# Mitigation of Wormhole Attack in VANETs using Trust based secure DV-Hop Localization Algorithm

*Thesis submitted in partial fulfillment of the requirements for the award of degree of*

**Master of Engineering**

in

**Information Security**


*Submitted By*

**Ritu Rani**

**(Roll No. 801433024)**

Under the supervision of:

**Ms. Tarunpreet Bhatia**

Lecturer, CSED

**Mr. Vinod Kumar Bhalla**

Assistant Professor, CSED



COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004


**July 2016**

# CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, *"Mitigation of Wormhole Attack in VANETs using Trust based secure DV-HOP Localization Algorithm "*, in partial fulfilment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Ms. Tarunpreet Bhatia, Mr. Vinod Kumar Bhalla* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Ritu Rani
Ritu Rani
801433024
ME (IS)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

**(Ms. Tarunpreet Bhatia)**
Lecturer, CSED

**(Mr. Vinod Kumar Bhalla)**
Assistant Professor, CSED
Thapar University, Patiala

**Countersigned by**

**Dr. Manpreet Singh**
Head
Computer Science and Engineering Department
Thapar University
Patiala

**Dr. S. S. Bhatia**
Dean (Academic Affairs)
Thapar University
Patiala

# ACKNOWLEDGEMENT

First of all, I would like to express my heartfelt appreciation to my supervisor Ms. Tarunpreet Bhatia and co-supervisor Mr. Vinod Kumar Bhalla for their constant guidance, great support, immense patience and valuable advice throughout my research at the Thapar University, Patiala. They helped me in finding research topics, proposing solutions and verifying results. Without their cooperative attitude, endless efforts and advices, this research would have never been possible. It has been a great honour and pleasure for me to do research under their supervision. I sincerely would like to thank Dr. Maninder Singh, Head of the Department, Computer Science engineering, Thapar University, Patiala for his support during my work.

Last but not the least I would like to thank my parents, my colleagues and friends for their encouragement and love.

Ritu Rani

(801433024)

# ABSTRACT

Vehicular Ad-hoc Network (VANETs) is an encouraging approach that aids the vehicles to form a self-organized network in the absence of centralized infrastructure. It is the constituent of MANET and supports intelligent transport system (ITS). Each node is moves freely in ad-hoc network and therefore vehicles are not stable. Due to lack of centralized architecture, security becomes the crucial aspect of ad-hoc network. Cryptographic techniques such as digital signatures and encryption are unable to give the significant results to deal with the wormhole attacks. Wormhole attacks are the most dangerous attacks that hinder the routing operation by introducing wormholes nodes that create tunnel among themselves in order to create the disturbance in the network. In order to deal with this issue, an algorithm is proposed in this research work that would mitigate the severe effects of the wormhole attacks in order to improve the network performance. The range-free localization technique i.e. DV-Hop Algorithm provides the list of trusted nodes when the trust factor of each node is calculated on the basis of RTT. The parameters evaluated by simulating the VANET environment in NS2 are Packet Delivery Ratio (PDR), Throughput and End to End delay has shown the effective results using the proposed algorithm.

*Keywords:* VANET, RTT, Anchor nodes, Trust and DV-Hop

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVATIONS

| | |
|---|---|
| VANETs | Vehicular Ad-hoc Network |
| V2I | Vehicle to Infrastructure |
| V2V | Vehicle to Vehicle |
| WAVE | Wireless Access Vehicular Environment |
| DSRC | Dedicated Short Range Communication |
| RSU | Road Side Unit |
| OBU | On Board Unit |
| AODV | Ad hoc On-Demand Distance Vector |
| RTT | Round Trip Time |
| AN | Anchor Nodes |
| WADP | Wormhole Attack Detection and Prevention |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| NAM | Network Animator |
| TCL | Tool Command Language |
| PDR | Packet Delivery Ratio |
| E2E Delay | End to End Delay |
| RREQ | Route Request |
| RREP | Route Reply |

# CHAPTER 1
# INTRODUCTION

## 1.1 Introduction

With the increase of large amount of vehicles on road every day, safety becomes a major concern nowadays. Due to the excessive speed of vehicles, lots of people lost their lives accidently. To reduce the road accidents, one possible way is to exchange the information among vehicles on time which helps them to analyse the traffic environment [1]. The information can be exchanged between vehicles in a vehicular ad-hoc network known as VANETs. VANETs are appearing as an encouraging field in wireless technology which aims to create a mobile network in which vehicles communicate with each other in the absence of centralized architecture that helps to improve the road safety by exchanging the messages among vehicles or by providing new convenient services to the road users [2]. It is the promising technology that supports Intelligent Transport System (ITS). VANET is a subclass of MANET that uses the moving vehicles as nodes to build a self-organized network and the nodes move freely within the network coverage area. VANETs differ from MANETs due to various reasons such as: High flexibility, quickly changing network topology, time constraint, indefinite network size etc [3].

VANETs are the special case of ad-hoc networks that involves Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication for security and non-security applications [4]. The communication between vehicles is achieved through a medium i.e. Wireless Access Vehicular Environment (WAVE). If the distance among vehicles is short then the communication can be done between vehicles through Dedicated Short Range Communication (DSRC) which operates on 5.9GHz frequency band and provides 6 to 27 Mbps data rate over 1000ms communication range [5]. In VANETs, Road Side Unit (RSU), On-Board Unit (OBU) and Application Unit (AU) are the main components that help the vehicles to communicate with each other. Usually, OBU is a peer device which is mounted on the vehicles and exploits the services provided by RSUs. OBU consist of sensors to send secure data and reliable messages to other vehicles. RSU is equipped with the device which is located on the road side. RSU act as a provider because it provides the

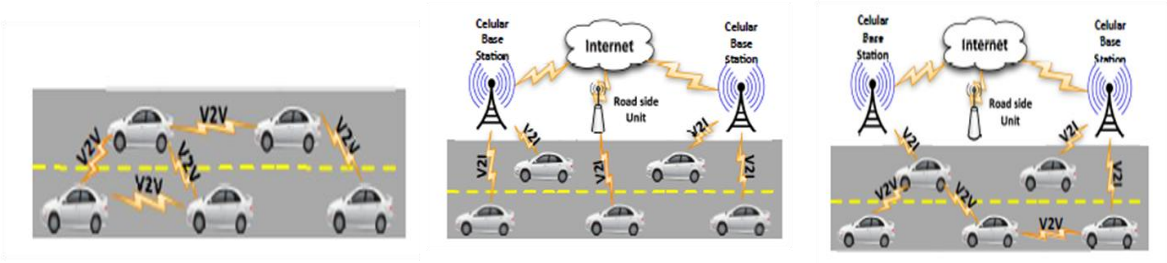
services, internet connectivity and helps to enlarge the communication range by reorganizing the information to other OBUs. AU is a device which is mounted on the vehicles that uses the services provided by the RSU with the help of OBU [6].

VANETs have certain advantages such as providing frequent information to the drivers, reduction of road accidents etc. It also provides safety and non-safety applications. The ultimate goal of VANETs is to transfer the messages among vehicles efficiently. The transferred messages have a great impact on the driver's behavior if the unauthorised user alters the messages which results to change the network topology. In VANETs, attackers create a problem by launching numerous attacks which lead to disturb the network condition and security may be threatened by disclosing Ids, sending bogus information, forging data, jamming the traffic, violating privacy etc. So, security is still an open issue in the ad-hoc network.

## 1.2 VANET Framework

Due to the support of Wireless communication in VANETs, it makes possible for the vehicles to exchange information between vehicles. The ad-hoc nature of VANET helps to deploy three types of communication:

- **Vehicle to Vehicle (V2V) communication:** This is also known as inter-vehicle communication in which vehicles communicate with each other without any infrastructure support and can be engaged for security applications.
- **Vehicle to Infrastructure (V2I) communication:** V2I allows the vehicles to communicate with RSUs to gather information.
- **Hybrid Communication:** This is a combination of V2V and V2I communication. In Hybrid communication, vehicles can communicate with RSUs in a single or multi-hop fashion depending upon the distance.




(a) V2V Communication (b) V2I Communication (c) Hybrid Communication

Figure 1.1: VANETs Framework [7]

## 1.3 VANET Characteristics

As MANETs and VANETs both have some trivial characteristics such as no centralization node, self management, short bandwidth but VANETs have some exclusive characteristics that make it more challenging which are discussed below:

- **High Flexibility:** A vehicular ad-hoc network is highly flexible due to fast speed of vehicles which makes harder to predict the node's position in VANETs.
- **Quickly changing network topology:** Due to high flexibility and the irregular speed of vehicles, the vehicles may leave or join the network in very short duration. This leads to change the network topology frequently.
- **Indefinite network size:** The network size in VANETs is geographically indefinite because VANETs can be carried out for one city, distinct cities or for countries.
- **Time constraint:** To make the decisions accurate, the information in VANETs must be conveyed to the nodes within time. Otherwise the system becomes worthless.
- **Frequent change of information:** Due to the ad-hoc nature of VANETs, the nodes collect information from other vehicles and RSUs. This result frequently changes of information among vehicles.
- **Improved physical security:** As the VANET nodes are physically secured which makes harder to compromise the nodes physically and lowers the consequences of infrastructure attack.

## 1.4 Applications of VANETs

Number of applications has been developed due to the communications among vehicles which leads to transfer the ample amount of information to the drivers and travellers. This leads to increase the road safety and convenience to the drivers. To deploy VANETs, applications play an important role that can be categorized into two categories [1] [7]:

i. **Safety Applications:** The main goal of safety applications is to provide the security on road in order to reduce the collision among vehicles by focusing on the following points:
   - **Collision Avoidance:** Collision can be avoided if drivers get alert before few minutes of vehicle collision.
   - **Traffic Signal Warning:** It includes lane change warning, speed warning which helps the drivers to run their vehicle safely and leads to cooperate driving.
   - **Traffic Signal Violation:** RSUs broadcast the messages to alert the vehicles about signal violation.
   - **Traffic accumulation:** Traffic can be accumulated by sending alerts like trouble, mishap to the drivers so that they can choose alternate route to stay away from accidents.

ii. **Comfort Applications:** These applications focus on the comfort level of the drivers and come under non-safety applications. These applications are also known as Entertainment applications. It provides services like sharing movies, songs, internet access, information of weather etc between the vehicles in the network.

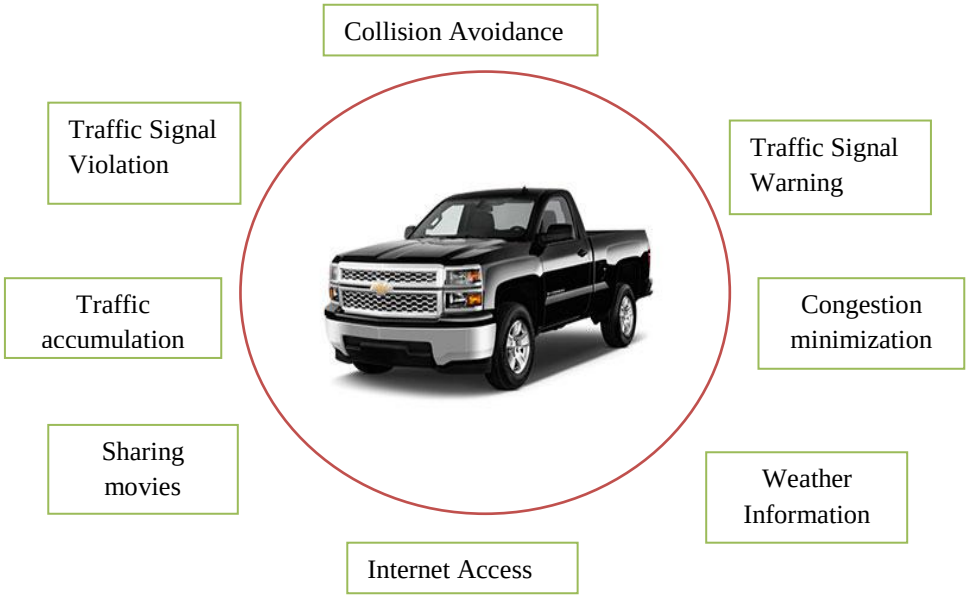



Figure 1.2: Road Safety and Comfort Applications of Vehicular Networks

## 1.5 Challenges in VANETs

There are different kind of challenging issues comes under VANETs that may be technically, socially, economically and security bases challenges:

- **Network administration:** Due to high flexibility in the nodes in VANETs, the network topology changes frequently which makes harder to use and maintain tree structures.
- **Collision control:** The indefinite network size is a big challenge in VANETs. During the traffic jam, the traffic load increases and network becomes congested and collision appears in the network.
- **Security:** Security is a major issue in VANETs. In VANETs, Due to its ad-hoc nature the vehicles exchange information with each other by transferring the messages in the network for security applications. So safety of the messages must be satisfied by stopping the messages from being altered.
- **Time critical:** VANETs are time analytical where the messages among vehicles should be exchanged within time which leads to lower the collision in the network. Fast cryptographic algorithm should be used to achieve the time constraint.

- **High mobility:** As in VANETs, nodes move at very high speed which helps the vehicles to run dynamically in irregular directions. Hence, it becomes difficult to know the node's position.
- **Data consistency:** In security perspective, data consistency came out to be major challenge in ad-hoc networks. In VANETs, even the genuine node perform mischievous activities that results to disrupt the whole network.

## 1.6 VANET Routing Protocols

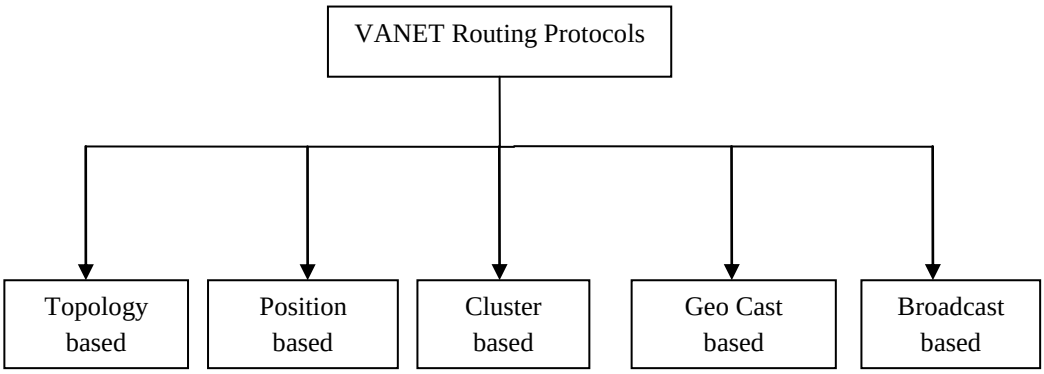



Figure 1.3: Topology based routing in VANETs

VANET routing protocols are divided into five categories: Topology based, Position based, Cluster based, Geocast routing, Broadcast routing.

- **Topology based routing protocols:** To carry out packet forwarding, these protocols use links information that exist in the network. Topology based routing protocols are further divided into proactive (Table-driven) and reactive (On-demand) routing protocols. In proactive routing protocols, every node maintain routing table in order to store the routing information about other nodes. Routing information is updated either periodically or when the network topology changes. They do not need a route discovery mechanism. DSDV and OLSR are the proactive routing protocols. In reactive routing protocols, routes are determined on-demand by following the route discovery process. DSR and AODV are the reactive routing protocols.
- **Position based routing protocols:** This is also known as geographic routing protocol. In order to select the next forwarding hops, these protocols use the

geographic positioning information [8]. These protocols are useful because there is no need to create and preserve the global route among source and destination. Position based greedy V2V protocols and DTN come under position based routing protocols.

- **Cluster based routing protocols:** In cluster based routing, clusters are formed and there is one node designated as cluster head which is responsible for broadcasting the packets to the other nodes. Cluster head perform two types of functions i.e. intra-cluster and inter-cluster management functions. Intra-cluster exchange information with other nodes using direct links and inter-cluster exchange information with other nodes via cluster headers [9].
- **Geocasting routing protocols:** These are location based multicast routing protocols. The main objective of these protocols is to transfer the packets from source to destination within the pre-defined geographical region [10].
- **Broadcast routing protocols:** These protocols are used to broadcast the messages that need to be scattered among vehicles beyond the transmission range. These protocols are useful for describing the road conditions, sending emergency alerts, providing the weather information and for advertisements.

Table 1.1: Comparison of routing protocols in ad-hoc networks

| **Types of protocols** | **Topology based protocols** | **Position based protocols** | **Cluster based protocols** | **Geo cast routing protocols** | **Broadcast protocols** |
|---|---|---|---|---|---|
| Forwarding Method | Wireless multihop | Heuristic | Wireless multihop | Wireless multihop | Wireless multihop |
| Map prerequisite | No | No | Yes | No | No |
| Virtual Infrastructure provision | No | No | Yes | No | No |
| Real Traffic flow | Yes | Yes | No | Yes | Yes |

## 1.7 Outline of AODV protocol

AODV is a reactive routing protocol because it finds the route to destination when it is needed. It comprises two phases: Route Discovery phase and Route maintenance phase.

- **Route Discovery phase:** In route discovery phase, source discovers path to destination by broadcasting RREQ packet. Each RREQ packet contains the source id, destination id, source sequence number, destination sequence number, TTL fields and broadcast id. When the route request packet is received by the intermediate node, it either sends RREP to the source node if it founds valid path in its own cache or forwards it to other node. Before forwarding the packet, the intermediate node stores all the possible information such as address of the previous node and broadcast id extorted from source route incorporated in a data packet. It also maintains a timer so that it can be able to delete the entry if the reply is not received before the timer expires.

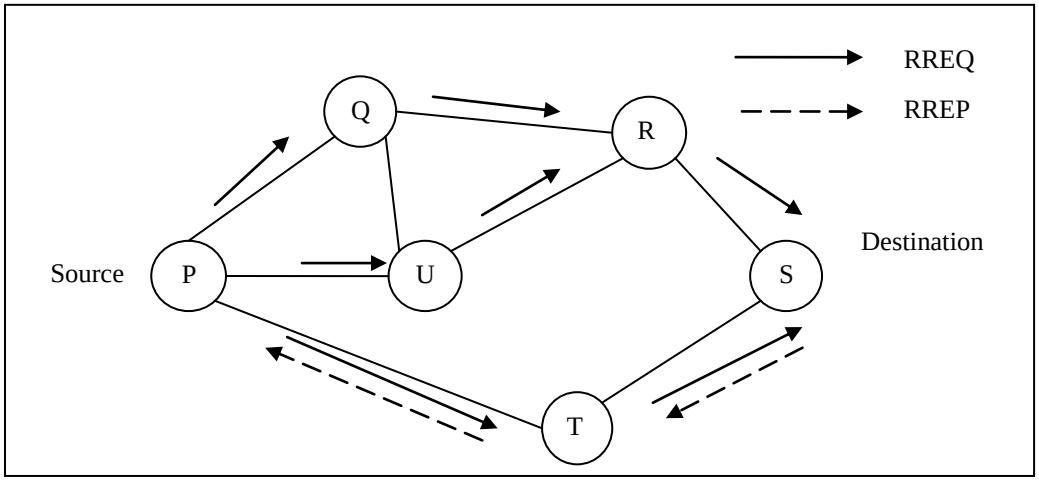



Figure 1.4: Broadcasting RREQ packets to discover path and RREP packets to reply back to the source node

- In Figure 1.4 Node P wants to deliver packet to node S. Firstly it will discover path by broadcasting the RREQ packets to their respective nodes. If the respective nodes already receive the same packet from the nodes, then they will discard the packet and rebroadcast the packets to discover the path for destination. This process continues until the route is not discovered. When the

packet reaches to the destination node S, the node S prepares a route reply by adding data and forwards it to the source node P again.

- **Route Maintenance phase:** In route maintenance phase, if any link is broken then route is maintained by sending RERR packet to the respective nodes so that they can update their own cache and can be able to start a new route discovery process.

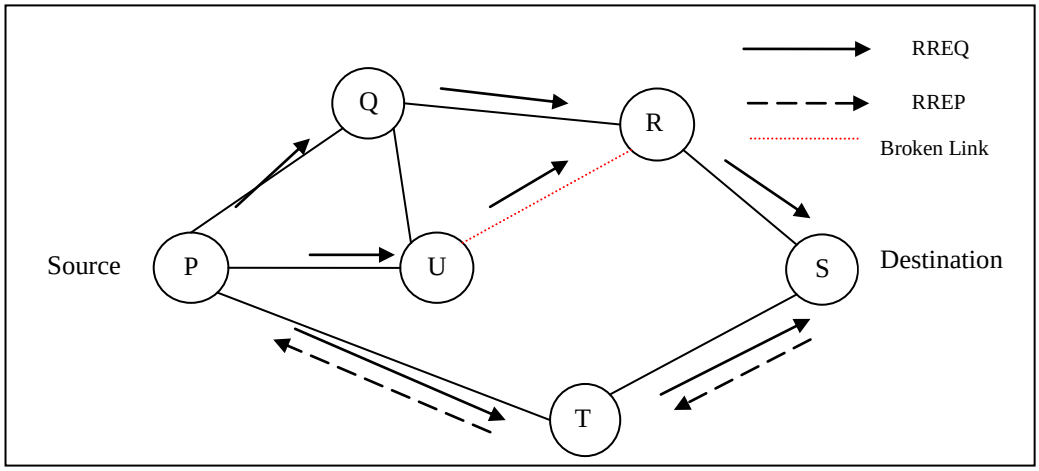



Figure 1.5: Route Maintenance phase in AODV

In Figure 1.5 link is broken between node U and node R, then RERR packet is propagated to the source node back so that it can again start a route discovery process.

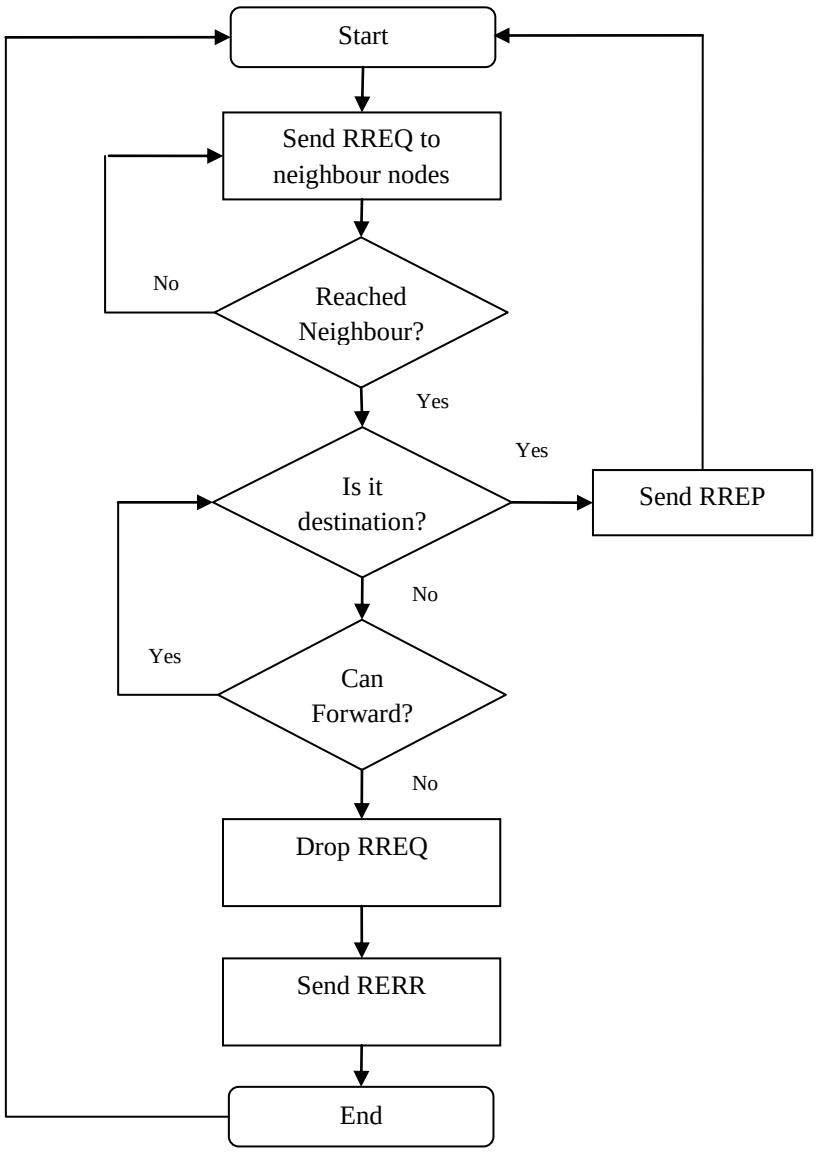



Figure 1.6: Flowchart of AODV

## 1.8 Organisation of Thesis

- Chapter 2 reflects security in vanets
- Chapter 3 summarizes the literature review related to the detection of attacks in wireless networks
- Chapter 4 demonstrates the problem statement and its objectives
- Chapter 5 describes the simulator used
- Chapter 6 defines the proposed work and implementation
- Chapter 7 validates the results of the proposed work
- Chapter 8 concludes the research work and discusses its future aspects

# CHAPTER 2
# SECURITY IN VANETS

## 2.1 Security issues in VANETs

Security is the major concern in VANETS to maintain the security in wireless environment. Adversaries launch different type of attacks to disrupt the whole network by tampering the original messages. So, before we analyze diverse attack categories, we look at how attackers are classified on the basis of their nature and scope to destruct the system as follow [11]:

- **Active attackers:** These attackers are very harmful for the system because they generate the packets by modifying the actual content of the message and do not forward the acknowledged message.
- **Passive attackers:** These attackers spy on the wireless medium to gather useful information which may be moved to other attackers but do not engage in the communication process of the network.
- **Insider attackers:** These attackers are the legitimate users of the network and have the concrete knowledge of the network. They are very dangerous as compared to other attackers because it's simple for them to fire attacks against the network.
- **Outsider attackers:** These are invaders who have goal to exploit the network but they generate lesser problems as compared to the insider attackers.
- **Rational attackers:** These attackers launch attacks for the purpose of getting personal benefits.
- **Local attackers:** These attackers fire an attack which is confined to a particular area.

## 2.2 Attacks in VANETs

There are diverse attacks that harm the security of the VANETs by disturbing the whole network and the confidentiality of vehicles. The attacks that have drastic effect on the services of the system are discussed below:

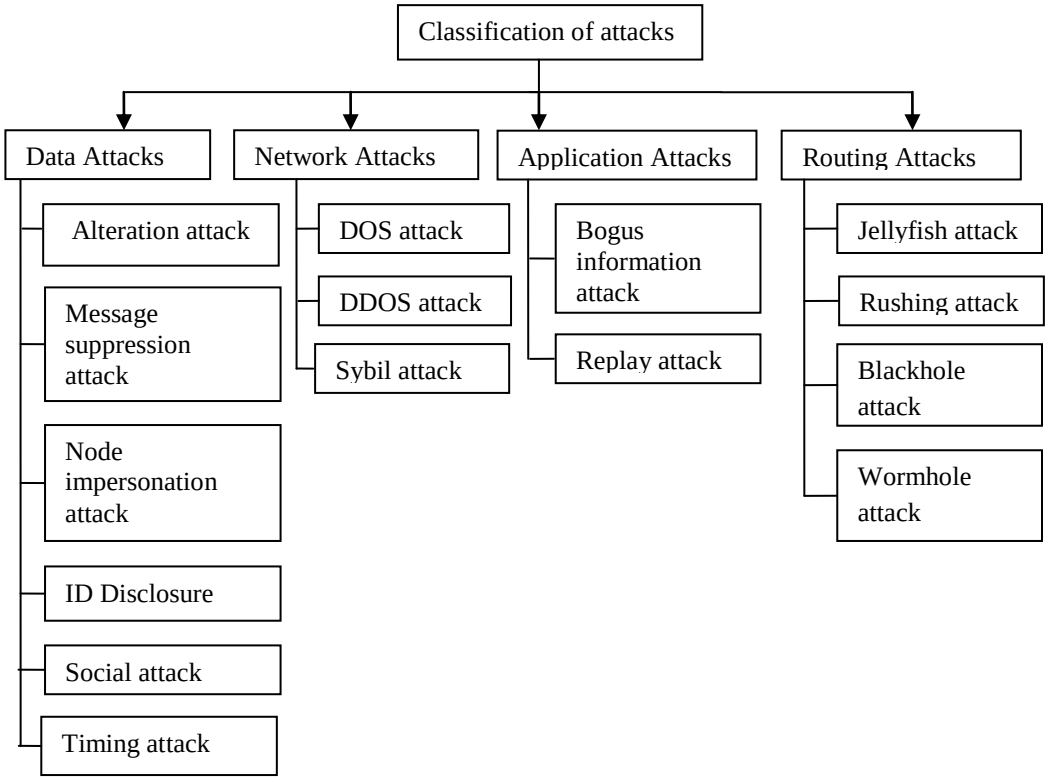



Figure 2.1: Classification of attacks

**2.2.1 Data Attacks:** These are the attacks in which attacker tampers the data and forwards the fake data in the network. Following attacks come under the category of data attacks:

- **Alteration attack:** This is the attack in which an attacker modifies the actual content of the message and forwards it in the network. Thus creates confusion in the whole network.
- **Message suppression attack [12]:** In this attack, an attacker suppresses the packets by selectively dropping the packets which include the critical information for the receivers and these packets are used by attacker at some other time. It prevents to give congestion alerts to the road users so that they cannot be able to alter their path and they have to forcibly wait in the traffic.
- **Node impersonation attack:** This is the network attack in which attacker modifies the original content of the message and forwards it in the network by claiming that message has been originated from the authorised user. Greedy algorithm is used to detect and isolate the node impersonation attack.

- **ID Disclosure:** This is the network attack in which attacker tracks the location of destination node by disclosing the identity of nodes in the network. Observer looks at the destination node and relay the virus to the neighbours of the destination node so that ID and the location of the destination node can be taken.
- **Social attack [13]:** The main goal of this attack is to puzzle and fascinate the vehicle by sending correct and incorrect messages so that driver gets upset. It indirectly creates the problem in the network so that authenticated user exhibits angry behavior which is the main objective of the attacker.
- **Timing attack [14]:** Timing attack is very crucial for safety applications. This is the attack in which an adversary adds some time slot in the authentic message but do not modify the content of the message and thus create a delay in the authentic message. With this the collision occurs, thus it creates a major problem for the drivers because drivers do not receive the information on time.

**2.2.2 Network attacks:** These are the attacks in which attackers directly affect the vehicles by disturbing the whole network. There are the following attacks that come under network attacks are:

- **Denial of Service (DOS) attack:** DOS is one of the dangerous attacks in VANETs. In DOS attack, attackers use the vehicle resources and create a troublesome situation by jamming the communication channel so that authenticated users cannot be able to access the network services. For e.g. Jamming attack is the DOS attack
- **Distributed Denial of Service (DDOS) attack:** In DDOS attack, attacker use the multiple computers to launch attack and uses the different locations and time slots to send messages to other vehicles. The main goal of the DDOS attack is to halt the network.
- **Sybil Attack [2]:** Sybil attack allows an attacker to create multiple false identities known as Sybil nodes which will behave as a normal node. It provides false belief to other vehicles by sending erroneous messages such as traffic jam etc and each message contains the formulated id. The main objective of an attacker is to disturb the whole network for their personal benefits.

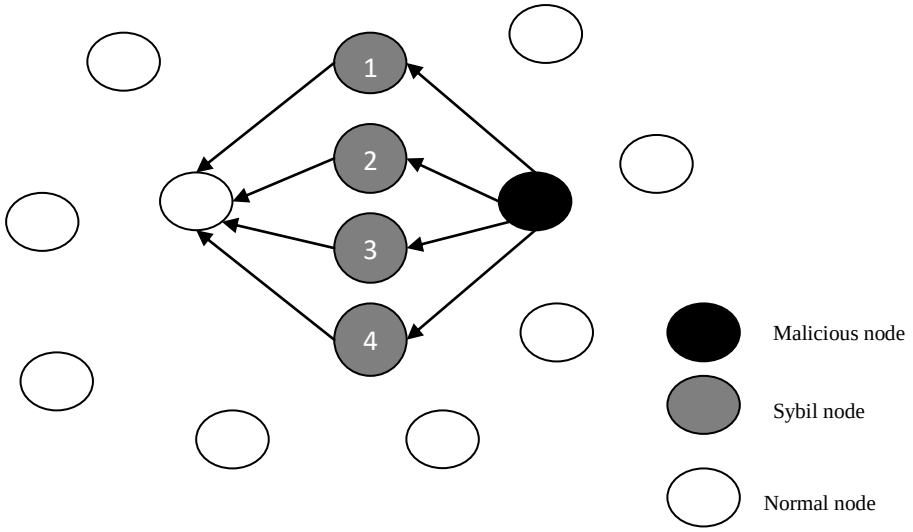



Figure 2.2: Sybil attack

In Figure 2.2, node 1, node 2, node 3 and node 4 are the Sybil nodes that use the identity of others while communicating with the other nodes to confuse and collapse the network.

**2.2.3 Application attacks:** These are the attacks in which attacker modifies the content of the message for taking personal advantage. The attacks described below are the application attacks:

- **Bogus information attack [15]:** In Bogus information attack, the adversary may be outsider or insider. The main objective of an adversary for launching this attack is to send erroneous or bogus information in the network to create disturbance and for his personal benefits.
- **Replay attack:** In replay attack, the attacker takes an advantage by replaying past messages in order to confuse the authorities and creating a jam among vehicles.

**2.2.4 Routing attacks:** These are the attacks in which attacker spoofs the routing information by launching diverse attacks on routers which are described below:

- **Jellyfish attack [16]:** In Jellyfish attack, attacker introduces delay in the packets instead of silently dropping the packets as is done by the Blackhole and Wormhole attack. In this attack, attacker node became a part of network

after getting access of it. This results the degradation of QOS in the network and end-to-end delay.

- **Rushing attack:** In this attack, every node before broadcasting the data, first established an authentic way to the destination node using a routing protocol such as AODV, DSR etc. The attacker set a fast transmission path by exploiting the duplicate suppression mechanism to forward the packets. With this process the destination node accepting the packets those are propagated faster than the multi-hop normal route and start dropping the original packets. This forms the rushing attack.

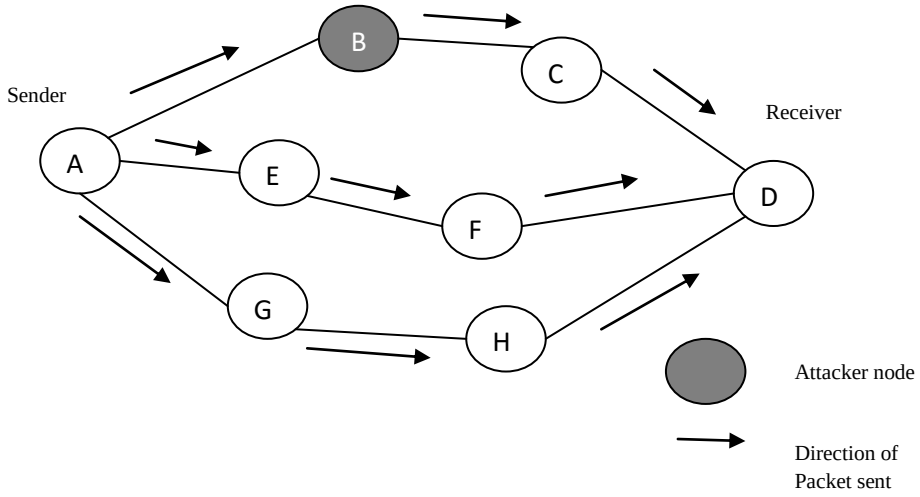



Figure 2.3: Rushing attack

In Figure 2.3, A is the sender node and D is the receiver node. When node A forwards packet to receiver node, if there is an attacker present then he will accept the packet and forward it with the high transmission speed as compared to the other nodes. In this way, receiver found this path as a valid route and discards the packets that came from other routes.

- **Blackhole attack:** In this attack, an attacker introduces a malicious node in the network which attracts all other nodes and pretending as the original one. When all other nodes make a false belief on the malicious node and start sending packets through the malicious node then it selectively drop the packets.

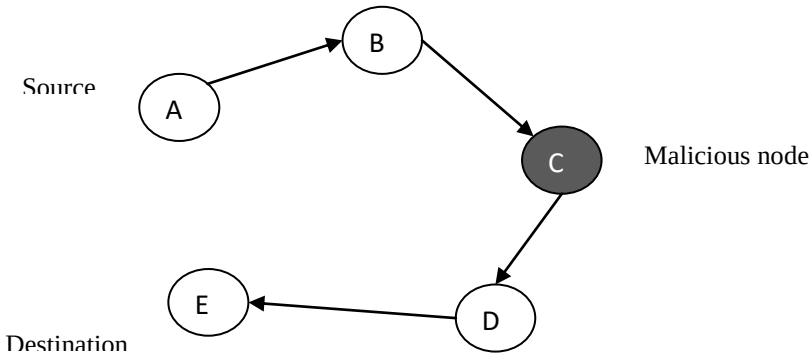



Figure 2.4: Blackhole attack

In Figure 2.4, Node A is the source node and Node E is the destination node. The attacker node introduces the malicious node i.e. Node c which pretends as an original node. When source node sends packet to the destination node, then the malicious node selectively drop the packets in the network which degrades the communication among nodes.

- **Wormhole attack:** This is the attack in which attacker joins the two faraway parts of ad-hoc network using an additional communication channel as tunnel. The tunnel records the ongoing communication at one network position and transmits the recorded communication at other network position. This process is also known as tunnelling [17]. To launch this attack, attacker introduces two malicious nodes which are assumed as neighbour nodes that help to transfer the data using tunnel. The malicious nodes attract the other nodes by advertising the shortest path among them so that they can be able to transfer the packets from one network to another network. The path introduced to transfer the packets is harder to predict because it is not a part of real network. Figure 2.5 below shows the wormhole attack where node P (Source) wants to transmit packets to node T (Destination). M1 and M2 are the attacker nodes which are neighbours of node P and T and tunnel is created between them which records the ongoing communication, tampering the data and forward it to the destination.

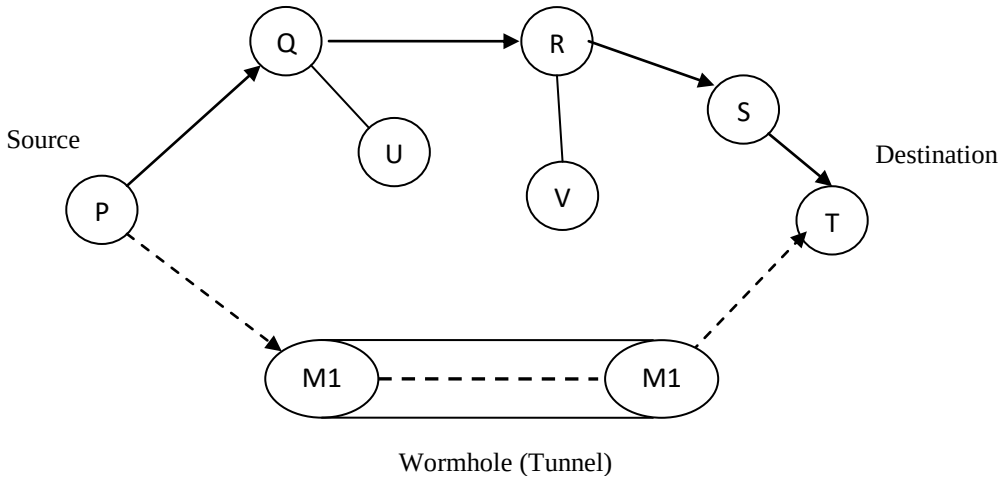



Figure 2.5: Wormhole attack

**Classification of wormhole attacks**

Wormhole attacks can be categorized into two ways: Wormhole attacks based on implementation process and Wormhole attacks based on the communication medium

i. **Wormhole attacks based on implementation process [18]:** Wormhole attacks can be launched using various modes that are described below:

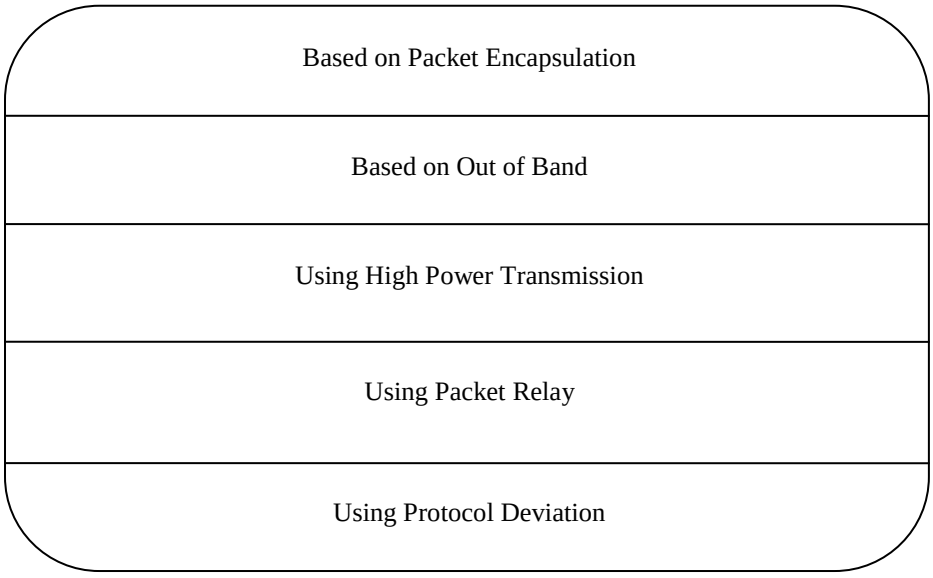



Figure 2.6 Various modes to launch wormhole attacks

- **Wormhole attack based on packet encapsulation:** In this mode, when the source node broadcast the packets, the malicious node encapsulates the packet and forwards it to the colliding node that decapsulates the packet and again

rebroadcast the packet to second colliding node. This results that wormhole is created between two colliding nodes by creating the virtual tunnel in the network.

- **Wormhole attack based on out of band:** In this mode, two malicious nodes are introduced that uses the direct wireless link or long range directional wireless link to forward the route request. This mode is hard to launch because it requires special hardware.
- **Wormhole attack using high power transmission:** In this mode, when the malicious node gets RREQ then it forwards the route request with a high power and the other nodes do not have that capability in the network. The node which listens high power broadcast must be malicious node that receives it and further rebroadcast to the destination.
- **Wormhole attack using packet relay:** In this mode, malicious node relay packets among two nodes that are far apart to convince them that they are neighbours.
- **Wormhole attack using protocol deviation:** In this mode, malicious node does not comply with the protocol rules and broadcast the packets without backing off to launch wormhole attack. The main purpose of broadcasting the packets without backing off is to be the first at the destination so that no legitimate request is received by the destination.

**ii. Wormhole attacks based on the communication medium**

Wormhole attack can be categorized into two ways based on the communication medium: Out of band wormhole attack and in band wormhole attack.

- **Out of band wormhole attack:** Here, the attackers create a direct link to transfer the data among two endpoints and it requires external communication medium between two end points
- **In band wormhole attack:** Here, the attacker makes an overlay tunnel over the actual wireless medium and it does not use any external communication medium between two end points.

## 2.3 Countermeasure against Wormhole attack

There are many researchers who put efforts to defend against wormhole attacks by changing the hardware design and different solutions are provided by them. It is very difficult to defend the wormhole attack with the software approach only. So, in this section we are going to discuss the related work to defend against wormhole attacks

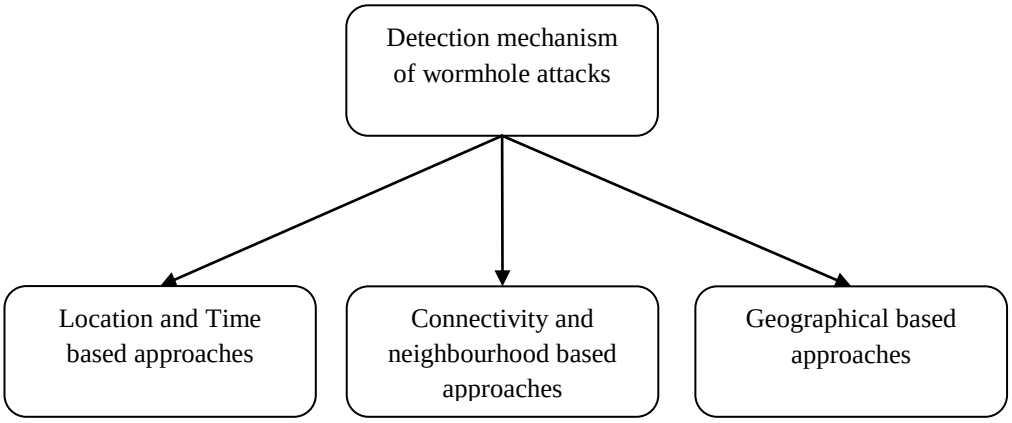



Figure 2.7: Countermeasure against wormhole attacks

- **Location and Time based approach:** The location based approach is the wormhole detection approach which uses the location information to identify the malicious nodes. While time based approach detects the anomalies which are based on the time mismatch of the forwarding packets [19].
- **Connectivity and neighbourhood based approach:** The connectivity based approach rely on connectivity information of the nodes without requiring additional hardware and location/time information. The neighbourhood based approach detects the wormhole by knowing the characteristics of the neighbour nodes. LEAP is a protocol that comes under neighbourhood based approach.
- **Geographical based approach:** The geographical based approach relies on the geographic position information to identify the malicious nodes. WGDD (Wireless Geographic Distributed Detection) is an example of geographical based approach.

## 2.4 Security Requirements

The following security requirements must be satisfied before deploying the VANETs:

- **Authentication:** Authentication means that the message is developed by the authentic user. To satisfy the authentication, vehicles react upon the receiving message that is received from other vehicle. To do this process, every message consist a key and a certificate at sender side. When the message forwards it to receiver side, it checks the key and certificate to verify the message. This causes an overhead while signing each message. So to reduce this problem, Elliptic curve cryptography (ECC) is provided.
- **Availability:** Availability means that the information must be available all the time whenever needed by the authentic users without affecting the performance of the network even if it is under attack. DOS attacks slow down the network by do not providing the services to the legitimate users and by using the large bandwidth with the consumption of more resources which affects the availability and the results may come out be the dangerous. A small delay in the message also affects the availability which makes the message worthless and creates a disturbance in the network.
- **Non-Repudiation:** Non repudiation means once a message is sent by the sender then he/she cannot deny that the message is not sent by him/her. Non-repudiation helps to identify an attacker after he has launched an attack and detects the compromised nodes. When destination node receives message from source node then the source node cannot deny having sent that message which signifies that the authenticity is sufficient reliable. In some fields, Non-repudiation is also known as Auditability.
- **Privacy:** The privacy of a node can be assured by keeping useful information away from the unauthorised users. To achieve the privacy, temporary keys should be used which will change frequently. These keys can be used once at a time and expires after usage. Privacy is enforced to eliminate the timing attacks. The pseudonym of privacy is confidentiality.
- **Integrity:** Integrity implies that the data should not be tampered while exchanging the messages during communication between sender and receiver. It assures that the message being sent over the network is never corrupted. In order to preserve the integrity, digital signatures are used.

# CHAPTER 3
# LITERATURE REVIEW

## 3.1 Literature Review

In this section, the details about various research works that has been done to secure VANETs [1-3]. At the end of this section, Table 3.1 shows the comparison of various techniques to detect different attacks in ad-hoc network.

V. Obado et al. [20] presented an exploitation of Hidden Markov Model (HMM) Viterbi algorithm for the detection of wormhole attack which is computed for a hidden state transition based on the maximum probabilities. In the research work, shortest path simulation is done using MATLAB to simulate the shortest paths among a source node and destination node. For detecting the wormhole, a threshold probability of 0.5 was set by the HMM Viterbi wormhole detection approach. If the probability of hidden least cost state is greater than threshold, which illustrates the presence of wormhole attack.

M.G-Otero et al. [21] implemented two procedures which are based on range-free localization methods for the detection of wormhole. In the proposed work, First procedure performed the detection process simultaneously by using the localization procedure to find the node's position and the second procedure followed the post-localization detection approach to validate the estimate node position and detected the malicious nodes.

A. K. Fatehpuria et al. [22] presented wormhole attack prevention by verification of digital signatures. The proposed work has identified two types of wormhole attacks: hidden and exposed attacks by using a mechanism delay per hop indication that detects the pinpoint location of wormhole and prevent it. It has followed two phases to identify the attacks. In the first phase, verification of digital signature is done to depict the presence of wormhole or not and in the second phase, delay/hop is analyzed using RTT mechanism.

Harikishan et al. [23] proposed a novel approach called IDS using Fuzzy inference system to encounter the intrusion behavior within the network. Using Sugeno Fuzzy Inference approach and ANFIS editor, an accurate attack was detected. In proposed work, MATLAB and ANFIS editor is used for experimentation and KDD CUP

dataset is used for detecting the anomaly based intrusion with the use of fuzzy inference approach.

V. K. Upadhay et al. [24] proposed a WPAODV technique for the detection and prevention of wormhole. The WPAODV is based on the hybrid model that encapsulates the location, neighbour node and hop count approach. In the proposed scheme, WPAODV extends the AODV by adding one extra feature in it i.e. after detection, WPAODV will bypass the path that is having a wormhole. To detect whether the route is having a wormhole or not, the WPAODV used divide and conquer mechanism over the route recommended by AODV. The main objective of the proposed scheme is to detect the wormhole in the route recommended by AODV.

S. Shamaei et al. [25] presented a two-phase detection mechanism to detect and prevent the wormhole attacks. In the first phase, it checks whether tunnel exists or not on the selected path by calculating the average delay per hop. If the average delay per hop is higher than the predefined threshold than the wormhole existence can be imagined and in the second phase it depicts the existence of wormhole attacks and discovers the malicious node. The proposed scheme detects the in band and out of band attacks without requiring any additional hardware.

J. Biswas implemented WADP [26] i.e. Wormhole attack detection and prevention technique by modifying the AODV routing protocol. The modification in AODV is done by doing addition of two extra fields in the route reply packet that is the IP of intermediate node and the unique number assigned to it. Assumption is made in the proposed work i.e. only authentic nodes know the information. If the node does not able to specify the right IP and number then it will be considered as malicious node. WADP is an enhancement of WAP algorithm. False positives are removed in the WADP algorithm by using the node authentication process and it also helps to know the exact location of wormhole node. Thus this process is considered as a double verification for the detection of wormhole attack.

R. Karthiga et al. [27] proposed a state traversal mechanism incorporate with finite state machine (FSM) to identify network intrusion with the use of optimized pattern matching algorithm and are also responsible for reduction of memory space required during the implementation of FSM. To achieve this goal, longest common substring algorithm is used and then the outcomes are correlated with the AC algorithm and the bit split algorithm. By following this approach, proposed algorithm has achieved the

goal of reduction of 26% memory compared with the AC algorithm for total string patterns.

Panja et al. [28] implemented IDS using neuro fuzzy classifiers to classify the network activities. They have also merged the Genetic Algorithm along with the Artificial Neural Fuzzy Inference System (ANFIS) to optimize data classification. In this research work, the neuro-fuzzy classifiers are used for the classification of initial network traffic. Fuzzy inference system determines he behavior of activity whether it is normal or malicious. It creates the fuzzy rule by using the human knowledge. The main goal of the proposed system is to reduce the number of false positives in IDS.

A. Aggarwal et al. [29] proposed a beacon node mechanism with neighbour node discovery for the detection and prevention of wormhole attack. The proposed technique detects the wormhole by the use of deviation in routing information among neighbours and it does not require any location information and additional hardware. The main goal of the proposed technique is to detect the wormhole in the route recommended by the AODV with the use of divide and conquer technique that will make all possible combinations of nodes. If any combination comes out to be suspicious, it will be considered as malicious.

M. Shahryari et al. [30] presented a cluster based approach to detect wormhole attacks. This approach is implemented in static and mobile networks. The proposed clustering technique is based on the 1M-Leach protocol and it follows four modules that are setup, verification of members, routing cluster heads and steady state. The proposed method is suitable for larger networks. It does not require additional hardware and having little processing overhead. Thus the network consumes the low energy. The simulation is done using NS2 simulator by evaluating the packet drop, throughput, delay and energy consumption.

S. Kaushal et al. [31] presented a Delphi method to detect the wormhole attack. By using the AODV protocol and hop count method, malicious node can be detected and a fresh path is provided for transferring the packets to their destination. For the detection of wormhole, delay per hop is calculated by every path in the network. If the delay per hop is found high for some path then it will be considered as malicious. The main advantage of Delphi method is that it does not require any additional hardware and the main disadvantage is that it cannot not pinpoint the location of wormhole because wormhole nodes change the route length in a certain manner so that it cannot

be detected. So to overcome this problem, geographic distributed detection method can be used to detect the wormhole location.

CHEN Ting [32] proposed IDS based on the principle of Back propagation (BP) neural network to solve the efficiency problems such as slow training process and slow detection. The proposed BP algorithm and IDS was implemented using four modules: packet capturing, data analysis and processing, neural network and alarm generator to detect the malicious activity in the network.

Liang Hu et al. [33] presented a feature selection algorithm and three neural network algorithms to enhance the development of IDS. Back Propagation (BP), Radial Basis Function (RBF) and Neural Networks with Random Weights (RNN) were the three algorithms used to figure out the feasibility of the IDS combined with the feature selection algorithm. The proposed work includes data collection, data preprocessing, intrusion detection and response modules to detect the intrusion based on ANNs. In data preprocessing phase, features are selected to lower the dimension of original data. Using feature selection algorithm original data dimension is reduced and for classification-BP, RBF and RNN algorithms are implemented.

Khattab M. Ali et al. [34] proposed intelligent IDS to protect communication between vehicles by firing Blackhole attacks. To build intelligent IDS, Proportional Overlapping Scores (POS) method is used to decrease the features of the trace file generated from network simulator and this file is used for classification. These features represent the behavior of vehicles whether it is normal or malicious. The intelligent IDS used ANN and fuzzified data to detect Blackhole attacks and also proposed a hybrid detection i.e. anomaly and misuse detection to detect these attacks.

S. Eidie et al. [35] introduced an efficient method to detect and prevent wormhole nodes in ad-hoc network using ADOV. Detection and prevention of wormhole is done by doing no modification in routing algorithm. The proposed method used the neighbour information in order to avoid the wormhole. It has followed two phases. In the first phase, all nodes are checked in the route to know that they are 1-hop neighbours or not to find the honesty of the nodes. In the second phase, detection of wormhole is done setting a predefined threshold. If the value of hop neighbours is found high than the threshold, then the node is announced as the malicious node. The proposed algorithm has detected all types of attacks of wormhole with 100% detection rate and is not useful for small tunnel attacks.

S. Nivedha [36] proposed a new fresh algorithm to detect and prevent the wormhole nodes in the MANET environment. In the research work, route discovery process is initiated in the first step and then the routing table is maintained by the every node which is traversed. If the traversed path does not exist in the routing table, then the path is announced as malicious. Also the RTT is computed for every consecutive node. If the RTT is found high than the threshold, then the nodes are considered as the authenticated nodes. In simulation results, the proposed scheme has increased the packet delivery ratio and reduced the control overhead.

B. Awad et al. [37] developed a new model based on hop-count metric known as WAP for the detection and prevention of wormhole attack. In the research work, evaluation of nodes is done on the pre-packet basis without requiring energy consumption techniques. The simulation is done in the MATLAB and achieved 99.7% detection rate and 98.4% accuracy rate

S. K. Arora et al. [38] presented a combined approach to detect Blackhole and wormhole attack. The combined technique consisted the RTT, buffer length and packet delivery ratio during the routing strategy in order to find the malicious nodes and the malicious routes are prevented by the intrusion detection system (IDS). The simulation of the proposed work is done in the NS2 simulator and computed the throughput, packet delivery ratio and normalized routing load.

P. Amish et al. [39] proposed a method to detect and prevent the wormhole attack in WSN using Ad-hoc on demand Multipath Vector (AOMDV) routing protocol which is the extension of AODV. This protocol is based on the RTT. In the research work, RTT is calculated for each node. If the computed RTT is lower than the threshold RTT for some route, then it will be depicted as wormhole link is present in that route. The advantage of using AOMDV is that it has low overhead and end to end (E2E) delay.

A. Radhika et al. [40] presented the detection and prevention of DOS attack i.e. Blackhole and wormhole attack in MANETs using Antnet routing algorithm based on ant colony optimization (ACO) scheme. In the proposed work, solutions are provided to defend against Blackhole and wormhole attacks. During the Blackhole detection, BACKWARD ANT sequence no. is checked in the routing table of ACO. If it is found higher than the threshold value, then the node is added into the blacklist and suspected to be malicious. During the wormhole detection, packet leash mechanism has been introduced to detect the wormhole nodes.

G. Elumalai et al. [41] proposed two algorithms for the detection of wormholes in the wireless sensor network. First is the centralized algorithm that assigned the central node to analyze the forwarding behaviour of each node in the network and second is the Distributed Detection Algorithm (DAWN) against wormhole detection by changing the flow directions caused by wormholes in order to send packets to the destination node. NS2 simulator has been used to implement the proposed technique.

Table 3.1: Comparison of various techniques to detect different attacks in ad-hoc network

| **Techniques/ Algorithm used** | **Tools/ Simulator** | **Attacks covered** | **Wormhole Detection/ Prevention/ Both** | **Simulation Results** | **Comments** |
|---|---|---|---|---|---|
| HMM Viterbi [20] | MATLAB | Wormhole | Detection | Distance measurements, Detection Rate | Due to recursive nature of proposed scheme, it has minimized the computational overheads. |
| Range-free localization [21] | - | Wormhole | Detection | Localization and Detection | Efficient scheme to detect attacks under good channel conditions |
| Digital Signature [22] | OPNET modeler 14.0 | Wormhole | Both | Average route discovery time, hops per route, delay, packet sent and received | Capable to detect and prevent attacks using Delphi and Digital signature |
| FIS [23] | MATLAB and ANFIS editor | DOS attack, U2R, R2L, Probe attack | Detection | Checked whether data is normal or attack one | Efficient to detect different intrusions in computer networks |
| WPAODV [24] | NS2 | Wormhole | Both | Time taken to recognize wormhole, Overhead | Effective approach that consumes lower power to detect wormholes |

| | | | | | |
|---|---|---|---|---|---|
| Two-phase mechanism [25] | NS2 | Wormhole | Both | FDR, FNR, Energy Consumption, Detection Time | Proposed scheme can be integrated into any routing protocol to detect all types of attacks |
| WADP [26] | MATLAB | Wormhole | Both | Eliminates False positives, Delay Per Hop | Can't able to detect hidden wormhole attack |
| PMNIDS [27] | SNORT | DOS | Detection | Memory Reduction | Efficient to locate patterns having larger pattern length |
| ANFIS [28] | WEKA using KDD 99 Dataset | DDOS | Detection | Detection Rate, False Positive Rate | Benefit of learning through patterns and easy classification of its functionality |
| Beacon node mechanism, NND [29] | - | Wormhole | Both | Threshold, Detection Ratio, PDR, Energy Consumption | Capable to detect wormholes by deviating the routing information among neighbours |
| Cluster based approach [30] | NS2 | Wormhole | Detection | PDR, Throughput, Delay, Energy Consumption | Efficient method for larger networks |
| Delphi [31] | NS-2.35 | Wormhole | Prevention | Packet loss, Throughput, E2E Delay | Minimizes the packet loss problem |
| BPNN [32] | WEKA using KDD CUP 99 Dataset | DDOS | Detection | Miss Rate, Error Rate | Capable to detect real time accuracy and having sufficient theoretical foundation |
| ANN [33] | WEKA using KDD 99 Dataset | DDOS | Detection | Accuracy, False Positive Rate , False Negative Rate | Adequate to Figure out the feasibility and IDS by applying |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | feature selection and neural network algorithms |
| ANN [34] | SUMO, MOVE, NS2 | Blackhole | Detection | Classification Rate, Alarm Rate | System requires extra memory to store data and approach is computationally heavy |
| WANI [35] | Omnet-pp | Wormhole | Detection | Detection Rate, Accuracy | Not efficient mechanism for small tunnel attacks |
| New Fresh Algorithm [36] | NS2 | Wormhole | Both | PDR, E2E Delay, Throughput | Minimization of overhead by proposed scheme |
| WAP [37] | MATLAB | Wormhole | Both | Detection Rate, Accuracy Rate | Proposed model is easy to use because it doesn't require manifold computations |
| Combined Approach [38] | NS2 | Blackhole and Wormhole | Detection | Throughput, PDR, Normalized Routing Load | Analyzed that Blackhole attack is more dangerous than wormhole attack |
| AOMDV [39] | NS2 | Wormhole | Both | Average Throughput, E2E Delay, PDR | No special hardware is needed for the detection and prevention of wormhole attack |
| ACO, Ant net routing [40] | NS2 | Blackhole and Wormhole | Both | Detection Rate, Threshold | Blackhole attack is not only detected but prevented also because of adding threshold in ACO |
| Centralized | NS2 | Wormhole | Detection | Throughput, | Effective |

| | | | | | |
|---|---|---|---|---|---|
| Algo, DAWN [41] | | | | Total loss | technique to get successful detection rate |

# CHAPTER 4

# PROBLEM STATEMENT AND OBJECTIVES

## 4.1 Problem Statement

As discussed earlier, Security is the critical aspect in the vehicular network because this network lacks infrastructure so it is vulnerable to numerous attacks. So there is need to secure the ad-hoc networks. One of the most dangerous attacks is the wormhole attack that hinder the routing operations in order to disturb the whole network by silently dropping the packets so that authenticated user can not be able to get services even in case of necessity. A lot of work is done to deal with this attack but there is still need of improvement and need to design a mechanism which can be able to detect the wormhole attack. The detection could be done through various techniques such as cryptography, IDS or localization etc. But cryptography techniques do not provide the best solution to detect these type of attacks. So in the research work, some work is done to detect the wormhole attack using DV-hop algorithm under range-free localization technique.

## 4.2 Gaps in study

Vehicular networks are vulnerable to many security threats which disturb the whole network by degrading its performance. Number of solutions has been proposed till date by various researchers as discussed in literature survey. Some of them include the range based localization while others use range free localization. Though a lot of research has been conducted there are still a lot of demerits with these works. Some utilize the GPS facility while some work without using any GPS. Some are limited to known attacks only. Some are based on trust factor and some evaluate using the Round Trip Time (RTT). So there is still some more work needs to be done on the wormhole attacks in VANET environment so that an efficient system could build up to improve the network performance.

## 4.3 Motivation

VANETs (Vehicular Ad-hoc Network) are known for creating the self-organised network by allowing the vehicles to communicate with each other in the absence of

fixed infrastructure. The communication among vehicles can be done by transferring the messages such as lane change, traffic jam, collision etc. It is an application of MANETs. The main goal of VANET is to provide the safety on the roads in order to reduce the collision of vehicles. The safety applications such as traffic signal warning, collision avoidance, road status etc. and the advantages of vehicular communication enhance the security on the roads. In the past few years, wireless technology has gained popularity in the world of data communication. In fact, the interest in this area has grown considerably. The excitement about vehicular networks is that it deals with the open challenges and provides ample range of solutions. But there are some technical challenges that still need to overcome that are: high mobility, quickly changing network topology, data delivery, speed of vehicles etc. In VANETS, even having so many applications and advantages, there are flaws as well. As VANET lacks infrastructure, so it is susceptible to many attacks. The one of the most threatening attack is wormhole attack that creates tunnel among two malicious nodes in order to disturb the whole network by silently dropping the packets. Security is the crucial aspect for every field but it is a serious issue in ad-hoc networks. VANETs also need to be secured. Many researchers have done lot of work in this field but still there is need of more research in VANETs in order to overcome the flaws.

## 4.4 Objectives

- To simulate the wormhole attack in VANETs
- To detect the wormhole nodes using the concept of localization
- To check the effect on the network, compute the performance metrics such as Throughput, Packet Delivery ratio, and End to End Delay
- Comparison results achieved in three cases – when no attacker node is present, when attacker node is present and the proposed algorithm

# CHAPTER 5
# SIMULATOR USED

## 5.1 Overview of Network Simulator (NS2)

NS2 is the network simulator having version 2 which is object oriented and discrete event driven developed at UC Berkley with the support of various organisations in 1989. It simulates range of IP networks and implements some MAC layer protocols, network protocols that include TCP and UDP and routing algorithms etc. It is based on two languages i.e. C++ and OTcl (extension of Tcl script i.e. Object oriented Tcl) [42]. NS simulator executes user command scripts. In order to use NS simulator, you program in OTcl script language that initiates event scheduler objects, network component objects to set up a network topology and network setup modules that notifies the traffic sources by notifying the time of start and stop of transmitting packets with the help of event scheduler. NS is not only written in OTcl but also in C++. To minimize the event processing time, the event scheduler objects and network component objects are compiled using C++.

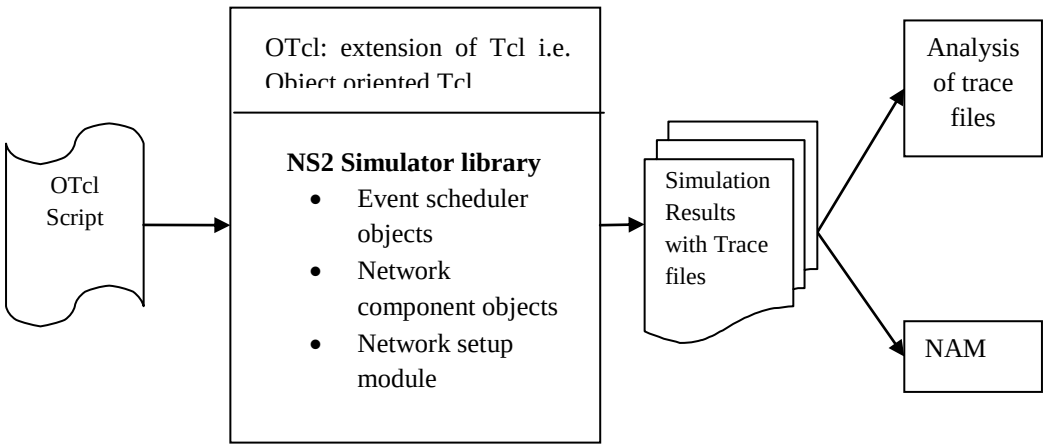



Figure 5.1: User view of NS2 program

**5.1.1 Tool Command Language (TCL):** Tcl is a tool command language that contains tcl scripts. It is dynamic programming language used for making desktop and web applications.

**5.1.2 Network Animator (NAM):** It is animated tool that helps to view the packet traces. It provides graphical interface (GUI) that provides information about number of packet drop at each link. Following Figure 5.2 shows the GUI view of NAM

-

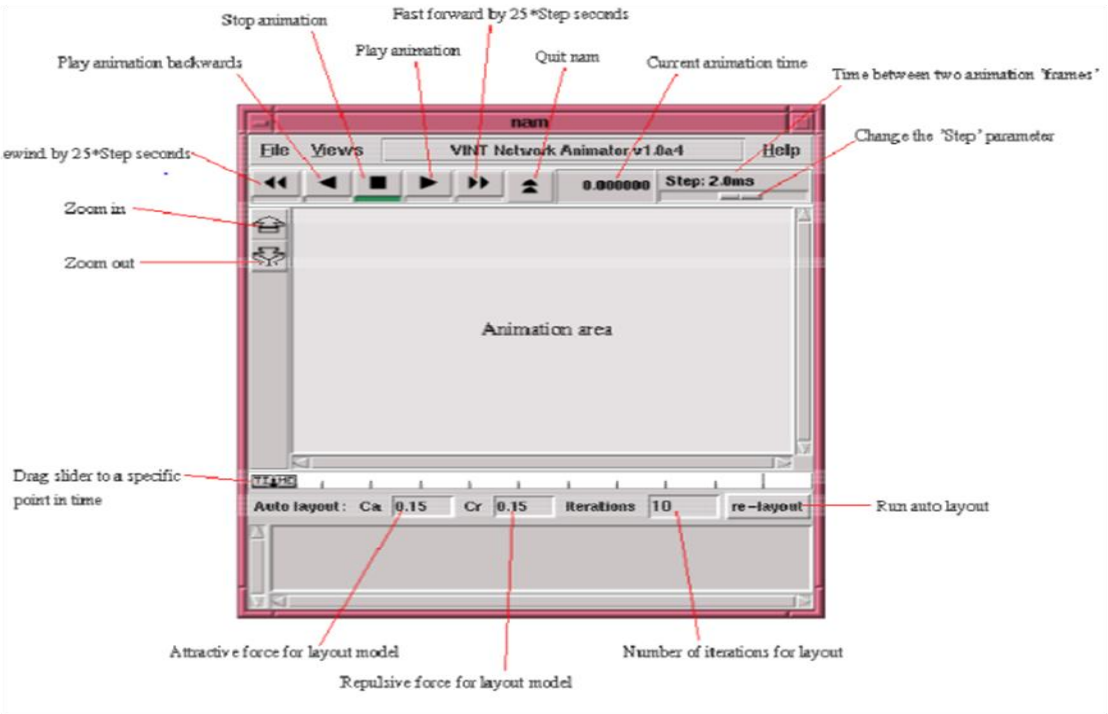



Figure 5.2: GUI view of NAM

**5.1.3 Trace file:** Trace file is the file that follows the ASCII format having 12 different fields.

| Event | Time | From node | To node | Pkt type | Pkt Size | Flags | Fid | Src addr | Dest addr | Seq num | Pkt id |
|---|---|---|---|---|---|---|---|---|---|---|---|

Figure 5.3: 12 fields of trace file

- Event: specifies the type of event
- Time: Time of the event occurrence
- From node: Input node of link of the link during the occurrence of event
- To node: Output node of link of the link during the occurrence of event

- Pkt type: Specifies packet type whether it is CBR or TCP
- Pkt size: Specifies the packet size
- Flags: Specifies flags used
- Src addr: Source node address
- Dest addr: Destination node address
- Seq num: Specifies the network layer protocol packet sequence number
- Pkt id: Exclusive id of the packet

# CHAPTER 6

# PROPOSED ALGORITHM AND IMPLEMENTATION

## 6.1 Proposed Algorithm

In network devices, broadcasting of packets among source and destination is handled by the routing protocols such as AODV, DSR etc. When these protocols start route discovery process in order to establish the path, then some new nodes join the path and old nodes leave it. So in this scenario, attacker node can also join the network and disrupts the functionality of the whole network. So, in the proposed algorithm efforts have been applied to mitigate the wormhole attack in VANETs. Our proposed algorithm uses the concept of range free localization scheme i.e. DV-hop algorithm which is based on the trust and the time factor to detect the wormhole nodes.

### 6.1.1 Localization Techniques

Localization of nodes is very critical to find the location of node through specialized algorithm in the ad-hoc network. Localization is the process of finding the nodes location. If the nodes do not know their geographical position then the data and information to find the location of node becomes worthless. Global Positioning System (GPS) is one way to determine the nodes location but it is commonly agreed that it is not best solution for the wireless ad-hoc network applications because of its limitations [43]. Firstly, it becomes very expensive when there are large number of nodes exist in the network. Secondly, it consumes high energy. Many researchers have been proposed algorithm to solve the localization issue; however, most of the proposed algorithms are application specific and most of the results are not applicable in ad-hoc networks. The solution of localization techniques for wireless ad-hoc network can be categorized into two ways [44]:

- **Range based localization:** Range based localization measures the actual distance between nodes for finding the location of nodes. It is based on distance based and angle estimation approach. The techniques that are used in range based localization are Angle of Arrival (AOA), Received Signal Strength Indicator (RSSI), Time of Arrival (TOA) and Time Difference of Arrival (TDOA) in order to estimate the nodes position.
- **Range free localization:** Range free localization uses connectivity

information in order to determine the nodes location. Range free localization scheme is cost-effective because there is no need of additional hardware and collects the nearby nodes information to find the location of node. DV-hop is one of the range-free localization algorithms estimates the range among nodes by using hop count.

### 6.1.2 DV-Hop algorithm

DV-hop measures the range among nodes by using hop count [43][45]. The process of locating nodes is divided into three phase:

Phase1: The anchor nodes broadcast its information such as coordinates and hop count (initially $h_c = 0$) into the network. The information is circulated to the whole network through neighbour nodes. When the neighbour nodes receive information, the value of $h_c$ is incremented by one. With this process unlocalized nodes are able to find number of hops from the anchor nodes.

Phase 2: In this phase, the anchor nodes record the position information and hop distance of other anchor nodes. So, the average hop distance is calculated among anchor nodes and from unlocalized node to anchor node using the following equation [45]:

$$d_i = \frac{\sum_{i \neq j} \sqrt{(x_i - x_j)^2 - (y_i - y_j)^2}}{\sum_{i \neq j} hop_{ij}} \qquad (1)$$

where $(x_i, y_i)$ $(x_j, y_j)$ are the anchor coordinates of node i and j , $hop_{ij}$ is the minimum number of hops between the anchor nodes i and j

Phase 3: To measure the shortest distance, unknown nodes use triangulation method to measure their positions from anchor nodes by using hop count

## 6.2 Modules of the proposed algorithm

These modules are divided into four categories: Routing Module in route is established among source and destination, Launch wormhole attack module, localization process module to locate the position of nodes and Detection module which results detection of wormhole node. The entire overview of the proposed algorithm is given in the Figure 6.1

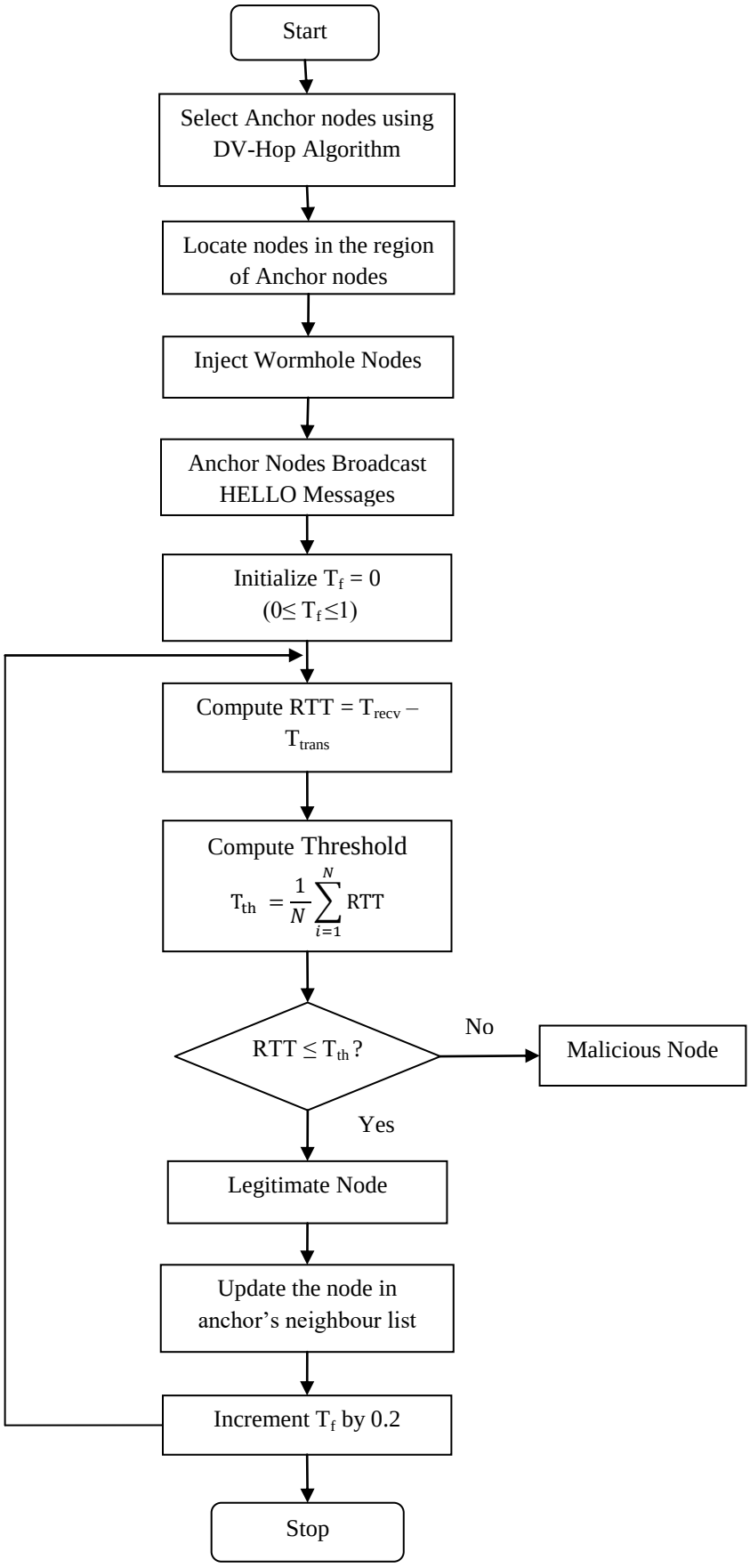



Figure 6.1 Overview of Proposed Algorithm

### 6.2.1. Routing Module

The need to establish the route between the source and the destination is to forward the packets without any intrusion of the malicious node. Source node establish route by sending RREQ messages to the destination node through intermediate nodes. Then the intermediate nodes first check its routing table to match the destination address. If not found, forward the packets to the neighbour nodes. This process continues until the destination address is not found in the routing table. When the destination node is found, RREP message is sent to the source node. But it is still possible some malicious intrusion is approaching the established route to degrade the network performance. In the next step, the wormhole nodes are introduced to create a malicious environment in VANETs which will further be detected using the localization process implemented with the trust and time factors.

### 6.2.2. Localization process module

The range free localization process locates the nodes in the VANET environment by implementing the DV-hop algorithm. The process of localization begins by first creating random nodes in the network. Further by implementing the DV- hop algorithm on the set of created nodes would result in generation of the anchor nodes that are randomly selected. These anchor nodes are a way to calculate the average hop distance from the unlocalized node to the anchor nodes as well as among the anchor nodes themselves. This average hop distance is certainly calculated using the equation (1).

```
#*******************DISTANCE from Anchor Node and node  *********************#

for {set i 0} {$i < 34 } { incr i } {
     puts "\n"
    puts $r "\n"

     for {set j 1} {$j < 34 } { incr j } {

                                set dx [expr $xx($i) - $xx($j)]
                                set dy [expr $yy($i) - $yy($j)]

                                set dx2 [expr $dx * $dx]
                                set dy2 [expr $dy * $dy]

                                set h2 [expr $dx2 + $dy2]

                                set h($i-$j) [expr pow($h2, 0.5)]
puts "distance of node($i) from node($j) = $h($i-$j)"

$ns at 1.2 "$ns trace-annotate \"distance of node($i) from node($j) = $h($i-$j)\""


#puts $r "distance of node($i) from node($j) h($i-$j) = $h($i-$j)"
$ns at 1.1 "$node($i) label $h($i-$j)"
```

Figure 6.2 Calculation of average hop distance from anchor node to unlocalized node

### 6.2.3 Wormhole Attack module

The anchor nodes calculate the RTT for each node and set the threshold in its routing table for every node localized in its region. Then the anchor node broadcasts the HELLO messages to its neighbour nodes. In return, the nodes reply with acknowledgement. Because of the presence of wormhole nodes in the region, the packets get attracted towards -them. These packets are never forwarded to the anchor nodes within the time threshold due to which end to end delay increases. But the wormhole nodes send acknowledgement to the anchor nodes pretending to be the legitimate nodes.

Wormhole attack is implemented in ns2 simulator. A malicious behavior is created in NS2 by modifying the files of routing protocol such as AODV.cc and AODV .h and using tcl script in which we introduce line of code that make its nature malicious.

```
$ns_ at 217.0 "[$node_(1) set ragent_] wormhole"
$ns_ at 0.0 "$node_(1) label wormhole"
$ns_ at 0.0 "[$node_(3) set ragent_] wormhole"
$ns_ at 0.0 "$node_(3) label wormhole"
```

Figure 6.3 Creation of two wormhole nodes in tcl script

Following is the screenshot of NS2 simulator utilizing NAM.

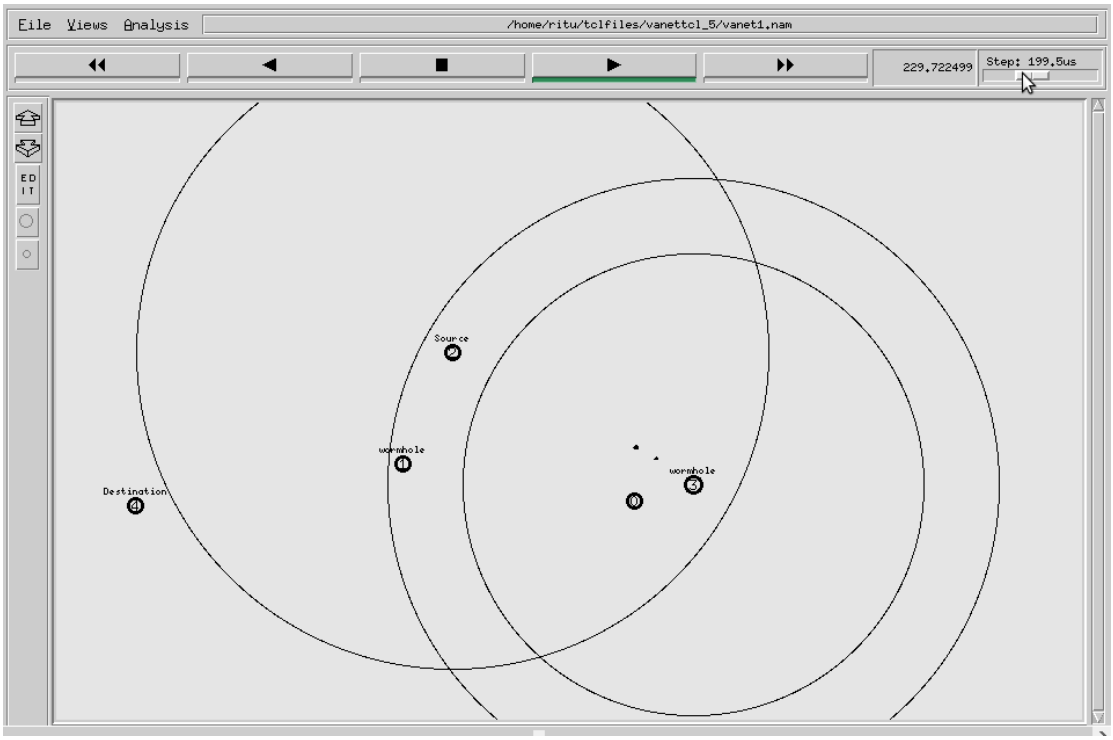



Figure 6.3 (a) Source node broadcast packets to wormhole nodes

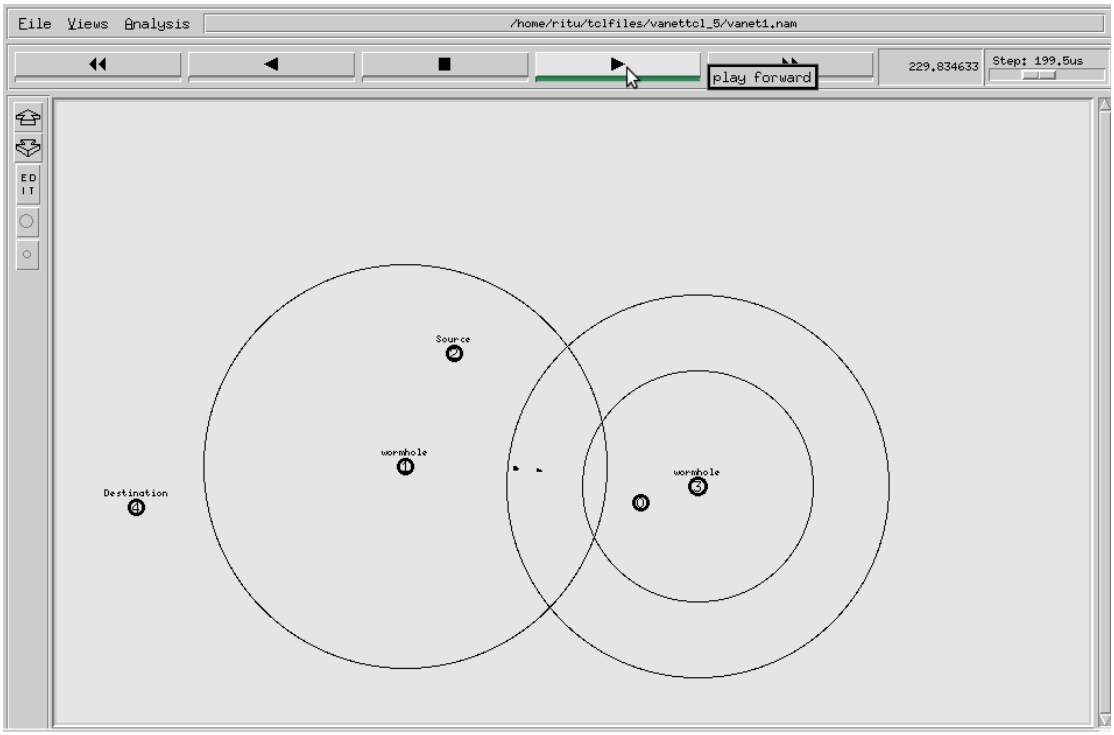



Figure 6.3 (b) Wormhole node broadcasts packet to another wormhole node

In Figure 6.3 (a) and Figure 6.3 (b) depicts the graphic view of wormhole attack in NS2 simulator using NAM tool where node 2 is the source node, node 4 is the destination node, node 1 and node 3 are the wormhole nodes that create a tunnel in the network . These wormhole nodes threaten the security of the network by dropping the packets instead of forwarding them to the destination.

### 6.2.4 Detection Module

The anchor nodes will broadcast HELLO messages in the network and will simultaneously set the trust factor, $T_f = 0$. In response to these HELLO messages the neighbour nodes will send the acknowledgement. But it is also possible that the acknowledgement is sent by the wormhole node. So in order to detect the wormhole nodes, a time threshold is set using the formula:

$$T_{th} = \frac{1}{N}\sum_{i=1}^{N} RTT$$

This means the nodes are required to acknowledge the anchor nodes within the obtained time threshold. Now, to determine the time threshold of each node, the time to send acknowledgement between the anchor node and the localized node is calculated using the formula of Round Trip Time (RTT):

$$RTT = T_{recv} - T_{trans}$$

So the nodes having the RTT less than equal to the time threshold will be considered as the legitimate node and will be eventually updated in the anchor node's neighbour list. Every time the neighbour list is updated with the new legitimate node the time factor is incremented at the anchor node by 0.2. This way only the trusted nodes are updated in the neighbour's list, while the malicious nodes are removed from the network.

The input values that have been used in the proposed algorithm are:

- $N_i$ = Number of nodes in the network
- $T_f$ = Trust Factor
- RTT = Round Trip Time between the anchor node and the localized node
- AN = Anchor Nodes
- $T_{th}$ = Time Threshold

**Input:** $N_{i,}$ $T_{f,,}$ RTT, AN
**Output:** Legitimate node, Malicious Node

for each node N
Apply DV-Hop;
Select AN;
Compute Hop Distance ();
{

$$d_i = \frac{\sum_{i \neq j} \sqrt{(x_i - x_j)^2 - (y_i - y_j)^2}}{\sum_{i \neq j} hop_{ij}}$$

}
return Hop Distance ;
if (Hop Distance Computed)
{
Inject Wormhole Nodes;
}
For each node in the AN region
{
Initialize $T_f$ =0;
RTT = $T_{recv}$ - $T_{trans}$;
Threshold $T_{th} = \frac{1}{N} \sum_{i=1}^{N}$ RTT;
}
if (RTT ≤ $T_{th}$)

Legitimate node;

else
Malicious node;

For all $N_i$ = = Legitimate
{
Update $N_i$ in the AN neighbour list;
Increment $T_f$ by 0.2;
}

Figure 6.4 Pseudocode of the proposed algorithm

# CHAPTER 7

# SIMULATION SCENARIO AND RESULTS

## 7.1 Simulation Environment and its Parameters

In this section, the proposed work is implemented using ns2 simulator. A dynamic set of mobile nodes is considered in order to set up a vehicular environment. The simulation results are discussed. Performance metrics such as throughput, packet delivery ratio and end to end delay are computed. The initial parameters taken during the simulation are represented in the following table:

Table 7.1: Parameters taken during simulation

| Parameters | Values |
|---|---|
| **Simulation Time** | 1000s |
| **Number of mobile nodes** | 25 |
| **Traffic Type** | UDP |
| **Topology** | Random |
| **Ad-hoc routing protocol** | AODV |
| **Size of Packet** | 1000 bits |
| **Antenna type** | Omni |
| **Channel type** | Wireless |
| **Network interface type** | Physical/ Wireless physical |
| **Radio Propagation Model** | Two ray ground |
| **Interface Queue Type** | Drop Tail |
| **MAC Protocol** | IEEE 802.11 |
| **Speed** | 20 |

## 7.2 Performance Metrics

- **Packet Delivery Ratio (PDR):** PDR is the ratio of the total number of packets received by the destination to the total number of packets delivered by the source. Mathematically, it can be defined as:

  PDR = Total number of received packets/ Total number of delivered packets

- **Throughput:** When the number of packets is transmitted from one node to another node within a specified time interval, then it is known as throughput of the network. It is usually measured in bytes/sec or kilobytes/sec.
- **End to End delay (E2E delay):** The data transmitted during the average time period from one end to another end.

## 7.3 Simulation Results

Figure 7.1 represents the graph of PDR for the defined number of malicious nodes. The number of malicious nodes varies from 2 to 8. It can be clearly seen that the trend of Packet delivery is decreased from 50.18 to 33.05. But when the proposed algorithm is applied on the number of malicious nodes the PDR values increased from 78.6 to 45.12 on the number of malicious nodes 2 and 4 respectively.

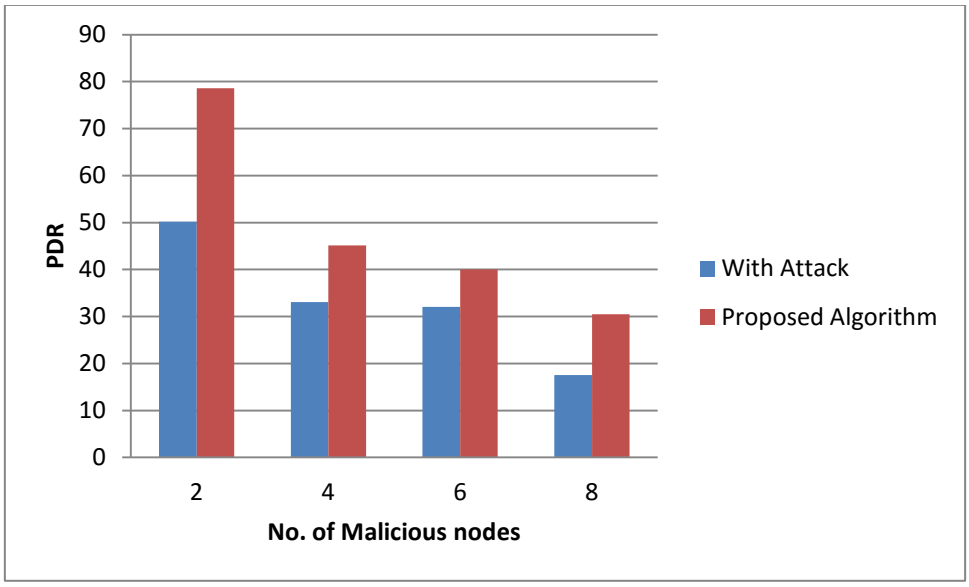



Figure 7.1: PDR vs No. of malicious nodes

Figure 7.2 represents the graph of Throughput for the defined number of malicious nodes. The number of malicious nodes varies from 2 to 8. It can be clearly seen that the trend of throughput is suddenly increased 20.92 to 30.84 on the number of malicious nodes 2 and 4 respectively and then it kept decreasing 30.84 to 16.36 on the remaining malicious nodes in the graph. While by applying the proposed algorithm, a significant increase in the throughput value can be noticed.

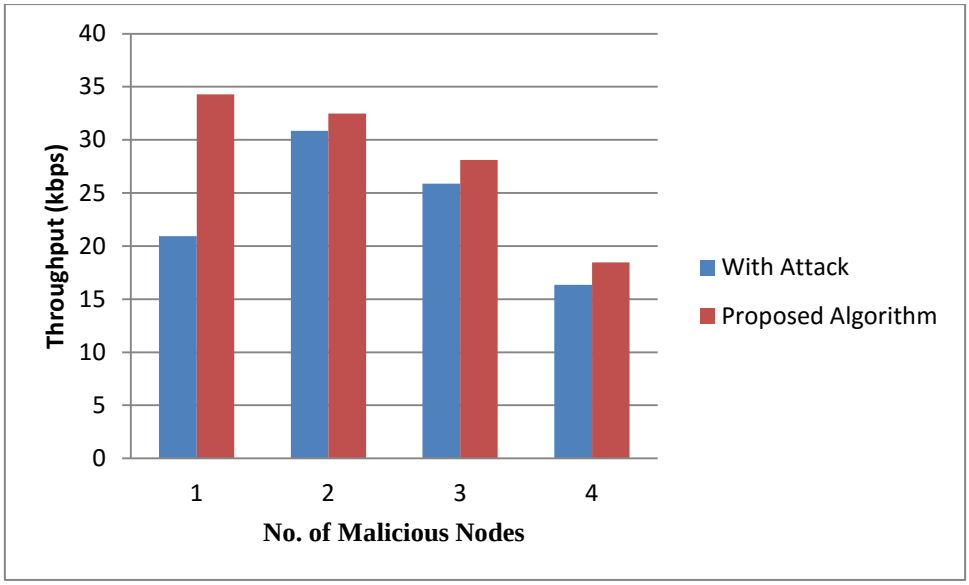



Figure 7.2 Throughput vs No. of malicious nodes

Figure 7.3 represents the End to End delay which is increasing with the increase in the number of malicious nodes in the network. On an average, End to End delay is increasing with the increase in number of malicious nodes by the value of 2.28. The proposed algorithm is able to give the desired results i.e. to decrease the end to end delay among the source and destination.

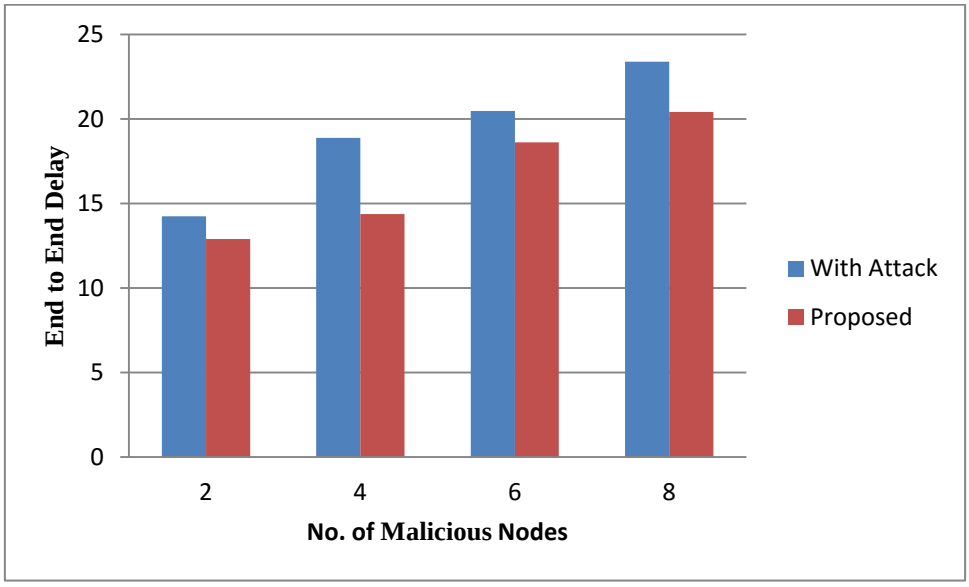



Figure 7.3 End to End Delay vs Number of malicious nodes

Figure 7.4 gives us the comparison of PDR values calculated during the without attack, with attack and by implementing the proposed algorithm. Without attack is considered as the normal VANET environment in which no malicious activity is performed. It is depicted from the following graph that the PDR values of normal

environment are significantly decreasing when the attack is performed, but the proposed algorithm successfully raises the values close to the normal environment values. For example, the PDR value on 25 no. of nodes in the normal environment 93.12 is decreased to 50.18 when the attack is launched. The proposed algorithm successfully raises this decreased value to 78.6 which is close to the normal environment.

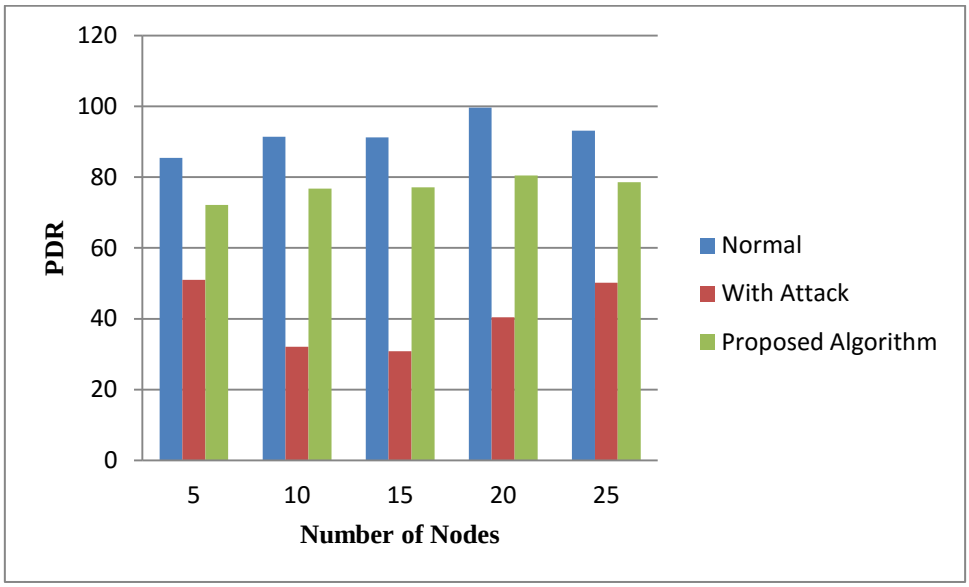



Figure 7.4: PDR vs Number of Nodes

Figure 7.5 shows the comparison of throughput under normal environment, with attack and the proposed algorithm. It is clearly shown in the graph that throughput value on 5 no. of nodes in the normal environment is 32.55 kbps which is decreased to the value 28.1 kbps after the launch of attack. But the proposed algorithm again successfully raised the throughput value to 30.25 kbps.

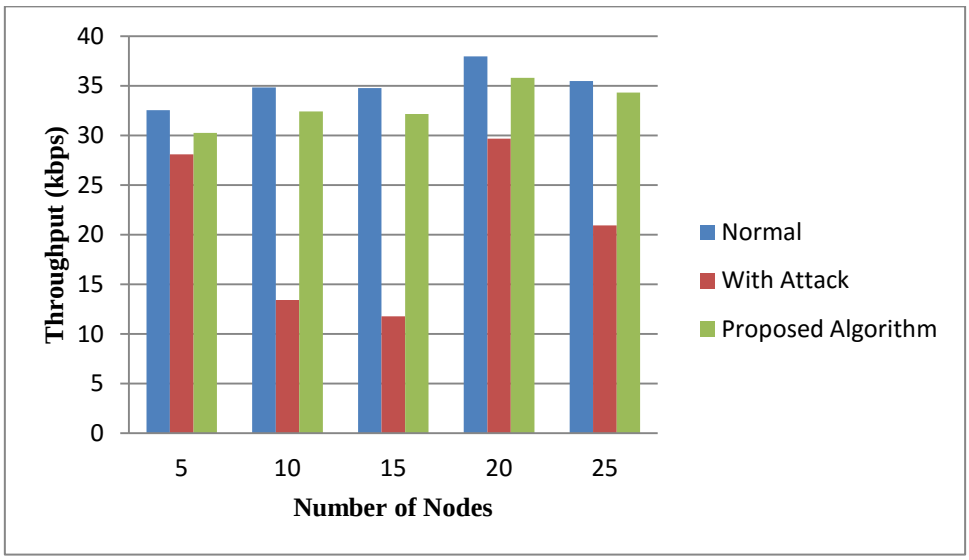


Figure 7.5: Throughput vs Number of Nodes

Figure 7.6 depicts the End to End delay under normal environment, with attack and proposed algorithm. The End to End delay on 15 no. of nodes in the normal environment is 13.37 and this is increased to 27.05 during the launch of attack. The proposed algorithm decreases the value to 22.34 which shows that although the values could not reach the normal environment values but successfully were able to decrease the delay in order to improve the network performance.

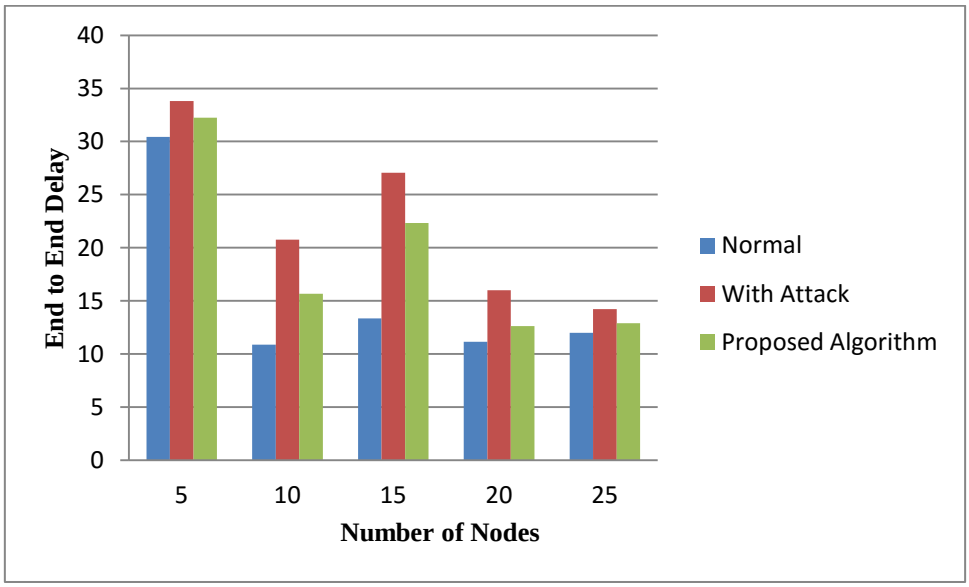



Figure 7.6: End to End delay vs Number of Nodes

# CHAPTER 8

# CONCLUSION AND FUTURE WORK

## 8.1 Conclusion

Security is the considerable problem to implement in VANETs because it is inherently vulnerable to mischievous attacks. Each node is an independent unit in VANETs, thus each node without sufficient security is prone to be compromised. One of the most dangerous attacks is the wormhole attack that disturbs the whole network and degrades the performance of the network. In this thesis, an effective model is proposed to detect the wormhole attack in DV-HOP algorithm using range free localization technique. The performance metrics such as packet delivery ratio, throughput, and end to end delay are evaluated without attack, with attack and with the proposed algorithm. The results show that the proposed algorithm is successfully able to give the desired results. While evaluating the PDR the values decreased on an average from 90.25 in the normal environment to 40.83 after launching the wormhole attack. The proposed algorithm mitigates the effects of wormhole attack by increasing the value to 70.68 on an average. Similarly, the throughput as well as the end to end delay shows the effective results after implementing the proposed algorithm on the attack environment. The main advantage of the proposed algorithm is that it is simple and cost effective because it does not require any- additional hardware, clock synchronization and position information.

## 8.2 Future Scope

The proposed algorithm has been proved fruitful to mitigate the effects of wormhole attack in the VANET environment by efficiently improving its network performance. So, in future the proposed algorithm can be used to mitigate the effects of other attacks such as Sybil attack, Blackhole, Jellyfish attack etc and hybrid attacks. Moreover, the proposed algorithm can be implemented using other routing protocols such as DSR, DSDV etc.

# REFERENCES


[1] R.S. Raw, M.Kumar and N.Singh, "Security challenges, issues and their solutions for VANET," *Internaltional journal of Network Security & Its Applications (IJNSA),* vol. 5, no. 5, pp. 95-105, 2013.

[2] A.Y.Dhak, S.Yahya and M.Kassim, "A Literature Survey on Security Challenges in VANETs," *International Journal of Computer Theory and Engineering,* vol. 4, no. 6, pp. 1007-1010, 2012.

[3] R. G. Engoulou et al. “VANET security surveys," in *Computer Communications,* Canada, 2014.

[4] B.Mokhtar and M.Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," *Alexandria Engineering Journal,* vol. 54, no. 4, pp. 1115-1126, 2015.

[5] B. Patel and K. Shah, “A Survey on Vehicular Ad hoc Networks," *IOSR Journal of Computer Engineering (IOSR-JCE),* vol. 15, no. 4, pp. 34-42, 2013.

[6] A.Singh and M.Singh, "A comprehensive review on vehicular ad hoc network," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 4, no. 4, pp. 462-468, 2015.

[7] F.Cunha et al."Data Communication in VANETs: A Survey, Challenges and Applications," in *INRIA Saclay*, France, 2014.

[8] R.Kumar and M.Dave, "A Comparative Study of Various Routing Protocols in VANET," *IJCSI International Journal of Computer Science Issues,* vol. 8, no. 4, pp. 643-648, 2011.

[9] U.Nagaraz and P.Dhamal, "Broadcasting Routing Protocols in VANET," *Network and Complex Systems,* vol. 1, no. 2, pp. 13-18, 2011.

[10] U. Nagaraj, M. U. Kharat and P. Dhamal, "Study of Various Routing Protocols in VANET," *IJCST,* vol. 2, no. 4, pp. 45-52, 2011.

[11] S. S. Tangade and S. S. Manvi, "A Survey on Attacks, Security and Trust Management Solutions in VANETs," in *2013 Fourth International Conference on Computing, Communications and Network Technologies*, Tiruchengode, 2013.

[12] G. Samara, W. A. H Al-Salihy and R. Sures, "Security issues and challenges of vehicular ad hoc networks (VANET)," in *2010 4th International Conference on New Trends in Information Science and Service Science (NISS)*, Malaysia, 2010.

[13] I. A. Sumra et al. "Classes of attacks in VANET In Electronics,, (pp. 1-5). IEEE." in *2011 Saudi International in Electronics, Communications and Photonic Conference (SIECPC)*, Riyadh, 2011.

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

[15] V. H. La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey," *International journal on AdHoc networking systems (IJANS),* vol. 4, no. 2, pp. 1-20, 2014.

[16] H.P.Chatar and S.Waghmare, "Vehicular Ad Hoc Networks (VANETS): Attacks and Challenges: A Survey," *International Journal of Electronics, Electrical and Compuational System (IJEECS),* vol. 4, no. 4, pp. 60-64, 2015

[17] M.G.Sanaei et al. "ROUTING ATTACKS IN MOBILE AD HOC NETWORKS: AN OVERVIEW," *Sci.Int. (Lahore),* vol. 25, no. 4, pp. 1031-1034, 2013.

[18] S. Suri, "Different Methods and Approaches for the detection and removal of Wormhole Attack in MANETS," *International Journal of Engineering and Technical Research (IJETR),* vol. 1, no. 5, pp. 14-18, 2013.

[19] M. Sookhak et al., "Geographic Wormhole Detection in Wireless Sensor Networks," *PLOS one,* vol. 10, no. 1, 2015.

[20] V. Obado, K. Djouani and Y. Hamam, "Hidden Markov Model for Shortest Paths Testing to Detect a Wormhole Attack in a Localized Wireless Sensor Network", *Procedia Computer Science,* vol. 10, pp. 1010-1017, 2012.

[21] M. Garcia-Otero and A. Poblacion-Hernandez, "Detection of Wormhole Attacks in Wireless Sensor Networks Using Range-Free Localization," in *2012*

*IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Barcelona, 2012.

[22] A. K. Fatehpuria and S. Raghuwanshi, "An Efficient Wormhole Prevention in MANET Through Digital Signature", *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 3, 2013.

[23] A.Harikishan and P.Srinivasulu , "Intrusion detection system using fuzzy inference system," *International Journal of Computer & Organization Trends*, vol. 3, no. 8, pp. 345-352, 2013.

[24] V. K. Upadhya and R. K. Shukla, "WPAODV: Wormhole Detection and Prevention Technique", *International Journal of Advanced Networking and Applications*, vol. 5, no. 3, p. 1922, 2013

[25] S. Shamaei and A. Movaghar, "A Two-Phase Wormhole Attack Detection Scheme in MANETs", *The ISC International Journal of Information Security*, vol. 6, no. 2, pp. 183-191, 2015.

[26] J. Biswas, A. Gupta and D. Singh, "WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol", *2014 9th International Conference on Industrial and Information Systems (ICIIS)*, pp. 1--6, 2014.

[27] R. Karthiga and P. Suresh, "Optimization of Pattern Matching Algorithm for Network Intrusion detection System," *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, vol. 2, no. 1, pp. 20-24, 2014.

[28] B. Panja, O. Ogunyanwo and P. Meharia, "Training of Intelligent Intrusion Detection System using Neuro Fuzzy," in *IEEE/ACIS International Conference on Software Engineering, Artificial Intlligence, Networking and Parallel/Distributed Computing (SNPD)* , Las Vegas, NV, 2014.

[29] A. Aggarwal and A. Saxena, "Wormhole Detection and Prevention Scheme using Beacon Node Mechanism with Neighbor Node Discovery", *International Journal of Computer Science and Information Technologies(IJCSIT)*, vol. 5, no. 5, pp. 6620-6625, 2014.

[30] M. Shahryari and H. R. Naji, "A cluster based approach for wormhole attack detection in wireless sensor networks", *JACST*, vol. 4, no. 1, p. 95, 2015.

[31] S. Kaushal and R. Aggarwal, "Avoidance of Wormhole Attack by using Delphi method",*International Research Journal of Engineering and Technology (IRJET)*, vol. 2, no. 7, 2015.

[32] C. Ting, "Detection system and the realization of the principle of BP neural network based intrusion," in *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, Nanchang, 2015.

[33] L. Hu, Z. Zhang, H. Tang and N. Xie, "An Improved Intrusion Detection Framework Based on Artificial Neural Networks," in *2015 11th International Conference on Natural Computation (ICNC)*, Zhangjiajie, 2015.

[34] K. M. A. Alheeti, A. Gruebler and K. D. McDonald-Maier, "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars," in *2015 Sixth International Conference on Emerging Security Technologies (EST)*, Braunschweig, 2015.

[35] S. Eidie, B. Akbari and P. Poshtiban, "WANI: Wormhole Avoidance using Neighbor Information", *Information and Knowledge Technology (IKT), 2015 7th Conference on*, pp. 1--6, 2015.

[36] S. Nivedha and S. S. Narayanan, "Detection and Prevention of Wormhole Attack in MANET using New Fresh Algorithm", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 4, no. 5, 2015.

[37] B. Awad and T. Barhoom, "BT-WAP: Wormhole Attack Prevention Model in MANET Based on Hop-Count," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 7, pp. 600-606, 2015.

[38] S. K. Arora and H. Monga, "Combined Approach for the Analysis of Black Hole and Worm Hole Attack in MANET", *Indian Journal of Science and Technology*, vol. 9, no. 20, 2016.

[39] P. Amish and V. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol", *Procedia Computer Science*, vol. 79, pp. 700-707, 2016.

[40] A. Radhika and D. Haritha, "Detection and Prevention of Blackhole Attack, Wormhole Attack in MANET Using ACO", *International Journal of Engineering and Applied Sciences (IJEAS)*, vol. 3, no. 1, 2016.

[41] G. Elumalai and U. Vasudevan, "Worm Hole Attack Detection in Wireless Sensor Network", *Engineering and Science*, vol. 1, no. 2, pp. 85--95, 2016.

[42] E. Altman and T. Jimenez, "NS Simulator for beginners," in *Lecture notes*, France, 2003.

[43] N. A. Alrajeh, M. Bashir and B. Shams, "Localization Techniques in Wireless Sensor Networks," *International journal of Distributed Sensor Networks*, p. 9, 2013.

[44] A. S. and P. Bharti, "Localization Techniques for Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 116, no. 12, pp. 13-18, 2015.

[45] H. Yang, Q. Wang and Z. Liu, "A wireless sensor network DV-HOP localization algorithm," in *2013 International Conference on Information Science and Computer Applications*, China, 2013.

# LIST OF PUBLICATIONS

[1] R. Rani, T. Bhatia, " A Survey on Machine Learning and Data Mining Techniques for real time intrusion detection system," in *2nd IEEE International Conference on Computer and Technology (ICETECH,* Coimbatore, pp. 639-345, 17th & 18th March 2016.

[2] R. Rani, T. Bhatia, V. Bhalla, "Mitigation of Wormhole Attack in VANETs using Trust based secure DV-HOP Localization Algorithm" (Communicated)

# VIDEO LINK

https://www.youtube.com/channel/UCepQh-p7k6hqI5iGDFZ7dOA

# Ritu Thesis

ORIGINALITY REPORT

| 14% | 8% | 12% | 0% |
| --- | --- | --- | --- |
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES