Detection & Prevention of Sybil attack using Artificial Bee Colony Algorithm in proximity of Closeness Centrality

Dissertation submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted By

Harpreet Kaur

(801533008)

Under the supervision of:

Mr. Sumit Miglani

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2017

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "Detection & Prevention of Sybil attack using Artificial Bee Colony Algorithm in proximity of Closeness Centrality ", 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 Mr. Sumit Miglani 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.

Harpreet Kaur

Harpreet Kaur

801533008

ME (IS)

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

(Mr. Sumit Miglani)

Assistant Professor, CSED

Thapar University, Patiala

ACKNOWLEDGEMENT

While bringing out this thesis to its final form, I came across a number of people whose contributions in various ways helped my field of research and they deserve special thanks. It is a pleasure to convey my gratitude to all of them.

First and foremost, I would like to express my deep sense of gratitude and indebtedness to my supervisor Mr Sumit Miglani for his invaluable encouragement, suggestions and support from an early stage of this research and providing me extraordinary experiences throughout the work. Above all, his priceless and meticulous supervision at each and every phase of work inspired me in innumerable ways. I specially acknowledge him for his advice, supervision, and the vital contribution as and when required during this research. His involvement with originality has triggered and nourished my intellectual maturity that will help me for a long time to come. I am proud to record that I had the opportunity to work with an exceptionally experienced Professor like him.

I am highly grateful to Dr Maninder Singh Head, Department of Computer Science and Engineering for their kind support and permission to use the facilities available in the Institute.

ABSTRACT

Vehicular ad-hoc networks (VANETs) are the wireless network in which vehicles are equipped with devices that communicates with each other via data packets. VANETs are mainly advocated for applications such as traffic collision detection, toll collection, controlling traffic congestion, weather forecasting, road diversion warning, car maintenance etc. Security of VANETs are vulnerable to various attacks such as Denial of Service (DoS), GPS Spoofing, Message Alteration, Black hole, Wormhole attack, Spamming attack, Node Impersonation attack, Sybil attack, Man-In-The-Middle attack etc. One of the most hazardous attack is Sybil attack in which malicious vehicle mislead other vehicles by duplicating multiple identities and generating false information. The genuine vehicle believes this false information and hence leads to road accidents, traffic congestion, chaos etc. We have proposed a method to secure VANETs from Sybil attack using Artificial Bee Colony (ABC) Algorithm in proximity of closeness centrality. This algorithm optimizes node position by monitoring nodes and calculating shapely values. Thus enhancing network performance which is demonstrated in simulation results.

Keywords— VANET, Artificial Bee Colony, Sybil attack, closeness centrality, AODV

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVATIONS

VANET	Vehicular ad-hoc networks
MANET	Mobile ad-hoc networks
ITS	Intelligent Transportation System
OBU	On Board Unit
RSU	Road side unit
V2V	Vehicle to Vehicle
GPS	Global positioning system
V2I	Vehicle to Infrastructure
WAVE	Wireless Access in Vehicular Environments
DSRC	Dedicated Short Range Communication
DOS	Denial of service attack
DDOS	Distributed Denial of service attack
CALM	Continuous Air-Interface, Long and Medium Range
LTE	Long Term Evolution
DSDV	Destination Sequenced Distance Vector
ZRP	Zone routing protocol
TORA	Temporal ordered routing algorithm
GPSR	Greedy Perimeter stateless Routing
GSR	Geographical Source Routing
ABC	Artificial Bee Colony
IVG	Inter-vehicle Geo-cast
OBDR	Optimized Broadcast based directional Routing
CBLR	Cluster based location Routing

Chapter 1
Introduction

1.1 VANETS

Wireless communication is becoming an emerging demand for development of new technologies. Being inexpensive, wireless network such as MANETs (Mobile ad-hoc network) and VANETs (vehicular Ad-hoc network) are key component for communicating and providing services in urban areas. VANETs enhances ITS (Intelligent transportation System) [2] which aims at providing road safety and other numerous applications such as weather forecast ,traffic on the road, traffic-jams, online services, traffic monitoring by roadside infrastructure, broadcasting information, collision prevention and internet connections. VANETs is considered as a subclass of MANETs [1]. VANETs is a self-configuring network which consists of vehicles, roadside infrastructure and base stations. VANETs are the wireless network in which vehicles are equipped with devices which communicates with each other via data packets. In this type of network, vehicles are referred to as mobile nodes. These nodes keep on moving and therefore changing the network topology frequently. The Equipment deployed on these mobile nodes called as OBU (On Board Units) [3] which facilitates Vehicle-to-vehicle communication. The infrastructure deployed on road side are called as RSU (Road Side Unit. On board units and road side units also communicates with each other and shares information regarding traffic warning and road condition to enhance security. In this way, it helps to prevent road accidents and traffic congestion. In VANETs nodes moves freely and constantly changes their locations. Therefore, there is a constant demand of information related to current location of vehicle, shortest route from source to destination, traffic lights etc.

In the given figure 1.1, the basic layout of VANETs is depicted. Vehicular Ad-hoc network consists vehicles, roadside infrastructure, buildings, and internet service providing station, sensors, GPS system [4] and servers. This network do not support any infrastructure and the vehicles moving as considered as nodes. Vehicles in this type of network is vulnerable to various network attacks such Man-in-the-middle attack, masquerading, denial of service,

Sybil attack, wormhole attack etc. Roadside infrastructure are immobile devices which have internet access. Roadside units also provide current location of vehicles travelling through particular area.

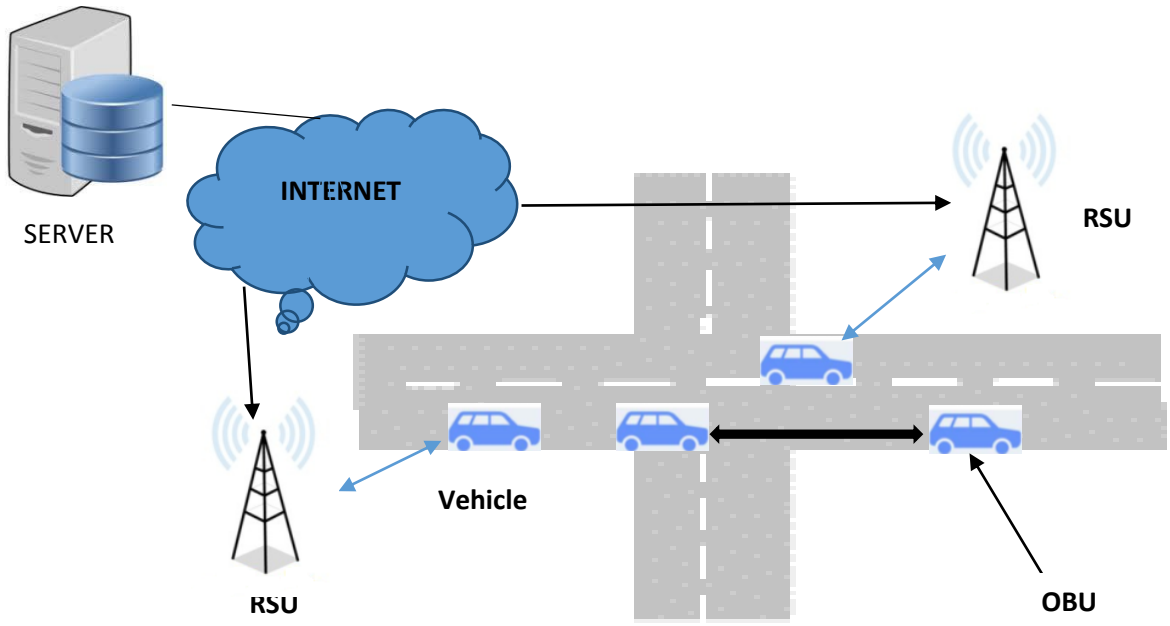


Figure 1.1 Basic scenario of VANETs

1.2 Type of Communication in VANETs

In VANETs, for reliable communication up to date information is needed. This information includes messages from one vehicle to warn another vehicle or message from any authoritative system to all other vehicles regarding safety. The information can be broadcasted by roadside infrastructure as environmental warning. This information can be sent to all vehicles if the position and location is known.

To provide up to date information, system also needs efficient routing protocols which has minimum bandwidth, low latency rate, less power consumption. The main goal of communication is cost-effective distribution of data across the network. These type of

communication helps to create ITS (intelligent transportation system). There exists three types of communications in VANETs

1. **Vehicle-to-Vehicle (V2V):** - V2V or car-to-car communication in VANETs is type of communication where different vehicles which act as mobile node share data via packets through multi-hop connection. The information these vehicles share with each other includes, warning message related to road accident occurred, warning of road condition, traffic congestion, traffic signals, speed & direction of preceding vehicles and information to prevent collision. These vehicles move at very high speed, therefore require safety messages on current condition. Vehicles have OBU (On Board Unit) deployed through which communication takes place. V2V communication is vulnerable to some attacks like Denial of Service (DoS), data tampering, active interfering, leakage of information, and impersonation.

   In V2V communication, vehicle send data over the distance of 300m and supports bandwidth of 5, 10 & 20 MHz [5]. Two types of message broadcasting exists in V2V communication, naïve broadcast and intelligent broadcast [6]. (i).In naïve broadcasting, vehicles receives broadcast message only from front and ignores message coming from behind. In case of emergency, if a vehicle receives packet from front and behind with same message, it will not broadcast the message further to vehicle behind it assuming that the vehicle behind will broadcast message to rest of the vehicles. In this type of broadcasting, packet delivery rate is less due to packet collision. (ii) In intelligent broadcasting, number of packet broadcasted is restricted and also acknowledgement of packet received is sent to source node, hence less collision than naïve broadcasting. Figure 1.2 shows inter vehicle communication.

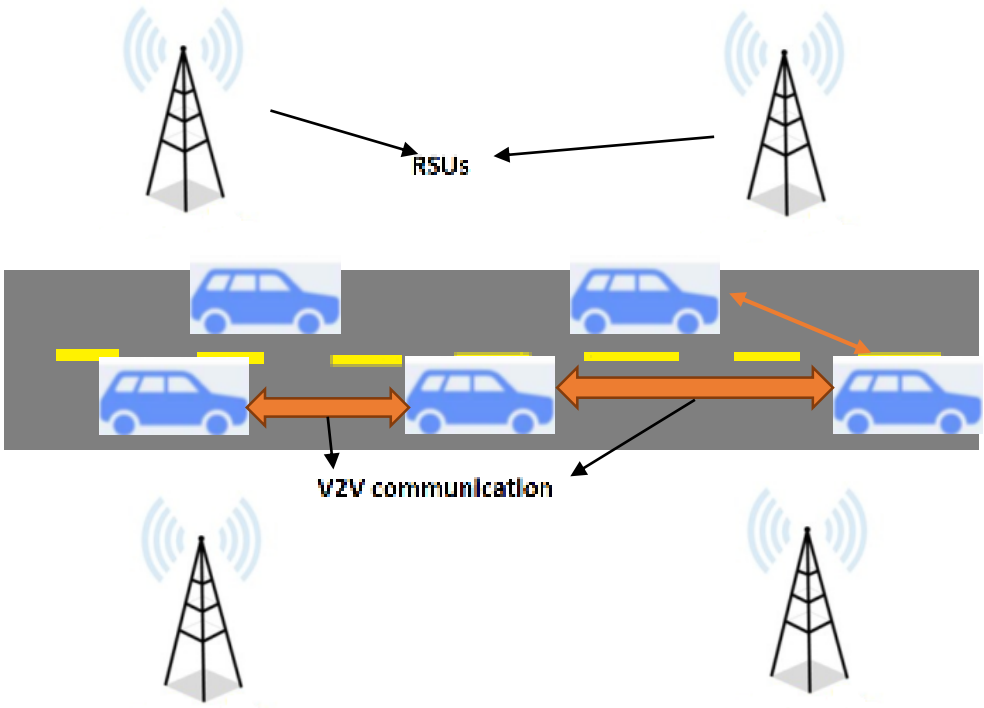


Figure 1.2 Vehicle to Vehicle Communication

2. **Vehicle-to-infrastructure (V2I): -** Vehicle to infrastructure type of communication is wireless communication between roadside unit or highway infrastructure and vehicles. V2I is commonly known as V2X communication to mitigate road accidents, also to ensure safe mobility of vehicles. The roadside infrastructure are equipped with special devices called RSU (Road side units). V2I supports bandwidth of 63 MHz [5]. The main aim for communication between vehicle and roadside infrastructure is to provide following real-time and on-demand applications as: -

- Speed Management
- Warning of critical situations like accident, environmental disaster.
- Rail crossing
- Emergency services.
- Prior notification of traffic jam
- Multimedia services like video games, online shopping etc.

3. **Infrastructure-to-infrastructure (I2I): -** Type of communication between different roadside infrastructures. When vehicle wants to send data at distant places or to vehicle which do not lie in source vehicle's range, first data will be forwarded to local RSU. Further that local RSU will forward packet through multi-hop communication to final RSU which lies in range of target vehicle. RSUs also communicate with sensors, detectors, CCTV cameras located along highways or road in urban areas. These provide information for application like measuring speed of vehicle, automatic toll collection, parking system, presence of service station, signals for pedestrian etc.

1.3 Applications of VANETs

Firstly, information regarding car safety and driver's assistance to alert him, which includes weather forecast of particular area, traffic warning or brake warning by preceding car and warning of diversion of road.

Secondly, information in the form of entertainment of passengers. VANETs also provide access to internet, interactive games and chatting among other vehicles.

Thirdly, local information as fuel prices, presence of any services stations, tourist information or just a parking space information.

Fourthly, online information for car maintenance. This includes online assistance from car mechanic in case of emergency brake failure.

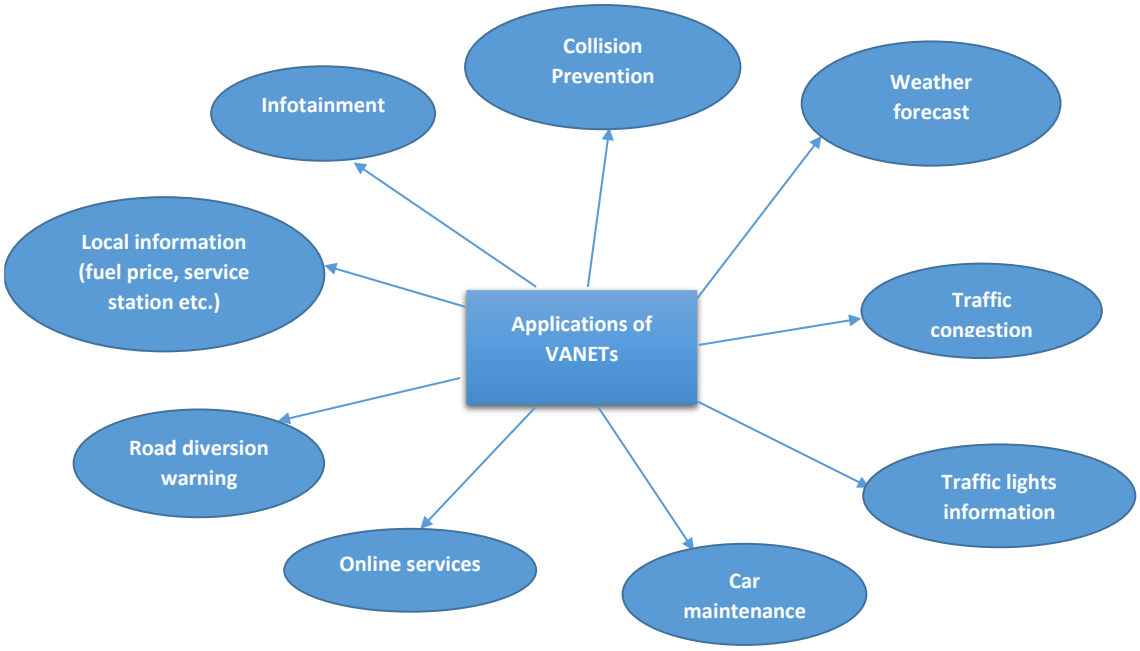


Figure 1.3 Applications of VANETs

1.4 Technologies in VANETs

VANETs also referred to as intelligent transportation system (ITS). ITS [7] is a term used for efficient route establishment, minimum road traffic solutions, and emergency services in all the modes like – road, rail, sea and air. It focuses on reliable transmission of packets in inter-vehicle or from vehicle to some other central authority (RSUs & base stations). The main objective is to develop and integrate new technologies and integrated systems to achieve road safety, traffic monitoring, save energy, performance up gradation and establishing seamless communication in the network. There are several new technologies used in VANETs such as Wi-fi, GSM, Bluetooth, and WAVE (Wireless Access in Vehicular Environments).

1.4.1 WAVE: - WAVE is also called IEEE/p 802.11 [8**].** WAVE being from IEEE 802.11 family, proposed wireless connection for vehicular networks. WAVE provides two type of device deployment system, first RSU (similar to base station) and second is OBU (similar to mobile station). With communication of these two device secure applications like collision avoidance, road safety, navigation, tracking location of each vehicle, toll collection, emergency services etc. becomes easier.

1.4.2 DSRC: - Another advancement is DSRC (Dedicated Short Range Communication) [9] protocol. DSRC protocol was designed for communication of V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-infrastructure) in VANETs. DSRC uses frequency of 5.850-5.925 GHz. This frequency range and other services helps to form a de-centralized network using beacons frames sent from OBUs and RSUs. Thus, ensuring efficient performance of application in VANETs such as public safety and navigation. DSRC also provide some guard bands of 70MHz. This guard band is further sub-divided into seven bands. DSRC only has a potential to meet such low latency and high speed requirement for navigation and traffic control.

1.4.3 CALM: - The another emerging standard developed by ISO TC204 /WG16 is CALM (Continuous Air-Interface, Long and Medium Range) [10]. In VANETs, when vehicles move at high speed, disconnections between inter-vehicle and vehicle-to-infrastructure occurs. CALM ensures continuous network connection which is accomplished by using a broad range of communicating networks and devices like mobile terminals, WLAN networks, and the short-range (DSRC) microwave and infrared (IR).

1.4.4 GPS (Global Positioning System): - Now, to have the knowledge of each vehicle GPS [11] system is used. GPS was first launched by US Army. In this, satellite network is used to track the motion of vehicle. GPS system continuously send coded information for current location estimation of each vehicle in network. Thus, helps in better network performance by sending data to desired node. But, sometimes GPS does not perform satisfactorily in urban areas where vehicles have multipath. So achieve more accuracy, GPS system can integrated with INS (Inertial Navigation System). Here in figure below, GPS is depicted with a satellite network to estimate location of vehicles in urban areas. The satellite continuously send coded information to the vehicles, high buildings and RSUs so that if source node wants to send data packets, it must have an estimate of location where the destination node lies.

1.4.5 LTE: -Another hybrid technique used for upgrading network performance is the LTE (Long Term Evolution) [12]. LTE is 4^{th} generation wireless communication services used in cellular networks with very high speed data transmission rate. LTE provides more scalability, reliability and high mobility. Thus, enhancing network performance with seamless connectivity.

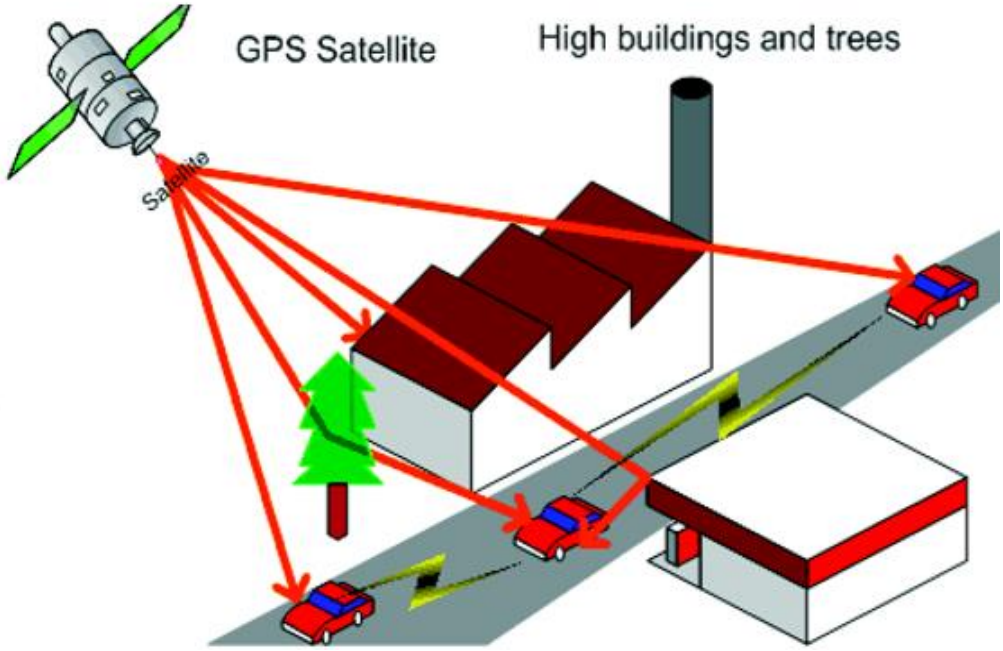


Figure 1.4 Use of satellite system for vehicle localization [13]

1.5 Features of VANETs:-

1. **Dynamic and frequent moving nodes: -** In VANETs, vehicles moves at high speed therefore topology changes frequently. Also, the vehicles keep on changing the direction which leads to breakage of link. In MANETs, nodes freely move in random direction whereas in VANETs movement of vehicles can be predicted by road topology, traffic signals and regulations.
2. **Density Variation: -** Due to mobility of vehicle at high speed, density of network varies according to road condition and traffic. Traffic is congested in urban area than rural area. There is more accumulation of vehicles near traffic lights on weekdays. Density also varies due to network connectivity. In VANETs, there are large number of nodes whereas in MANETs limited number of mobile nodes communicates.
3. **Node Traceability [14]: -** In MANETs, node moves in irregular manner which makes it difficult to trace each and every node in the network. But in VANETs vehicles can be traced easily. The traceability of vehicle can be known by roads, vehicle moving ahead,

roadside infrastructure. These vehicles can be assigned individually unique IDs to distinguish it from other vehicles in dense area.

4. **Type of area for communication: -** In urban areas, due to presence of building and traffic vehicle moves with less speed and there is mostly vehicle-to-infrastructure (V2I) communication. In rural areas or on highways, there is less roadside infrastructure and traffic. Thus vehicle-to-vehicle (V2V) form of communication exists.
5. **Power consumption: -** MANETs have limited battery power as device acting node is very small. Power consumption in VANETs is less than MANETs. In this type of network, vehicle are equipped with On board sources which supply battery power, hence external source is required.
6. **Signal Strength: -** Due to high mobility of nodes, signal strength varies largely. The signal fades with the presence of obstacles like building, towers, other vehicles interference etc. in urban areas. Inability of signal to reach its destination vehicle can degrade transmission efficiency. Thus signal strength is must require feature for effective communication of vehicle in the network.

1.6 Security Requirements of VANETS:-

1. **Authentication and Integrity: -** In VANETs, each vehicles must check the authenticity [15] of packets passed in the network. Each vehicle should be provided certificates whenever it enters the network and also revocation should be done when it leaves the network. The nodes in the network should only respond to messages sent by authorized members and the integrity of message transmitted should be checked that the original message is not tampered while transmitting between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication.
2. **Data Confidentiality: -** While transmitting sensitive data from vehicle-to-vehicle (V2V) or vehicle-to-Infrastructure (V2I), encryption schemes can be used to ensure data confidentiality and security in the network.
3. **Access Control: -** Only legitimate vehicles should have access to the services provided. These services are provided by remote nodes.

4. **Non-repudiation:-** The vehicle which sends the messages to other vehicles must not deny that the message is not sent by him. For example: - If a vehicle A sends message "clear road ahead" to vehicle B. Then vehicle B which receives the message must verify the identity of vehicle A.
5. **Privacy:** - The messages transferred within the network must be accessed only by authorized vehicles. Also, the identity of each and driver's personal information must not be disclosed [14].
6. **Scalability:** - VANETS should have ability to add or remove any number of vehicles in the network without any loss of data packets. The network must be designed in such a way that if any new vehicle is added, network's administrative complexity and its performance remains same.
7. **Efficiency and robustness:** - VANETS must have capability of offering and delivering services even under various attacks. While transferring messages small overheads, computational cost, processing delays and error rate should be used.
8. **Availability: -** The network must provide assured communication between vehicles even under bad condition or under different kind of attacks. Network must only provide services only to legitimate vehicle [15].
9. **Vehicle ID Traceability: -** Each vehicle in network have unique identification ID which helps to verify real identities when messages are sent across network.
10. **Anti-jamming: -** Sometimes, malicious nodes sends forged messages to legitimate nodes to interfere in communication and degrade network performance.
11. **Impersonation: -** Malicious vehicles masquerades as legitimate vehicles or duplicate itself with identity (Sybil attack) and sends forged messages to mislead other vehicles in network.

Chapter 2

Security Challenges and routing protocols

2.1 Security challenges in VANETs: -

1. **Bogus information: -** Malicious nodes transmit wrong information to mislead other nodes in the network. For example: - Node A sends incorrect message "Road blocked ahead" rather than sending "Road clear" message to ease its movement on road [16].
2. **Denial of Service (DoS) and Distributed denial of Service (DDoS):** - DoS attack [17] is a type of attack in which malicious node can jam the channel making services and information unavailable for legitimate user. Distributed Denial of Service is another form of DoS attack in which number of malicious nodes attack legitimate node from various locations. Thus legitimate node becomes deprived of services and resource provided by the network. This kind of attack reduces performance and efficiency of network.
3. **Black hole attack: -** In black hole attack [18], a number of malicious nodes refuses to transmit the packets to destination. This results in packet loss. For example: -In the given figure, if node A wants to send packet to node E. node A will broadcast message for route discovery. This broadcasted message is received by node B and node C. Node C is a malicious node, it will reply back to node A confirming it the path to destination node. After receiving reply from node C, node A will think it is valid route and forwards data packets to node C. Now here node C act as black hole node (malicious node) which may discard the packet or forward the packet to unauthorized node. This leads to dropping of packet i.e. black hole attack.

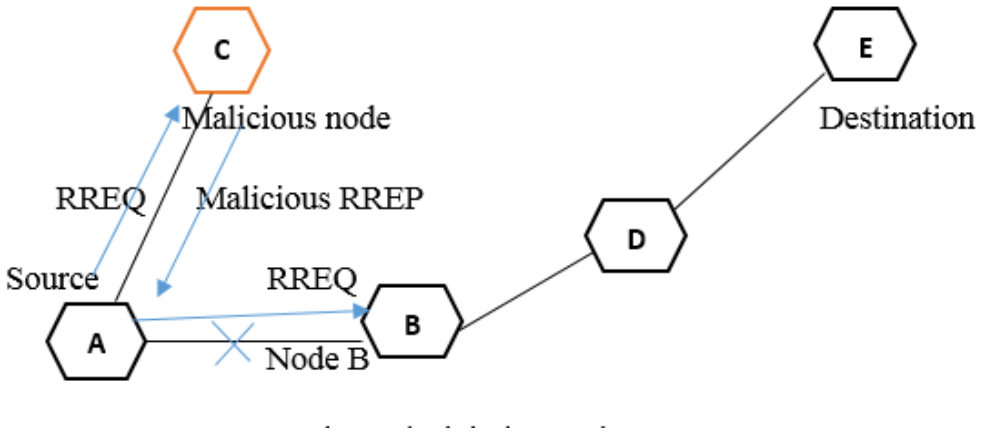


Figure 2.1 Black hole Attack

4. **Sybil attack: -** In this type of attack, attacker generates multiple fake identities which simulates multiple nodes in the network. Thus other nodes realize that there are number of nodes available at the same time. This creates chaos, security risk and traffic congestion in VANETs [].

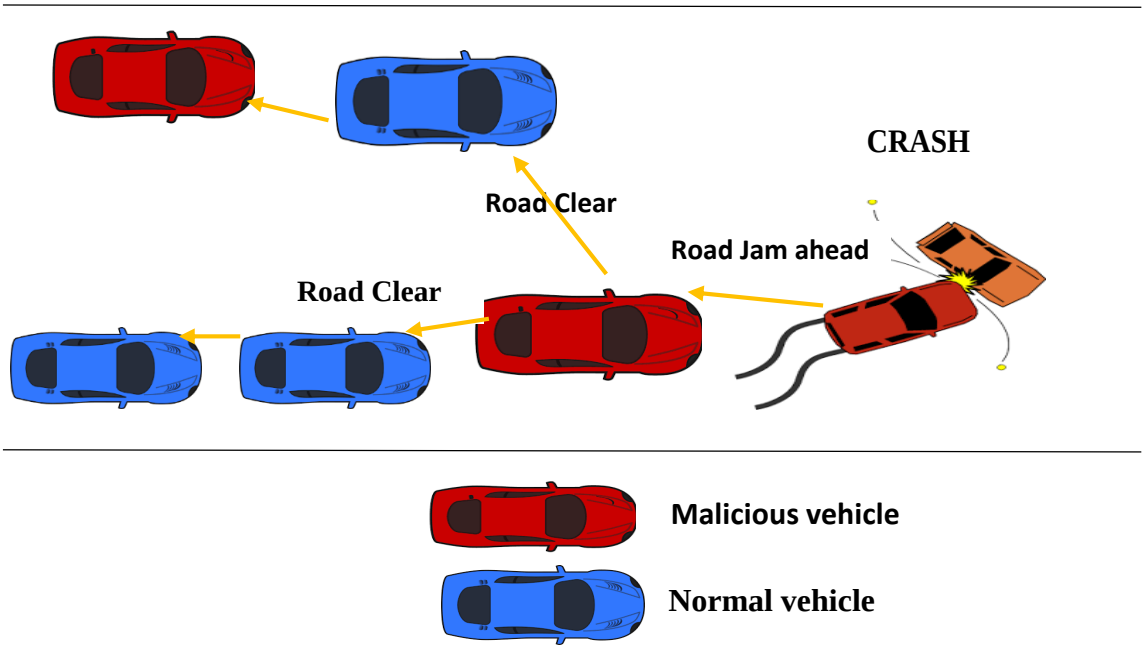


Figure 2.2 Sybil Attack

When there occurs any accident, the crashed vehicle sends alert message to other vehicle behind it, so that other vehicles change their direction.in figure 2.2, the crashed car sends alert message “Road Jam ahead” to vehicle behind it, so as to avoid traffic congestion on that particular area. But the malicious vehicle further sends wrong message “Road clear” to trouble other vehicle or to create traffic congestion. Hence with the presence of these two malicious vehicle, vehicular networks are unable to work in efficient and correct manner.

5. **Malware and spams: -** Malware and spams slows down the communication in VANETs. These can be spread insider malicious nodes. This causes legitimate vehicles to digress from their destination as these malwares convey wrong information and messages. Malwares can enter in the network while updating OBU and RSU’s software. It also steals driver’s personal information [19].
6. **Man-In-The-Middle (MITM) attack: -** In this type of attack, malicious node act as intermediately node between source and destination and tries to listen the communication. Malicious node can also inject malicious code or false packets between the nodes [20].

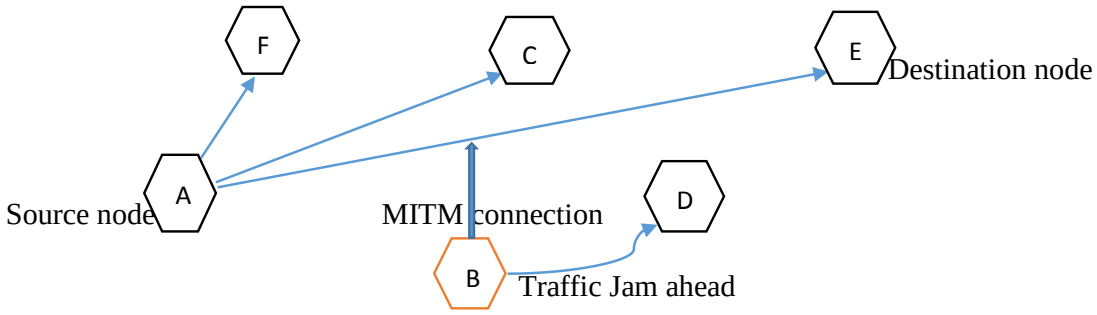


Figure 2.3 Man-In The-Middle Attack

In the above figure, malicious node B listens the conversation between node A and node E. Also, node B sends false message “Traffic Jam ahead” to mislead node D.

7. **Wormhole Attack: -** wormhole attack [21] is launched by one or more malicious vehicle in the network. These vehicles creates tunnel, a short fake route. In this attack,

one vehicle captures data packet from one location and transmits it to other malicious node at distant location. This is easily launched by compromising any one or more legitimate vehicles in the network. The tunnel created by malicious nodes has high transmission capacity which lure nodes to follow that route. Wormhole attack results in routing disruption and packet drop. Attacker can also collect and manipulate data packets. In Figure given below given depicts wormhole attack. The source node G wants to send packet to destination node A. The two attacker nodes C and D creates a tunnel and let other nodes think that it is the short path to send packets. This tunnel created has high transmission range. Thus, source node sends the packets through tunnel rather than sending via node B, E and I.

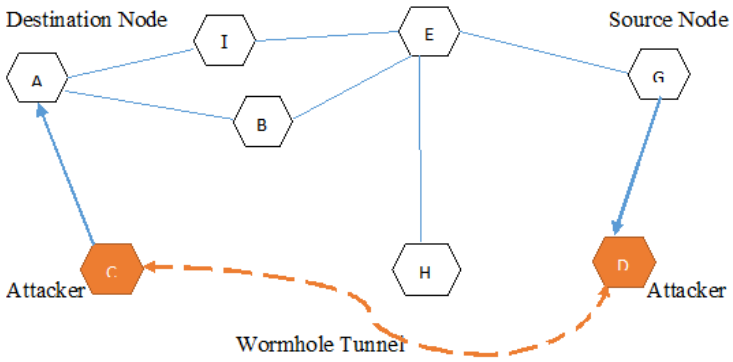


Figure 2.4 Wormhole Attack

8. **Illusion Attack: -** In illusion attack [22], malicious vehicle broadcast false warning message related to road condition, traffic congestion, weather forecast etc. to create illusion for other vehicles. This illusion creates chaos, performance degradation, & car accidents. Authentication approaches cannot secure the network from such attacks because vehicle which broadcasts message is itself the part of network, he can broadcast false warning by misleading the sensors of vehicle.
9. **Impersonation Attack: -** In this kind of attack, an attacker node impersonates or acquire identity of legitimate vehicle. By impersonating, attacker node can use the services and resources in the network. Also, it can disrupt the transmission of packets

from source to destination. Man-In-The-Middle attack is an example of impersonation attack.

10. **Rushing Attack: -** Whenever source node broadcast a route request packet in the network to establish connection using on demand routing protocol, malicious node replies to the routing request. When the legitimate node reply to the same request to source node, source node discards the packet believing it as a duplicate or fake one. Thus, the route discovered by source node contains malicious node as intermediate node. Being intermediate node, attacker can listen the communication or collect the data packet from source node [23].
11. **Information Disclosure: -** when an attacker compromised a legitimate node, he can disclose driver's personal information, vehicle's unique ID or its current geographical location. This attack leads to various other attacks like impersonation, Sybil attack, Denial-Of-Service, repudiation attack etc.
12. **Location Spoofing: -** GPS (Global Positioning system) is used to track location of each vehicle in the network. Attacker spoofs the information in GPS satellite and enters false reading regarding current location and route of vehicle. Hence, this causes other vehicle think that different vehicle are present at same location. Intruder produces signals stronger than signals produced by actual satellite by using GPS simulator.

2.2 Routing Protocols used in VANETs

Block diagram shows the different routing protocols categorized into five categories which are explained below:

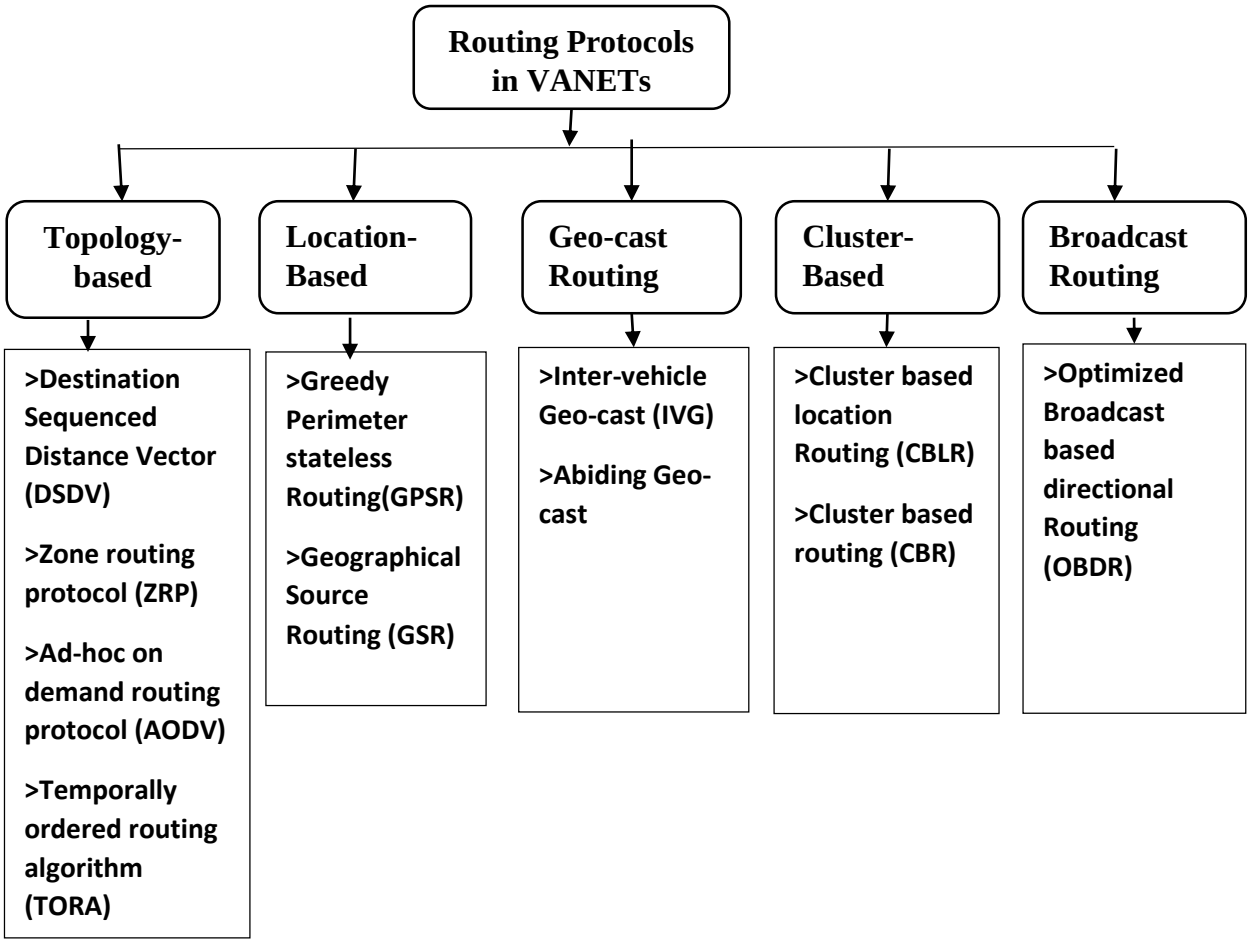


Figure 2.5 Routing Protocols in VANETs

2.2.1 TOPOLOGY BASED ROUTING PROTOCOLS

Routing protocols are used to discover efficient route to transfer packets from source to destination. Topology based routing protocols [24] are divided into three categories, Proactive, reactive and hybrid protocols. In proactive (table driven) routing, a table is maintained that contains information of each node in the network. In reactive, when there is a need to send packet to destination, route discovery is done. This causes delays as

compared to proactive. In proactive there is additional memory overhead as table is maintained for each node. In hybrid, both proactive and reactive routing protocols are used.

- **Destination-sequenced distance vector (DSDV)** [25]is a proactive protocol in which every node send its routing table to the next hop in order to reach the destination node and each node when receiving the table update its information accordingly which include destination node, next hop and hop count information. Figure 1.6 shows the working of DSDV algorithm.

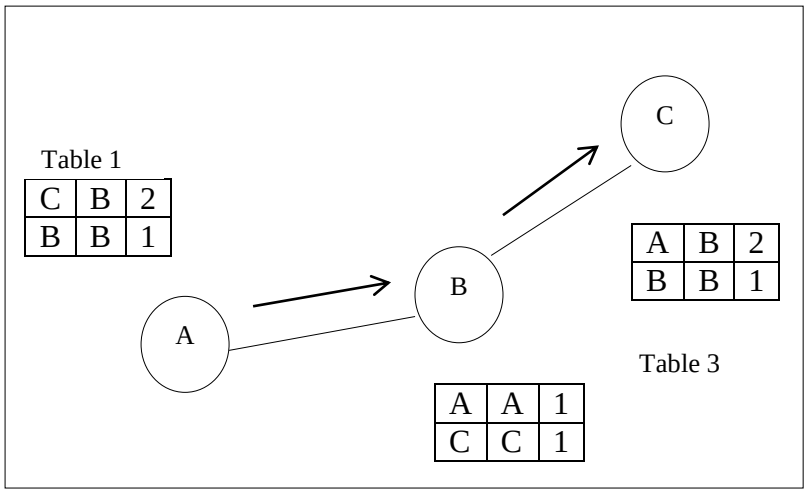


Figure 2.6 DSDV protocol

Node A, B, C has routing table 1, 2, 3 respectively. When node A broadcast its routing table to its immediate neighbor B which is at one hop distance then both A and B update its routing table. Node A wants to reach the destination C which is at 2 hop distance via B route. In this way when C receives the routing information of A and B, it also updates its table as shown the figure 2.6.

- **Zone routing Protocol: -** zone routing protocol [26] is a hybrid routing protocol which uses both reactive and proactive routing protocols. In reactive protocols to discover routes, query packets are sent globally across the network. This feature is used in ZRP instead the query packet is sent to the neighboring nodes in the zone. ZRP partitions network in number zones to provide flexibility for discovering routes. Zones are created on the basis of zone

radius say zone radius β. Zone boundary is defined by zone radius. The number of nodes in the zones will depend on value of β, if the hop count of nodes is equal to or less than β, then these nodes will lie in zone. All the nodes in the network have their own particular zones. Whenever a node A wants to send packets to destination node D, it will broadcast message to peripheral nodes (nodes whose hop count is equal to β). Peripheral node will further check whether destination node lies inside the zone or outside. If destination node lies inside the zone proactive routing mechanism is used called IARP (Intra-zone routing protocol) and if the destination node lies outside the zone reactive routing mechanism is used called IERP (Inter-zone routing protocol).

- **Adhoc on demand distance vector routing protocol (AODV):** In AODV [27], mobile nodes can be able to establish the communication dynamically via multi hop routing. Each node does not need to maintain the routing information of every other node. This preserves the energy of the sensor nodes when they are in inactive state or we can say they do not take participate in the communication. AODV defines three types of messages which are: Route request (RREQs), Route replies (RREPs) and Route errors (RERRs). RREQs messages are broadcasted to find the routes, RREPs ensure that routes are finalized and RERRs generate the error message which indicates the link has been broken in an active state of network. Two phases of AODV are explained as below:

1. **Route discovery phase:** In this phase, source node broadcast RREQ packet in order to start the communication with destination node by discovering the routing path. RREQ packet contains TTL field, address of source and destination node, source node id, destination node id and broadcast id. The neighbor nodes when receive the packet then they send the acknowledgment packet to the source node that indicates whether there is presence of valid routing path or not. The neighboring node keeps all the useful information which is later verified by the sender. There is one counter which lists all the entries and it may delete the entry from the table if there is no reply packet came from the destination node. Figure 2.7 below shows the routing discovery phase of AODV.

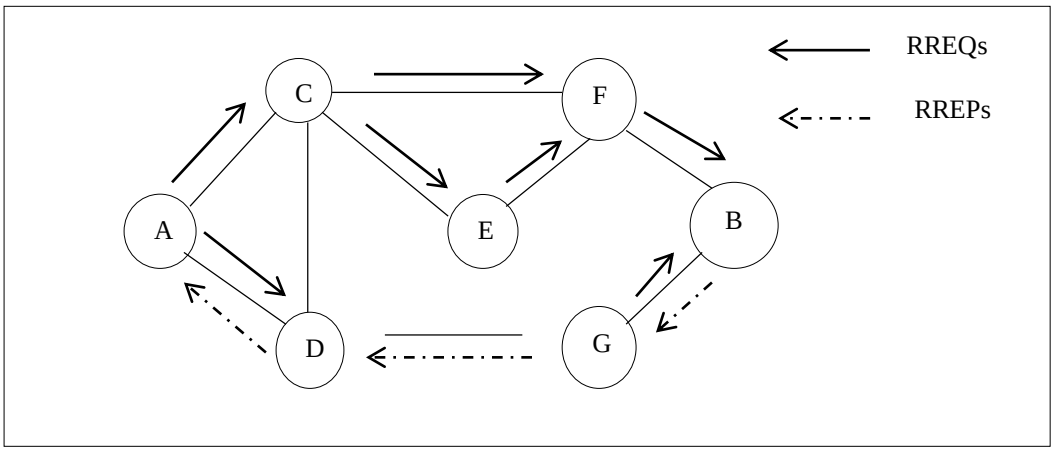


Figure 2.7 Route discovery phase of AODV

Source node A wants to send the data packet to destination node B, so A broadcast the RREQ packet to its neighbor. If the neighboring nodes in the route already receive the packet from other nodes then they discard the packet otherwise process the packet. Destination node on receiving the data packet from source node sends the reply acknowledgement with RREP by adding the required information such as address, TTL, sequence number and acknowledgment id.

2. **Route maintenance phase:** if any link has been broken between the nodes, then RERR message packet is broadcasted which update all the neighboring nodes that they start the route discovery process again in order to create the new links.

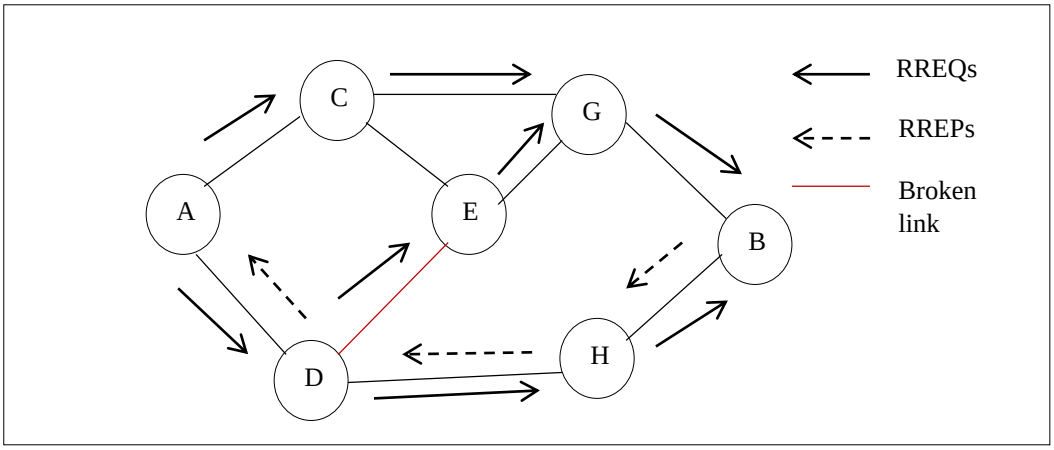


Figure 2.8 Route maintenance phase of AODV

Figure 2.8 shows that the link between E and D has been broken, so they start to broadcast the RERR message packets to the nodes.

- **TORA (Temporally ordered Routing Algorithm): -** Temporally ordered routing algorithm [28] is distributed in nature. TORA works by building a directed graph in which source node acts as a root node. As tree follows hierarchical structure, in the same way packets travels from upward to downward connection. When the packet is broadcasted, the neighboring nodes which have downward connection to destination node should reply, otherwise the node which have upward direction should discard the packet. TORA uses three steps, QRY, UPD and CLR. Whenever source node needs to send packet to destination, QRY message is used to create route, UPD is used to maintain discovered route and CLR message is used to erase the route after the transmission of packets. TORA provides route to all nodes in the network. TORA is not efficient for dynamically changing network like VANETs because it provides route to all nodes, hence overhead increases.

2.2.2 POSITION-BASED ROUTING PROTOCOLS

Unlike topology-based protocols, position-based routing protocols [29] do not depend on established routes. In this type of routing, information is sent from source to destination using position destination node. This position of destination node and the neighboring node at one hop count is tracked by GPS (geographical positioning system). The information regarding destination is stored in packet header. There are three categories of position based routing protocol, non-DTN (non-delay tolerant network), DTN (Delay tolerant network) and hybrid. In non-DTN, packet is sent to closest neighboring nodes using greedy algorithm. In DTN, packet is forwarded in carry-and-forward strategy. In hybrid both non-DTN and DTN are combined. We are discussing some position-based routing protocols

- **GPSR (greedy perimeter stateless routing): -** GPSR is a position based routing protocol in which two forwarding schemes are used, namely, greedy forwarding and perimeter forwarding. In greedy forwarding, the source node will forward the packet to node which closest to destination. Thus packet is sent using this forwarding. Greedy forwarding fails when there is no node closest to destination node than the current node itself. This state is called local maximum. When local maximum state is encountered, perimeter forwarding

is used with Right Hand Rule (RHS). GPSR is best suitable for areas with less traffic like highways. Performance degrades in urban areas because communication between vehicles is difficult with obstacles like buildings and trees.

- **GSR (Geographical Source Routing): -** It is a source driven routing protocol designed for routing in urban areas. This overcomes the problem of GPSR routing protocol. In GSR, vehicle uses digital map to find shortest path to destination vehicle Dijkstra algorithm. This path comprises of sequence of fixed intersection. Each packet has to follow these sequence of fixed intersections to reach to desired destination. GSR also uses greedy forwarding to forward packet between two intersections involved in transmission. If local maximum problem occurs, carry & forward technique is used. Limitation of GSR is that vehicular traffic information is not considered so shortest-path is not best path. As GSR uses sequence of fixed intersection, it performs worst in dynamic networks.

2.2.3 GEOCAST ROUTING PROTOCOL

- **IVG (Inter vehicle Geocast) routing protocol: -** In IVG routing protocol [30], vehicles are informed of risk affected area to multicast group regarding warning of danger on road. For this purpose risk area is clearly determined by considering location of obstacle and driving directions affected. The vehicle which is damaged alerts multicast group by broadcasting a message. All the neighbors who receives message verifies alert by calculating differ-time-backoff which promotes farthest node rebroadcast message.
- **Abiding Geo-cast: -** In abiding geo-cast [30] (stored geo-cast), packets have particular lifetime which is defined by sensors. Packets in abiding geo-cast is delivered to all vehicles in geo-cast region. To forward message three approaches are used.
    i. **Server approach: -** In server approach, server stores the geo-cast message and using geo-cast routing protocol message is delivered to destination zone.
    ii. **Election approach: -** In ZOR (zone of relevance) area, a vehicle is elected to store geo-cast message which further retransmits it periodically to other vehicles.
    iii. Neighbor approach: - In neighbor approach, geo-cast message is stored by all the nodes.

    In VANETs, abiding geo-cast facilitates the advertising applications and warning drivers about accident in their driving direction.

2.2.4 CLUSTER-BASED ROUTING PROTOCOL

To implement cluster-based routing protocol [31], network is first divided into clusters. Each cluster is headed by cluster head (CH). There two types of communication i.e. inter-cluster and intra-cluster communication. In intra-communication nodes inside cluster communicate by sending packet to closest node or by direct link. In inter-communication, cluster head communicate via multi-hop communication to transfer packets. Here we are discussing two cluster-based protocols, namely CBLR (cluster based location routing) protocol and CBR (cluster based routing) protocol.

- **CBLR (Cluster based location routing): -** In the formation of cluster, each node broadcasts a message and waits for reply in predefined time. If cluster head (CH) replies, the node becomes the member of cluster. Otherwise, node becomes cluster head. CH maintains a table with the entries like address of each node, node ID, signatures, etc. Every time when a node wants to send packet, it checks first whether the destination node is in same cluster or in other. If the destination node lie in some other cluster, source broadcast LREQ (location request) packet and each CH checks the address of destination whether it belongs to their cluster or not. When a valid destination CH receives the LREQ, it replies with LREP (location reply) to source node. CBLR is highly efficient in dynamic networks as it updates source and destination node's location before transmission of data.
- **CBR (cluster based routing): -** In CBR, the area is divided into respective square grids. All the nodes in grid is considered as clusters. CH uses two messages, LEAD and LEAVE message. LEAD message is broadcasted by CH to all its neighbors with location of its location and coordinates. LEAVE message is broadcasted when CH wants to leave grid. Data packets are routed from source to destination by CH across these grids.

2.2.5 BROADCAST-BASED ROUTING PROTOCOL

In broadcast based routing [32], message is broadcasted to all nodes in network. The message can be emergency, weather-forecast., traffic sharing information, announcement and advertisement. These types of routing performs better in small networks as compared to large networks because lot of bandwidth is wasted in broadcasting message using

flooding technique. OBDR (optimized broadcast based directional routing) is discussed below.

- **Optimized Broadcast based Directional routing (OBDR): -** It is an optimized method for broadcast based routing which uses two-key information i.e. direction of destination node and directive beamform angle θ. The message to destination is broadcasted based on geographic information. Further this geographic information consists of two parameters. One is destination direction and another is angle θ which provides assurance that message will reach the destination. Directive antennas can be used to implement this routing protocol. This protocol performs better, since it wastes less bandwidth.

Chapter 3

Literature Survey

VANETs being a means of communication in vehicular nodes is vulnerable to many network attacks. These attacks includes Denial-Of-Denial (DoS), Distributed Denial of Service, wormhole, Man-In-The-Middle (MITM), black hole attack, malware & spams etc. In our research work, we will be focusing on Sybil attack. Various researchers have proposed defense methodologies to detect and prevent Sybil attack in various networks like peer-to-peer network, Wireless sensor network (WSN), Social networks, VANETs, and MANETs.

3.1 Sybil attack in Wireless Sensor Networks (WSN)

B.TRIKI et al. [33] proposed the system for preventing and detecting Sybil attack in MWSN (Military wireless sensor network. Detection of attack is based upon RFID. Author used two types of authentication methods. Firstly, he used RFID tags that are embedded in soldiers for their authentication and certification. Secondly, certifications are used by soldiers for authenticating their neighbors. The solution also preserves the privacy of the soldiers because temporal pseudonyms are used, real identity is only known to team leader which is used as cluster head. Hence it prevents intruders from tracing the movement of soldiers while changing their identities from one zone to another.

S. Moradi et al. [34], author presented a distributed system based upon mobile agents to detect Sybil attack in WSN. The proposed algorithm consists of two phases namely, Network development phase & Network maintenance phase. In network development phase, nodes in the network are uniformly distributed and base station selects reliable nodes (5, 10, 15 nodes) randomly to which agent packet is sent. The node that receives agent packet is chosen as agent node. Network maintenance phase, mainly focuses on identifying adversary nodes. Protocol used for routing is Ad-hoc on demand distance vector routing protocol and CSMA/CA is used to avoid packet collision. This method uses local information of sensors to detect attack and removes Sybil nodes from participating in routing.

R.Lakhanpal et al. [35] proposed hybrid approach to detect and prevent Sybil attack using MAC and MAP (message authentication and passing) technique. This paper uses three predefined parameters, location, identity and timestamp of nodes. Location is assigned by MAC address of nodes and MAP is used for packet transmission after completely verifying identity and timestamp of associated nodes.

3.2 Sybil attack in Social network applications

R.Devi et al. [36] proposed an algorithm to detect and block Sybil nodes in social networks. Improved knowledge discovery tree algorithm is used to calculate threshold values of established connection between nodes. Sybil node is detected and eliminated by using various parameters like frequency of each node, variance, and trust relationship length of each node.

P.W.L.Fong et al. [37] proposed a decentralized defense for mobile users using MobID. In their research work, devices used two networks, (a) network of friends (contains authorized nodes) and (b) network of foes (contains suspicious nodes). Based on these two networks, device determines whether the device is Sybil node or not and use of K-mean clustering yields high probability in detecting bogus identities.

H.Yu et al. [38] presents a SybilGuard protocol for social network and the edges between two users depicts relationship based on human established trust. Suspicious nodes may create bogus identities but very few trust relations. A group of honest nodes and Sybil nodes with one million in number is considered for result evaluation. Further an optimized technique of SybilGuard is proposed called SybilLimit [39]. This guarantees that social networks are fast mixing networks which was assumed (not evaluated in real world networks) in previous research work

3.3 Sybil attack in Ad-hoc Network

T.Zhou et al. [40] proposed a light-weight, scalable framework for the detection of Sybil attack. In this the privacy of each vehicle is preserved in the network. The framework used is called P2DAP (Privacy-Preserving Detection of Abuses of Pseudonyms). This framework distributed the responsibility to semi trusted third party to detect attack while maintaining anonymity of vehicle.

Navneet et al. [41] detected Sybil attack by extension of AODV (ad-hoc on demand distance vector) protocol using a new field called SCID (secondary ID) along with sequence number. SCID provides unique identity to all nodes in network.

P.Gu et al. [42] detected Sybil attack based on vehicle driving pattern. Eigen values of DPM (driving pattern Matrices) are used for representing of driving pattern of vehicles. The detection of unusual driving pattern of vehicle is evaluated by Mahalanobis distance. This method shows high rate of detection and less error rate.

P.V.Kumar et al. [43] proposed model, PBVA (Privacy Batch Verification Algorithm) for Sybil attack prevention. This classifies the multiple request received from different vehicles, thus provides immediate response with minimum time delay to emergency vehicle. This method also prevents Sybil attack by restricting timestamp by RSUs (roadside units).

S.Sharma et al [44] used timestamp series approach to detect Sybil attack in VANETs. In this, node is suspected as Sybil node if it contains more than one timestamp of last Roadside unit (RSU). RSU provides timestamp to each vehicle and vehicles are not allowed to use timestamp of other vehicles. If more than one message contain same timestamp series, it is considered as Sybil attack. Also this paper compares the research with existing EBRS (Event Based Reputation System) which yields better results from EBRS.

Figure 3.1 PBVA model [44]

Figure 3.1 shows multiple request to same RSU at same time. This request to RSU from car, truck, ambulance and communication with base station at the same time. The request for needed services is processed based on batch verification algorithm.

3.4 Drawbacks of Existing techniques

Many existing technologies researchers have been proposed in past few years related to detection and prevention of Sybil attack. These provide efficient and reliable solution to tackle with Sybil attacks. This attack have been discussed considering various wireless networks like MANETs, VANETs, social network applications, wireless sensor network etc. But, still there are some drawbacks or flaws which makes the network vulnerable and advantage the attacker to gain access over the network. Here we are providing some drawbacks that needs to have a concern.

1. In [35] a lot of memory is consumed to maintain the matrix which contains parameters like node ID, timestamp, MAC address, energy value of all nodes.in [A distributed method based on mobile agent to detect Sybil attacks in wireless sensor networks] each node maintains matrix of every visited node's location and identity with respect to time as History. This also results in memory consumption.
2. In [37], author assumes that the person only share their identity (e.g. public key) with which he/she has off-line relationship. In social networks, attacker can impersonate the identity of authorized person and can gain information. Thus, sharing of keys needs secure methodology.
3. Issuing of certificate or digital signatures by roadside unit to each vehicle passing through it, involves additional overhead.
4. Unnecessary broadcasting the messages results in wastage of bandwidth and energy.
5. While exchanging sensitive information (e.g. Node ID) or issuing a certificate, a secure encryption algorithm is required.
6. In order to process emergency nodes [prevention of Sybil attack and PBVA], normal nodes may have to wait for long period of time, hence delay in their processing time.

Chapter 4

Problem Statement

4.1 Problem Statement

VANETs are the technologies which aims at providing life safety on roads by sharing real-time information regarding traffic congestion, vehicle collision, emergency, road status etc. This information is shared by broadcasting beacon frames. When information is broadcasted, it aware the driver to tackle the abnormal arising situations on highways or in urban areas. VANETs are the major component of Intelligent Transportation System which provides safer and secure communication between vehicle to vehicle and vehicle to roadside unit.

As VANETs provides a number of safety and non-safety applications, it is also vulnerable to attacks that previously discussed in chapter 2. These attacks results in number of road accidents in countries like India, US, Japan etc. Attackers through various commonly known attacks like Denial of Service, repudiation, Sybil attack, impersonation, bogus information attack etc. creates chaos and mislead drivers which leads to hazardous road accidents and also troubles the pedestrians.

My research work focused on detecting and preventing Sybil attack. Though many approaches have been used like Identity-based, Cryptography based, Location based approaches etc. but still these do not provide the desired results, so an ABC (artificial bee algorithm) algorithm is used and applied to optimize the network performance.

4.2 MOTIVATION

In India, the number of deaths occur in every ten minutes is three through road accidents only. In 2015, 14800 people were killed as compared to year 2011 in which 13600 were the number of deaths [45]. There was an increase of death rate by 3 percent from year 2014

to 2105. In US, there is an increase of 7.7 percent in death rate due to road accidents i.e. number of deaths in 2015 is 35,200 than 32,600 in 2015. These road accidents not only causes human deaths but also results in loss in productivity and property damages [46].

Hence, the number of road accidents occurring daily motivated me to work on secure communication with low computation cost, better performance and less delay. There are various researches done in securing VANETs but still there are some drawbacks related to efficiency, throughput and performance of network that needs the concern.

4.3 OBJECTIVES

1. To simulate Sybil attack in VANETs
2. To implement proposed approach on Sybil attack by using artificial bee colony.
3. Compare performance under network Sybil attack and network with AODV protocol on the basis of three parameters throughput, time delay and packet drop.

Chapter 5

IMPLEMENTATION

5.1 ARTIFICAL BEE COLONY (ABC) ALGORITHM

Many swarm intelligence algorithms have been proposed in past years. These algorithm simulates the general behavior of animals like birds, ants, fish or bees. Such algorithm helps to solve problems. Some of them are Ant Colony Optimization (ACO), Artificial Bee Colony (ABC), Particle Swarm Optimization (PSO), Firefly Algorithm (FA) etc. Artificial bee colony algorithm [47] is a population-based stochastic algorithm used for optimization technique. ABC is a new meta-heuristic approach that simulates the behavior of honey bees. It was proposed in 2005 by Karaboga.

In ABC algorithm, there are two types of bee categories, employed bees and unemployed bees (onlooker and scout). There are equal number of food sources and employed bees. Each type of bee have particular job in the hive. The task of employed bees is to exploit the food source. These food sources are initially searched by scout bees. Food source are exploited till it gets exhausted. Thus these source are then abandoned and the employed bees of abandoned food source becomes scout bee and search new for new food source randomly. All the employed bees share their information with onlooker bees in the hive. This information about the position of food source and the amount of nectar it contains. Onlooker bees on the given information goes to all the regions and chooses the best food source according to the probability (P_i), given as: -

$$P_i = \frac{\mathrm{fit}_n(\overrightarrow{x_n})}{\sum_{n=1}^{SN} \mathrm{fit}_n(\overrightarrow{x_n})}$$

Where, SN is total number of food sources,

fit_n is the fitness value of i^{th} solution.

Initialization Phase: - For all food sources $\underset{x_n}{\rightarrow}|$'s initialization by scout bees is done. Each food source $\underset{x_n}{\rightarrow}|$ contributes to the solution vector for optimizing problem. Each of the food source $\underset{x_n}{\rightarrow}|$ holds $m|$ variables, ($\underset{x_n}{\rightarrow}|$ = 1, 2,……. m). These variables are optimized. The following equation defines initialization process.

$$X_{ni} = l_i + rand(0,1) * (u_i - l_i) \qquad - (1)$$

Where l_i= lower bound of i^{th} solution

u_i= upper bound of i^{th} solution

rand(0,1)=any random number within range [0,1]

Employed Bees Phase: - Employed bees search food sources ($\underset{v_n}{\rightarrow}|$) which is having more amount of nectar in the neighborhood of previous food source ($\underset{x_n}{\rightarrow}$) in its memory. Each bee x_n produces new solution v_n. By finding new food source ($\underset{v_n}{\rightarrow}|$), bees evaluates its fitness value. The new food source is determined by equation,

$$v_{ni} = x_{ni} + \phi_{ni} (x_{ni} - x_{ki}) \qquad - (2)$$

where x_k is randomly selected source of food

ϕ_{ni} is random number in range (-1,1)

After deterring new food position its fitness value is calculated by greedy selection between new food source($\underset{v_n}{\rightarrow}|$) and old food source ($\underset{x_n}{\rightarrow}|$). The fitness value is calculated as: -

$$fit_m\left(\underset{x_m}{\rightarrow}\right) = \begin{cases} \frac{1}{1+f_m\left(\underset{x_m}{\rightarrow}\right)} 3) & \text{if } f_m\left(\underset{x_m}{\rightarrow}\right) >= 0 \\ 1+abs\ \left(f_m\left(\underset{x_m}{\rightarrow}\right)\right) & \text{if } f_m\left(\underset{x_m}{\rightarrow}\right) < 0 \end{cases} \qquad - (3)$$

where $f_m\left(\underset{x_m}{\rightarrow}\right)|$ is objective function value of $\left(\underset{x_n}{\rightarrow}\right)|$ solution.

Onlooker Phase: - All the employed bees share the information of their food sources with onlooker bees. On the basis of information shared by employed bees, onlooker bees determines the probability (P_n) using fitness value generated by employed bees.

$$P_i = \frac{\text{fit}_n(\overrightarrow{x_n})}{\sum_{n=1}^{SN} \text{fit}_n(\overrightarrow{x_n})} \quad \text{- (4)}$$

Scout Bee Phase: - Scout bees are unemployed bees which searches new food positions randomly. The food source are abandoned as these source got exhausted by employed bees. Then such employed bees are converted to scout bees which randomly searches for new food sources. Again, the solution to new food source id defined by equation (1).

5.2 General flow of ABC algorithm

→ Initialize food positions for all employed bees.

- x_i(i= 1,2,……,SN)

→ Repeat until cycle <= Maximum number of cycle.

Step 1: Produce new solution v_i for the employed bees using (2) and evaluate them.

Step2: Apply the greedy selection process for the employed bees.

Step3: Calculate the probability values p_i for the solutions x_i using (4)

Step4: Produce the new solutions v_i for the onlookers for the selected solutions x_i depending on p_i and evaluate them.`

Step 5: Apply the greedy selection process for the onlookers.

Step6: Determine the abandoned solution for the scout, if exist, and replace it with a new randomly produced solution x_i using 2)

Step 7: Memories the best solution achieved so far.

Step8: cycle =cycle+1

→ End

5.3 Closeness Centrality

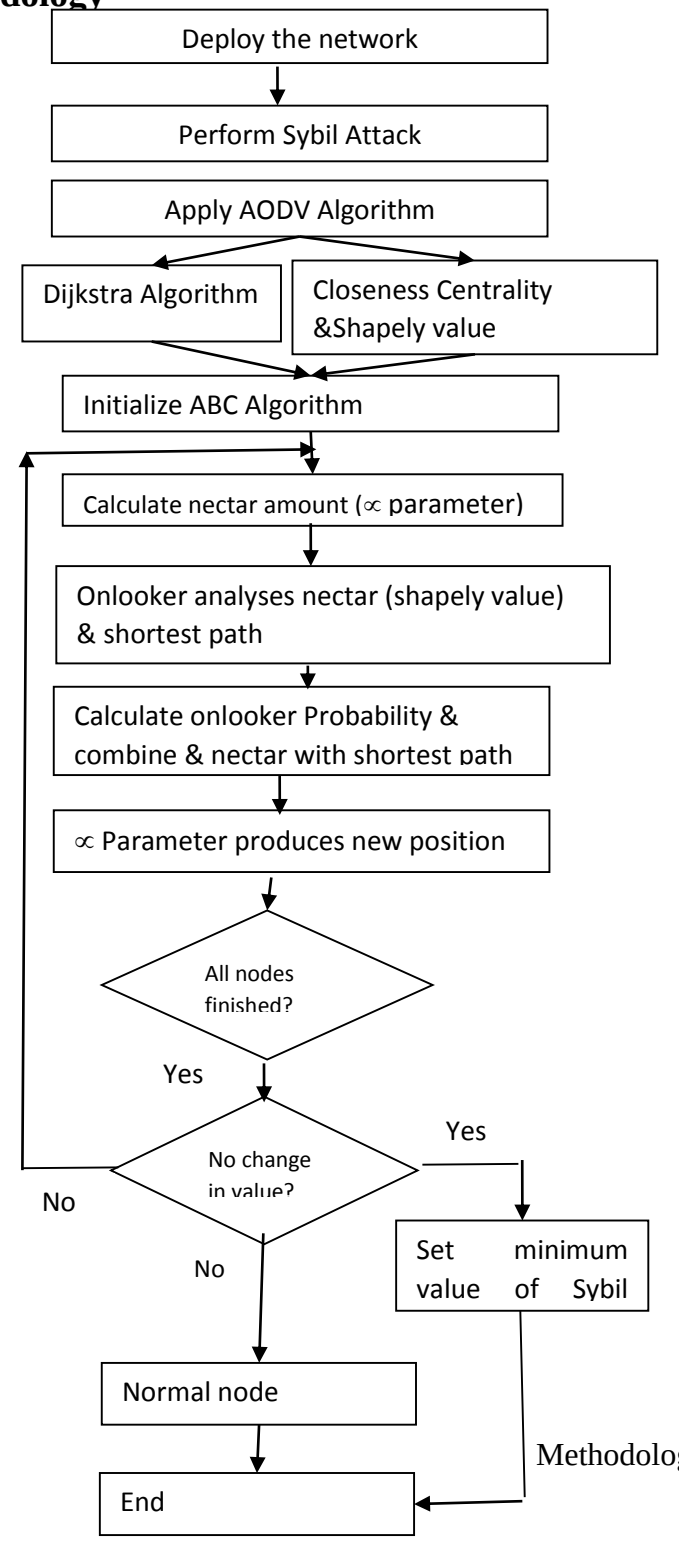
Closeness centrality [48] try to capture how close the particular node is to any other node in the network. This means how easily the node can reach to other node. It is reciprocal to farness. The farness can be calculated as: -

For a given graph G, farness of any vertex u is calculated as

Farness [u] = $\sum_{\substack{v \in V \\ D(u,v) \neq \infty}} D(u,v)$ -(1)

For calculating closeness centrality, $Cc[u]= \frac{1}{farness[u]}$ -(2)

5.4 Methodology



Methodology of proposed work

Module 1: Inject Sybil Nodes in network

First of all, nodes in the network is deployed in ns3 simulator. For injection of Sybil nodes/ attacker nodes in network. We have set the maximum effective value of shortest path and centrality to Sybil nodes.

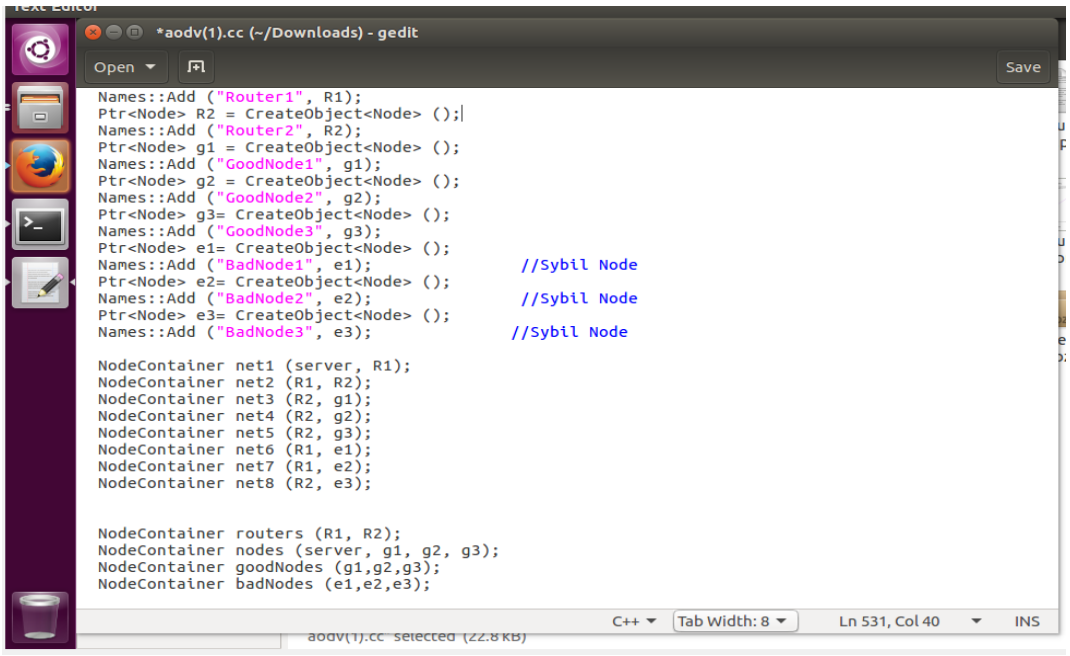


Figure 5.2 Injecting Sybil nodes

Module 2: Apply AODV Algorithm

In this module, we have applied AODV algorithm for routing packets. Generally AODV algorithm is used to route packets through shortest path from their source to destination. But due to the presence of Sybil nodes and their effective values all the data packets pass through these attacker nodes. As a result, packets are dropped and hence this reduces throughput and time delay.

Module 3: Prevention of Sybil Attack

We applied AODV algorithm to the network using shortest path (dijkstra algorithm) and closeness centrality which initializes ABC algorithm. Closeness centrality is used to monitor how network topology is changed. In our work, the initial position of nodes is taken as closeness centrality input. ABC algorithm is used for monitoring all the nodes in the network whether value of nodes is converging or not. In this algorithm, nectar amount

i.e. ∝ parameter is calculated which controls shapely value (shortest distance) between two nodes. If the nodes converges the ∝ parameter then it is considered as non-attacker node, otherwise it is attacker node and hence it is given minimum value. This enforces AODV algorithm to ignore Sybil nodes and prevent Sybil nodes. In

```
  //Closeness Centrality
  float *CC = new float[n];
  float sum = 1;
cout<<""<<endl;
cout<<"Centrality"<<endl;
  for(int i = 0; i < n; i++){
    sum = 1;
    for(int j = 0; j < m; j++){
      sum += SP[i][j];
    }
    CC[i] = 1/sum;
  }

for(int i = 0; i < n; i++){
cout<<CC[i]<<" ";

}
cout<<""<<endl;
```

Figure 5.3 Code for closeness centrality

The above figure is a code for closeness centrality. In this it is calculating the sum of shortest distances between the nodes. Since, we explained earlier that closeness centrality is reciprocal of farness. So it is calculating the inverse of sum of shortest distances. Closeness centrality is computed for each node i.

Module 4: Comparison of attack detection by P2DAP and ABC algorithm

P2DAP is a light-weight, scalable framework for the detection of Sybil attack. In this the privacy of each vehicle is preserved in the network. The framework used is called P2DAP (Privacy-Preserving Detection of Abuses of Pseudonyms). This framework distributed the responsibility to semi trusted third party to detect attack while maintaining anonymity of vehicle. Comparison is done using three parameters i.e. throughput, time delay and packet drop. The results are shown by plotting graphs.

Chapter 6

Simulation results

6.1 Installation

1. Download NS-3.26 allinone package.
2. Unzip the package.
3. Run the command
   ./ build.py –enable-examples –enable-tests
4. Then run
   ./waf –d debug –enable-examples –enable-tests configure

6.2 Aim of proposed work

The aim of the proposed work is to secure the Vehicular Ad-hoc network from the Sybil attack by the use of Artificial Bee Colony (ABC) algorithm that results in less packet drop, reducing time delay and giving high throughput.

The code is developed in C++ and run on NS3 simulator. The positioning of the Nodes are optimized by the ABC algorithm and corresponding time delay, throughput and drop packets rate are demonstrated, calculated and graphs are plotted in NetAnim and how the packets are being sent is shown in Netanim.

6.3 Performance Analysis in Network Animator (NetAnim): -In this category, we performed analysis of network with ABC algorithm and compared it with the performance analysis of network without ABC. We do the performance analysis on the basis of three performance metrics, time delay, throughput, and packet drop are compared and result are shown in graph 6.3, 6.4 and 6.5.

6.3.1 Attack Simulation without ABC: The figure shows that the nodes are not optimized due to which there are multiple pseudo nodes and data is also being sent to these pseudo nodes.

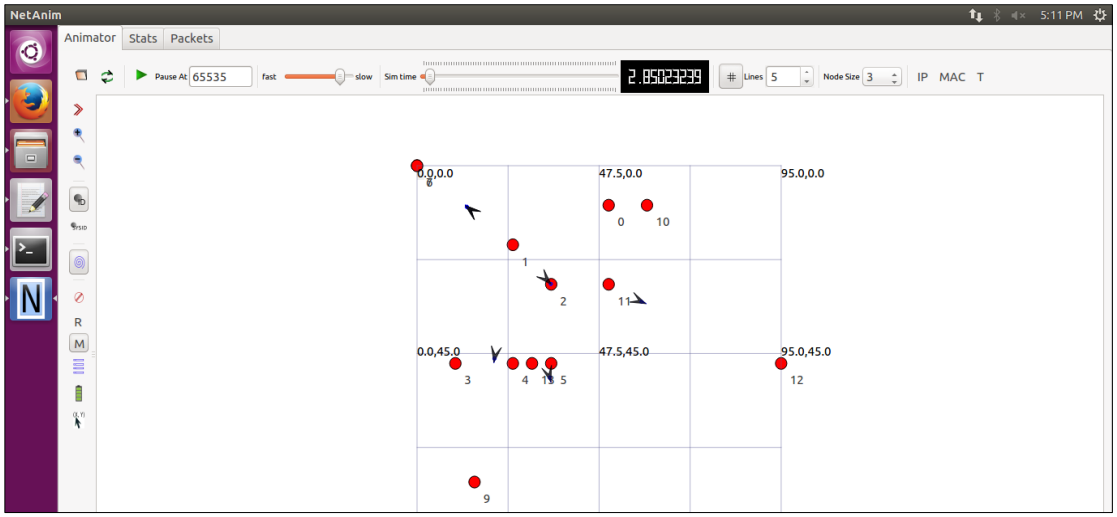


Figure 6.1 Transmission of Packets

6.3.2 Attack Simulation with ABC: The figure shows two Sybil nodes with black colored nodes and other normal nodes. This shows that nodes are being optimized and less packet drop via Sybil nodes.

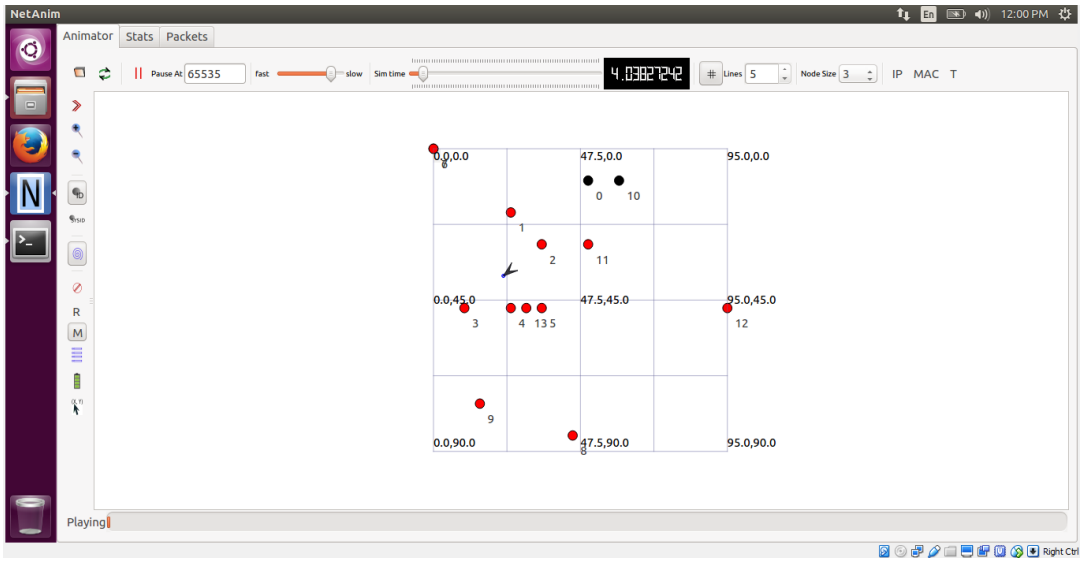


Figure 6.2 Presence of Sybil Nodes

6.4 Parameters used in simulation (Table 6.1)

Parameters	Values
Number of Mobile nodes	15
Topology	Dynamic
Channel type	Omni
Routing protocol	AODV
Size of packet	1024 bits
Simulation time	80s
MAC protocol	IEEE 802.11
Channel type	Wireless

6.5 Performance metrics

1) **Throughput: -** In general, throughput is the maximum number of packets processed in particular time interval i.e. the number of packets delivered from source to destination successfully. Throughput in vehicular ad-hoc network is defined as maximum packets delivery ratio between mobile nodes.

2) **Drop packet: -** Packets dropping starts when Sybil nodes duplicating the identities of authorized vehicles and start generating the flood of false information and disrupt the overall communication.

3) **Time Delay: -** It is defined as the time taken by packets to reach from source to destination. Sybil nodes increase the delay by injecting the false information which mislead the other vehicles and the packets are unable to reach on time to desired destination.

6.6 Simulation Results

The figure 6.3 shows the comparison graph in which throughput decreases with P2DAP technique and when we use ABC algorithm for their prevention, then it optimizes the network performance and hence throughput increases.

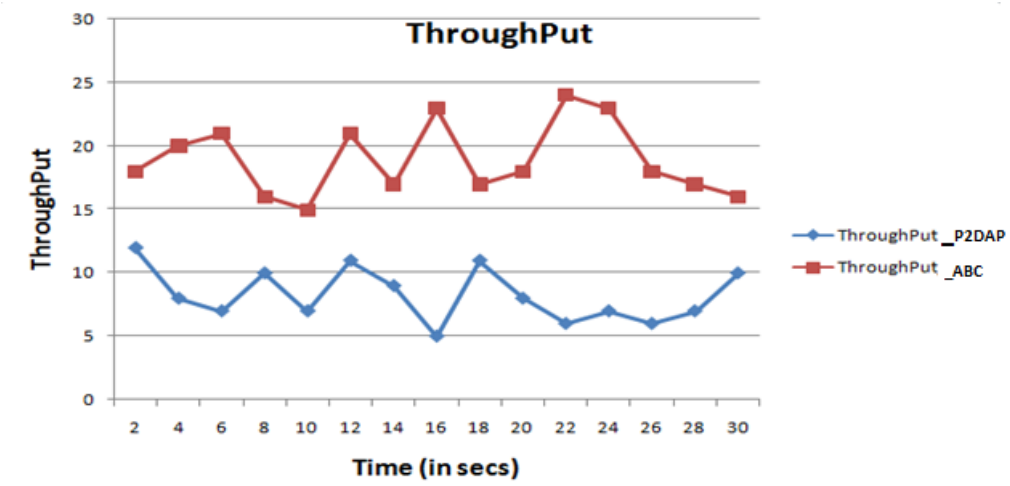


Figure 6.3 Throughput versus time

The figure 6.4 shows packet dropping which is more when P2DAP technique is used. ABC algorithm tries to minimize the packet drop ratio by removing the Sybil nodes.

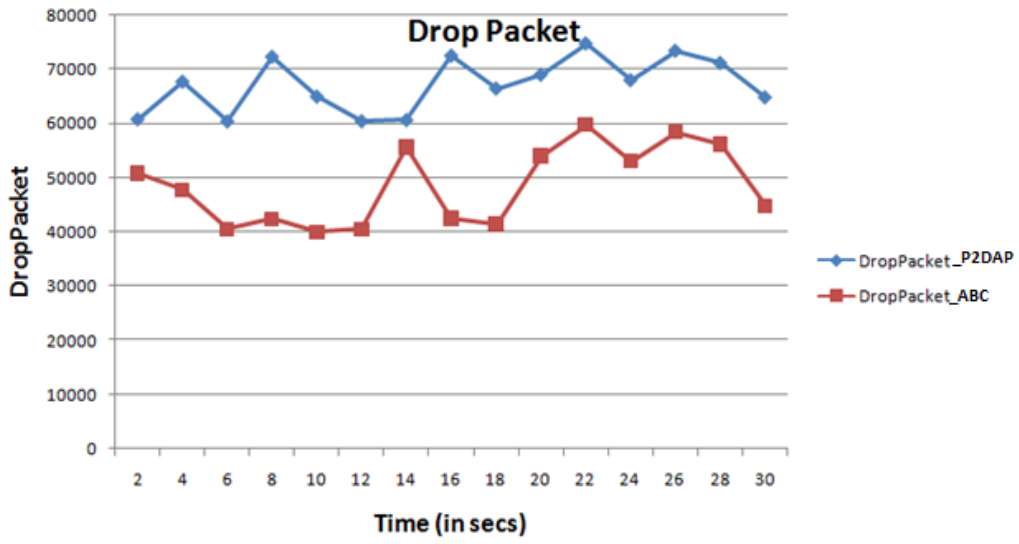


Figure 6.4 Packet Drop Versus time

The figure 6.5 shows the graph of comparison between Time delay of network with ABC and with P2DAP technique. The proposed technique is that network gives better result with ABC as compared to network with P2DAP technique. The proposed technique decreases the time delay of delivered packets as compared to the without ABC algorithm.

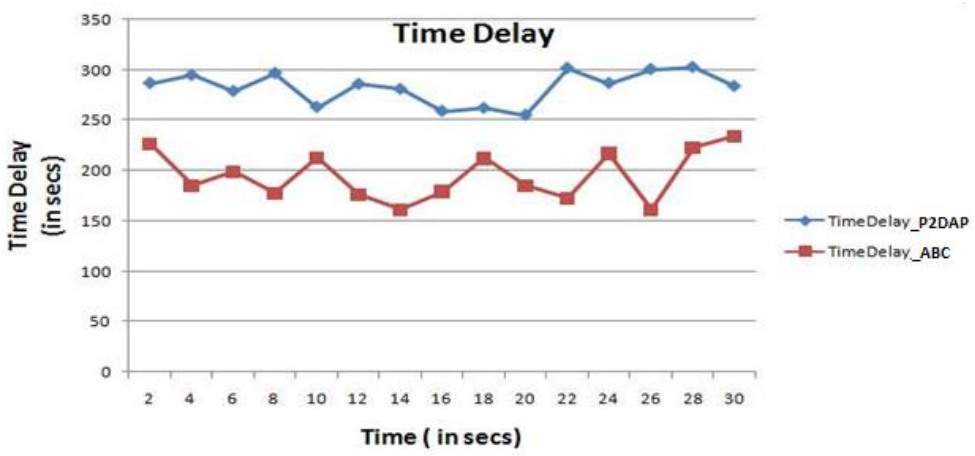


Figure 6.5 Time delay

CHAPTER 7

CONCLUSION & FUTURE SCOPE

7.1 Conclusion

VANETs are the emerging technologies in today's world for secure and safe driving on roads in urban areas and on highways. Along with the use of VANETs, it also becomes vulnerable to attacks. One of the main attacks is Sybil attack that degrades the network performance. In our research work, we have simulated the Sybil attack and its detection and prevention is performed using ABC algorithm in proximity of the closeness centrality. The performance of network is evaluated on the basis on three metrics, throughput, packet drop and time delay. Using the ABC algorithm, network performs better and shows optimized results.

7.2 Future scope

Our proposed algorithm yields an efficient results in terms of network performance in VANETs. This mitigates and prevents the Sybil attack. Hence our proposed algorithm can also be used to detect and prevent other hazardous attacks like wormhole attack, jellyfish attack, black hole attack etc.

REFERENCES

[1] B.Mokhtar, M.Azab, "Survey on Security Issues in Vehicular ad hoc Networks," *Alexandria Engineering Journal*, pp. 1115-1126, 2015.

[2] F.Li, Y.Wang, "Routing in vehicular adhoc networks : a survey," *Veh. Technol Magazine, IEEE*, pp. 12-22, 2007.

[3] S.K.Bhoi, P.M.Khilar, "Vehicular communication : a survey," *IET network*, vol. 3, no. 3, pp. 204-217, 2014.

[4] S.Gaglione, A.Innac, S.P. Carbone, S.Troiri, A.Angrisano, "Robust estimation methods applied to GPS in harsh environments," in *European Navigation Conference (ENC)*, 2017, 2017.

[5] V.D.khairnar, K.Kotecha, "Performance of Vehicle-to-vehicle Communication using IEEE 802.11p in Vehicular Ad-hoc network Environment," *International Journal of Networks Security & Its Applications(IJNSA)*, vol. 5, no. 2, 2013.

[6] K.Rawat, J.Hazrati, "Vehicular Ad-hoc Network," *International Journal of Information & Computation Technology*, vol. 4, 2014.

[7] T.Sujitha, S.P.Devi, "Intelligent Transportation System for Vehicular Ad-Hoc Networks," *International Journal of Emerging Technology and Advanced Engineering*, vol. 4, no. 3, 2014.

[8] S.A.M.Ahmed, S.H.S Ariffin, N.Fisal, "Overview of Wireless Access in Vehicular Environmental(WAVE) Protocols and Standards," *Indian Journal of science and Technology*, vol. 6, no. 7, 2013.

[9] S.B.Mer, "Smart Vehicle-to-vehicle communication with 5G Technology," *International Journal on Recent and Innovation trends in Computing and Communication*, vol. 3, no. 5, 2015.

[10] S.A.Mohammad, A.Rasheed, "VANET Architecture and Protocol: A survey," *Communication Technologies for Vehicles* , pp. 95-105, 2011.

[11] L.Pu,Z.Liu,Z.Mang,X.Yang,K.Zhu,L.Zhang, "Implementing on-board diagnostic and GPS on VANET to safe the vehicle," in *Connected Vehicles and Expo (ICCVE)*, Shenzhen, China, 2015.

[12] Z.H.Mir,F.Filali, "LTE and IEEE 802.11p for vehicle networking : a performance evaluation," *EURASIP Journal on Wireless Communicating and Networking*, 2014.

[13] A.M Vegni,M.Biagi, R.Cusani, "Smart Vehicles,Technologies and Main Applications in Vehicular Adhoc Networks," in *Vehicular Technologies-Deployement and Applications*, 2013.

[14] A.K.Panghal,S.Rani, "Vehicular Ad-hoc Network (VANET) - Privacy and Security," *International Journal of Advanced Research in Computer Science*, vol. 6, no. 2, 2015.

[15] Security Challanges,Issues and their solutions for VANET, "R.S.Raw,M.Kumar,N.Singh," *International Journal of Network Security & Its Applications*, vol. 5, no. 5, 2013.

[16] V.H.La, A.C.Valli, "Security Attacks and Solutions in Vehicular Adhoc Networks :A Survey," *international Journal on Adhoc Networking Systems(IJANS)*, vol. 4, no. 2, 2014.

[17] V.Raghuwanshi, S.Jain, "Denial of Service Attack in VANET : A survey," *International Journal of Engineering Trends and Technology(IJETT)*, vol. 28, no. 1, 2015.

[18] V.Kumar, R.Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Adhoc Network," *Procedia Computer Science*, vol. 48, pp. 472-479, 2015.

[19] S.N.Ganesh, R.S.Ranjani, "Security Threats on Vehicular Adhoc Networks(VANET) : A Review Paper," *International Journal of Electronics Communication and Computer Engineering*, vol. 4, no. 6, 2013.

[20] Z.Chen, S.Guo, K.Zhang, Y.Yang, "Modelling of Man-in-the -middle attack in the Wireless Networks," in *Wireless Communications,Networking and Mobile Computing*, Shanghai, China, 2007.

[21] B.K.Joshi, M.Soni, "Security assessment of AODV protocol under wormhole and DOS attacks," in *Contemporary Computing and Informatics(IC3I)*, Noida, India, 2016.

[22] N.Lo, H.Tsai, "Illusion Attack on VANET Application- A Message Plausibility Problem," in *Globlecom Workshops*, Washington,DC,USA, 2007.

[23] Sukiswo, M.R.Rifquddin, "Performance of AOMDV routing protocol under rushing and flooding attacks in MANET," in *Information*

Technology,Computer, and Electrical Engineering(ICITACEE), Semarang,Indonesia, 2015.

[24] K.N.Qureshi, A.H.Abdullah, "Topology based routing protocols for VANET and their Comparison with MANET," *Journal of Theoretical and Applied Information Technology,* vol. 58, no. 3, 2013.

[25] E.Mahdipour, A.M.Rahani, E.A.Minian, "Performance Evaluation of Destination Sequenced Distance Vector (DSDV)," in *International conference on Future Networks*, 2008.

[26] T.P.T.Minh, T.T.Nguyen, D.Kim, "Location Aided Zone routing Protocol," in *20th Conference on emerging Technologies & Factory Automation(ETFA)*, 2015.

[27] N.Nisaar, N.Naja, A.Jamali, "Lightweight authentication based scheme for AODV in adhoc networks," in *International Conference in Wireless Technologies,Embedded and Intelligent System(WITS)*, 2017.

[28] S.Thawani, H.Upaddhyay, "Security TORA against Sybil attacks in MANETs," in *International Conference on Futuristic Trends on Computational Analysis and Knowledge Management(ABLAZE)*.

[29] N.Goel, G.Sharma, I.Dhyani, "A study of position based VANET routing protocols," in *International Conference on Computing Communication and Automation (ICCCA-2016)*, 2016.

[30] S.Allal, S.Boudjit, "Geocast Routing Protocols for VANETs: Survey and Guidelines," in *6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Italy, 2012.

[31] A.P.Shreevatsan, D.Thomsan, "An Optimal Weighted Cluster Based Protocols for MANET," in *International Conference on Data Mining and Advanced Computing (SAPIENCE)*, 2016.

[32] M.Ganziginger, W.J.Hymas, T.Schutt, "Securing Broadcast Based AdHoc Routing Protocols," in *Prevasive Computing and Communication Workshops*, 2007.

[33] D.Sharma, S.Thakur, "Sybil-Decline: A Survey on Novel Trusted Identify and Threshold Basec Path Rank for Sybil Attack Identification in Social Network," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 4, no. 6, pp. 663-669, 2014.

[34] S.Moradi, M.Alvadi, "A distributed method based on mobile agent to detect Sybil attacks in Wireless sensor networks," in *Eighth International*

Conference on Information and Knowledge Technology (IKT), Hamedan, Iran, 2016.

[35] R.Lokhanpal, S.Sharma , "Detection & Prevention of Sybil attack in Adhoc Network using Hybrid MAP & MAC Technique," in *International Conference on Computation of Power, Energy and Communication (ICCPEIC)*, 2016.

[36] R.Devi, M.Hemalatha, "Sybil Identification in Social Networks using SICT and SICTF Algorithms with Improved KD-Tree," *Journal of Therotical and Applied Information Technology*, vol. 56, no. 2, pp. 443-451, 2013.

[37] P.W.L.Fong, "Preventing Sybil attacks by Privilige Attenuation: A Design Principle for social Network Systems," in *Security and Privacy (SP)*, Berkeley, CA, USA., 2011.

[38] H.Yu, M.Kaminsky, P.B.Gibbons, A.Flexman, "Sybil Guard: Defending against Sybil Attacks via Social Networks," in *Conference on Applications, technologies, architecture, and protocols for computer communications*, Pisa, Italy, 2006.

[39] H.Yu, Phillip.B, G.M.Kaminsky, F.Xiao, "SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks," in *IEEE Symposium on Security and PrivacyIEEE Symposium on Security and Privacy*, 2008.

[40] T.Zhou, R.R.Choudhury, P.Ning, K.Chakrabarty, "Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Area in Communications,* vol. 29, no. 9, 2011.

[41] Navneet, R.Gill, "Sybil Attack Detection and Prevention Using AODV in VANET," *IJCSMS International Journal of Computer Science & Managemnt Studies* , vol. 13, no. 7, pp. 333-339, 2013.

[42] P.Gu, R.Khatom, Y.Begriche, A.Serhrouchni, "Vehicle Driving Pattern Based Sybil Attack Detection," in *IEEE 18th International Conference on High Performance Computing and Communications*, Paris, France, 2016.

[43] P.V.Kumar, M.Maheshwari, "Prevention of Sybil attack and priority batch verification in VANETs," in *Information Communication and Embedded Systems (ICICES)*, Chennai, India, 2014.

[44] S.Sharma, "A Defensive Timestamp Approach to Detect and Mitigate the Sybil Attack in VANETs," in *Contemporary Computing and Informatics (IC31)*, Noida, India, 2016.

[45] "www.newindianexpress.com," January 2009. [Online]. Available: http://www.newindianexpress.com/nation/2017/jan/09/three-people-die-every-10-minutes-in-road-accidents-in-india-1557786.html.

[46] "http://edition.cnn.com," 7 July 2016. [Online]. Available: http://edition.cnn.com/2016/07/07/health/us-highest-crash-death-rate/index.html.

[47] Samiksha, A.Kaur, "Vehicle to Road Side Unit Communication to detect the Sybil Attack and Prevention using ABC Optimization Technique," *International Journal of Modern Computer Science and Applications (IJMCSA),* vol. 4, no. 4, 2016.

[48] L.Qiao, Y.Shi, S.Chin, "An Empirical Study on the Temporal Structural Charaterstics of VANETs on a Taxi GPS Dataset," *IEEE Access,* pp. 722-731, 2017.

List of Publications

[1] Harpreet Kaur, Sumit Miglani, "Detection and Prevention of Sybil attack using Artificial Bee Colony Algorithm in proximity of Closeness Centrality," *International Conference on Smart Technologies for Smart Nation* (SmartTechCon 2017)(Accepted).

Video link

https://youtu.be/fO6xRwnK0vU

Plagiarism Report