABDULKADER

January 2018

Chairman : Azizol bin Hj Abdullah, PhD
Faculty : Computer Science and Information Technology

Vehicular ad hoc networks (VANETs) can potentially increase road safety dramatically by providing drivers with more time to adequately respond to dangerous situations. To safeguard VANETs from abuse, they need a security infrastructure to ensure security requirements like authentication, confidentiality, and availability. First threat is on VANET availability: The network has to always be available even if it undergoes attack. To do this, it must use alternative mechanisms while making sure that it does not affect its performance. A Blackhole attack is considered one of the most harmful and active attacks example on the availability of VANETs. Second threat is on confidentiality: Confidentiality ensures that the data is only accessible to the designated recipient and that other users cannot access the data. It therefore ensures that the data remains untouched until it is received by the designated recipient. Wormhole attack is the most sophisticated and hostile attack example against VANET confidentiality. Third threat is on authentication: Vehicles must only respond to messages that are sent by legitimate network members. Thus, authenticating the sender of a message is vital. One of the most especially dangerous attacks example on authority in VANET is referred to as the Sybil attack. These kind of threats can impact on the VANET's applications like safety application and road congestion management application, so that, it will increase the road accidents. They can hide emergency massages like collision warning and traffic jam warning massages. This study suggests a framework that can be used for secure VANET communication in city scenario. In our framework we use Ad hoc On demand Distance Vector (AODV) because it is the most suitable routing protocol for VANET and the current routing protocols have mostly been designed for

MANETs. AODV can be applied in VANETs because it is able to deal with continually evolving topology and high mobility speed of VANET. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules, so that our framework can provide secure communication in VANET via modifying AODV. Our framework categorises the requirements for the VANET protection design via modifying AODV into three: Insure the Availability of VANET and its Services Algorithm (IAVSA), Protect Data Dissemination Algorithm (PDDA), and Secure Vehicles Authentication Algorithm (SVAA). The OMNET++ simulation program is used to justify the proposed algorithms. This is done based on the specific parameters such as (number of malicious nodes, number of normal nodes, and maximum speed). In instances when Blackhole and wormhole attacks take place in IAVSA and PDDA, a high detection rate that is close to 99% is observed. Furthermore, when a Sybil attack takes place, SVAA can identify 97% of the Sybil attacks. The simulation also illustrates that it had a high packet delivery ratio and low end-to-end delay.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

KOMUNIKASI SELAMAT DALAM RANGKAIAN AD HOC KENDERAAN DENGAN MENGGUNAKAN AD HOC TERUBAH SUAI VEKTOR JARAK ATAS PERMINTAAN

Oleh

ZAID A. ABDULKADER

Januari 2018

Pengerusi : Azizol bin Hj Abdullah, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Rangkaian ad hoc kenderaan (VANET) berpotensi meningkatkan keselamatan jalanraya secara dramatik dengan menyediakan pemandu dengan lebih banyak masa untuk memberi respons yang memadai terhadap situasi berbahaya. Untuk melindungi VANET daripada penyalahgunaan, mereka memerlukan infrastruktur keselamatan bagi memastikan keperluan keselamatan seperti pengesahan, kerahsiaan, dan ketersediaan. Ancaman pertama adalah mengenai ketersediaan VANET: Rangkaian harus selalu tersedia walaupun ia mengalami serangan. Bagi melakukan ini, ia mesti menggunakan mekanisme alternatif sambil memastikan ia tidak mempengaruhi prestasinya. Serangan 'Blackhole' dianggap salah satu contoh serangan yang paling berbahaya dan aktif terhadap ketersediaan VANET. Ancaman kedua adalah kerahsiaan: Kerahsiaan memastikan bahawa data hanya boleh diakses oleh penerima yang ditetapkan dan pengguna lain tidak boleh mengakses data. Oleh itu, pastikan data tidak disentuh sehingga diterima oleh penerima yang ditetapkan. Serangan 'Wormhole' adalah contoh serangan yang paling canggih dan bermusuhan terhadap kerahsiaan VANET. Ancaman ketiga adalah pada pengesahan: Kenderaan hanya perlu memberi respons kepada mesej yang dihantar oleh ahli rangkaian yang sah. Oleh itu, mengesahkan penghantar mesej adalah penting. Salah satu contoh serangan paling berbahaya mengenai kuasa di VANET disebut sebagai serangan Sybil. Ancaman seperti ini boleh memberi kesan kepada aplikasi VANET seperti keselamatan aplikasi dan aplikasi pengurusan kesesakan jalan raya, supaya ia akan meningkatkan kemalangan jalan raya. Mereka boleh menyembunyikan mesej kecemasan seperti amaran perlanggaran dan mesej amaran kesesakan jalan raya. Kajian ini mencadangkan satu rangka kerja yang boleh digunakan untuk komunikasi VANET yang selamat dalam senario bandar. Dalam rangka kerja kami, kami menggunakan Vektor Jarak atas Permintaan Ad hoc (AODV) kerana ia adalah protokol penghalaan yang paling sesuai untuk VANET dan protokol penghalaan semasa kebanyakannya direka untuk MANET. AODV boleh digunakan di VANET kerana ia mampu menangani topologi yang terus berkembang dan kelajuan mobiliti tinggi VANET. Oleh kerana AODV tidak mempunyai mekanisme keselamatan, nod jahat boleh melakukan banyak serangan hanya dengan tidak bertindak menurut peraturan AODV, supaya rangka kerja kami dapat memberikan komunikasi yang aman di VANET melalui mengubah AODV. Rangka kerja kami mengkategorikan keperluan untuk reka bentuk perlindungan VANET melalui mengubah AODV menjadi tiga: Menginsuranskan Ketersediaan VANET dan Algoritma Perkhidmatannya (IAVSA), Melindungi Data Penyebaran Algoritma (PDDA), dan Algoritma Pengesahan Kenderaan Selamat (SVAA). Program simulasi OMNET ++ digunakan untuk membenarkan algoritma yang dicadangkan. Ini dilakukan berdasarkan parameter tertentu seperti (bilangan nod jahat, bilangan nod biasa, dan kelajuan maksimum). Dalam keadaan apabila serangan 'Blackhole' dan 'Wormhole' berlaku di IAVSA dan PDDA, kadar pengesanan tinggi yang hampir 99% diperhatikan. Tambahan pula, apabila serangan Sybil berlaku, SVAA dapat mengenal pasti 97% serangan Sybil. Simulasi juga menggambarkan bahawa ia mempunyai nisbah penghantaran paket yang tinggi dan kelewatan hujung ke hujung yang rendah.

ACKNOWLEDGEMENTS

First of all, all praise to Allah the most merciful who have given the opportunity to attain to this level.

I owe a great many thanks to a great many people who helped and supported me during the writing of this thesis. My deepest thanks to my supervisor, Dr. Azizol bin Hj Abdullah, the guide of the project, for guiding and correcting various documents of mine with attention and great care. He has gone through the thesis and made the necessary corrections, where needed. Again, I am heartily thankful to my supervisor, whose encouragement, guidance and support from the initial to the final phase enabled me to develop an understanding of the subject.

I would like to say thanks my committee members, Dr. Mohd Taufik Abdullah and Associate. Prof. Dr. Zuriati Ahmad Zukarnain. I would like to express appreciation for their insightful comments, questions, criticisms, and suggestion of the work. I express my thanks to the Dean, Faculty of Computer Science and Information Technology and the Dean, School of Graduate Studies. I would also thank Institution and faculty members without whom this project would have been a distant reality.

Last but not least, I would like to thank my family. The constant inspiration and guidance kept me focused and motivated. I am grateful to my dad for giving me the life I ever dreamed. I can't express my gratitude for my mother in words, whose unconditional love has been my greatest strength. The constant love and support of my wife. The reason that I able to finish the project as possible. I also extend my heartfelt thanks to my family and well-wishers.

I certify that a Thesis Examination Committee has met on 29 January 2018 to conduct the final examination of Zaid A. Abdulkader on his thesis entitled "Secure Communication in Vehicular Ad Hoc Network using Modified Ad Hoc on Demand Distance Vector" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Lilly Suriani Affendey, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Nur Izura binti Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Nor Fazlida binti Mohd Sani, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Jemal Abawajy, PhD
Professor
Deakin University
Australia
(External Examiner)

NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 26 April 2018

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Azizol bin Hj Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zuriati Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Mohd Taufik Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ________________________________ Date: ________________

Name and Matric No.: ____

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ____
Name of
Chairman of
Supervisory
Committee: ____

Signature: ____
Name of
Member of
Supervisory
Committee: ____

Signature: ____
Name of
Member of
Supervisory
Committee: ____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	Ad hoc On demand Distance Vector
AU	Application Unit
DDOS	Distributed Denial Of Services
DMV	Department of Motor Vehicle sector
DOS	Denial Of Services
DSR	Dynamic Source Routing
DSRC	Dedicated Short Range Communication
EDR	Event Data Record
GPS	Global Positioning System
HC	Hope Count
HMAC	Hash Message Authentication Code
ITS	Intelligent Transportation System
IVC	Inter vehicle communication
MAC	Message Authentication Code
MAC address	Media Access Control address
MANET	Mobile ad hoc Network
ms	millisecond
N1HN	One Hop Neighbor
N1HN(S)	One Hop Neighbor of Source Node
OBU	On Board Unit
OLSR	Optimized Link State Routing
P2P	Peer-2-Peer
PDA	Personal Digital Assistant
PDR	Packet Delivery Ratio
RERR	Rout Error
RREP	Rout Reply
RREQ	Rout Request
RSSI	Received Signal Strength Indicator

RSU	Road Side Unit
RTT	Round Trip Time
SAT	Short Authentication Token
SUMO	Simulation of Urban Mobility
TA	Trusted Authority
TPD	Tamper Proof Device
TTL	Time To Live
V2I	Vehicle to Infrastructure
V2V	Vehicle to vehicle
VANET	Vehicular ad hoc Network
Veins	Vehicular Network Simulation
WAVE	Wireless Access in Vehicle Environment
WHO	World Health Organization
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

Each day, the lives of numerous people around the world are taken and so much more become injured due to traffic accidents. According to the World Health Organisation (WHO), about 1.24 million people die each year due to road accidents, and around 20 to 50 million people suffer from nonfatal injuries because of road traffic crashes (Organization, 2013). Over the next two decades, it is expected that these figures will rise by 65% unless a mechanism to prevent this is implemented. Vehicular communication networks were mainly developed because of the need to spread information about road safety among vehicles so that accidents can be prevented and road safety can be improved (Eiza et al., 2013). The industry and the academic society have widely accepted that when vehicles and road transportation systems cooperate, the road efficiency and driver's safety can be improved and the environmental impact can be reduced. As a result, more attention and research efforts have been dedicated to the development of vehicular ad hoc networks (VANETs). Several studies have been conducted with the aim of providing a common platform to enable inter-vehicle communications (IVCs). IVCs are important in dynamic route scheduling, traffic condition monitoring, emergency-message dissemination, and safe driving (Yang et al., 2007). The assumption is that every vehicle is equipped with wireless communication equipment that will offer connectivity to the ad hoc network. VANETs are categorised as a special type of mobile ad hoc networks (MANETs).

However, they are made distinct by their several key features as well. VANETs have highly mobile network nodes, which mean that their network topology is continually changing. Consequently, the condition of the communication link between two vehicles is affected by this fast variation. This link is also susceptible to disconnection due to the movements of the vehicles and the drivers' unpredictable behaviours. Fortunately, one can predict their mobility along the road because they still have to adhere to the traffic networks and its rules and regulations. Compared to MANETs, VANETs typically possess higher transmission power and higher computational capability. The VANETs' distinct characteristics give rise to several routing issues that have to be addressed before these networks can be deployed effectively. The most challenging problem is possibly the high mobility of the network and the frequent variations in the topology of the network (Blum et al., 2004). The vehicular networks' topology can change the vehicles change lanes or velocities. Current routing protocols have mostly been designed for MANETs. AODV routing protocol can be applied in VANETs because it is able to deal with continually evolving topology and high mobility speed of VANET (Altayeb and Mahgoub, 2013).

In VANETs, the different nodes like the vehicles and roadside units (RSUs) are typically furnished with processing, sensing, and wireless communication capabilities. Both Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications make it possible to have safety applications that can send out warnings about road accidents, traffic conditions (e.g. emergency braking, congestion, icy road), and other related transportation scenarios. Because AODV has no security mechanisms, malicious nodes can perform many attacks on the availability, confidentiality, and authentication of VANET and its applications (Li and Song, 2016).

1.1 Problem Statement

There are certain advantages to VANET technology, such as reduced amounts of road accidents and a more pleasant driving and travelling experience due to the simplification of payment processes for parking, tolls, fuel, etc. (Engoulou et al., 2014). Road users use different applications for traffic management, safety and efficiency, infotainment, comfort, warning, maintenance, network gaming, and music sharing. An exchange of messages, such as the distribution of emergency messages, traffic incidents and warnings about road condition that improve driving efficiency and traffic safety, is involved in these applications.

In VANETs, there are dangerous and critical consequences to a security breach. Moreover, given its highly dynamic environment that is characterised by the frequent and instantaneous arrival and departure of vehicles and the short duration for the connection periods, it is practically difficult to deploy a complete security solution. It also has to handle specific configurations and constraints.

An accurate and efficient collaborative intrusion detection framework to secure vehicular networks (AECFV) is the current existing framework for sensing and removing malicious nodes from VANET (Sedjelmaci and Senouci, 2015). AECFV is well-suited to the characteristics of VANET, such as the rapid topology change and the high mobility of the node. This is attained by using the proposed secured clustering algorithm. This algorithm takes into account both the network's vulnerability and node's mobility during the formation of a cluster. Clusters are created with good connectivity and high stability. Election of cluster heads (CHs) is based on the vehicle's trust-level and the node's mobility. However, this approach has the following weaknesses (Kerrache et al., 2016): (i) it requires a large amount of time to form a cluster and elect a cluster head; (ii) it does not have realistic assumptions about stable clusters in urban environments; and (iii) there is no trust in the absence of RSUs, and thus intruder nodes are not punished even if intrusions are detected by the IDS. However, to sense the malicious nodes in VANET, AECFV relies on vehicular GPS. Thus, the system will fail to function properly in a tunnel or a location with no GPS signal (Paul and Islam, 2012).

The Ad hoc On demand Distance Vector (AODV) is the most suitable routing protocol for VANET (Altayeb and Mahgoub, 2013). The AODV routing protocol does not need any central administrative system to control the routing process (Maurya et al., 2012). It tend to reduce the control traffic messages overhead at the cost of increased latency in finding new routes. AODV reacts relatively fast to the topological changes in the network and updates only the nodes affected by these changes. In AODV, if a node has to choose between two routes, the up-to-date route is always chosen. Whereas AODV can be applied to large scale ad hoc network, it suit the urban environment (Paul and Islam, 2012). Position determining services is not required for AODV, for this reason it works in tunnel and under grand parking.

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules (Jamali and Fotohi, 2016). Thus, it could threaten VANET security requirements like authentication, confidentiality and availability (Leinmuller et al., 2008).

Availability is most important factor which needs to be taken care in VANET (Kumar and Shakar, 2017). It assures that the network is efficient and useful data is available at any operational time. As most interchanged messages in VANET affect the road traffic safety, this requirement is critical in this environment. This precarious security prerequisite for VANET which serve to save the users life is an important target for most of the attackers.

Confidentiality is an important security requirement for VANET as it ensures that data are only accessed by intended user (Al-Sultan et al., 2014). In absence of confidentiality the exchange of data between nodes in vehicular network are susceptible to attack. In such cases, the attacker collects the information by exploiting user‵s privacy on the location of the vehicle and its routes. It therefore ensures that the data remains inaccessible until it is received by the designated recipient.

Authenticity is one of foremost challenge in VANETs security (Kumar and Shakar, 2017). Due to this all the existing nodes in the network must authenticate before the available services are accessed. Hence any desecration or attack during the process of identification and authentication creates serious concern for the network. So to ensure the authenticity in the VANET it is necessary to secure the authentic node from intruders those are using fabricated identity. The importance of identification authentication process arises from the facts that it is frequently and continuously used whenever vehicle needs to interact with the network services.

1.2 Objectives

In order to address the research problem that was described in the preceding section, the main objective is producing secure Vehicle Ad hoc Network (VANET) via modified Ad hoc On Demand Distance Vector (AODV) to protect VANET security perquisites, the focus of this research will be on the following sub-objectives:

1. To propose an algorithm that will ensure the availability of VANET and its services on city roads.
2. To propose an algorithm that will protect the confidentiality and validity of VANET on city roads.
3. To propose an algorithm that will secure the authentication of vehicles on city roads.

1.3 Scope of Research

The studies focus on the security of a vehicular ad hoc network (VANET). VANETs are wireless networks that have nodes that are either the fixed road units or the highly mobile vehicles. Nodes communicate in infrastructure mode with the fixed equipment on the roads and they communicate in ad hoc mode with each other. Thus, the VANETs' characteristics are essentially a combination of the characteristics of the wireless medium and the characteristics of the various topologies in the infrastructure and ad hoc modes. Like the other systems for communication and data processing, there are different kinds of threats and attacks that threaten VANETs. The lack of an energy problem and the capacity of an on board unit (OBU) to accommodate numerous microprocessors impart the vehicles with vital processing and computing capacities. Unlike a regular ad hoc network, two significant advantages for VANET nodes are represented by this. Furthermore, because VANETs are highly mobile, the feasibility of attacks is affected by the two stated advantages.

Ad hoc On Demand Distance Vector (AODV) routing protocol is an up-to-date path to the destination because of using destination sequence number. Reactive protocols like AODV tend to reduce excessive memory requirements and the route redundancy. AODV responses to the link failure in the network and updates only the nodes affected by these changes. It can be applied to large scale ad hoc network. AODV has no security mechanism and is vulnerable to many kinds of attacks that manipulate its routing control mechanisms.

VANET is vulnerable to several attacks, because the nature of its open access medium. Blackhole attack is considered as one of the most serious threats to the availability of VANETs (Mejri et al., 2014). Blackhole intrudes the routing function (Lee and Jeong, 2016). In a Blackhole attack, malicious nodes change the routing information and make it seem as if they are the destinations. They then take all the packets moving on the networks and discard them. All the packets that are delivered to the malicious node are not sent to the other nodes anymore. A wormhole attack is considered as the most threatening and sophisticated attack on the confidentiality of VANET (Chan and Alam, 2014). During a wormhole attack, the attacker can use wormhole links to forward each packet without changing the packet transmission. It is able to do this by routing it to a remote node that has no authorization (Ji et al., 2015). Hence, when they receive the packets that are rebroadcast by the attackers, some nodes will be led to believe that they near the attacker. Because they can change network topologies and circumvent packets to conduct further manipulation, many functions in the network are severely threatened by wormhole attackers. The Sybil attack is one of the most especially harmful attacks on VANET authority (Park et al., 2013). Douceur first introduced the Sybil attack in the context of peer-to-peer networks (Lee et al., 2013). In a Sybil attack, a malicious sender can forge multiple fake identities (called Sybil nodes) so that normal nodes can be impersonated. Majority of applications based on VANET, such as pre-crash sensing and warning, cooperative forward collision warning, and local hazard notification, require vehicles to cooperate (Neha and Bevish, 2015). Sybil attack can accomplish a particular task by attempting to represent itself using multiple fake identities. They generate these multiple identities using the set of pseudonyms of their own on board unit (OBU) or by impersonating the identities of other vehicles so that they would be tagged as malicious. Such attacks result into privacy leakage and caused degradation in network performance. The security is the most important issue in VANET. Thus, security mechanisms are designed to protect VANET confidentiality, ensure the availability of VANET, and provide authentication to secure vehicles. Furthermore, it is significantly important to provide secure VANETs on city roads.

1.4 Methodology

Extensive simulations were performed using SUMO, so that the proposed framework can be evaluated. OMNeT++ is categorised as a modular discrete event network simulator (Rehman et al., 2013). One of the main features of OMNeT++ is that it can combine a network's small building blocks by taking advantage of that network's modular structure. The mobility model utilised to produce the traffic greatly affects the accuracy of the simulation results that were obtained in vehicular networks. Therefore, a realistic vehicle network can be simulated using the mobility model defined in (Institute of Transportation Systems Berlin, 2013). This model produces a trace file that the OMNeT++ can use, lane changes, including collision free movement, and maintenance of distance between vehicles. A Manhattan Grid map that was provided by SUMO was used in the simulation of this work. For all scenarios, the vehicles velocity ranged from 20 Km/h to 100 Km/h, while the density was in the range of 50 to 300 vehicles to be as a realistic city. Three different kinds of attackers were considered in our simulations. The first attack was directed towards the availability of VANET, then on VANET confidentiality and finally on the node authentication. We use six type of performance metrics to determine the performance of our work and compare it with the summation results of the current work.

1.5 Research Contributions

The main contribution is producing secure Vehicle Ad hoc Network (VANET) via modified Ad hoc On Demand Distance Vector (AODV) routing protocol to protect VANET's security fundamental, sub-contributions of this research can be described as follows:

1. Insure the Availability of VANET and its Services Algorithm

VANET is a network without any infrastructure. It is also a MANET. One important distinction is that in VANET, the movement of nodes is strictly warned. Black hole attack is an extremely threatening attack that lowers the availability of VANET. Therefore, to ensure the availability of VANET, we developed an algorithm known as the Insure the Availability of VANET and its Services Algorithm (IAVSA). IAVSA makes use of a two-phase detection technique (i.e. analysis of the node behaviour and calculation of the route reply (RREP) packet's originality). This technique can detect a malicious node with high accuracy (i.e. low false positive and high detection rates). It also has the ability to alert all the legitimate nodes to halt communication with an attacker node that is found on the city roads for VANETs. Furthermore, the rules used in IAVSA specify the behaviour of the nodes while the source node determines which nodes are the intruders. It denotes the behaviour using the packet transmission of the route reply (RREP) and route request (RREQ) packets. Thus, this monitoring technique helps determine if there are any malicious nodes within the network. Furthermore, IAVSA allows each node to choose its best one hop node with the node that possesses a lower mobility speed. It then selects a proxy route and one transmission route. The path that possesses the shortest mobility speed and hop count have more priority and are therefore utilised for data transmission. Consequently, the route with the second priority is selected as the proxy route. Two routes are selected so that if any link break or error takes place during the transmission route, the proxy route selected can still be used for transmission. Thus, the time for choosing another route is reduced in the case of any link breakage. Simulation results revealed that compared to the existing algorithm which is an accurate and efficient collaborative intrusion detection framework to secure vehicular networks (AECFV)), IAVSA was able to achieve a lower false positive ratio and higher detection ratio. Because it selected the most dependable route to the destination, it was able to attain a higher packet delivery ratio, lowest communication overhead, lowest detection time, and lowest average values for the end-to-end delay.

2. Protect Data Dissemination Algorithm

VANET is a type of emerging ad hoc network that offers two vehicles an avenue to efficiently communicate. Several researchers have recently observed that it has the ability to improve safety measures and higher communication. However, these researchers also emphasised that VANET is plagued with several problems especially in terms of security. The amount of vulnerable security threads observed in the VANET has risen. Confidentiality thread is one of VANET's security threads. Wormhole attack is considered as one of the most dangerous attacks on the confidentiality of VANET. This study proposes the Protect Data Dissemination Algorithm (PDDA) for the detection and removal of these kinds of attacks and to ensure the confidentiality of VANET. PDDA identifies wormhole attackers by sensing the two nodes' link lifetime, route redundancy, and route reliability from source to destination. The link lifetime is identified because in the VANET, the nodes move at high speed and there is a break in communication if a node goes out of coverage. In this system, a Round Trip Time (RTT) is calculated when the source node broadcasts a packet. The RREP is sent by the destination node to the sender node within a given time frame. It also calculates the RTT for every possible route from the source to its destination. Then, all the possible routes with the same RTT are listed down, along with some of the relay nodes that transmit route request (RREQ) at 1-hop neighbours. Route aggregation is then allowed at this time, so that all nodes can be a part of the network. The RTT is computed for each route when route request (RREQ) is transmitted through its next 1-hop members. The reception of RREP at the source takes place at a specific time; source stamps are used to calculate the RTT for its routes or route. Lastly, all the routes that have a link lifetime are listed along with the RTT and number of hops. It was observed that PDDA had promising results in terms of detection ratio, packet delivery ratio, false positive ratio, detection time, average end-to-end delay, and communication overhead. It was also observed that using the concept of round trip time in reliable algorithms for VANETs has great promise in helping attain confidential data transmission.

3. Secure Vehicles Authentication Algorithm

This study proposes a Secure Vehicles Authentication Algorithm (SVAA) with the aim of enhancing the security of vehicles authentication within the VANET environment. One of the most dangerous attacks on the VANET authentication (Sybil attack) was identified from the network and a secure route that can be used to communicate was provided. In SVAA, a unique Short Authentication Token (SAT) is given to every registered legitimate user (i.e. generated by Department of Motor Vehicle sector (DMV)). For authentication purposes, the SAT that is produced for each vehicle is also kept in each road side unit (RSU). RSU then calculates hash massage authentication code for the vehicle 'V_{HMAC}' using the SAT and user ID. To identify a Sybil attack, it needs to check if $V_{MAC} = V_{HMAC}$. If the RSU is able to identify the attacker, it will begin distributing information about the attacker vehicle and it will also instruct the source node to choose another route. Furthermore, both trusted and untrusted authorities are used to identify a Sybil attack. Initially, RREQ packets are sent by the sender to their neighbour nodes. Afterwards, the RSU makes an observation of the Received Signal Strength Indicator (RSSI) values for every node that receives the packets of the sender node. Then, reply packets that contain the MAC address from the neighbour nodes are sent in return. During the last part of the classification, the false RSSI values are moved to the Department of Motor Vehicle Sector so that the Sybil attacker can be accurately identified. The performance of the SVAA algorithm was assessed using extensive simulations. The results were then compared to the performance of the accurate and efficient collaborative intrusion detection framework to secure vehicular networks (AECFV). Promising results were exhibited by SVAA in terms of higher detection ratio, high packet delivery ratio, lower false positive ratio, lowest detection time, lowest average end-to-end delay values, and lowest communication overhead.

1.6 Thesis Organisation

This thesis is structured as follows:

Chapter 1 introduces readers to the basic of the Vehicular ad hoc Network. This chapter provide the general problem statement that derives the objective of this study. It also gives a brief description of our methodology. Then this chapter gives a summary of achievements in a form of a list of Contributions.

Chapter 2 provides a summary of the vehicular ad hoc network, specifically describing what it is and what security challenges it faces. The chapter demonstrated the VANET architecture, the importance of VANET application, the VANET's routing protocol, security perquisites in VANET, challenges in VANET, and security attacks in VANET. It also clearly demonstrated the mechanism for Ad Hoc on Demand Distance Vector Routing Protocol (AODV). This section also presented previous work that researchers conducted on the detection and removal of malicious nodes from VANET. It also examined how previous works have protected VANET against the three most harmful threats on confidentiality, availability, and authentication.

Chapter 3 provides the methodology that this research utilised. This chapter examined the simulation tools to evaluate the proposed framework and demonstrate the simulation parameter and mobility model. This chapter also demonstrated the scenarios for the three types of attacks that affect the confidentiality, availability, and authentication. Furthermore, this chapter clarified the performance metrics used. It also provided the simulation results used for the current framework AECFV. The simulation results used was based on the detection rate, detection time, false positive rate, packet delivery ratio, average end-to-end delay, and overhead.

In Chapter 4, the VANET availability is briefly discussed, along with the Blackhole attack and how it is one of the most common attacks on VANET availability. Every step needed to protect VANET availability is discussed. This chapter also provides a discussion on the Insure the Availability of VANET and its Services Algorithm. Furthermore, it presents the simulation result for the detection ratio, end-to-end delay, false positive rate, packet deliver ratio, detection time, and overhead. Finally, the results gathered from the research experiments were analysed and discussed before being compared to the current approach in AECFV.

In Chapter 5, the wormhole attack, which is one the most dangerous attacks on VANET confidentiality, is discussed briefly. Every step needed to protect VANET confidentiality is discussed. It also provides a discussion on the research methods involved, the Protect Data Dissemination Algorithm, the simulation result for detection ratio end-to-end delay, false positive rate, detection time, overhead, and packet deliver ratio. Finally, the results gathered from the research experiments were analysed and discussed before being compared to the current approach in AECFV.

In Chapter 6, the authentication in VANET is discussed in brief, as well as the Sybil attack, which is one the most dangerous attacks on VANET availability. Every step needed to protect VANET availability is discussed. It also provides a discussion on the research methods involved, Secure Vehicles Authentication Algorithm, the simulation result for detection ratio, end-to-end delay, false positive rate, detection time, overhead, and packet deliver ratio. Finally, the results gathered from the research experiments were analysed and discussed before being compared to the current approach in AECFV.

Chapter 7 contains the conclusion of the proposed algorithms, PDDA, IAVSA, and SVAA. It also presents the achievements of the research, the challenges, and information about future work.

REFERENCES

Abbas, Sohail, Merabti, Madjid, Llewellyn-Jones, David, and Kifayat, Kashif. (2013). Lightweight sybil attack detection in manets. *IEEE systems journal,* 7(2), 236-248.

Abumansoor, Osama, and Boukerche, Azzedine. (2012). A secure cooperative approach for nonline-of-sight location verification in VANET. *IEEE Transactions on Vehicular Technology,* 61(1), 275-285.

Akbar, Muhammad Sajjad, Qayyum, Amir, and Khaliq, Kishwer Abdul. (2015). Information delivery improvement for safety applications in VANET by minimizing Rayleigh and Rician fading effect. *Vehicular Ad-hoc Networks for Smart Cities* (pp. 85-92): Springer.

Ali, Fayaz, Shaikh, Faisal Karim, Ansari, Abdul Qadir, Mahoto, Naeem Ahmed, and Felemban, Emad. (2015). Comparative analysis of VANET routing protocols: on road side unit placement strategies. *Wireless Personal Communications,* 85(2), 393-406.

Alimohammadi, Mahdiyeh, and Pouyan, Ali A. (2015). Sybil attack detection using a low cost short group signature in VANET. In *Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference*.

Al-Kahtani, Mohammed Saeed. (2012). Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference*.

Alotaibi, Eiman, and Mukherjee, Biswanath. (2012). A survey on routing algorithms for wireless ad-hoc and mesh networks. *Computer networks,* 56(2), 940-965.

Al-Sultan, Saif, Al-Doori, Moath M, Al-Bayatti, Ali H, and Zedan, Hussien. (2014). A comprehensive survey on vehicular Ad Hoc network. *Journal of network and computer applications,* 37, 380-392.

Altayeb, Marwa, and Mahgoub, Imad. (2013). A survey of vehicular ad hoc networks routing protocols. *International Journal of Innovation and Applied Studies,* 3(3), 829-846.

Anand, Anjali, Aggarwal, Himanshu, and Rani, Rinkle. (2016). Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks. *Journal of Communications and Networks,* 18(6), 938-947.

Arellano, Wilmer, Mahgoub, Imad, and Ilyas, Mohammad. (2014). Veins extensions to implement a message based algorithm for Dynamic Traffic Assignment in VANETs simulations. In *High-capacity Optical*

Networks and Emerging/Enabling Technologies (HONET), 2014 11th Annual.

Ashraf, Mohsin, Bilal, Harris, Khan, Imran Ahmad, and Ahmad, Farooq. (2016). Vanet Challenges of Availability and Scalability. *VFAST Transactions on Software Engineering,* 10(2).

Azees, Maria, Vijayakumar, Pandi, and Deborah, Lazarus Jegatha. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems,* 10(6), 379-388.

Babu, M Rajesh, and Usha, G. (2016). A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET. *Wireless Personal Communications,* 90(2), 831-845.

Bansal, Pooja, Sharma, Shabnam, and Prakash, Aditya. (2015). A Novel approach for Detection of Distributed Denial of Service attack in VANET. *International Journal of Computer Applications,* 120(5).

Barghi, Saman, Benslimane, Abderrahim, and Assi, Chadi. (2009). A lifetime-based routing protocol for connecting vanets to the internet. In *World of Wireless, Mobile and Multimedia Networks and Workshops, 2009. WoWMoM 2009. IEEE International Symposium*.

Bawa, Kanika, and Rana, Shashi B. (2015). Prevention of black hole attack in MANET using addition of genetic algorithm to bacterial foraging optimization. *International Journal of Current Engineering and Technology,* 5(4).

Bernardos, Carlos J, Soto, Ignacio, Calderón, María, Boavida, Fernando, and Azcorra, Arturo. (2007). Varon: Vehicular ad hoc route optimisation for nemo. *Computer Communications,* 30(8), 1765-1784.

Bhoi, Sourav Kumar, and Khilar, Pabitra Mohan. (2014). Vehicular communication: a survey. *IET Networks,* 3(3), 204-217.

Biswas, Subir, and Mišić, Jelena. (2010). *Proxy signature-based RSU message broadcasting in VANETs.* In *Communications (QBSC), 2010 25th Biennial Symposium*.

Blum, Jeremy J, Eskandarian, Azim, and Hoffman, Lance J. (2004). Challenges of intervehicle ad hoc networks. *IEEE transactions on intelligent transportation systems,* 5(4), 347-351.

Bouali, Tarek, Senouci, Sidi-Mohammed, and Sedjelmaci, Hichem. (2016). A distributed detection and prevention scheme from malicious nodes in vehicular networks. *International Journal of Communication Systems*.

Cadger, Fraser, Curran, Kevin, Santos, Jose, and Moffett, Sandra. (2013). A survey of geographical routing in wireless ad-hoc networks. *IEEE Communications Surveys and Tutorials,* 15(2), 621-653.

Chan, King Sun, and Alam, Mohammad Rafiqul. (2014). Topological comparison-based wormhole detection for MANET. *International Journal of Communication Systems,* 27(7), 1051-1068.

Chen, Honglong, Lou, Wei, and Wang, Zhi. (2015). On providing wormhole-attack-resistant localization using conflicting sets. *Wireless Communications and Mobile Computing,* 15(15), 1865-1881.

Cherif, Mohamed Oussama, Senouci, Sidi-Mohammed, and Ducourthial, Bertrand. (2013). Efficient data dissemination in cooperative vehicular networks. *Wireless Communications and Mobile Computing,* 13(12), 1150-1160.

Choi, Hyoung-Kee, Kim, In-Hwan, and Yoo, Jae-Chern. (2011). Secure and efficient protocol for vehicular ad hoc network with privacy preservation. *EURASIP Journal on Wireless Communications and Networking, 2011*(1), 716794.

Cunha, Felipe, Villas, Leandro, Boukerche, Azzedine, Maia, Guilherme, Viana, Aline, Mini, Raquel AF, and Loureiro, Antonio AF. (2016). Data communication in VANETs: Protocols, applications and challenges. *Ad Hoc Networks,* 44, 90-103.

Dhamgaye, Anup, and Chavhan, Nekita. (2013). Survey on security challenges in VANET 1.

Dhariwal, Sumit, and Tiwari, Harshvardhan. (2014). WIDPS: Wormhole Attack Intrusion Detection and Prevention Security Scheme in MANET. *International Journal of Computer Applications,* 105(10).

Dhenakaran, SS, and Parvathavarthini, A. (2013). An overview of routing protocols in mobile ad-hoc network. *International Journal of Advanced Research in Computer Science and Software Engineering,* 3(2).

Dixit, Mayank, Kumar, Rajesh, and Sagar, Anil Kumar. (2016). VANET: Architectures, research issues, routing protocols, and its applications. In *Computing, Communication and Automation (ICCCA), 2016 International Conference*.

Duarte, Joao M, Kalogeiton, Eirini, Soua, Ridha, Manzo, Gaetano, Palattella, Maria Rita, Di Maio, Antonio, Rizzo, Gianluca A. (2017). A multi-pronged approach to adaptive and context aware content dissemination in VANETs. *Mobile Networks and Applications*, 1-13.

Eiza, Mahmoud Hashem, Ni, Qiang, Owens, Thomas, and Min, Geyong. (2013). Investigation of routing reliability of vehicular ad hoc networks. *EURASIP journal on wireless communications and networking,* 2013(1), 179.

Elsadig, Muawia Abdelmagid, and Fadlalla, Yahia A. (2016). VANETs security issues and challenges: A survey. *Indian Journal of Science and Technology,* 9(28).

Engoulou, Richard Gilles, Bellaïche, Martine, Pierre, Samuel, and Quintero, Alejandro. (2014). VANET security surveys. *Computer Communications,* 44, 1-13.

Eze, Elias C, Zhang, Sijing, and Liu, Enjie. (2014). Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward. In *Automation and Computing (ICAC), 2014 20th International Conference*.

Feiri, Michael, Pielage, Rolf, Petit, Jonathan, Zannone, Nicola, and Kargl, Frank. (2015). Pre-distribution of certificates for pseudonymous broadcast authentication in VANET. In *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st.*

Feng, Xia, Li, Chun-yan, Chen, De-xin, and Tang, Jin. (2016). A Method for Defensing against Multi-source Sybil Attacks in VANET. *Peer-to-Peer Networking and Applications*, 1-10.

Fuentes, José María de, González-Tablas, Ana Isabel, and Ribagorda, Arturo. (2010). Overview of Security Issues in Vehicular Ad-Hoc Networks.

Garcia, Estrella, Campo, Celeste, Garcia-Rubio, Carlos, and Rodriguez-Carrion, Alicia. (2016). A Bandwidth-Efficient Dissemination Scheme of Non-Safety Information in Urban VANETs. *Sensors,* 16(7), 988.

Ghosh, Mainak, Varghese, Anitha, Kherani, Arzad A, and Gupta, Arobinda. (2009). Distributed Misbehavior Detection in VANETs. In *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE.*

Giannetsos, Thanassis, and Dimitriou, Tassos. (2014). LDAC: A localized and Decentralized Algorithm for Efficiently Countering Wormholes in Mobile Wireless Networks. *Journal of Computer and System Sciences, 80*(3), 618-643.

Gosman, Catalin, Dobre, Ciprian, and Cristea, Valentin. (2010). A Security Protocol for Vehicular Distributed Systems. In *Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2010 12th International Symposium*.

Goyal, Sweety, and Rohil, Harish. (2013). Securing MANET against Wormhole Attack using Neighbor Node Analysis. *International Journal of Computer Applications,* 81(18), 44-48.

Grover, Jyoti, Kumar, Deepak, Sargurunathan, M, Gaur, Manoj Singh, and Laxmi, Vijay. (2010). Performance Evaluation and Detection of Sybil Attacks in Vehicular Ad-Hoc Networks. *Recent Trends in Network Security and Applications*, 473-482.

Grover, Jyoti, Laxmi, Vijay, and Gaur, Manoj Singh. (2014). Sybil Attack Detection in VANET using Neighbouring Vehicles. *International Journal of Security and Networks,* 9(4), 222-233.

Hassan, Jahan, and Jha, Sanjay. (2004). On the Optimization Trade-offs of Expanding Ring Search. In *International Workshop on Distributed Computing.*

Hossain, Md Shohrab, and Atiquzzaman, Mohammed. (2009). Stochastic Properties and Application of City Section Mobility Model. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE.*

Hussain, Rasheed, and Oh, Heekuck. (2014). On Secure and Privacy-Aware Sybil Attack Detection in Vehicular Communications. *Wireless personal communications,* 77(4), 2649-2673.

Institute of Transportation Systems Berlin. (2013). Simulation of Urban MObility (SUMO). from http://www.dlr.de/ts/en/desktopdefault.aspx/tabid-9883/16931_read-41000/

Isaac, Jesús Téllez, Zeadally, Sherali, and Camara, José Sierra. (2010). Security Attacks and Solutions for Vehicular Ad hoc Networks. *IET communications,* 4(7), 894-903.

Jaiswal, Kriti, and Prakash, Om. (2014). An analysis of vanet topology based routing approach on various parameters. *International Journal of Computer Science and Information Technologies,* 5(4), 4975-4980.

Jamali, Shahram, and Fotohi, Reza. (2016). Defending against Wormhole Attack in MANET Using an Artificial Immune System. *New Review of Information Networking,* 21(2), 79-100.

Jayapal, Cynthia, and Roy, S Sujith. (2016). Road traffic congestion management using VANET*.* In *Advances in Human Machine Interaction (HMI), 2016 International Conference*.

Jayavel, J, Venkatesan, R, and Ponmudi, S. (2014). A TDMA-Based Smart Clustering Technique for VANETS. *Journal of Theoretical and Applied Information Technology,* 65(2).

Ji, Shiyu, Chen, Tingting, and Zhong, Sheng. (2015). Wormhole attack detection algorithms in wireless network coding systems. *IEEE Transactions on Mobile Computing,* 14(3), 660-674.

Jiang, Daniel, and Delgrossi, Luca. (2008). IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE.*

Jiang, Qiangfeng, and Manivannan, D. (2016). Triangle-based routing for mobile ad hoc networks. *Pervasive and Mobile Computing,* 33, 108-126.

Kaddoura, Maher, Ramanujan, Ranga, and Schneider, Steven. (2005). Routing optimization techniques for wireless ad hoc networks. In *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-*

Assembling Wireless Networks. SNPD/SAWN 2005. Sixth International Conference.

Karagiannis, Georgios, Altintas, Onur, Ekici, Eylem, Heijenk, Geert, Jarupan, Boangoat, Lin, Kenneth, and Weil, Timothy. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys and Tutorials,* 13(4), 584-616.

Karnadi, Feliz Kristianto, Mo, Zhi Hai, and Lan, Kun-chan. (2007). Rapid generation of realistic mobility models for VANET. In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*.

Kerrache, Chaker Abdelaziz, Lagraa, Nasreddine, Calafate, Carlos T, Cano, Juan-Carlos, and Manzoni, Pietro. (2016). T-VNets: A novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS. *Computer Communications,* 93, 68-83.

Khan, Junaid Ahmed, Ghamri-Doudane, Yacine, and Botvich, Dmitri. (2016). Autonomous Identification and Optimal Selection of Popular Smart Vehicles for Urban Sensing—An Information-Centric Approach. *IEEE Transactions on Vehicular Technology,* 65(12), 9529-9541.

Kim, Dong-uk, Kim, Hyo-won, Kim, Gisung, and Kim, Sehun. (2013). A Counterattack-Detection Scheme in Transmission Time-Based Wormhole Detection Methods. *International Journal of Distributed Sensor Networks,* 9(3), 184931.

Kim, Young-Dong, and Kim, Dong-Ill. (2013). IDS Scheme for Blackhole Attack on MANETs. *Future Information Communication Technology and Applications* (pp. 863-870): Springer.

Koutsonikolas, Dimitrios, Das, Saumitra M, Pucha, Himabindu, and Hu, Y Charlie. (2005). On optimal TTL sequence-based route discovery in MANETs. In *Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference*.

Kumar, Ankit, and Sinha, Madhavi. (2014). Overview on vehicular ad hoc network and its security issues. In *Computing for Sustainable Global Development (INDIACom), 2014 International Conference*.

Kumar, G Vijaya, Reddyr, Y Vasudeva, and Nagendra, Dr M. (2010). Current research work on routing protocols for MANET: a literature survey. *international Journal on computer Science and Engineering,* 2(03), 706-713.

Kumar, Kuldeep, and Arora, Sandeep Kumar. (2016). Review of Vehicular Ad Hoc Network Security. *International Journal of Grid and Distributed Computing,* 9(11), 17-34.

Kumar, Naveen, and Shakar, Arun. (2017). Classification and Analysis of various VANET Security Attacks. *International Journal of Security and Usability,* 1(1).

Kumar, Neeraj, and Chilamkurti, Naveen. (2014). Collaborative trust aware intelligent intrusion detection in VANETs. *Computers and Electrical Engineering,* 40(6), 1981-1996.

Kumari, S Vadhana, and Paramasivan, B. (2017). Defense against Sybil attacks and authentication for anonymous location-based routing in MANET. *Wireless Networks*, 1-12.

La Vinh, H., & Cavalli, A. R. (2014). Security attacks and solutions in vehicular ad hoc networks: a survey. *International journal on AdHoc networking systems (IJANS),* 4(2), 1-20.

Lal, Anu S, and Nair, Reena. (2015). Region authority based collaborative scheme to detect Sybil attacks in VANET*.* In *Control Communication and Computing India (ICCC), 2015 International Conference*.

Lang, Dominik, Corbett, Christopher, and Kargl, Frank. (2016). Security Evolution in Vehicular Systems*.* In *Fachgespräch Inter-Vehicle Communication 2016-(inter-veh-comm-2016).*

Lee, ByungKwan, and Jeong, EunHee. (2016). A Black Hole Detection Protocol Design based on a Mutual Authentication Scheme on VANET. *KSII Transactions on Internet and Information Systems,* 10(3).

Lee, ByungKwan, Jeong, EunHee, and Jung, Ina. (2013). A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET. *International Journal of Security and Its Applications,* 7(3), 1-10.

Lee, Uichin, and Gerla, Mario. (2010). A survey of urban vehicular sensing platforms. *Computer Networks,* 54(4), 527-544.

Lee, Uichin, Magistretti, Eugenio, Gerla, Mario, Bellavista, Paolo, and Corradi, Antonio. (2009). Dissemination and harvesting of urban data using vehicular sensing platforms. *IEEE Transactions on Vehicular Technology,* 58(2), 882-901.

Leinmuller, Tim, Schmidt, Robert K, Schoch, Elmar, Held, Albert, and Schafer, Gunter. (2008). Modeling roadside attacker behavior in VANETS*.* In *GLOBECOM Workshops, 2008 IEEE.*

Li, Chun-Ta, Hwang, Min-Shiang, and Chu, Yen-Ping. (2008). A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communications,* 31(12), 2803-2814.

Li, Wenjia, and Song, Houbing. (2016). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems,* 17(4), 960-969.

Lim, Joanne Mun-Yee, Chang, YoongChoon, Alias, MohamadYusoff, and Loo, Jonathan. (2015). Performance Modelling of Adaptive VANET with Enhanced Priority Scheme. *KSII Transactions on Internet and Information Systems (TIIS),* 9(4), 1337-1358.

Lo, Shou-Chih, Gao, Jhih-Siao, and Tseng, Chih-Cheng. (2013). A water-wave broadcast scheme for emergency messages in VANET. *Wireless personal communications,* 71(1), 217-241.

Maglaras, Leandros A. (2015). A novel distributed intrusion detection system for vehicular ad hoc networks. *International Journal of Advanced Computer Science and Applications (IJACSA),* 6(4), 101-106.

Mann, Navkiran, and Kumar, Neeraj. (2015). An Enhanced Secure Authentication Scheme for Vehicular Ad Hoc Networks *Emerging Research in Computing, Information, Communication and Applications* (pp. 335-343): Springer.

Maurya, Prashant Kumar, Sharma, Gaurav, Sahu, Vaishali, Roberts, Ashish, Srivastava, Mahendra, and Scholar, M. (2012). An overview of AODV routing protocol. *International Journal of Modern Engineering Research (IJMER),* 2(3), 728-732.

Mejri, Mohamed Nidhal, Ben-Othman, Jalel, and Hamdi, Mohamed. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications,* 1(2), 53-66.

Mokhtar, Bassem, and Azab, Mohamed. (2015). Survey on security issues in vehicular ad hoc networks. *Alexandria Engineering Journal,* 54(4), 1115-1126.

Nadeem, Adnan, and Howarth, Michael P. (2014). An intrusion detection and adaptive response mechanism for MANETs. *Ad Hoc Networks,* 13, 368-380.

Nagaraj, Uma, Kharat, MU, and Dhamal, Poonam. (2011). Study of various routing protocols in VANET. *IJCST,* 2(4), 45-52.

Neha, Roy, and Bevish, Jinila Y. (2015). A survey on security challenges and malicious vehicle detection in vehicular ad hoc networks. *Contemporary Engineering Sciences,* 8(5), 235-240.

OMNet++. (2015). What is OMNeT++?, from https://omnetpp.org/intro

Organization, World Health. (2013). Global status report on road safety 2013: supporting a decade of action: summary.

Papadimitratos, Panagiotis, Buttyan, Levente, Holczer, Tamás, Schoch, Elmar, Freudiger, Julien, Raya, Maxim, Hubaux, Jean-Pierre. (2008). Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine,* 46(11).

Park, Soyoung, Aslam, Baber, Turgut, Damla, and Zou, Cliff C. (2013). Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. *Security and Communication Networks,* 6(4), 523-538.

Patel, Dhyey, Faisal, Mohd, Batavia, Priyanka, Makhija, Sidharth, and Mani, M. (2016). Overview of routing protocols in vanet. *Int. J. Comput. Appl,* 136(9), 4-7.

Pattnaik, Omkar, and Pattanayak, Binod Kumar. (2014). Security in vehicular ad hoc network based on intrusion detection system. *American Journal of Applied Sciences,* 11(2), 337.

Paul, Bijan, and Islam, Mohammed J. (2012). Survey over VANET routing protocols for vehicle to vehicle communication. *IOSR Journal of Computer Engineering (IOSRJCE), ISSN*, 2278-0661.

Peng, Ya Li, Yin, Hong, and Yu, Peng. (2014). The Research of Bus VANET Protocol on Signal Attenuation and Delay Probability of Multi-Hop Forwarding. In *Advanced Materials Research*, 1030-1032, pp. 1841-1845, 201

Premasudha, BG, Ram, V Ravi, Miller, J, and Suma, R. (2016). A Review of Security Threats, Solutions and Trust Management in VANETs. *International Journal of Next-Generation Computing,* 7(1), 38-57.

Priyadharshini, C, and ThamaraiRubini, K. (2012). Predicting route lifetime for maximizing network lifetime in MANET. In *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference*.

Qazi, Shams, Raad, Raad, Mu, Yi, and Susilo, Willy. (2013). Securing DSR against wormhole attacks in multirate ad hoc networks. *Journal of Network and Computer Applications,* 36(2), 582-592.

Qian, Yi, and Moayeri, Nader. (2008). Design of secure and application-oriented VANETs. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE.*

Quyoom, Abdul, Ali, Raja, Gouttam, Devki Nandan, and Sharma, Harish. (2015). A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA). In *Computing, Communication and Automation (ICCCA), 2015 International Conference*.

Rasheed, Asim, Gillani, Saira, Ajmal, Sana, and Qayyum, Amir. (2017). Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications *Vehicular Ad-Hoc Networks for Smart Cities* (pp. 39-51): Springer.

Ratnani, Chandan, Vaghela, VB, and Shah, DJ. (2015). *A novel architecture for vehicular traffic control.* Paper presented at the Computational Intelligence and Communication Technology (CICT), 2015 IEEE International Conference on.

Rawat, Chandraprabha. (2014). Wormhole Attack Detection Protocol using Time Stamp with Security Packet. *International Journal of Computer Science and Information Technologies,* 5(1), 621-626.

Rehman, Sabih, Khan, M Arif, Zia, Tanveer A, and Khokhar, Rashid H. (2013). A synopsis of simulation and mobility modeling in vehicular ad-hoc networks (VANETs). *IOSR Journal of Computer Engineering (IOSR-JCE),* 15(2), 1-16.

Reina, DG, Toral, SL, Johnson, P, and Barrero, F. (2015). A survey on probabilistic broadcast schemes for wireless ad hoc networks. *Ad Hoc Networks,* 25, 263-292.

Saggi, Mandeep Kaur, and Kaur, Ranjeet. (2015). Isolation of Sybil attack in VANET using neighboring information. In *Advance Computing Conference (IACC), 2015 IEEE International.*

Sales, Thiago Bruno M, Perkusich, Angelo, de Sales, Leandro Melo, de Almeida, Hyggo Oliveira, Soares, Gustavo, and de Sales, Marcello. (2016). ASAP-V: A privacy-preserving authentication and sybil detection protocol for VANETs. *Information Sciences,* 372, 208-224.

Samara, Ghassan, Al-Salihy, Wafaa AH, and Sures, R. (2010). Security analysis of vehicular ad hoc nerworks (VANET). In *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference*.

Sarakis, Lambros, Orphanoudakis, Theofanis, Leligou, Helen C, Voliotis, Stamatis, and Voulkidis, Artemis. (2016). Providing entertainment app lications in VANET environments. *IEEE Wireless Communications,* 23(1), 30-37.

Satheesh, N, and Prasadh, K. (2014). Trust based ad hoc on demand distance vector routing protocol against wormhole attack. *Journal of Theoretical and Applied Information Technology,* 70(3).

Sedjelmaci, Hichem, and Senouci, Sidi Mohammed. (2015). An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Computers and Electrical Engineering,* 43, 33-47.

Sedjelmaci, Hichem, Senouci, Sidi Mohammed, and Abu-Rgheff, Mosa Ali. (2014). An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. *IEEE Internet of Things Journal,* 1(6), 570-577.

Shahabi, Sina, Ghazvini, Mahdieh, and Bakhtiarian, Mehdi. (2016). A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wireless Networks,* 22(5), 1505-1511.

Shakshuki, Elhadi M, Kang, Nan, and Sheltami, Tarek R. (2013). EAACK—a secure intrusion-detection system for MANETs. *IEEE Transactions on Industrial Electronics,* 60(3), 1089-1098.

Sheltami, Tarek, Basabaa, Abdulsalam, and Shakshuki, Elhadi. (2014). A3ACKs: adaptive three acknowledgments intrusion detection system for MANETs. *Journal of Ambient Intelligence and Humanized Computing,* 5(4), 611-620.

Shin, Jongho, Baek, Youngmi, and Son, Sang H. (2016). Fundamental Topology-Based Routing Protocols for Autonomous Vehicles. *In Embedded and Real-Time Computing Systems and Applications (RTCSA), 2016 IEEE 22nd International Conference*.

Shukla, Dilendra, Vaibhav, Akash, Das, Sanjoy, and Johri, Prashant. (2016). Security and attack analysis for vehicular ad hoc network—A survey. In *Computing, Communication and Automation (ICCCA), 2016 International Conference*.

Simaremare, Harris, Abouaissa, Abdelhafid, Sari, Riri Fitri, and Lorenz, Pascal. (2013). Secure AODV routing protocol based on trust mechanism. *Wireless Networks and Security* (pp. 81-105): Springer.

Sundararajan, TVP, Ramesh, SM, Maheswar, R, and Deepak, KR. (2014). Biologically inspired artificial intrusion detection system for detecting wormhole attack in MANET. *Wireless Networks,* 20(4), 563-578.

Torrent, Marc, Santi, Paolo, and Hartenstein, Hannes. (2005). Fair sharing of bandwidth in VANETs. In *Proceedings of the 2nd ACM International Workshop on Vehicular Ad hoc Networks.*

Trullols, O, Fiore, Marco, Casetti, Claudio, Chiasserini, Carla-Fabiana, and Ordinas, JM Barcelo. (2010). Planning roadside infrastructure for information dissemination in intelligent transportation systems. *Computer Communications,* 33(4), 432-442.

Varga, András, and Hornig, Rudolf. (2008). *An overview of the OMNeT++ simulation environment.* In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems workshops.*

Veins. (2017). What can Veins do?, from http://veins.car2x.org/

Whaiduzzaman, Md, Sookhak, Mehdi, Gani, Abdullah, and Buyya, Rajkumar. (2014). A survey on vehicular cloud computing. *Journal of Network and Computer Applications,* 40, 325-344.

Yang, Kun, Ou, Shumao, Chen, Hsiao-Hwa, and He, Jianghua. (2007). A multihop peer-communication protocol with fairness guarantee for IEEE 802.16-based vehicular networks. *IEEE Transactions on Vehicular Technology,* 56(6), 3358-3370.

Yu, Bo, Xu, Cheng-Zhong, and Xiao, Bin. (2013). Detecting sybil attacks in VANETs. *Journal of Parallel and Distributed Computing,* 73(6), 746-756.

Zaidi, Kamran, Milojevic, Milos B, Rakocevic, Veselin, Nallanathan, Arumugam, and Rajarajan, Muttukrishnan. (2016). Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection. *IEEE Transactions on Vehicular Technology,* 65(8), 6703-6714.

Zeadally, Sherali, Hunt, Ray, Chen, Yuh-Shyan, Irwin, Angela, and Hassan, Aamir. (2012). Vehicular ad hoc networks (VANETS): status, results, and challenges. *Telecommunication Systems,* 50(4), 217-241.