ENHANCEMENT OF SECURITY (ATTACK) IN VANET

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

DILJOT KAUR

11509863

Supervisor

SIMARJIT SINGH MALHI

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

May 2017

May 2017

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE546 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0011

Supervisor Name : Simarjit Singh Malhi **UID :** 15976 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Diljot Kaur	11509863	2015	K1519	9501397297

SPECIALIZATION AREA : Networking and Security **Supervisor Signature:** _____

PROPOSED TOPIC : Enhancement Of Security (Attack) In VANET

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	Parameter	Rating (out of 10)
1	Project Novelty: Potential of the project to create new knowledge	6.60
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	6.80
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.80
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.00
5	Social Applicability: Project work intends to solve a practical problem.	6.80
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.60

PAC Committee Members		
PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Pushpendra Kumar Paterlya	UID: 14623	Recommended (Y/N): Yes
PAC Member 3 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 4 Name: Kewal Krishan	UID: 11179	Recommended (Y/N): Yes
PAC Member 5 Name: Anupinder Singh	UID: 19385	Recommended (Y/N): NA
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

Final Topic Approved by PAC: Enhancement Of Security (Attack) In VANET

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11024::Amandeep Nagpal **Approval Date:** 05 Mar 2017

4/25/2017 12:36:02 PM

ABSTRACT

Vehicular ad-hoc network (VANET) is one of the recent and promising technologies to revolutionize the transportation system where vehicles can communicate by exchanging messages via wireless medium. It has received a lot of interest in the last few years. But still there are many issues that need to be resolved for its betterment and use in the transportation system. Though, security is of major concern whenever we talk about communication between entities in a network, therefore it needs to be addressed perfectly. In my dissertation-2, I present a security enhancement which when deployed will produce efficient results in the detection and prevention of malicious nodes in the system. With the detection of malicious nodes in the system, we will reduce the risk by selection of the trusted nodes and hence will increase system availability.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled "ENHANCEMENT OF SECURITY (ATTACK) IN VANET" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Simarjit Singh Malhi. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Diljot Kaur

R.No. 11509863

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled **"ENHANCEMENT OF SECURITY (ATTACK) IN VANET"** submitted by **Diljot Kaur** at **Lovely Professional University, Phagwara, India** is a bonafide record of his / her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

(Simarjit Singh Malhi)

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: _____
   HoD Name: _____
   Date: _____
2) **Neutral Examiners:**

External Examiner

Signature: _____

Name: _____

Affiliation: _____

Date: _____

Internal Examiner

Signature: _____

Name: _____

Date: _____

ACKNOWLEDGEMENT

I would like to take an opportunity to express my deep regard and thankfulness to all those who assisted me directly or indirectly during the dissertation work. Firstly, I would like to thank my supervisor, Mr. Simarjit Singh Malhi who helped me throughout the dissertation work. Without his guidance and support, it would not have been possible for me get to the right track and complete my dissertation work. His advice, encouragement and critics are source of innovative ideas, inspiration and causes behind the successful completion of this dissertation.

Faculty members of computer science and engineering department were also very supportive and helpful. Their encouragement and support to all the students is appreciable. I am highly obliged to work in such a cooperative environment and thankful to all the faculty members for their assistance.

I would also like to thank all my friends for their encouragement, consistent support and invaluable suggestions at the time I needed the most. I am grateful to my family for their love, support and prayers.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AODV	**Ad-Hoc on Demand Distance Vector Routing**
DSDV	**Destination Sequenced Distance Vector Routing**
DSRC	**Dedicated Short Range Communication**
GPS	**Global Positioning System**
LAN	**Local Area Network**
MAC	**Media Access Control**
MAN	**Metropolitan Area Network**
OBU	**On-Board Unit**
OFDM	**Orthogonal Frequency Division Multiplexing**
PKI	**Public Key Infrastructure**
RSU	**Road Side Unit**
WAN	**Wide Area Network**
WAVE	**Wireless Access in vehicular Environment**
WAN	**Wide Area Network**
WAVE	**Wireless Access in vehicular Environment**
VANET	**Vehicular Ad-Hoc Network**
V2V	**Vehicle to Vehicle**
V2I	**Vehicle to Infrastructure**
ITS	**Intelligent Transportation System**

LIST OF FIGURES

FIGURE NO:FIGURE DESCRIPTION **PAGE NO.**

LIST OF TABLES

TABLE NO:TABLE DESCRIPTION **PAGE NO.**

CHAPTER 1
INTRODUCTION

1.1 Introduction

A computer network is a telecommunication network or framework associated together with the end goal of sharing resources. Today the assets are also shared with the help of internet. Printer or a file server are the other shared resources. Nowadays, the internet itself considered a big computer network. There are so many resources that help in sharing the resources between the nodes like PCs, telephones, servers and other organizing equipment. Computer systems give a huge number of uses and administrations, for example, access to the World Wide Web, computerized video, advanced sound, shared utilization of use and capacity servers, printers, and fax machines, and utilization of email and texting applications and also many others. The Computer network can be divided into two types:

1) **Wired**
2) **Wireless**

Endeavors worldwide for setting up their organizations overall require frameworks. We can take the illustration of banking framework. With the distinctive servers show at better places they can exchange data adequately without over-burdening a singular server. In addition, they give and handle client questions and demand successfully and if one server gets down because of some reason, then different servers share it's workload with the goal of smooth working of the framework [43]. For setting up the associations, Ethernet links i.e. wired system or with the assistance of radio frequencies that can associate their frameworks overall i.e. remote systems.

A wired home system utilizes Ethernet link to associate the PCs to the system router. Wired home systems are more affordable, speedier, and more secure than remote systems. A remote home system gives the adaptability to associate your PCs to networks adaptor gadgets. But in today's most of the organization giving preferences to the wireless network over wired network. In advanced technology, we can easily handle the errors and improve the

security and privacy. A system must have the capacity to meet certain criteria; these are Performance, Reliability and Scalability. So picking remote systems is an entirely decent decision because, with the progressions, these sorts of existing dangers have been evacuated and controlled up to much degree.

1.2 Wired Networks

Wired networks mean that they are used cables to connecting the different systems with each other. A wired setup utilizes physical links to exchange information between various gadgets [39]. These are also known as the Ethernet cables. A wired system utilizes Ethernet link to associate the PCs to the system router. Wired home systems are more affordable, speedier, and more secure than remote systems. Comprehensively we have three topologies, the names of these topologies are given below (refer Figure 1.1):

1) **Star topology**
2) **Bus topology**
3) **Ring topology**

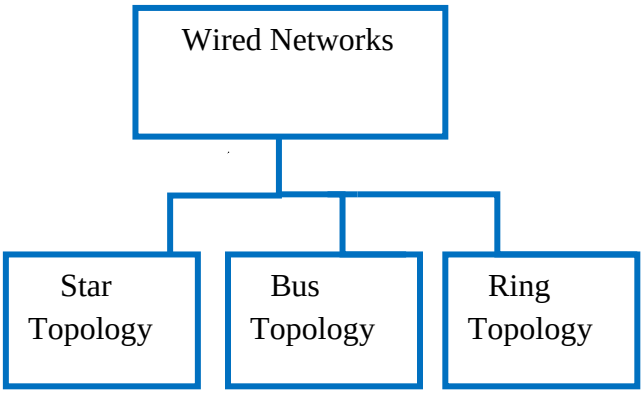


Figure 1.1: Wired Network Classification [39]

Star topology

A star topology is a topology that is used for a LAN (local area networks). It is known as the first-star topology in which all the Pcs are connected to a centralized device that is known as the single server. A Centralized system is responsible for sharing all types of

information. The fundamental preferences of a star system are that one breaking down hub does not influence whatever is left of the system so, if a link flops, just a single hub will be cut down. The main problem of this type of network is if the server is down then the system stops to work.

Bus topology

Bus topology is a second topology in which every PC and system gadget are associated with a single link or cable. It functions admirably when you have a little system. It requires less link length than a star topology [40]. The disadvantages of this type of systems are hard to recognize the issues if the entire system goes down. Only one system at one point able to send the data if at any time two systems send the data at the same time then they collide with each other and destination fails to receive data from any of this system.

Ring topology

In the last, we have ring topology. Ring topology works same like star topology. A ring topology is a PC arranges setup where the gadgets are associated with each other in a circular or ring shape [44]. The data is sent around the ring until it achieves its last goal. Ring topologies are utilized as a part of both LAN and WAN setups. The ring topology was most regularly utilized as a part of schools, workplaces, and littler structures where systems were littler. All information being exchanged over the system must go through every workstation on the system, which makes it slower than a star topology. The whole system will be affected in the event if one workstation closes down.

1.3 Wireless Networks

A remote system access applications and data without wires. This gives flexibility, movement of applications to various parts of a building, city or about any place in the world. Remote systems permit individuals to cooperate with email or use the Internet from any area from where they want [41]. So the establishment of wiring is absent in these systems. This correspondence is favored by homes, undertakings including both little and huge ones to avoid wires and thus, utilize the remote systems.

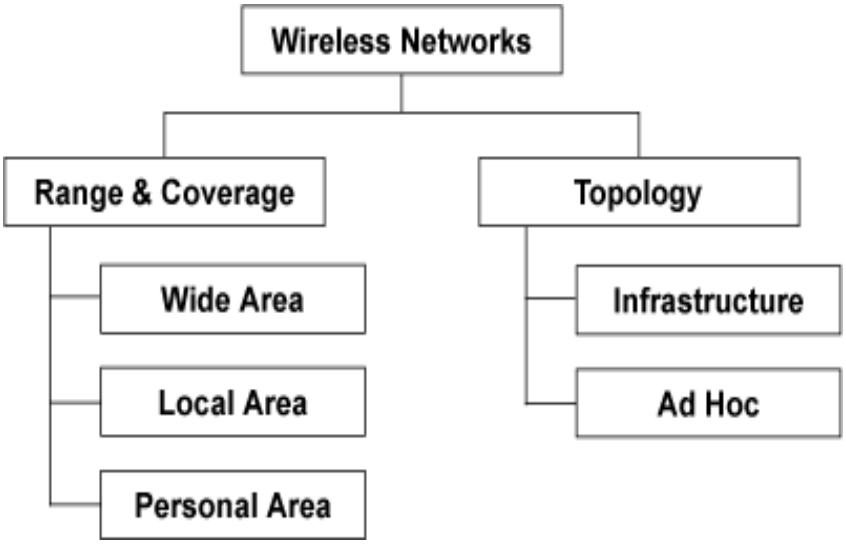


Figure 1.2: Wireless Network Classification [41]

The remote systems depend on radio waves to send and get information. Remote systems utilize radio waves to connect gadgets such as when we connect a laptop to the internet and for business applications. Wireless networks can be classified into two categories (refer Figure 1.2).

1) Range and Coverage based

Wireless WANs: These types of remote networks cover large ranges, for example, between towns and urban areas or city and suburb. In this, all types of communication are maintained by satellites or antennas. Networks are based upon 2G and overall network is administered by ISP. The performance issue is still there.

Wireless MANs: These types of remote networks cover cities, that connect various LAN. It is also known as fixed wireless based infrastructure networks.

Wireless LANs: These types of remote networks cover small areas or building, i.e., when we were connecting to the internet inside the university campus. It covers up to 100m range. The utilization of spread-range or OFDM technologies may permit clients to move inside a local area zone and still stay connected with the system.

Wireless PANs: These types of remote networks cover very small areas, i.e., Bluetooth and infrared communication. It covers up to 30m range only.

2) Topology Based

Infrastructure based Networks: These types of networks in which we have the access point. In this, all the communication are done through the access point. It requires centralized access point for connection and to transfer data from one system to another system. Without access point, communication can't take place.

Ad Hoc Networks: These types of networks in which we do not need an access point. In this, all the communication are done directly. It does not requires centralized access point for connection and to transfer data from one system to another system, the data directly transfer between the system. In this without an access point, communication held. Ad Hoc networks can easily be installed as compared to infrastructure-based networks.

Now I would explain my Research area, i.e., VANET in which I am doing my research work after explaining broad topic explanation, computer networks, and its types wired and wireless and all the topologies that are required for the network.

1.4 Introduction to VANET

Vehicular Ad-hoc Network is a class of MANET. Vehicular Ad hoc Network delivers secure and non-secure information to the drivers. In today's scenario transportation system plays a vital role [42]. Traffic safety has been the main concern for many countries. Many accidents are caused by insufficient traffic information and by slow driver reaction to local visual and acoustic inputs. VANETs (Vehicular Ad-hoc Networks) overcome these problems by enhancing both the accuracy of traffic information and the delivery of alarms, thus provide help to avoid crashes. In VANET, cars commune through the help of wireless channel. They send packets straight forward to their neighbors inward radio range. Alternatively, intermediary cars route and forward packets to destinations. Communication is peer-to-peer, without centralized coordination. In VANETs, cars can exchange routine information such as current speeds, locations, directions, as well as emergency alarms like notifications of emergency braking, etc. With VANETs, cars can collect more accurate traffic information electronically.

VANETs are becoming the most relevant wireless mobile technology. It's one of the more capable to employ Intelligent Transportation Systems (ITS). VANETs are different from MANETs regarding high node mobility, large-scale networks, a geographically constrained topology that is highly dynamic, strict real-time deadline, unreliable channel conditions, unavoidably slow deployment, uneven connectivity between nodes, driver behavior and frequent network fragmentation. A VANET is a particular kind of Mobile Ad-hoc network (MANET) that delivers messages in between a nearby motor vehicles and roadside equipment. There are two categories of nodes: On-Board Units (OBU) and Roadside Units (RSU). OBU provides the communication capabilities among the vehicles, while RSUs are placed along the road and constitute the network infrastructure. RSUs work as a router between the vehicles. With the use of Dedicated Short Range Communication (DSRC) radios, OBUs can link the vehicle to RSUs.

1.5 Applications of VANET Security

The safety of Vehicular Ad-hoc Network is most serious problems. VANETS, applications play an important role that is categorized into:

- **Safety Related Application:**

Related to the safety of the user. These are further classified into three:

Collision Avoidance: From some examination, 60% mishaps can be rid off if drivers get cautioning a moment before the crash. On the off chance that a driver gets a notice message on time, a crash can be avoided**.**

Cooperative Driving: If drivers can get the indication for activity related notices like varying speed warning. These signs can participate in safe driving.

Traffic Optimization: Maximized with the use of transferring signals like jam, accidents, etc. to the vehicles.

• **User Based Application**:

Supplies the customer infotainment.These are classified in the following ways:

Peer to peer application: are functional to facilities like distributing songs, movies, etc. between the motor vehicles in the system.

Internet Connectivity: User required to interrelate the web constantly (internet all the time).

Other services: Utilized in another user by application alike payment examine to gather the toll assessment, to find the position of petroleum station, eating place, etc.

1.6 Intelligent Transportation Systems

Intelligent transportation systems (ITS) (refer Figure 1.3) is the best application of Vehicular Ad-hoc network of Vehicle-to-vehicle and vehicle-to-infrastructure communication based upon LAN (local area network). The problem of traffic and congestion are increasing day by day. OBU provides the communication capabilities among the vehicles, while RSUs are placed along the road and constitute the network infrastructure. RSUs work as a router between the vehicles [46]. Communication is done in between the vehicle to vehicle, vehicle to road side unit and road side unit to road side unit.

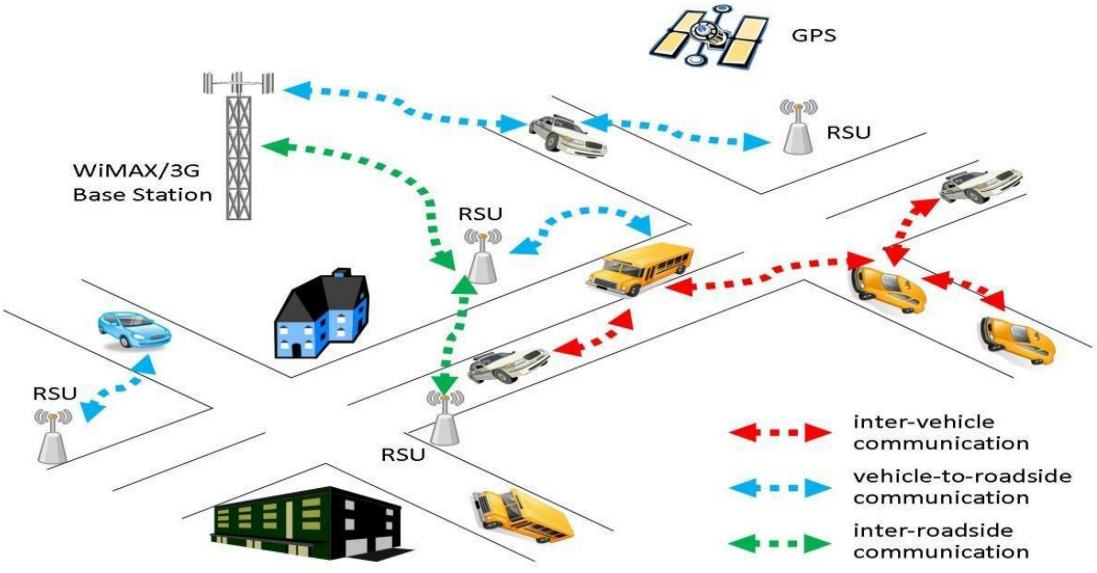


Figure 1.3: Vehicular communication systems [46]

ITS applications are infotainment and comfort, traffic management, road safety and autonomous driving.

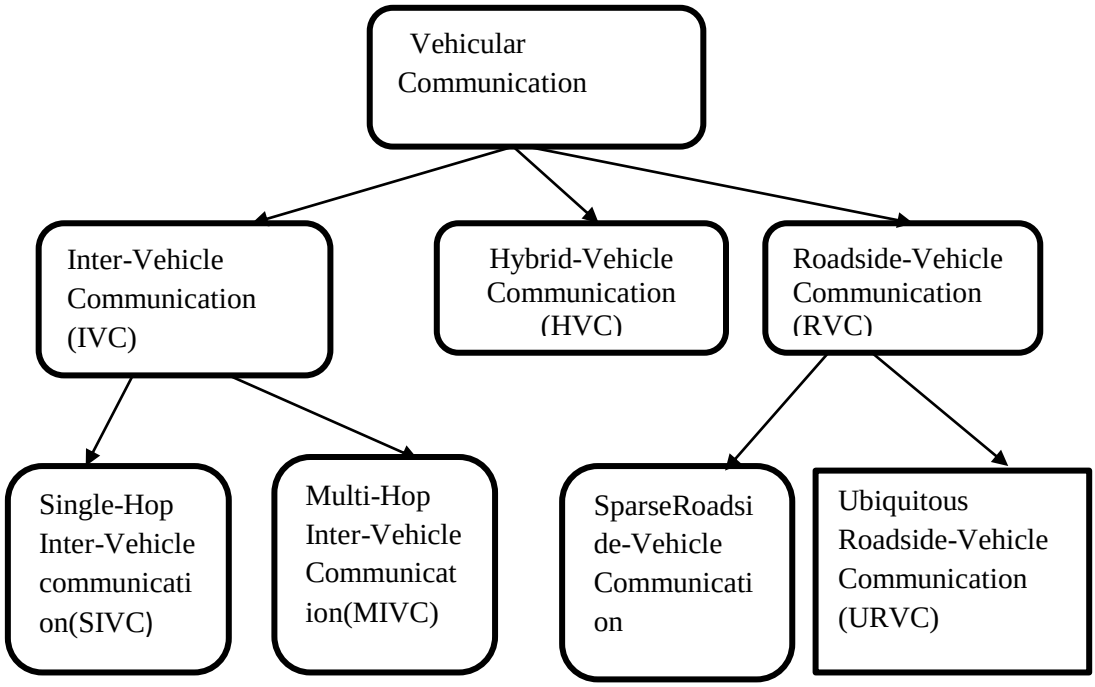


Figure 1.4: Vehicular communication

- **Inter-Vehicle Communication**

Inter-vehicle communication mainly focuses on the vehicle communication without the help of roadside unit (RSU). IVC (inter-Vehicle communication) is mainly a single-hop network and multi-hop networks. It is a infrastructure-free network only sometimes we needed the OBU (on-board unit). The main differences between the SIVC and MIVC are Single-hop inter-vehicle communication (SIVC) is used in short range type communication but MIVC used for large range communication.

SIVC: It sends a message to only that vehicle which is in the range of transmission.

MIVC: It sends a message to that vehicle also which are not in the range of transmission.

- **Roadside-to-Vehicle Communication Systems**

All the communication are done in between Roadside unit and OBU. Two types of infrastructure are there SRVC and URVC.

SRVC: It helps in communication with the help of hot spots. It gives information about accidents, prices of a gas station and availability of parking.

URVC: It is one type of high-speed communication which requires full investment for the coverage of all road-side unit.

- **Hybrid Vehicular Communication Systems**

HVC helps in extend the range of roadside-vehicle communication (RVC). Helps in increase the connectivity or range of RVC.

1.7 VANET Standards

Standards are simplifying the results of new products by comparing it with the results of old or already developed products. Many types of standards that are available for different like routing in VANET, security in VANET (standards are needed for radio access for communication in Vehicle-to-vehicle, Vehicle-to-roadside unit and roadside unit to roadside unit [45]. The main motive of standards to secure the functionality of a Vehicular Ad-hoc network by providing the safety of the driver, improvement in traffic and reduce the number of accidents.

Dedicated Short Range Communication (DSRC)

Europe and Japan in 2003 developed the dedicated short range communication. It helps in vehicle-to-vehicle and vehicle-to-infrastructure communication. DSRC (refer Figure 1.5) is short to medium range communication. Based on IEEE 802.11p standard which derived earlier from IEEE 802.11a standard. Low overhead is the main function of dedicated short range communication. It helps in giving the information of traffic, accidents and about the conditions of roads. WAVE Communication are held with the help of On-Board Units (OBU) and Roadside Units (RSU). OBU provides the communication capabilities among the vehicles, while RSUs are placed along the road and constitute the network infrastructure.

RSUs work as a router between the vehicles. With the use of Dedicated Short Range Communication (DSRC) radios, OBUs can link the vehicle to RSUs.

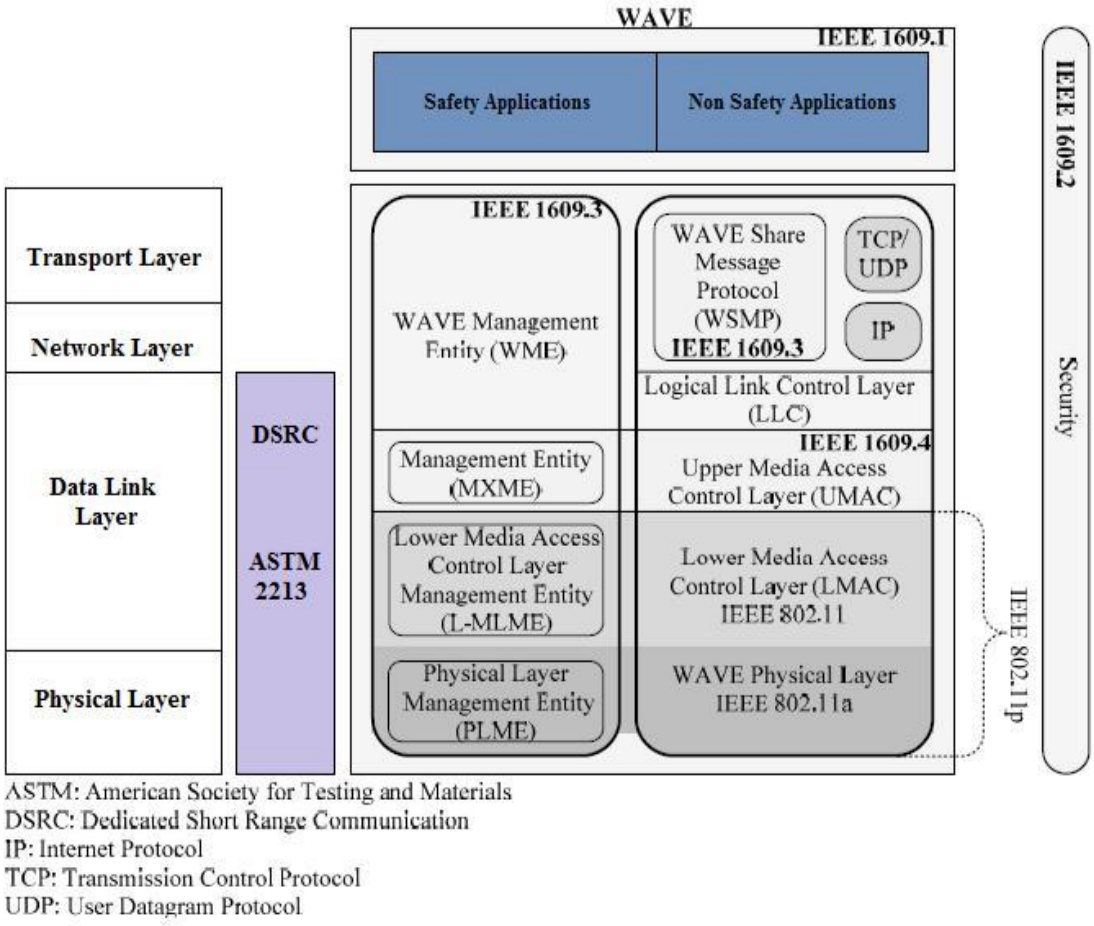


Figure 1.5: WAVE/DSRC [45]

In WAVE two types of application are there first one is safety-related application and second one non-safety related application. In DSRC IEEE standards are handled by the upper layers. In this manner, IEEE 802.11a standard moved to IEEE standard 802.11p and renamed DSCR as WAVE. The WAVE standard turned out to be all around acknowledged. WAVE utilizes the OFDM (orthogonal frequency division multiplexing). A brief description of IEEE 1609/802.16e guidelines is given in the below Table 1.1.

IEEE Standard	Description
IEEE Standard 1609	Defines the VANET architecture, model for communication, mechanisms for security and wireless communication physical access in VANET. Defines the necessary components of VANET like RSU, OBU and WAVE Standard for communication.
IEEE Standard 1609.1-2006	Provides interoperability Explains the main components of WAVE architecture
IEEE Standard 1609.2-2006	Security attributes for WAVE and VANET applications are defined which protect the system from various attacks like spoofing, replay and eavesdropping
IEEE Standard 1609.3-2007	Specifies routing protocols for secure communication between source and destination. Defines multiple upper/lower layers in WAVE networking services, introduced IP for WAVE applications which simply denied WAVE Short Message Protocol
IEEE Standard 1609.4-2006	Contains information regarding the enhancement of media access control layer so as to support WAVE
IEEE Standard 802.16e	Along with interoperability it adds an additional functionally of multi vendor broadband wireless access.

Table 1.1: IEEE standards [45]

1.8 VANET Security

Security is the main issue in VANET. The security issues must be addressed and solved by the successful deployment of VANETs. Since the drivers and the vehicles in VANETs rely on shared information to make decisions, they would be vulnerable to malicious and misbehaving nodes; so proper mechanisms need to be implemented for detecting and avoiding attacks for such malicious nodes [47]. VANET requires security to

employ the wireless environment and serves users with safety and non-safety approaches. Attacker produces distinct kinds of attack in the vehicular environment. The aim of the attacker is to establish issues for rest of users by modifying the message content in the network. Unintended users can be categorized accordingly:

Passive Attackers: These attackers listen to gather activity data which might be passed on to the different attacker. As these attackers don't take an interest in the correspondence procedure of the system, so these attackers are called passive.

Active Attacker: Either produce or composing the packet with wrong information or don't forward the data.

Insider Attackers: Reliable customer of the system and have in-depth information about association. When they have all data about the system, then it's simple for them to dispatch attacks.

Outsider Attackers: These type of attacks are done by the outside person who is not the part of the system.

Malicious Attackers: They are actually not being benefited personally from the entire attack, so the main motive is to disrupt the functioning of the network or to harm others. They are known to be the dangerous one.

Rational attacker: Their main concern is being benefited personally, and are mainly concerned about nature of the target.

Local attacker: This kind of attack is area specific in nature with a limited scope.

VANET technology represents positive benefits, alike a minimal amount of road mishappenings. Road users employ various applications for safety and efficiency, traffic management, warning, comfort, maintenance, music sharing and network gaming. These applications involve the exchange of messages such as emergency message distribution, traffic incidents and road condition warnings that enhance traffic safety and driving efficiency.

1.9 Security Attributes

The security services of VANETs typically need to meet the following needs:

Integrity: Integrity is to deal the accuracy, consistency, and the completeness of messages during transmission. To prevent attackers from altering or injecting messages, an integrity of messages should be ensured. Also, a reliable time source for accurate time synchronization and a reliable positioning system for precise location sequence might be used to secure message against attacks alike replay-strike or position spoofing attack.

Availability: In VANETs, time critical messages such as emergency traffic information must be handled at any given time. If one channel is not available due to failure or attack, there must be alternative means to maintain vehicular network availability all the time.

Authentication: Every message exchanged must be authenticated to identify the sender of the message. Vehicles should react only to information or events generated by legitimate senders.

Non-repudiation: This service is designed to identify misbehaving nodes or attackers and prevent them from denying messages transmitted by them. Any vehicle-related information for communication, such as location, speed, and time, will be stored in a tamper-proof On-Board Unit. It also could be used by authorities for an investigation to reproduce the scene of an accident with the same series and content of the messages communicated prior to an accident.

Real-time constraints: Vehicles move with high velocity. In some situations like time-sensitive communication, a real-time response is essential, so time constraints should be respected.

Privacy: All driver information such as identity, location and speed, should be protected against unauthorized observers. Also, an observer should not be able to trace the routes of the vehicles.

1.10 Self-Organizing Establishment

VANETs require a modified form of trust establishment due to the highly dynamic nodes. Connection to the security infrastructure for verification may not be available all the time. Also, nodes may need to make a decision quickly based on unverified information, which is sent by unidentified nodes. Hence, for self-organizing trust establishment:

1) No trusted third party is involved. (e.g., online infrastructure).
2) No global knowledge is shared between the nodes.

Trust relationships in VANETs change dynamically with the duration of connection with neighboring nodes. The more time a node remains connected with its neighbors, the higher will be the trust established with them. Therefore, mechanisms for trust establishment are categorized as follows (refer Figure 1.6):

- **Direct establishment:** Trust is established through direct communication between nodes.
- **Indirect establishment:** Trust relationships are transferable as nodes share the information about their trust relationship with other nodes.
- **Hybrid establishment:** Trust is established by combining both direct and indirect mechanisms.

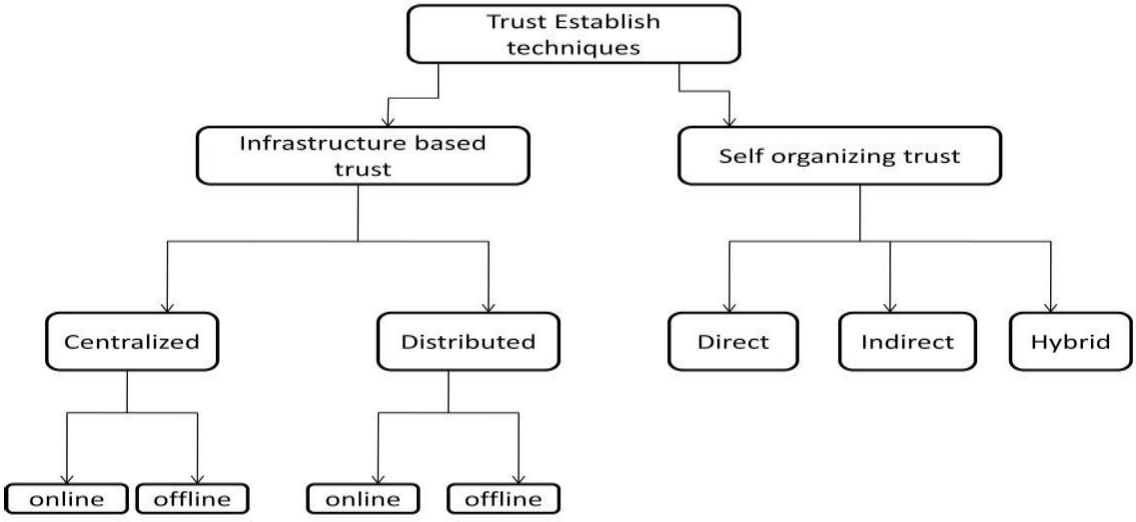


Figure 1.6: Trust establishment techniques

1.11 Challenging issues in VANET

1) **Technical Challenges:** The dealing of technical challenges is with the technical obstacles which can be determined prior to the operation of Vehicular Ad-hoc Network. Following are the few challenges:

- **Network Management:** Because of high mobility, the system topology and the channel circumstance transform quickly. Because of this, it is not possible to use structures such as tree because this design changes similar to the topology changes.

- **Congestion and Collision Control:** Challenge is generated by unbounded network size. Due to heavy traffic at the time of rush hours, there for system is very busy and accidents take place in the systems.

- **Environmental Impact:** For communication VANET uses the electromagnetic waves. With the help of environment, waves are exaggerated. It has been proved that in the deployment of the VANET, the main consideration is an environmental impact.

- **MAC Design:** Vehicular Ad-hoc Network usually practices the communal medium to correspond consequently. MAC Design is the foremost problem.

- **Security:** Vehicular Ad-hoc Network delivers the road security uses which are considered to be life serious hence safety of the communication must be contented.

2) **Social and Economical Challenges:** It is a major problem to encourage a corporation to construct a system that delivers the traffic signal contravention due to an customer may repel for example type of monitoring. So to encourage the VANET developer is a difficult task.

1.12 Routing Attacks in VANET

1) Denial of Service (DoS) Attack

The most dangerous attack in the network is Denial of Service (DOS) attack. In DOS attack (Figure 1.7) dummy or fake nodes are created to transmits fake messages like “path ahead is closed. It stops the communication between vehicle-to-vehicle and vehicle-to-

infrastructure. This type of attack is done to reduce the efficiency and performance of the system [48]. In the scenario given below the malicious node transmit the wrong information to RSU (roadside unit) that path is not available ahead so that RSU gives or transmit the wrong information to the other nodes which are behind the attacker node.

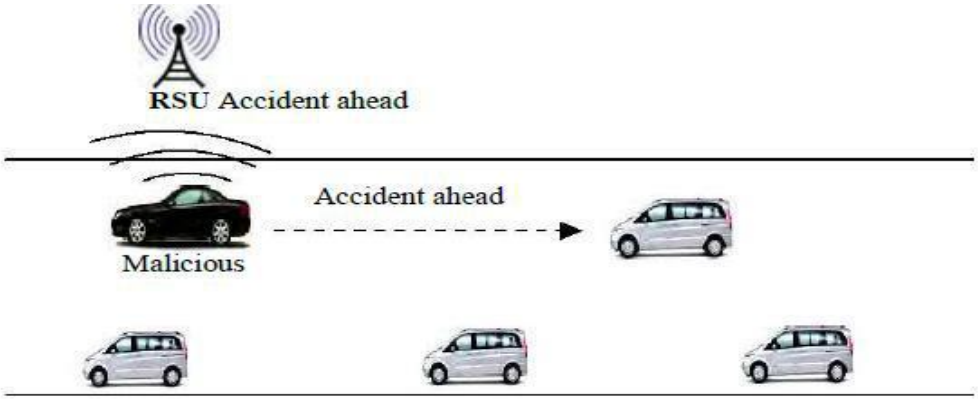


Figure 1.7: Denial of Service Attack [48]

2) Black Hole Attack

A black hole attack (refer Figure 1.8) in which the system movement is diverted. A black hole in which one node that is malicious itself participate in the networks and show that it has the smallest path that covers destination. When routing packets comes towards malicious node, it simply takes a packet and then sends it to the wrong place or wherever they want to send. Take an example the diagram given below in which genuine nodes sends messages to malicious nodes that path is not clear ahead when malicious nodes receives the message they are not transfer this message to the last nodes. The main motive of this attack is just to drop the packets.

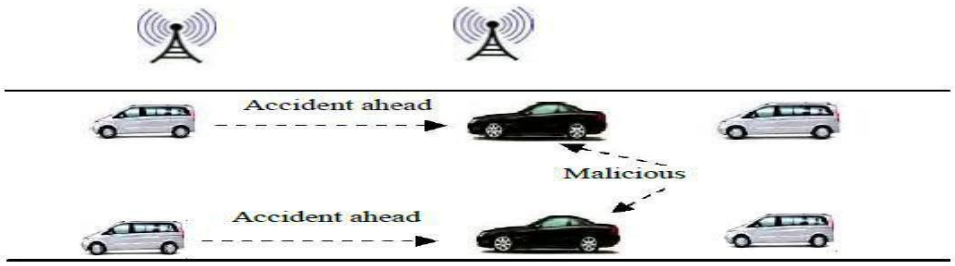


Figure 1.8: Black Hole Attack [48]

3) Wormhole Attack

It is just like Black Hole attack (refer Figure 1.9). In this tunnel is created in between two malicious nodes. From the one end it receives a packet, and from the other end it transmits the packet or broadcast the message in the network. The Tunnel is created to listen to the privacy information in the networks. This type of attack is more dangerous than Black Hole attack. Take a scenario given below in which two malicious nodes are present at the end of the tunnel to receives the data, to create a DoS attack in the networks and listen to the important information in the network.

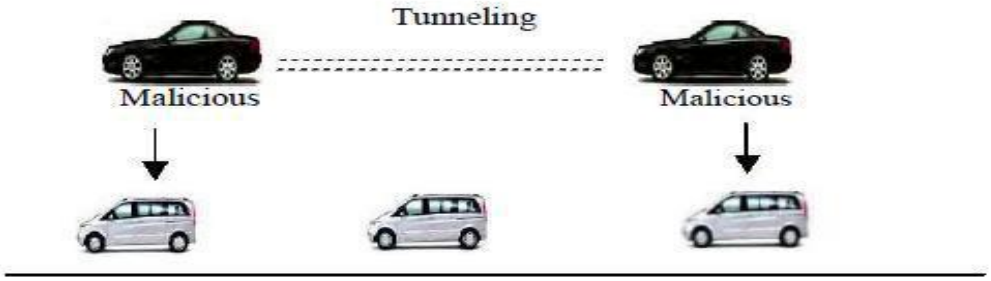


Figure 1.9: Wormhole Attack [48]

4) Sinkhole Attack

In Sinkhole attack (refer Figure 1.10) the malicious nodes are present, the work of malicious nodes broadcast the false route to the others nodes so that it can easily get the information and easily attract all the traffic. The motive of this attack is just to complicated the network performance and drops the packets.The scenario is given below:

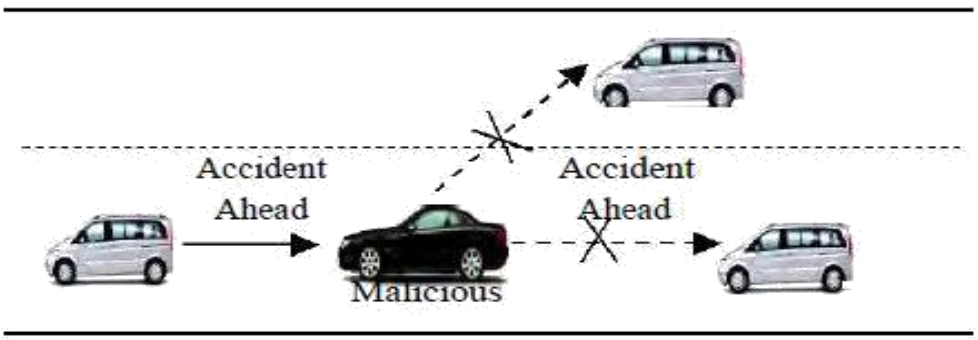


Figure 1.10: Sinkhole Attack [48]

5) Illusion Attack

In Illusion attack (refer Figure 1.11) tries to deliberately control his/her sensor readings for giving wrong information about his/her vehicle. The effect of this assault is that it can undoubtedly change the driver's behavior by spreading the wrong movement data and can bring about mishaps, congested roads and diminish the vehicular system by dropping the data transmission. The sensors of its vehicle to deliver and communicate the wrong activity data.

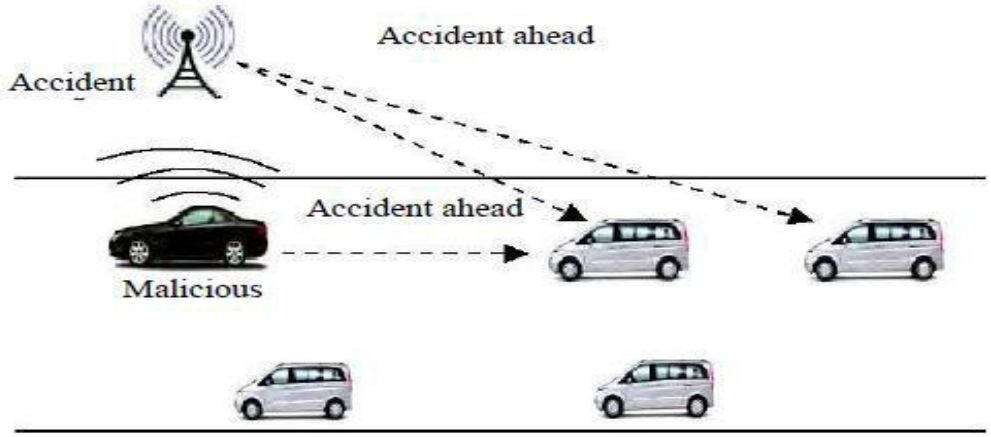


Figure 1.11: Illusion Attack [48]

6) Sybil Attack

In Sybil attack (refer Figure 1.12), the malicious vehicle makes an extensive number of false personalities with a specific end goal to assume control over the VANET and infuse fake data in the system to hurt the genuine vehicles. The motive of this attack is just to complicated the network performance and drops the packets. The scenario is given below:

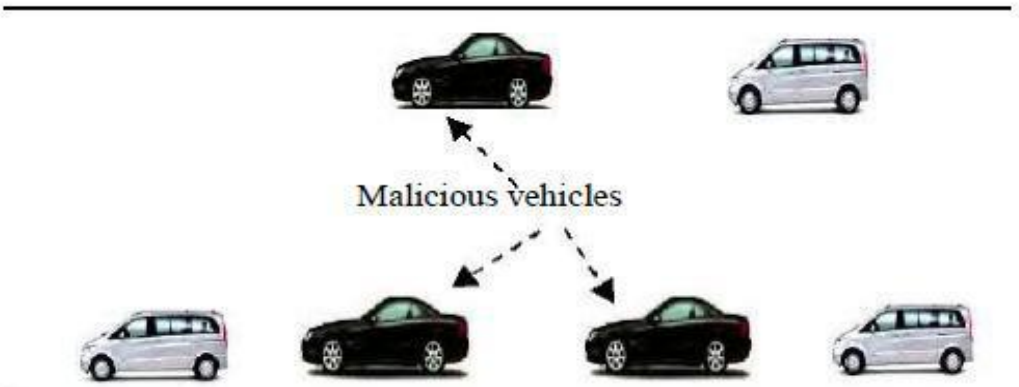


Figure 1.12: Sybil Attack [48]

1.13 Comparison between Attacks

Comparison between different types of attacks is given below in Table 1.2. The attacks we are discussed above the effects of these attacks and the requires of security in VANET is given below:

TYPES OF ATTACK	EFFECT	REQUIREMENTS OF SECURITY IN VANET
(DoS) Denial of Service Attack	Degrades system Performance Affects system efficiency	AVAILABILITY
Black Hole Attack	Causes loss of packets and tamper or drop them	AVAILABILITY
Warm Hole Attack	Prevents discovery of promising nodes to destination and causes loss of data packets	AUTHENTICATION & CONFIDENTIALITY
Sinkhole Attack	Either by tampering or dropping data packets it makes system activity Complicated	AVAILABILITY
Illusion Attack	Consumes system bandwidth by transmitting wrong Messages	AUTHENTICATION
Sybil Attack	Take over the control of network and thus induces false messages in the system	AUTHENTICATION

Table 1.2: Comparison of various attacks [48]

CHAPTER 2
REVIEW OF LITERATURE

Charles Harsch et al. (2007) "Secure Position-Based Routing for VANETs," Delivers a strategy which safeguards geographic position-based routing, accepted as the sufficient one for VC. Furthermore, focused on strategy presently selected & appraised in the Car2Car Communication Consortium and incorporated safety strategy defending the position-based routing operation and services which improve the systems strength. They recommend protection strategy, depending both on cryptographic essentials and prospect checks descriptive counterfeit position addition. Our execution and introductory estimations demonstrate that the security overhead is low and the proposed plot deployable [1].

Maxim Raya, Jean Hubaux (2007) "Securing vehicular ad hoc networks," This paper concentrate on the safety of systems. They delivered a brief hazard examine and plan suitable safety structural design. Moreover, explain few chief design arrangements immobile to be complete, which in few cases which have than simple technical significance. They delivered a place of safety rules and proved that they preserved isolation and observed the strength and efficiency [2].

Yi Qian, Nader Moayeri (2008) "Design of Secure and Application-Oriented VANETs," Recommended safe and used dispose system design structure for VANET and considered in cooperation safety needs of the interactions & necessities of possible Vehicular Ad hoc Network uses and facility. Different applications and private administrations are additionally allowed keeping in mind the end goal to bring down the cost and to empower VANET organization and appropriation. Security is one of the major issues that must be tended to before the deploy of VANETs can be effectively conveyed. Another critical issue is support of diverse applications and administrations in VANETs. A Planned system composed of two prime apparatus: a control system of application-aware and a combined direction-finding method. Moreover the system design structure, they additional study an amount of main permission technologies that are important to a realistic Vehicular Ad-hoc Network. The

research makes available an instruction for the design of a more protected and practical VANET [3].

Xiaodong Lin et al. (2008) "Security in Vehicular Ad Hoc Networks," We reviewed the modern consistency development which overspread the techniques of delivering safety favors & preserving driver isolation for Wireless Access in Vehicular Environments uses. They tackle two prime issues, official document repeal and provisional confidentiality protection, for building the values realistic. Moreover, a collection of unique safety strategy which is launched for gaining secure documentation repeal, and restrictive privacy conservation, which are measured amongst the foremost demanding design reason in VANET. VANET promising way to deal with encouraging street security for drivers and travelers. One of the extreme objectives in the outline of such systems administration is to oppose different pernicious misuse and security attack [4].

Gongjun Yan et al. (2008) "Providing VANET security through active position detection," Vehicle position is a standout amongst the most important bits of data in a Vehicular Ad-hoc Network (VANET). The fundamental commitment of this work is a novel way to deal with upgrading position security in VANETs. We attained limited safety by engaging by helping on-board radar to perceive adjoining motor vehicles and verify their disclosed integrates. Restricted safety is comprehensive and get the worldwide safety with the use of current position-based groups to generate a message system and with the use of active, demanding system verifying distant location in the sequence. The outcome is declared on the broadly conventional hypothesis that the huge greater part of motor vehicles is reliable and behaves correctly. Widespread simulations verify the excellence of recommending outcome by calculating speedy negotiated motor vehicles can be identified under several circumstances [5].

Tw Chim et al. (2011) "SPECS : Secure and Privacy Enhancing Communications Schemes for VANETs," This paper recommended two safe and confidentiality improving connections strategy for Vehicular Ad hoc Networks to tackle messages and cluster communication for inter related-vehicle communication so that security and privacy can be provided to vehicles and also followed the prospects of leasing RSU toward assisting auto graph confirmation procedure. Existing arrangements either depend intensely on a sealed equipment gadget or

can't fulfill the security necessity and don't have a viable message confirmation plot. In this paper, we give a product based arrangement which makes utilization of just two shared privileged insights to fulfill the protection necessity (with security investigation) and gives lower message overhead and no less than 45% higher effective rate than past arrangements in the message check stage utilizing the sprout channel and the paired inquiry procedures (through recreation examine). We likewise give the primary gathering correspondence convention to permit vehicles to confirm and safely speak with others in a gathering of known vehicles [6].

Zohreh Baniasadi et al. (2011) "Modeling Composite Intrusion Detection Systems Using Fuzzy Description Logics," In this paper, we propose another technique to help to oversee and to direct security in vast systems. We utilize Fuzzy Description Logics (FDL) to show a composite Intrusion Detection Framework (CIDS). We demonstrate that this half-breed technique is more productive than fresh ones in complex situations. In this intrusion detection system is used if any type of unauthorized access happens in the system [7].

Ajay Rawat et al. (2012) "VANET : SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS," This paper presents the wide spread research of available strikes & their available outcomes. (VANET) is a promising pattern in the system. A current type of MANET. In VANET motor vehicles are the nodes with flexibility so don't have permanent communications & handle secure and non-safe uses in a wireless intermediate which makes it susceptible to various strikes. Safety is the main significant apprehension in VANET because of open access medium [8].

Ben Ding et al. (2012) "An Improved AODV Routing Protocol for VANETs," In this paper, the AODV routing protocol is used. It is a very important routing protocol in MANET which can be used in VANET because MANET is a class of VANET so, the protocols which are used in MANET can be used in VANET but not directly, with some modification. Intelligent transportation systems (ITS) is the best application of Vehicular Ad-hoc network of Vehicle-to-vehicle and vehicle-to-infrastructure communication based upon LAN (local area network). The problem of traffic and congestion are increasing day by day.). OBU provides the communication capabilities among the vehicles, while RSUs are placed along the road and constitute the network infrastructure. AODV routing help in all this process [9].

Fuad A Ghaleb et al. (2013) "Security and Privacy Enhancement in VANETs using Mobility Pattern," It presented a sample dependent mis behavior identification prospects in Vehicular Ad hoc Networks. Simulation outputs showed with the aim of the place Anonymous Message on the basis of prospects having the capability to enhance safety & preserve confidentiality in Vehicular Ad-hoc Networks. This paper is introducing a versatility design based misconduct recognition approach in VANETs [10].

Ram Shringar Raw et al. (2013) "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET," Discussed about Vehicular Ad-hoc Networks & procedural and safety limitations, moreover described several main strikes and outcomes that which could be executed along side these strikes. In this article, we have talked about the VANET and its specialized and security challenges. We have additionally talked about some real assaults Furthermore, arrangements that can be executed against these assaults. We have thought about the arrangement utilizing diverse parameters. Ultimately we have examined the instruments that are utilized as a part of the arrangements [11].

Prashant Sangulagi et al. (2013) "Recognition and Elimination of Malicious Nodes in Vehicular Ad hoc Networks," This paper describes about the malicious nodes first detects the malicious nodes then eliminates it with the help of mobile agents. In this paper, they deployed the mobile agents on each node so that information of the neighbor's nodes can be collected and also for finding the path from source to the destination during routing. Software agents check the power of intermediate nodes for detecting the malicious nodes from intermediate nodes. Once the malicious node is resolved the substitute way is utilized from source to the goal for sending the data. To test the execution of the system by calculating the number of malicious nodes and number of paths that are available from source to destination. One critical property that describes VANETs is that they are self-arranging, self-making, and self-regulating and decentralized frameworks [12].

Sushil Sarwa, Rajeev Kumar (2013) "Selective Forwarding Attack and Its Detection Algorithms," Selective forwarding is a special type of attack in which malicious nodes acts as normal nodes. So by acting like normal nodes, it drops the packets and gathers the important information from the network. It is very difficult to obtain the selective forwarding attack because the attacker node always acts as a normal node and always clash with each

other whenever they want to change the integrity of data and damage to the VANET system. In this paper, we show a survey and find out the selective forwarding attack and also the pros and cons of this [13].

Merrihan Badr Monir et. al. (2013) "A Trust-Based Message Reporting Scheme For VANET," In VANET (Vehicular Ad Hoc Networks) to create the trust among vehicles is important for transfer the data so that data can be transferred securely and increase the performance of the network by reliability. In this paper, the proposed displays a decentralized trust administration in Vehicular Ad-Hoc Networks. Nodes are tested according to participation and interaction during different events. Node is assigned a level of class by results then some measurement of nodes is taken and find the most trusty nodes [14].

Richard Gilles Engoulou et al. (2014) "VANET security surveys," It provides a study of the safety problems & the limitations produced. Many Several classifiers of uses in VANETs are launched, also some safety necessities, pressure & convinced construction are recommended to resolve the safety issues. Lastly, worldwide safety construction for Vehicular Ad-hoc Network is recommended. The prime advantages of Vehicular Ad-hoc Network improved road security and vehicle security although defensive drivers isolation from strikes by adversary. Safety the most difficult problems in relation to Vehicular Ad-hoc Network while the information transferred circulated in open surroundings. This paper exhibits a study of the security issues and the difficulties they produce. The different classes of uses in VANETs are presented, and additionally, some security prerequisites, dangers and certain designs are proposed to take care of the security issue [15].

Jaya Sehgal, Poonam Arora (2014) "Delay Optimization in VANET Using Ant Colony Optimization and WI-MAX," VANETS is the most well-known system which is called Vehicular Ad Hoc Network. A Lot of work has been finished by the analysts in this network. From the Literature survey, VANETs is a continuous framework where the vehicles are moving and go with a rapid on the streets in the urban zones. There are numerous security issues like verification, crash discovery, blockage evasion, correspondence framework approach and so on. In this present work, we are showing a clever course ID approach if there should arise an occurrence of mischance event for Vehicle-to-vehicle. The clever vehicles are characterized separately for telling the direction and speed investigation. On the

off chance that some mischance over the system, the neighbor data vehicle stream will be performed. For Vehicle-to-vehicle communication bio-inspired approach has been recommended to distinguish the easy and safest path over the system [16].

Shamsul Jamel Elias et al. (2014) "A Comparative Study of IEEE 802.11 Standards for Non-Safety Applications on Vehicular Ad Hoc Networks," Vehicular Ad Hoc Networks (VANETs) is an essential part of ITS (intelligent transportation systems). The point is to give creative administrations identifying with different methods of transportation and movement of vehicles. These types of frameworks give clients to come to their goals better, more secure and more planned. In this study, we research the IEEE standards for Inter-vehicle communication The paper gives investigation of different remote measures by VANET and analyze their parameters [17].

Uzma Khan et al. (2014) "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks," The proposed calculation DMN-Detection of Malicious Nodes in VANETs enhances DMV Algorithm as far as successful determination of nodes which are malicious and consequently enhances the system execution. Its principle goal is to provide security to the communication network, safety to the users on roads. DMN (detection of malicious nodes) provides sufficient safety efforts to secure the system [18].

T.W. Chim et al. (2014) "VANET-based Secure and Privacy-preserving Navigation," In this paper, navigation scheme has been propose that uses the online street data gathered by a VANET (Vehicular Ad-hoc network) to alert the drivers for giving the correct direction. Security is the main issue while transferring the data between the nodes. To ensure the security of the drivers, the trusted authority is available to give the explanation to the driver who raises the query. Our plan satisfies all other fundamental security conditions. Utilizing the genuine maps of New York and California, we demonstrate the results regarding traveling and processing time [19].

Khaled Rabieh et al. (2015) "Layer based Scheme for Detecting Large amount of scale Sybil Attack in Vehicular Ad-hoc networks (VANETs)," We discuss a cross-layer plan to empower the Road side unit to distinguish vehicles with attacks. These vehicles with attacks don't occurs in their asserted areas, we are planning to control the areas of Vehicles. A test

parcel is sending to the network guaranteed area utilizing directionaliz reception apparatus to recognize the nearness of vehicle. On the off chance that the vehicle is in the normal area, it ought to have the capacity to get the test and send back a substantial reaction parcel. With a specific end goal to decrease the overhead and as opposed to sending challenge parcels to every one of the vehicles constantly, bundles are sent just when there is a doubt of Sybil assault. We likewise examine a few Sybil assault disturbing methods. The assessment comes about show that our plan can accomplish high recognition rate with the low likelihood of false caution. Moreover, the plan stand in need. In any case, the assailant may dispatch a Sybil assault by putting on a show to be numerous synchronous vehicles. This assault is extreme when a vehicle intrigues with others to utilize substantial qualifications to validate the Sybil vehicles. [20].

Mandeep Kaur, Manish Mahajan (2015) "A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDOS Attacks in VANETs," This proposed model has been designed to detect and the DDoS strikes in the Vehicular Ad hoc Network clusters to prevent misshapen in the form of Vehicular Ad hoc Network node break down, accident. The DDoS strike anticipation algorithm mechanism as the actual time strike discovery and transparency information refine algorithm with respect to safe guard along side the DoS and DDoS strike. The optional representation productivity has been gathered based on system weight, throughput, packet liberation ratio, etc. The investigational outputs have shown the efficiency of the considered representation in assessment with the existing models [21].

Mani Amoozadeh et al. (2015) "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving," Introduces a prime glance at the possessions of safety strikes on the statement channel and also sensor diversity of a linked car water course prepared to attain CACC. Their simulation outputs prove that an attack can reason important volatility in the CACC motor vehicle. Moreover, it has demonstrated how to calculate, alike degraded to ACC mode, might probably used to improved the safety and security of the associated motor vehicle streams. Alike classification depends greatly on board sensors alike cameras. Autonomous motor vehicle organizes established extremely harsh provisions on the safety of the communiqué canal used by the motor vehicle to replace in order as well as the manage reason that near complex driving works alike modify motor vehicle speed [22].

Jaydip Kamani, Dhaval Parikh (2015) "A Review of Sybil Attack Detection Techniques," Briefly presents various Sybil attack detection mechanism in VANET. In Vehicular Communication, the security system against the attacker is very important. Sybil attacks considered a major safety hazard to ad hoc systems and sensor systems. It is an attack in which an original identity of the vehicle is corrupted, or theft by an attacker to creates multiple fake identities. Detecting such type of attacker and the original vehicle is a challenging task in VANET [23].

Dalbir Singh, Amit Jain (2015) " Deterministic AODV Routing Protocol for Vehicular Ad-Hoc Network," In this paper, we at first examine the execution of AODV and OLSR, and further we enhance the execution of AODV with the help of trust values, by choosing only that node which is highly trusted. Route table should be updated by AODV with this purposed approach. AODV have the capacity to improve the end to end delay, throughput and packet delivery ratio [24].

Shiang-Feng Tzeng et al. (2015) " Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET," In this paper, we call attention to that the current IBV takes some security dangers. We present an enhanced plan that can fulfill the security and protection of the vehicles. Random oracle model is used by the proposed identity-based Batch Verification Scheme (IBV). The proposed IBV gives the security on the constant numbers instead of some messages. We demonstrate the effectiveness benefits of the proposed work through execution assessments as far as calculation and transmission overhead. The fundamental thought in vehicles, to send the data to roadside units (RSUs) or by different vehicles [25].

Nirav J. Patel, Rutvig H. Jhaveri (2015) "Trust based approaches for secure routing in VANET," In this paper, we introduce the review of different components to enhance routing by protocols in Ad-hoc network by improving the nodes trusted values in VANETs. VANET is multidimensional in which the vehicles constantly change their areas. Security is the main issue while transferring the data between the nodes [26].

Khattab M. Ali Alheeti (2015) "An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars," This paper proposed two techniques

that are anomaly based and mistreat detection to perceive the spiteful attack and also designed an ID scheme for Vehicular Ad hoc Networks with the use of Artificial Neural Networks for identifying Denial of Service (DOS) strikes. Using ns-2 simulator the outputs of this study are reviewed. The principle part of IDS is to identify the assault utilizing an information produced from the system conduct such as a follow record. The IDSs utilize the components extricated from the follow record as auditable information. In this paper, we propose oddity and abuse location to recognize the pernicious assault [27].

Dhavy Gantsou (2015) "On the Use of Security Analytics for Attack Detection In Vehicular Ad Hoc Networks," In this paper concentrating on attacks location, we demonstrate how execution from various sources at various layers Sybil nodes can be identified. A vehicular system (VANET) is a class of mobile ad hoc network based on top of the IEEE802.11p standard for a better flexibility to the remote networks. It is supporting to both vehicle-to-vehicle as well as vehicle-to-infrastructure. Furthermore, connect the vehicles to outside assets including cloud administrations, the Internet, and client gadgets while enhancing the street movement conditions. Intelligent transportation systems (ITS) is a key function of VANET. VANET security issues resolved by cryptographic methods [28].

Suwan Wang and Yuan He (2016) "A Trust System for Detecting Selective Forwarding Attacks in VANETs," This paper, we address the problem of distinguishing specific sending assaults by building a trust framework. The proposed way to deal with keep up this framework for the most part incorporates (1) Mutual monitoring is used for finding the attacks between nodes by using the local and global information and (2) detect of attacker node based upon abnormal or bad driving patterns of malicious nodes. Since both in-band and out-band data is used, our approach is powerful in generally low-thickness street conditions and strong to different situations, for example, the extraordinary rate of an malignant event or diverse street's range. VANET is a high natural portability and takes information sending as an essential instrument to share data among vehicles. Selective forwarding attack, are the attack in which masquerade nodes acts as normal nodes which drop data packets, damage the real or same form of data and damages the legitimacy of genuine VANETs applications. It is very difficult to obtain the selective forwarding attack because the attacker node always acts as a normal node and always clash with each other

whenever they want to change the integrity of data and damage to the VANET system. The results of our simulations show that our approach accomplishes a high fault tolerance with the help of by selecting most accurate nodes which are used for sending information, while in the mean time recognize attacker nodes with moderately high accuracy [29].

Greeshma Chirayil , Ashly Thomas (2016) "A Study on Cost Effectiveness and Security of VANET Technologies for Future Enhancement," Considers a few existing technologies such as CROWN, Vehicular Cloud and VANET-Cloud and a comparison on these is carried out. As the technology has to be used widely, there is a high need for a low-cost VANET technology with high security and Quality of Service. To go for any further developments, a through analysis of the available technologies is essential to get a closer view on the current scenario. The result of this study can open doors for a better technology for future VANETs. It is very effectively used in VANET, a spontaneous creation of the wireless system of vehicles for exchanging information between them, for improved traffic management and to ensure several users that are sufficiently up to date about the road and make safer and smarter decisions on the road by using transport networks [30].

Mandeep Kaur et al. (2016) "Protection Against DDOS Using Secure Code Propagation In The VANETs," Proposed model threats caused by the DDoS attack with the used of road side traffic management recommended a strong safety system to mitigate. The RTMU used several arithmetical calculations for traffic sample examines to detect the abnormality in data traffic among the cluster nodes. Also, all of the VANET nodes communicate with each other through RTMU. The outputs have provides efficiency of the recommend model to moderate the DDoS strike and make possible for horizontal transfer society. Vehicular Ad hoc Network used for mechanically determined vehicles in the forbidden surrounding. Although the human vehicles use the Vehicular Ad hoc Network for further ability, the mechanically determined vehicles entirely rely upon leading the Vehicular Ad hoc Network. Any invasion in the Vehicular Ad hoc Network by hackers can reason prime traffic chaos. A famous technique called as prankster attack which is used by army-force to plot attacks to reason extra injure as possible by self-centered drivers to create their method obviously [31].

Lim Kiho (2016) "Secure and Authenticated Message Dissemination in Vehicular Ad-hoc Networks and an Incentive-Based Architecture for Vehicular Cloud," In this paper VANETs

permits to motor vehicles to outline a self-manageable system. VANETs are likely to be widely deployed in the future, given the interest was shown by industry in self-driving cars and satisfying their customers's various interests. Problems related to Mobile Ad-hoc Networks (MANETs) such as routing, security etc. have been extensively studied. Even though VANETs are the special type of MANETs, solutions proposed for MANETs cannot be honestly applied to VANETs because all problems related to MANETs have been studied for small networks. Moreover, in MANETs, nodes can move randomly [32].

Kashma Jain, Dinesh Goyal (2016) "Design and Analysis of Secure VANET Framework preventing Black Hole and Gray Hole Attack," This paper scrutinized the effects of packet loss in the network due to Black Hole and Gray Hole attacks and also propositions a detection technique that competently detects both attacks in the network. In this research, paper simulation is completed by using the NS-2 simulator. In this research work, the attack is performed and detected on AODV routing protocol. Furthermore, to determine the effects of attacks on network performance simulation is performed on different network scenarios. Vehicular Networks are considered as the novel class of remote systems, likewise called as VANET (Vehicular specially appointed Networks). It is a key part of Intelligent Transport System (ITS). VANET innovation is distinguished for enhancing street security and transport effectiveness. In any case, because of late emerge in security issues in VANET. VANETs must have a protected route for correspondence which is very testing and imperative issue [33].

Farhan Jamil et al. (2016) "A comprehensive survey of network coding in vehicular ad-hoc networks," This paper introduces a complete study of system coding plans in VANETs. Network coding is an information handling method in which the stream of computerized information is improved in a system by transmitting a composite of at least two messages to make the system more powerful. We have many applications like distribution of content, data downloading, multimedia application, information spread and other key regions of VANETs in which organize coding plans are executed. This examines work will give a reasonable comprehension that how to arrange to code is executed in these VANETs to enhance execution, diminish delay and make the system more productive [34].

Hao Hu et al. (2016) "A Reliable Trust-based Platoon Service Recommendation Scheme in VANET," In this paper, we propose a dependable trust-based unit benefit proposal called REPLACE, to help the client not to pick that platoon vehicles which behaves badly. A point by point security examination is given to demonstrate that our proposed REPLACE plan is secure against attacks which are new and for on-off attacks, so that's the strength of our proposed work. In this vehicular platooning framework, a detachment head vehicle gives services to its client vehicles [35].

Ahmad Shaheen et al. (2016) "Comparison and Analysis Study between AODV and DSR Routing Protocols in VANET with IEEE 802.11b," In this paper, the AODV and DSR are performed in a VANET over two distinct situations. Both protocols are performed individually by different tasks and then evaluated the performances of both protocols. As we know that MANET is a class of VANET. The protocols which are used in MANET can be used in VANET but not directly with some modification [36].

Tareq Emad Ali et al. (2016) "Review and Performance Comparison of VANET Protocols: AODV, DSR, OLSR, DYMO, DSDV & ZRP," This paper is providing the brief study of ad-hoc protocols for routing that are being used in a Vehicular ad-hoc network. The vehicular network is providing communication among the vehicles that are moving on roads. The protocols that are being used for communication are being affected by the high speed of vehicles which is leading to the path breaks. The main motive of a vehicular network is the assembly of data system in vehicles which are moving on the roads. In this paper routing protocols has been compared on the basis of a delivery ratio of packets, delay, throughput etc [37].

Amrita Chakraborty, Arpan Kumar Kar (2017) "Swarm Intelligence: A Review of Algorithms," This paper describes the study of insect and animal based algorithms. This is the analysis of way in which these algorithms operate. The specified areas for these protocols have been introduced after the analysis of inspiration. Specific areas where these algorithms can be applicable have been highlighted. Swarm intelligence is an integral part of the artificial intelligence. This study is providing the basic concept of the technical aspects and the future scope of algorithms [38].

CHAPTER 3
PRESENT WORK

3.1 Problem Formulation

In order to have a clear scenario about the proposed work of detecting the Selective forwarding attack in which malicious nodes acts as a normal nodes in the Vehicular Ad-Hoc network, firstly I will try to discuss the working of my base paper that I have chosen to carry out my M.Tech dissertation work.

3.1.1 Previous Work

Wang Suwan and He Yuan (2016) "A Trust System for Detecting Selective Forwarding Attacks in VANETs," In this paper, we are working on the selective forwarding attack in which malicious nodes acts as a normal node by making the trust based system.

1) Mutual monitoring is used for finding the attacks between nodes by using the local and global information.
2) Detection of attacker node based upon abnormal or bad driving patterns of malicious nodes.

Since both in-band and out-band data is used. VANET is a high natural portability and takes information, to share the data among different vehicles. Selective forwarding attack, are the attack in which masquerade nodes acts as normal nodes which drop the data packets, damage the real form of data and damages the legitimacy of genuine VANETs applications. It is very difficult to obtain the selective forwarding attack because the attacker node always acts as a normal node and try to clash with each other whenever they want to change the integrity of data and so that damage occur in the VANET system.

Base Paper works as follows:

1) Make a Trust based system for detecting the malicious nodes. In this malicious nodes acts like normal node.
2) Attacker node is detected based upon the abnormal driving patterns.

3) Authentication of nodes is done with the help of Government Transportation Authority.
4) This approach reduce the chances of malicious nodes and achieves a high fault tolerance.
5) Evaluate the performance in terms of Transmission, Risk and Trust values.

Main features of the Base Paper were:

1) Finding the malicious nodes from the normal nodes by making the trust based system.
2) Authentication process is done by the Government Transportation Authority.

3.2 Objectives of the study

Security is the main issue in VANET. The security issues must be addressed and solved by the successful deployment of VANETs. VANET requires security to employ the wireless environment and serves users with safety and non-safety approaches. Attacker produces distinct kinds of attack in the vehicular environment. The aim of the attacker is to establish issues for rest of users by modifying the message content in the network so proper mechanisms need to be implemented for detecting and avoiding the malicious nodes.

Therefore my work is mainly towards the detection of malicious nodes in Vehicular Ad-hoc networks and securing the VANET node and monitoring with trust based system and use of Ant bee colony optimization so, that packet drops and overhead reduced by this.

The Objectives of my study are:

1) Detecting the malicious vehicles using Trust based system.
2) Implementation of Ad-Hoc On-Demand Distance Vector routing and optimization of the approach with Ant Bee Colony algorithm.
3) Evaluation of parameters such as transmit, risk and the trust values.
4) To validate the proposed approach with the existing one.

3.3 Proposed Work

We are working on the security in Vehicular Ad-hoc networks. Security is the main issue in VANET. In our proposed work (refer Figure 3.1) we are improving the security of vehicles by detecting the malicious nodes. Selective forwarding attack in which malicious nodes acts as a normal nodes so we are finding the malicious nodes with trust based system.

Firstly the deployment of vehicles in the networks then we performed the authentication of vehicles on the basis of GTA (Government transportation authority). By finding the source and destination nodes and coverage area then Ad-Hoc On-Demand Distance Vector routing is performed. The parameters used for proposed architecture are listed in Table 3.1.

Malicious nodes are detected on the basis of trust based system. Only trusted nodes carry the data. RSU (road side unit) are deployed in every block so that they communicate with the nodes and collect all the data of the malicious nodes. RSU transfer the collected data to GTA and send a report to GTA. Ant Bee Colony optimization is held on this process to improve the performance of the system. Evaluation of parameters on the basis of transmit, risk, packet delivery and the trust values are calculated.

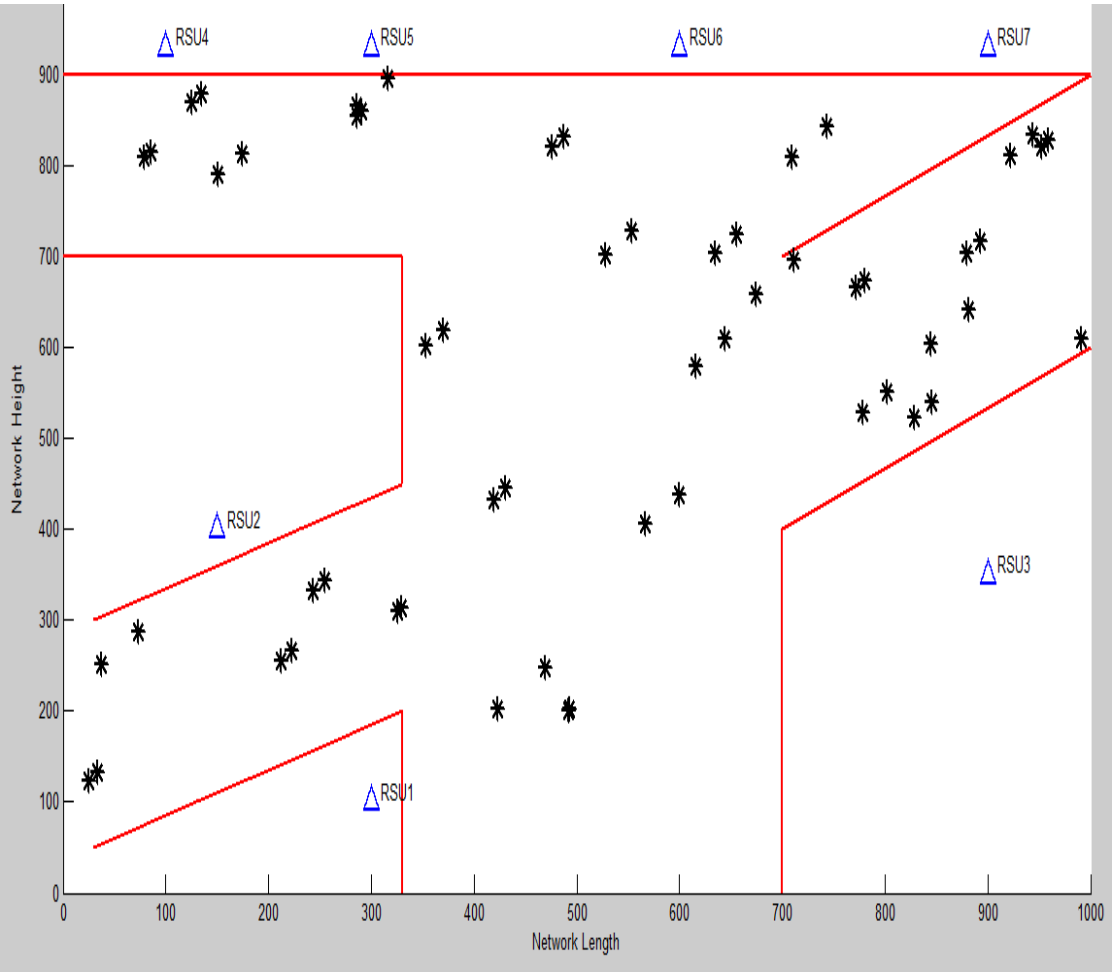


Figure 3.1: Architecture for proposed approach

Simulation Parameters	Values
1. Simulator	MATLAB 2013
2. Simulator Area	1000*1000
3. Number of Nodes	30
4. Simulation time	300 sec

Table 3.1: Parameters for proposed architecture

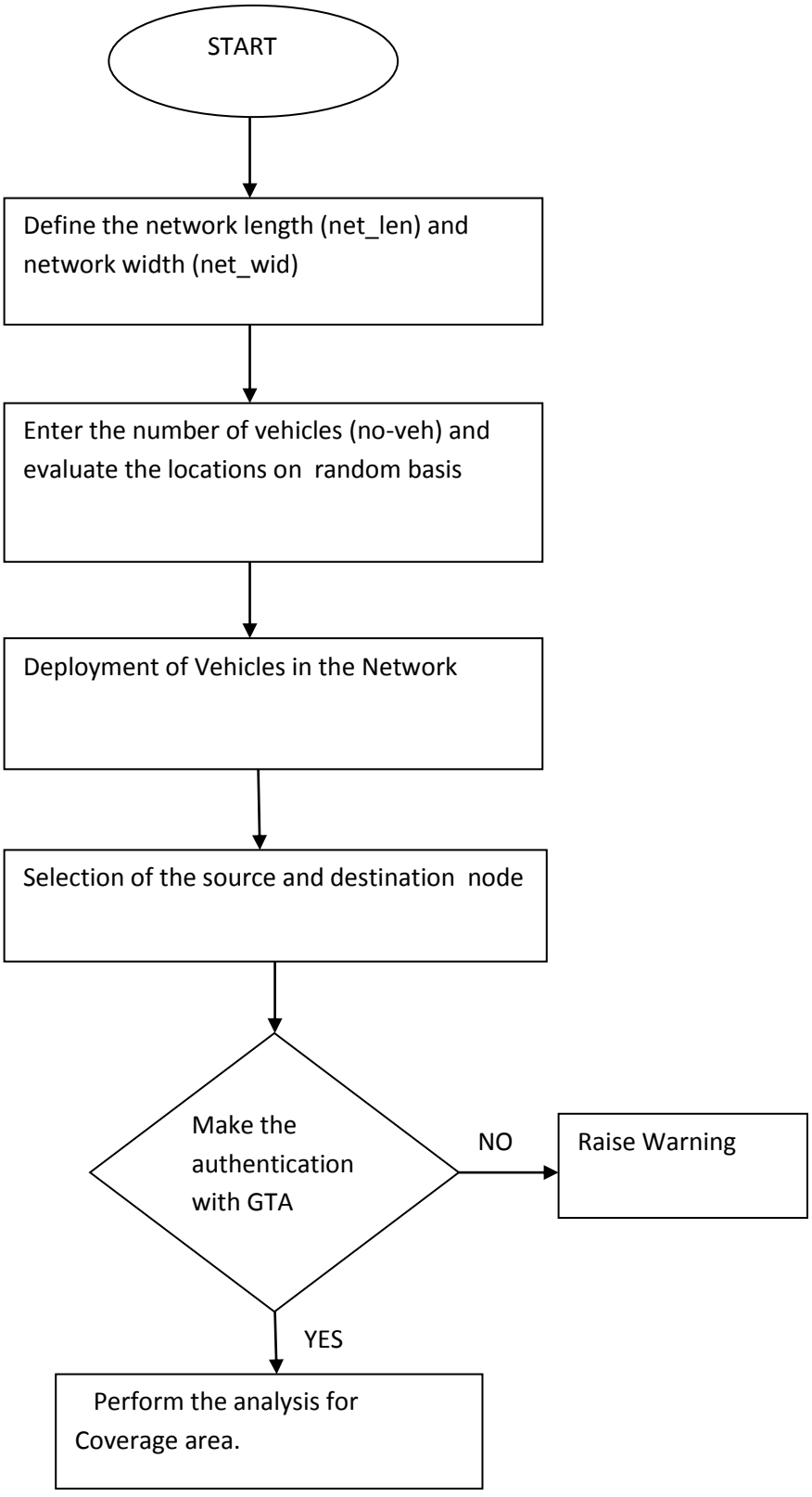
3.4 Assumptions

The following underlying assumptions have been made to evaluate the efficiency of proposed approach for urban environment. This approach has been designed for security in case of urban scenario. If the overhead increases, then we have to go for optimization. The randomness of vehicle has to be reduced, ie less is the randomness of vehicle, more stable is the state of vehicle, than the packet drop will be reduced. The mechanism attached with RSU and send report to the GTA.

1) RSU is used for monitoring the malicious nodes and recording the data and send to the GTA. RSU are set on every block in the network.
2) Implemented on highways where all the paths are already known.
3) Work is done in the low density area.
4) Amount of malicious nodes always less than the normal nodes in the network.

VANET requires security to employ the wireless environment and serves users with safety and non-safety approaches. Attacker produces distinct kinds of attack in the vehicular environment. The aim of the attacker is to establish issues for rest of users by modifying the message content in the network so proper mechanisms need to be implemented for detecting and avoiding the malicious nodes.

3.5 Research Methodology



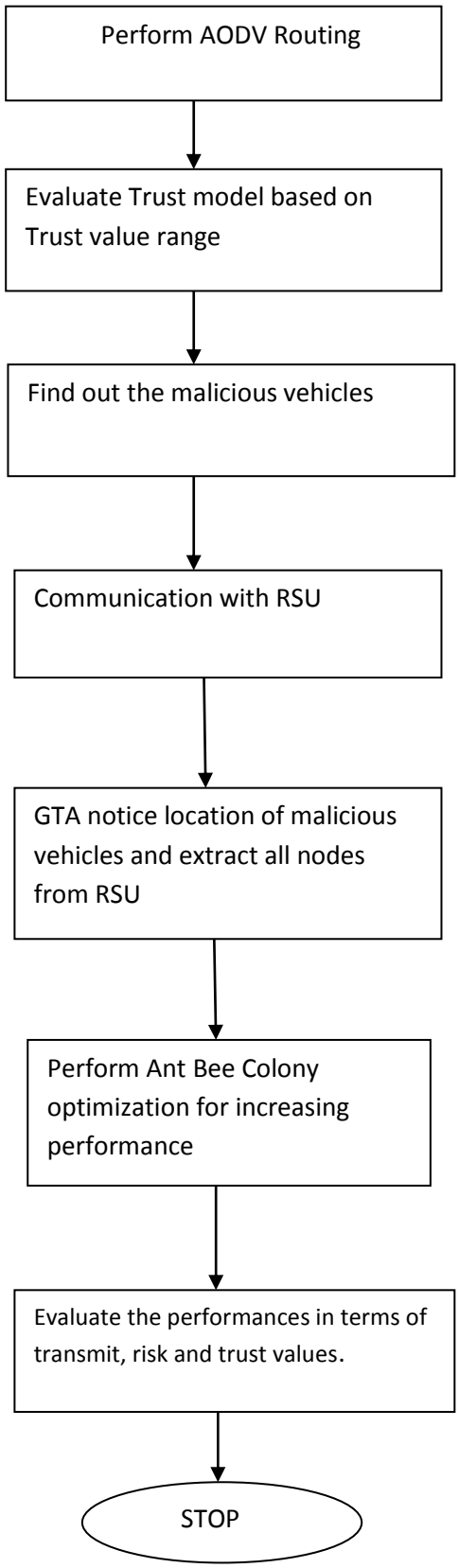


Figure 3.2: Flow chart for Proposed work

3.6 Code Snippets

As my proposed research is on detection of malicious node in Vehicular Ad-hoc network, therefore following code snippets as below.

```
if jj==0
   jj=1;
end
xnew(p)=xloc(malicious_veh(jj))+jpp(malicious_veh(jj));
ynew(p)=yloc(malicious_veh(jj))+jpp(malicious_veh(jj));
xnew(p+1)=rsu_x(id);
ynew(p+1)=rsu_y(id);
rsu_process_report(ip)=randint;
```

Figure 3.3: Malicious node detection

```
        for i=1:no_veh
           if gta_scores_veh(i)<0
              malicious_veh(i)=i;
              xloc_mal(jp)=xloc(i);
              yloc_mal(jp)=yloc(i);
              jp=jp+1;
           elseif gta_scores_veh(i)>=0 & gta_scores_veh(i)<=20
               new_come_veh(i)=i;
           elseif gta_scores_veh(i)>=20 & gta_scores_veh(i)<=40
               low_trust_veh(i)=i;
           elseif gta_scores_veh(i)>=40 & gta_scores_veh(i)<=60
               common_node_veh(i)=i;
           elseif gta_scores_veh(i)>=60 & gta_scores_veh(i)<=80
              high_trust_veh(i)=i;
           else
               monitor_veh(i)=i;


           end

        end

end
```

Figure 3.4: Trusted System

```
%%%%% RSU noticing speeds %%
p=1;
avg_speed=mean(speed_veh);
for j=1:numel(speed_veh);
    if speed_veh(j)>avg_speed
        rsu_n(p)=xloc(j);
        rsu_y(p)=yloc(j);
        high_speed(p)=speed_veh(j);

        p=p+1;

    else
         low_speed(p)=speed_veh(j);
           trust_val(p)=gta_scores_veh(j);
    end
end
```

Figure 3.5: RSU noticing speeds

```
% ABC Main Loop

for it=1:MaxIt

    % Recruited Bees
    for i=1:nPop

        % Choose k randomly, not equal to i
        K=[1:i-1 i+1:nPop];
        k=K(randi([1 numel(K)]));

        % Define Acceleration Coeff.
        phi=a*unifrnd(-1,+1,VarSize);

        % New Bee Position
        newbee.Position=pop(i).Position+phi.*(pop(i).Position-pop(k).Position);

        % Evaluation
        newbee.Cost=CostFunction(newbee.Position);

        % Comparision
        if newbee.Cost<=pop(i).Cost
            pop(i)=newbee;
        else
            C(i)=C(i)+1;
        end
        end
```

Figure 3.6: Optimization using ABC

CHAPTER 4
RESULTS AND DISCUSSION

4.1 Simulation

For my implementation and Results I used MATLAB simulator. MATLAB is a numerical processing and a programming language. Mathworks is used for developing the coding in MATLAB. MATLAB performed so many functions like manipulations of Matrix, function plotting, usage for calculations, for making the user interface and interfacing with different projects written with the help of MATLAB.

MATLAB is a fourth-era programming language. MATLAB is utilized by architects and researchers in many fields, for example, for image processing, for making controls systems in industries and for making smart designs. In MATLAB we have menu and toolbar, workspace, history, current directory, help browser, start button and command window where we write all the commands.

Some of the advantages and disadvantages of MATLAB are we can easily implemented the matrices and arrays in MATLAB and very easy to learn the programming languages in MATLAB. MATLAB increase the performance of the functions. Command line helps in performing so many functions in MATLAB. We can easily show the results in MATLAB with the help of plotting functions because MATLAB has so many functions of plotting. Programming elements of MATLAB are scripts, functions and the flow control blocks.

4.2 Implementation

For implementation process we use a MATLAB simulator for deploying the vehicles in the network and for showing the movement of nodes. Communication is always interrputed by the malicious nodes during transfer of data so, we are making this scenario for solving this problem. On this simulator we divide the road into two-way paths from east to west and south to north. Network length and width is taken by me is 1000*1000. Each vehicle is assigned with the ID (identity number) and randomly distributed these nodes in the

network. We are finding the malicious nodes from the 30 nodes which we are depoloyed on this Vehicular Ad-hoc network. In this the Selective forwarding attack means the malicious nodes which are acting like a normal node and further drops the data packet in the network and change the integrity of the data. So, our work is mainly towards the finding of malicious nodes from below given network.

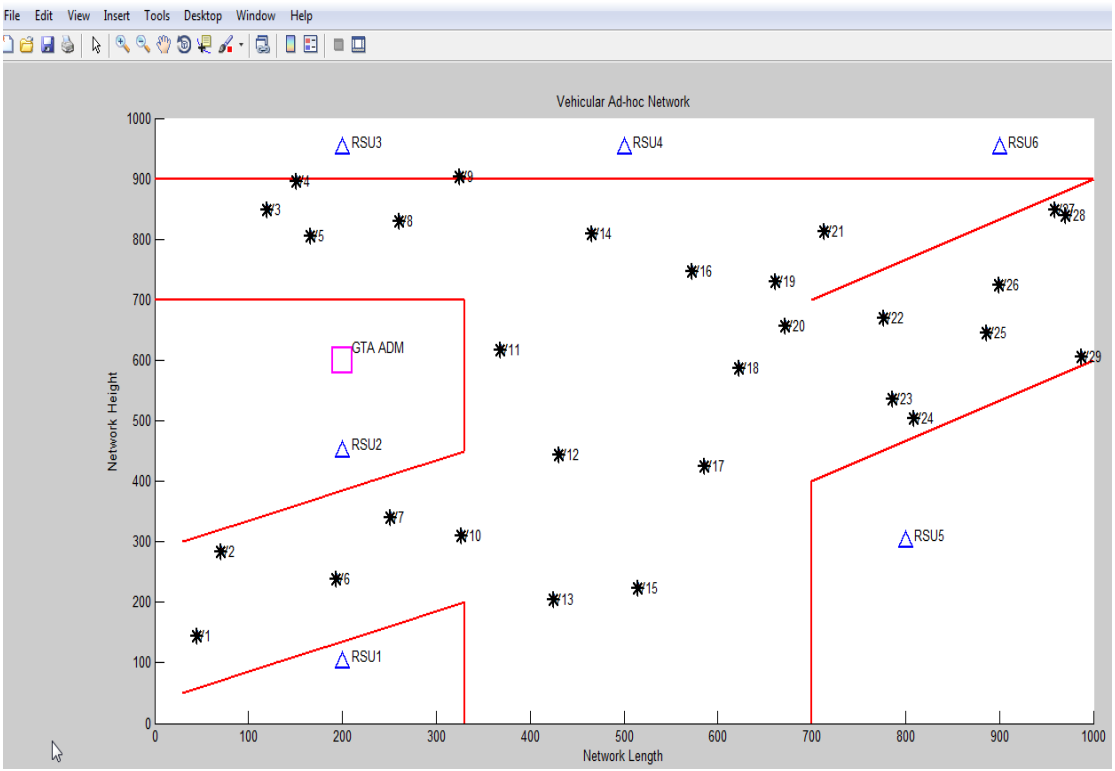


Figure 4.1: Proposed System Architecture

Figure 4.1 shows the RSU are deployed on each corner of the roads. The main head process is controlled by the GTA (Government Transportation Authority). It works as a database where all the data is stored which is captured by the RSU. GTA is same act as a centralized database. So for secure communication we assumed GTA and RSU. Here GTA process is also use for authentication for example if we enter the nodes more than 30 in dynamic network it raise a warning that this vehicle is not authenticated.

Malicious nodes is defined by making a trust based system. When malicious nodes are detected and comes in the range of coverage area than communicating is done with the help of RSU or monitoring by the RSU and save all the locations of malicious nodes in the

GTA database. Then we optimization with Ant bee colony to increase the performance of the system. Here we have some controllable parameters that are:

- Detection process numbers are in between 1 and 2.
- Number of vehicles and streets fixed.
- Malicious nodes occurrence speed and probability.
- Main head that is a GTA.

Here we evaluate the four parameters in our proposed work by using Ant Bee Colony optimization:

1) **Transmit:** It shows the probability to delivery of packets.
2) **Risk:** It shows the risk rate methods in malicious nodes for the high speed and the low speed.
3) **Trust:** Trust Based system is used for finding the trusted values.
4) **Packet delivery**: Successful delivery of a packet over the network.

RSU here use for capture the location of malicious nodes and for sending the report to GTA. RSU helped to save the locations of malicious nodes in GTA database.Communication of RSU is shown in Figure 4.2. For simulation parameters for Figure 4.1and Figure 4.2 refer Table 4.1.

Simulation Parameters	Values
1. Simulator	MATLAB 2013
2. Simulator Area	1000*1000
3. Number of Nodes	30
4. Simulation time	300 sec

Table 4.1: Parameters for simulation

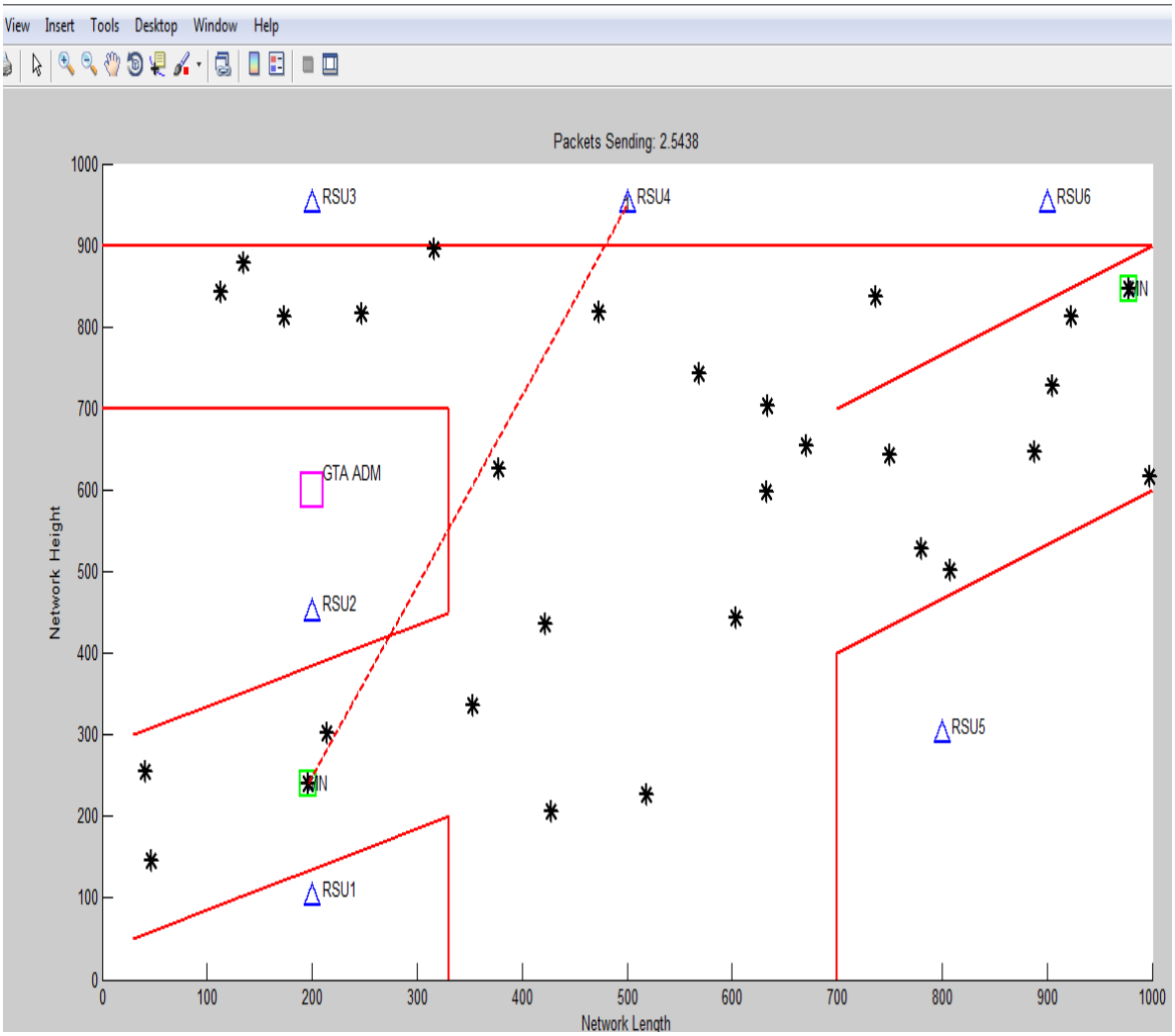


Figure 4.2: RSU communication in Proposed System

4.3 Simulation Results

For determining the efficiency of the system by finding the malicious nodes from the trust based system, we improve the performance of the system. Here we compare the results with the existing system. Perceptions are made by considering different parameters and in this manner looking at them against the new parametric values on the Vehicular Ad-hoc networks.

By doing the proposed model with the current one, results are appeared for the vehicles in the system whose main motive is just drop the data packets and change the

integrity of data. We are just improving the stability of the system. So, by this proposed system we can enhanced the security of the Vehicular Ad-hoc network.

On the basis of trusted based model we are finding the highly trusted nodes. Firstly find the nodes for routing with Ad-hoc on demand distance vector protocol then we are focusing on finding the malicious vehicles, low trust vehicles, high trust vehicles and the common nodes vehicles. Malicious nodes are then communicate with the Road side unit and road side unit save the locations of the vehicles and send all the information to the Government transportation authority in the form of reports.

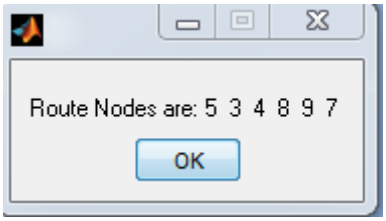


Figure 4.3: Selected Route nodes

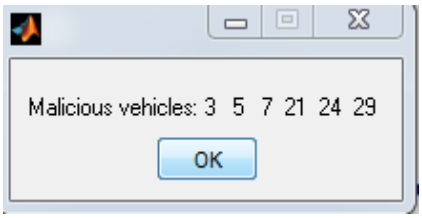


Figure 4.4: Malicious Nodes

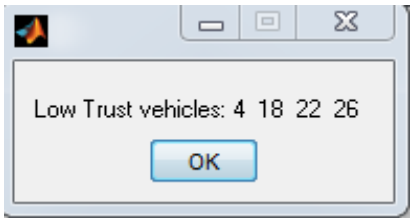


Figure 4.5: Low trust value vehicles

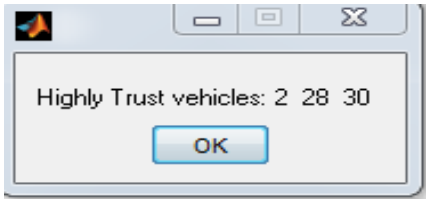


Figure 4.6: High trust value vehicles

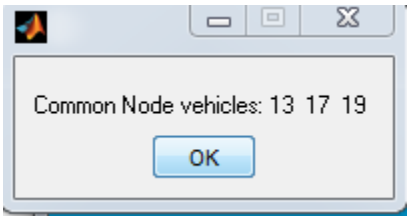
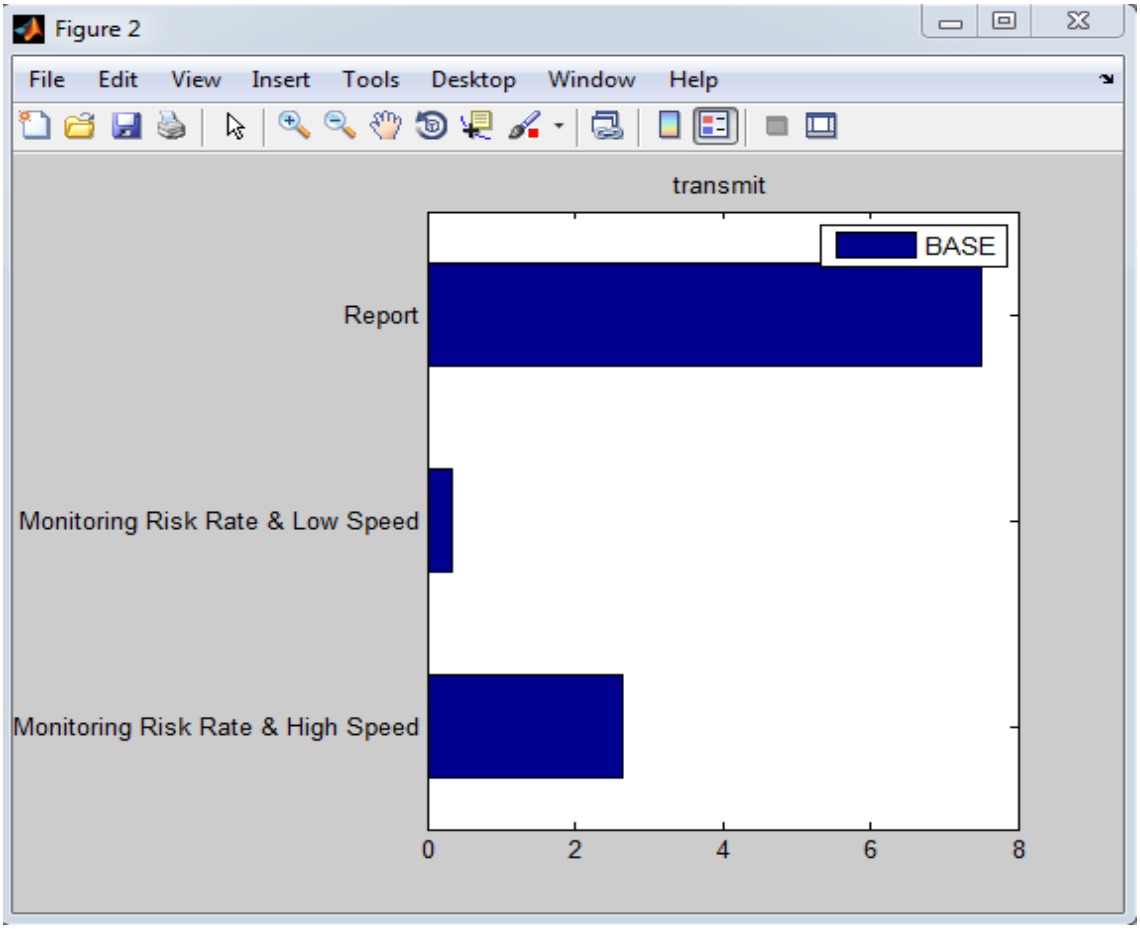


Figure 4.7: Common Node Vehicles

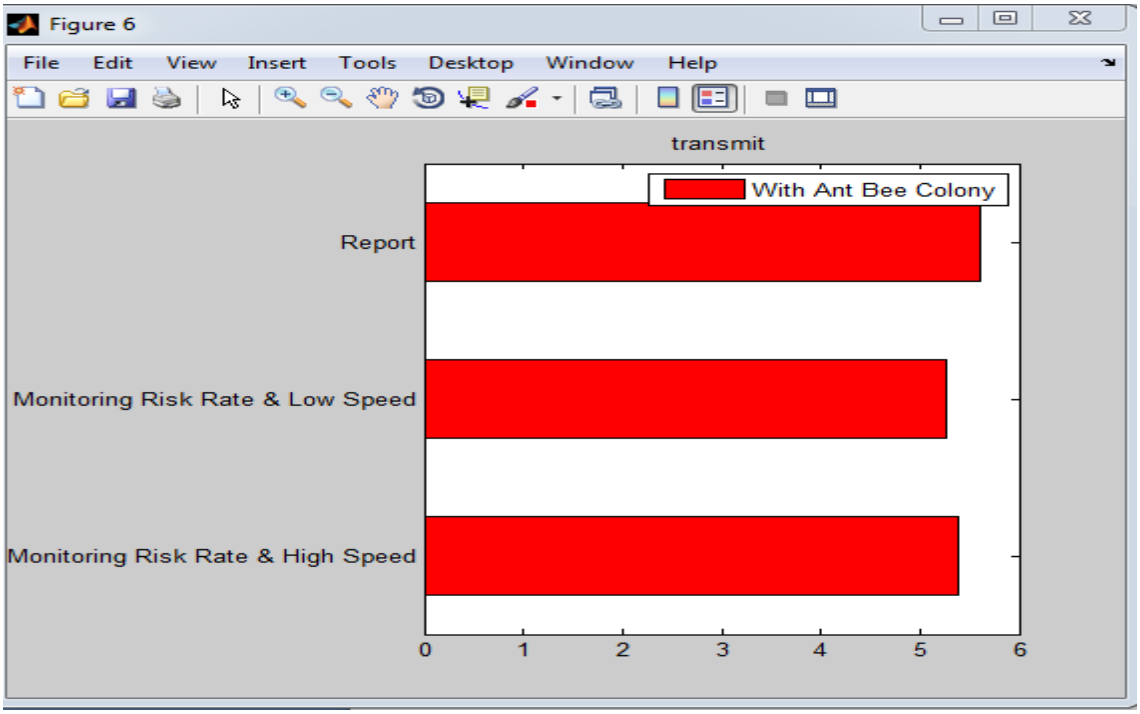
The Results are observed from different parameters. After studying the proposed model with the existing one four parameters are concluded that are: transmit, risk, trust and packet delivery.

Evaluation of transmit parameter:



(xlabel= Rate of change with respect to vehicle velocity in km/h)

Figure 4.8: Transmit Parameter without optimization



(xlabel= Rate of change with respect to vehicle velocity in km/h)

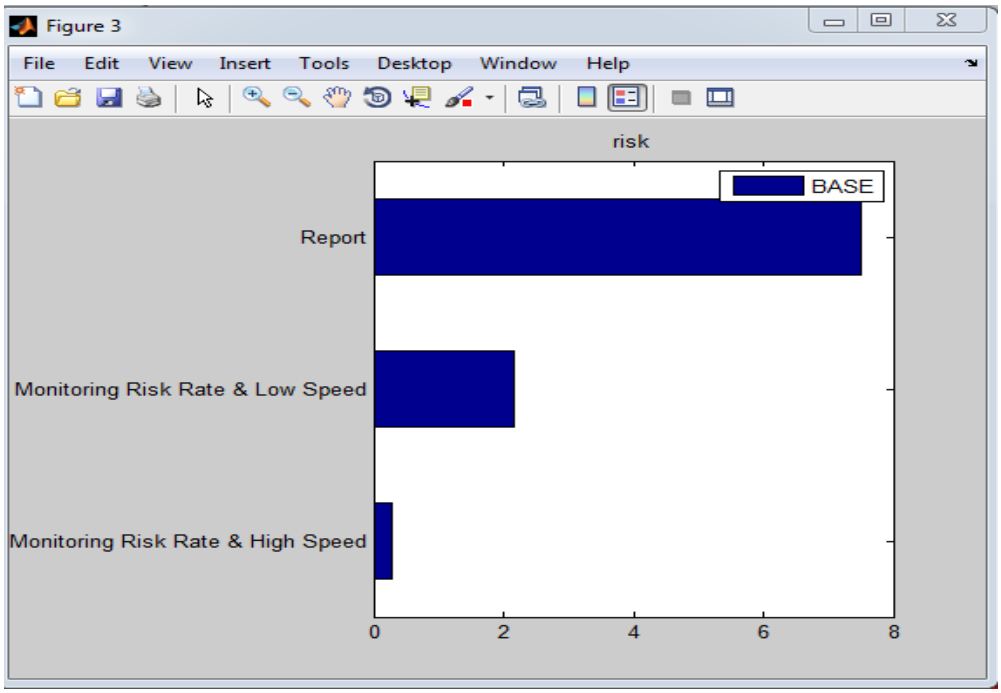
Figure 4.9: Transmit Parameter evaluation after optimization

Here we are considering the two methods for comparison, first one is the report and second one is the detection of driving patterns. On comparing the results of existing approach and the proposed approach, proposed approach comes out as a better then the existing one. Here the optimization is being done with the Ant Bee Colony algorithm. As the results are being compared (refer Figure 4.8 and Figure 4.9), when it comes to the monitoring risk rate, there is increase in detecting the risk for data transmission in case of proposed approach. When vehicles are moving at a high speed they are in the unstable state which is leading to increase in data transmission risk. So it depicts we should focus much more on monitoring the risk rate at higher speed as compared to the lower speed nodes.

Simulation Parameters	Value
Simulator	MATLAB2013
Methods for detection	Report and Driving Patterns
Optimization Algorithm	Ant Bee Colony

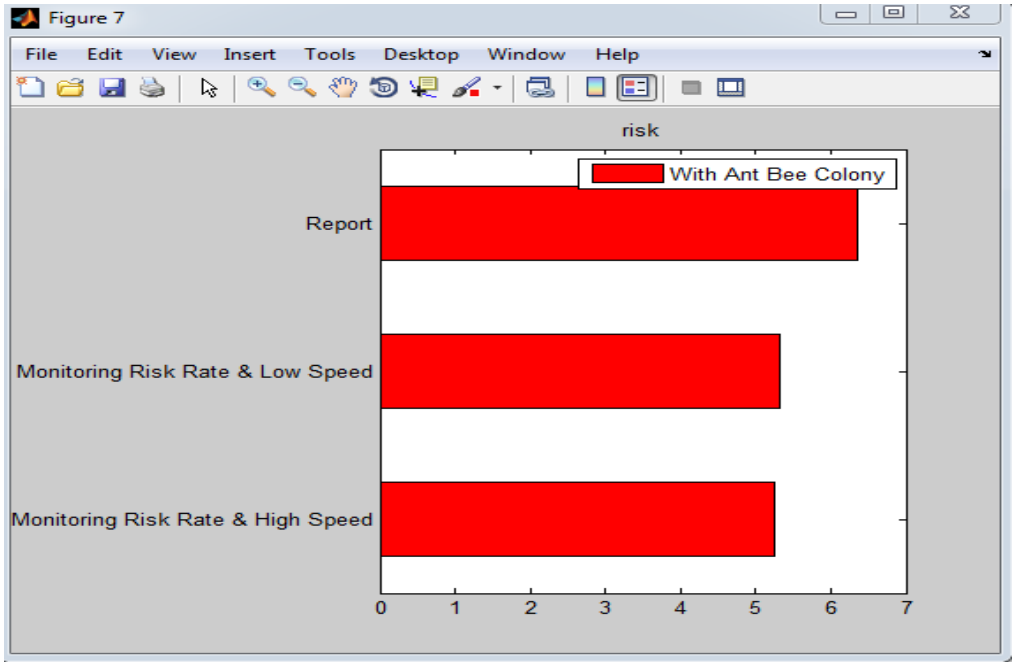
Table 4.2: Parameters for Simulation

Evaluation of Risk:



(xlabel= Rate of change with respect to vehicle velocity in km/h)

Figure 4.10: Risk evaluation without optimization

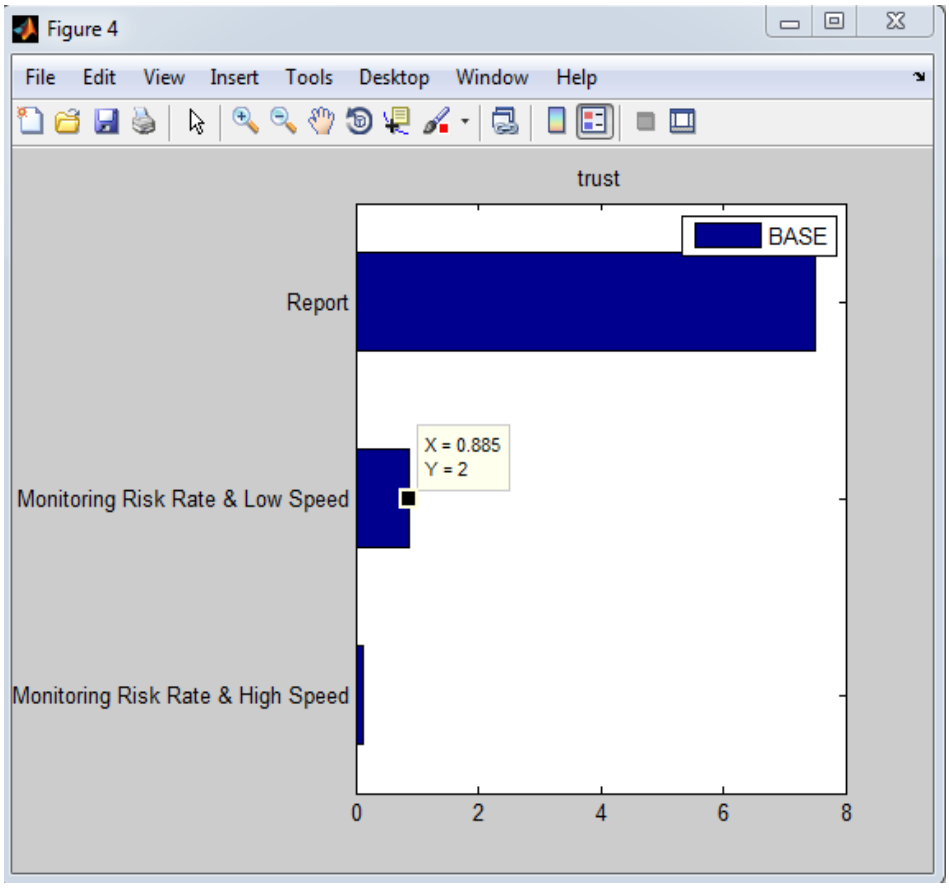


(xlabel= Rate of change with respect to vehicle velocity in km/h)

Figure 4.11: Risk evaluation with optimization

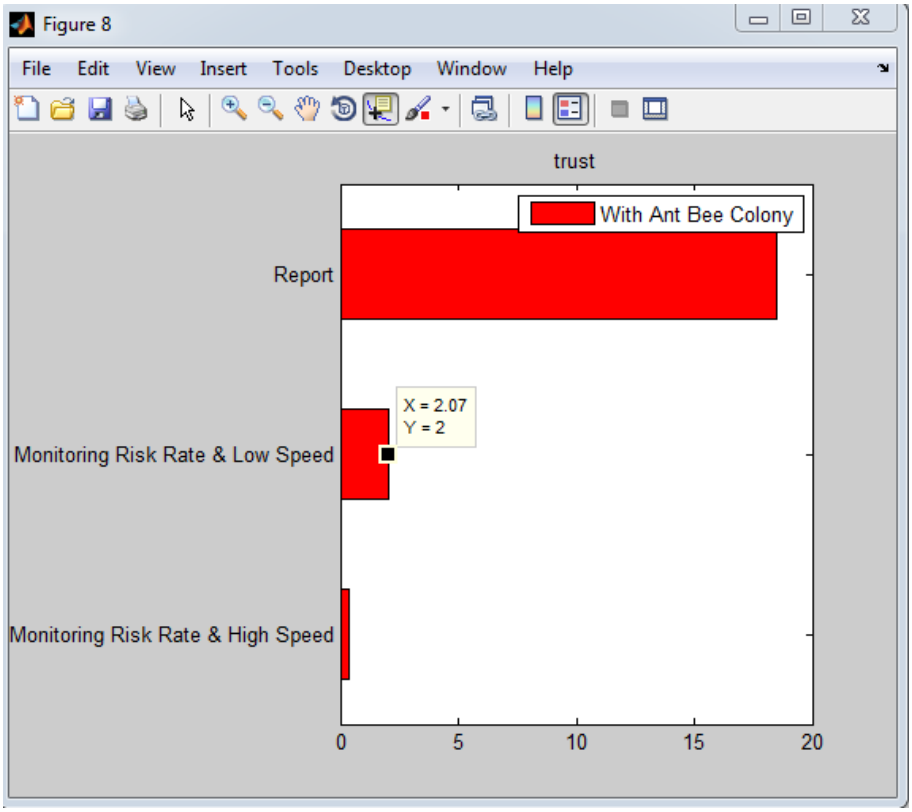
Here we are considering the two methods for comparison, first one is the report and second one is the detection of driving patterns. On comparing the results of existing approach and the proposed approach (refer Figure 4.10 and Figure 4.11), proposed approach comes out as a better then the existing one. Here the optimization is being done with the Ant Bee Colony algorithm. When it comes to compare the average risk for various driving pattern, slower speed vehicles appear to have a higher risk rate, which is depicting slower speed vehicles are having higher risk while transmitting the messages. This further leads to the affect on wide area network as they are not monitored completely. With the help of optimization algorithm monitoring the risk rate at slower speed has been taken into consideration.

Evaluation of Trust:



(xlabel= Rate of change with respect to vehicle velocity in km/h)

Figure 4.12: Trust evaluation without optimization



(xlabel= Rate of change with respect to vehicle velocity in km/h)

Figure 4.13: Trust evaluation with optimization

The above (refer Figure 4.12 and Figure 4.13) is supporting the assumption the nodes with the higher speed are having the decreased trust value in comparison the report methods. So the risk rate detection method is working accurately for the higher speed nodes in comparison of the slower ones.

Packet Delivery Ratio:

Increase in the number of vehicles is leading to increase in the network connectivity which is further reducing the chances of encountering network partition. When the density of network is sparse, vehicles are scattered, connectivity of the network becomes bottleneck, which is restricting the improvement in case of routing performance. With increase in the number of vehicles there is a increase in packet delivery ratio (refer Figure 4.14).

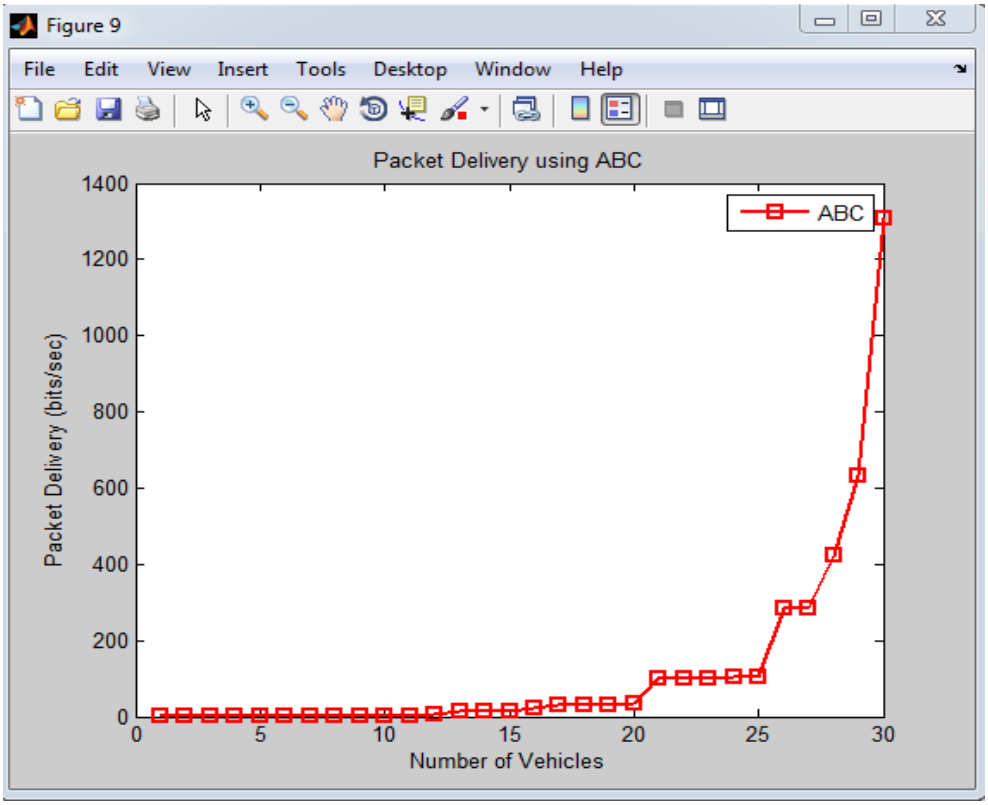


Figure 4.14: Packet delivery ratio with ABC optimization

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

We have proposed a system which is detecting the malicious node which appears to be a normal node. By detecting these nodes in the Vehicular Ad-hoc network we are improving the stability and performance of the system. Our work is taking into consideration how to improve the packet delivery ratio by the detection of malicious nodes and further enhancing the security of our system. Simulation results have shown that the proposed approach is better in terms of transmit, risk and the trust value of the nodes. These parameters are compared on the basis of two methods such as Vehicle behavior patterns and the Report. Our work is mainly focused on the compromised nodes and reducing the affect of these nodes in the Vehicular Ad-hoc networks. GTA (government transportation authority) is use as a admin for storing the locations of malicious nodes and capture process is done with the help of RSU. Therefore, by decreasing the malicious nodes and improving the routing with Ad-hoc on demand distance vector our network contribute to increased availability and performance of the system.

5.2 Future Work

Though our proposed work tried to introduce the model which is detecting the malicious nodes but still the work is pending. In this current scenario we are just detecting the malicious nodes and these nodes are storing in the GTA but further process is still remaining like blocking of the malicious nodes. We are not addressing any particular attack on general communication so in our further study we can redesigned the attacks also. Apart, from this we can also improve the Vehicle behavior patterns approach, for increasing the system performance and availability. For increasing the security of the whole network we can also work on the data security standards with AES and DES approach for encrypting the data packets. So, by adding some further steps or techniques we can easily enhance more security in the system.

REFERENCES

I. **Research Papers**

[1] C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs," *IEEE, 2007,* 2007 pp. 26–30.

[2] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security,* 2007, vol. 15, pp. 39–68.

[3] Y. Qian and N. Moayeri, "Design of Secure and Application-Oriented VANETs," *IEEE,* 2008, vol. 24, no.1, pp. 2794–2799.

[4] X. Lin, R. Lu, C. Zhang, H. Zhu, and P. Ho, "Security in Vehicular Ad Hoc Networks," *IEEE Communications Magazine* , 2008, vol.15, no. 4, pp. 88-95.

[5] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications,* 2008, vol. 16, no. 1, pp. 1–15.

[6] T. W. Chim, S. M. Yiu, and L. C. K. Hui, "SPECS : Secure and Privacy Enhancing Communications Schemes for VANETs," 2011, vol. 9, no. 2, pp. 189–203.

[7] Z. Baniasadi, A. Sanei, M. R. Omidi, and E. Eslami, "Modeling Composite Intrusion Detection Systems Using Fuzzy Description Logics," *International Symposium on Computer Networks and Distributed Systems (CNDS),* 2011, pp. 1–6.

[8] A. Rawat, S. Sharma, and R. Sushil, "VANET : SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS," *Journal of Information and Operations Management***,** 2012, vol. 3, no. 1, pp. 301-304.

[9] B. Ding, Z. Chen, Y. Wang, and H. Yu, "An Improved AODV Routing Protocol for VANETs," *IEEE*, 2011, vol. 7, pp. 1-5.

[10] F. A. Ghaleb, "Security and Privacy Enhancement in VANETs using Mobility Patterns," International Journal of Electronics, 2013, vol. 5, pp. 184-189.

[11] R. S. Raw, M. Kumar, and N. Singh, "SECURITY C HALLENGES , ISSUES A ND

THEIR SOLUTIONS FOR VANET," *International Journal of Network Security & Its Applications (IJNSA)*, 2013, vol. 5, no. 5, pp. 95–105.

[12] P. Sangulagi, "Recognition and Elimination of Malicious Nodes in Vehicular Ad hoc Networks (VANET ' s)," *Indian Journal of Computer Science and Engineering (IJCSE), 2013*, vol. 4, no. 1, pp. 16–22.

[13] S. Sarwa and R. Kumar, "Selective Forwarding Attack and Its Detection Algorithms : A Review," *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 2013, vol. 7, no. 7, pp. 918–921.

[14] M. B. Monir, M. Hashem, A. El, A. Adel, and A. Hamid, "A Trust-Based Message Reporting Scheme For VANET," *International Journal of Emerging Technology and Advanced Engineering, 2013*, vol. 3, no. 5, pp. 376-394.

[15] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, 2014, vol. 44, pp. 1–13.

[16] I. Engineering, "Delay Optimization in VANET Using Ant Colony Optimization and WI-MAX," *International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering*, 2014, vol. 3, pp. 1-8.

[17] S. J. Elias, M. Nazri, B. Mohd, R. B. Ahmad, A. Hanah, and A. Halim, "A Comparative Study of IEEE 802 . 11 Standards for Non-Safety Applications on Vehicular Ad Hoc Networks : A Congestion Control Perspective," 2014, vol. II, pp. 22–24.

[18] U. Khan, S. Agrawal, and S. Silakari, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks," *Procedia - Procedia Comput. Sci.*, 2015, vol. 46, no. Icict 2014, pp. 965–972.

[19] T. W. Chim, S. M. Yiu, and L. C. K. Hui, "IEEE TRANSACTIONS ON COMPUTERS VSPN : VANET-based Secure and Privacy-preserving Navigation," 2014, vol. 63 no. 2**,** pp. 510–524.

[20] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, and M. Younis, "Cross-Layer Scheme

for Detecting Large-scale Colluding Sybil Attack in VANETs," *Communication and Information Systems Security Symposium* , 2015, vol. 2, pp. 7298–7303.

[21] M. Kaur and M. Mahajan, "A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDOS Attacks in VANETs," *International Journal of Hybrid Information Technology*, 2015, vol. 8, no. 8, pp. 113–122.

[22] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. M. Zhang, and J. Rowe, "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving," *IEEE Communications Magazine*, 2015, no. 5, pp. 126–132.

[23] J. Kamani, "A Review on Sybil Attack Detection Techniques," *Journal for Research,* 2015, vol. 1, no. 1, pp. 27–31.

[24] D. Singh, "Deterministic AODV Routing Protocol for Vehicular Ad-Hoc Network," *International Journal of Recent Research in Mathematics Computer Science and Information Technology, 2015,* vol. 2, no. 1, pp. 259–264.

[25] S. Tzeng, S. Horng, T. Li, X. Wang, P. Huang, and M. K. Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET," IEEE on Transaction Vehicular Technology, 2015, vol. 9545, no. 1, pp. 1-12.

[26] N. J. Patel and R. H. Jhaveri, "Trust based approaches for secure routing in VANET : A Survey," *Procedia - Procedia Comput. Sci.*, 2015, vol. 45, pp. 592–601.

[27] K. M. A. Alheeti, A. Gruebler, and K. D. Mcdonald-maier, "An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars," , *Consumer Communications and Networking Conference (CCNC),* 2015, pp. 916–921.

[28] D. Gantsou, "On the Use of Security Analytics for Attack Detection In Vehicular Ad Hoc Networks*," International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC),* 2015, *vol. 2,* pp. 1-6.

[29] S. Wang and Y. He, "A Trust System for Detecting Selective Forwarding Attacks in VANETs," *Springer International Publishing Switzerland, 2016,* vol.4, pp. 377–386.

[30] G. S. Chirayil and A. Thomas, “A Study on Cost Effectiveness and Security of VANET Technologies for Future Enhancement,” *Procedia Technol.*, 2016, vol. 25, no. 1, pp. 356–363.

[31] M. Kaur and M. Mahajan, “Protection Against DDOS Using Secure Code Propagation In The VANETs,” *An International Journal of Engineering Sciences,* 2016, vol. 17, no. 1, pp. 573–577.

[32] K. Lim, “Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive- Based Architecture for Vehicular Cloud,” 2016, vol. 19, pp. 1-104.

[33] A. Info, “Design and Analysis of Secure VANET Framework preventing Black Hole and Gray Hole Attack,” *International Journal of Innovative Computer Science & Engineering* **,** 2016**,** vol. 3, no. 4, pp. 9-13.

[34] F. Jamil, A. Javaid, T. Umer, and M. Husain, “A comprehensive survey of network coding in vehicular ad-hoc networks,” *Wirel. Networks*, 2016, pp. 1-20.

[35] H. Hu, S. Member, R. Lu, S. Member, Z. Zhang, and J. Shao, “REPLACE : A Reliable Trust-based Platoon Service Recommendation Scheme in VANET,” 2016, *IEEE Transactions on Vehicular Technology*, vol. 9545, no. c, pp. 1–11.

[36] A. Shaheen, “Comparison and Analysis Study between AODV and DSR Routing Protocols in VANET with IEEE,” *Journal of Ubiquitous Systems & Pervasive Networks*, 2016, vol. 7, no. 12, pp. 7-12.

[37] T. E. Ali and L. A. Khalil, “Review and Performance Comparison of VANET Protocols: AODV, DSR, OLSR, DYMO, DSDV & ZRP,” *Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AICMITCSA)*, 2016, vol. 5, pp. 1-6.

[38] A. Chakraborty and A. K. Kar, “Swarm Intelligence : A Review of Algorithms,” Springer International Publishing AG, 2017, vol. 10, pp. 475–494.

II. Books

[39] Ad Hoc Mobile Wireless Networks: Protocols and Systems-2007 by C.K.Toh (Author)

[40] Computer Networks (5th Edition) by Andrew S. Tanenbaum (Author)

[41] Ad-Hoc Wireless Networks (1st Edition) by C. Siva Ram Murthy (Author)

III. Websites

[42] https://en.wikipedia.org/wiki/Vehicular ad hoc network

[43] http://www.trincoll.edu/Litc/its/computing/Pages/Wired.asp

[44] http://www.conceptdraw.com/examples/wireless-network-topology

[45] https://en.wikipedia.org/wiki/Comparison_of_wireless_data_standards

[46] http://sociallab.fer.hr/innosoc/case-studies/zagreb-2016/intelligent-transport-systems-and-vehicular-ad-hoc-networks/

IV. Reports and Official Documents

[47] http://www.ece.virginia.edu/mv/pubs/tutorials/icc2011/SP-4-addendum.pdf

[48] http://pnrsolution.org/Datacenter/Vol3/Issue3/16.pdf

APPENDIX

GLOSSARY OF TERMS

A

Attack

Ad-hoc

Authentication

Avaliability

C

Confidentiality

D

Dedicated Short Range Communication

DoS attack

I

Integrity

N

Network

Node

P

protocols

S

Security

V

Vehicular Ad hoc Network