Malicious Node Identification Routing and Protection Mechanism for VANET against Various Attacks

Zaid Abdulkader
Al Iraqia University, Baghdad, Iraq
Iraq
zaid.researchs@gmail.com

Azizol Abdullah, Mohd Taufik Abdullah, Zuriati Ahmad Zukarnain
Universiti Putra Malaysia
Malaysia
azizol@upm.edu.my

ABSTRACT: *VANET (Vehicular Ad-hoc Network) is a promising approach that provides safety measures and other application to the drivers on the vehicles. The focus of VANETs is to fulfill user's requirements on road side area which increases the safe and comfortable journey for users. It provides good communication like MANET (Mobile Ad-hoc Network) when there is no intruders exist in the network. In VANET, communication depends on road safety such as emergency situation, vehicles tracking, messages monitoring and tracking of vehicles. But many attackers like black hole attack, Wormhole attack and Sybil attack are more vulnerable to VANET. In order to provide efficient communication, we provide a Malicious Node Identification Routing mechanism which gives the valid route between two vehicles. To avoid several attacks, we introduce a Protection Mechanism that includes key management for preventing our network. Our proposed system provides efficient communication on VANET that focus on Throughput, End-to-End delay, Packet delivery ratio, Detection rate and Misdetection rate.*

Keywords: Black Hole Attack, Sybil Attack, Wormhole Attack, VANET, AODV Routing, Elliptical Curve Cryptography

Received: 14 June 2017, Revised 18 July 2017, Accepted 26 July 2017

1. Introduction

1.1 VANET

Nowadays, transportation becomes important to the human life. In few years, transportation introduced with attention to industries and academia by introducing communication between vehicles which named as VANET. In VANET, a large number of mobile distributed applications are applied on vehicles, using this many vehicles communicate each other on the road side. VANET are made up of vehicles and Road Side Units where vehicles are equipped with on-board units. Communication on

VANET can either be one-hop or multi-hop, where vehicles can pass messages directly to another vehicle or else they can pass between vehicles. There are two types of communication in VANET they are 1) Vehicle to Vehicle Communication 2) Vehicle to Road Side Units (RSUs). Since VANET is an application of MANET, it has some characteristics of MANET like working without using any infrastructure network. But VANET has some special characteristics such as 1) Large Scale Networks i.e. there must be thousands of vehicles on the roads; every nodes must be registered with the network, 2) Road Configuration, Traffic Laws, Speed Limits which does not affect mobility of vehicles and 3) Vehicles consists of increased resources such as large batteries, antenna and processing power. Based on these vehicles, several applications are introduced in the VANET, they are: 1) Safety Application, 2) Local Traffic Information system 3) IP based applications and 4) Automated Highways. VANET applications allow convenient driving while travelling and makes safer journey for users. Communicating with other vehicles allows convenient information exchange regarding any warning information and urgent information on the roads. VANET has several challenges to obtain efficient communication between vehicles such as 1) High mobility 2) Security 3) Location Awareness and 4) Real time delivery of messages [1]. Figure 1 describes the architecture of VANET.

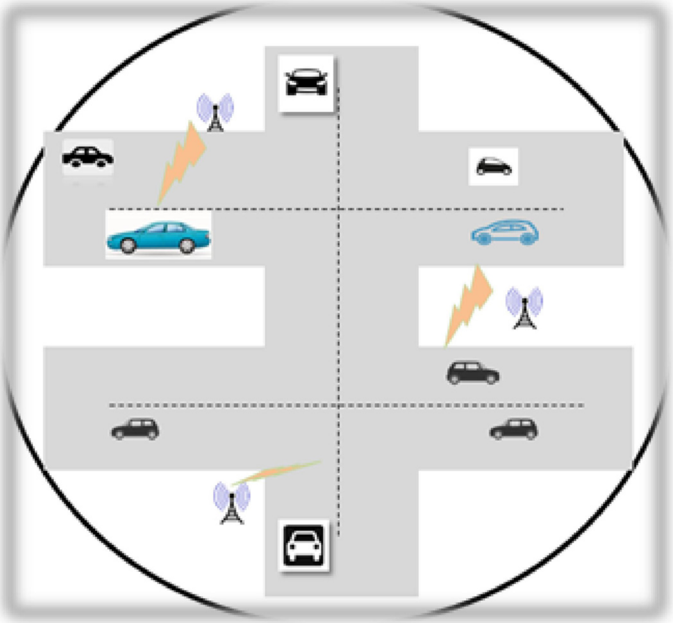


Figure 1. Architecture of VANET

In Paper [2], author proposed a new solution for protecting the VANET from Sybil attacks. Here a solution is provided for detection Sybil attacks in which the identification is based on two methods of authentication. The first method uses RFID tags which are embedded in vehicles. This helps to authenticate vehicles to RSU and allows vehicles to obtain shorter lifetime certificates. In the second method, certificates are used for authenticating the neighbor vehicles for communication. Here vehicular network considered here are divided into different zones which brought under control of different certification authorities. This several zones contain several RSUs and here one of them is selected as RSC (Road Side Controller). This solution has specific advantages that it avoids tracking of mobility of vehicles.

1.2 Attacks

1.2.1 Wormhole Attack

This is a severe attack in VANET, in which one or more malicious nodes creates a tunnel for transmitting data packets from one end of malicious node to other malicious node. Here these packets are broadcasted based on private network which is shared with malicious nodes. This worm hole allows the attackers getting a very higher role in comparison to other nodes. It is very challenging to detect and prevent the attack.

1.2.2 Sybil Attack

Sybil attack is another critical attack in the network at which attacker sends different message with multiple identities to other vehicles. Here the identities can be used to plan any other type of attack in the network. This forging identity leads to create an illusion due to large vehicles on the road side. This Sybil attack, disturbs generation of routes when multipath routing is used, attackers appears in several places in generated routes. This can affect the results of data aggregation several times in network.

1.2.3 Black Hole Attack

Black hole attack is also a severe attack in VANET; here a malicious node uses its routing protocol for advertising shortest path to the destination node by itself. A hostile node advertises availability of fresh routes irrespective of checking its own routing table. Using this way, attacker node will always have availability in replying route request and intercept data packet and retain it. In reactive routing, based on flooding malicious nodes replies will be received by sender node before receiving the original route (i.e. safe route) from normal node, hence at the end, malicious node creates forged route to the sender node [3].

In paper [4], author discussed a new technique that allows detecting and preventing wormhole attacks in the MANET. The main objective of this paper is that provides many possible routes when sending Route Request (RREQ) from source node to Destination node. These routes are used as reference for each other which help in finding the malicious nodes with suspicious behavior in that network. This process introduces three steps in the network for detecting; they are 1) Route redundancy, 2) Route aggregation and 3) Calculating Round Trip Time (RTT) of every listed routes. In Route Redundancy process, a slight modification is done in reactive routing protocol named AODV. In this routing, every path is considered for packet transmission and destination accepts only first receiving RREP and source calculates the round trip time for all routes in the network. Here there is a main disadvantage is that, when any link of node gets break while transmitting then there is a possibility of packet loss.

A modified AODV algorithm is proposed in [5], which improves security and performance of MANET network against black hole attack. Here the routing process is done based on monitoring the behavior of nodes in the network by broadcasting RREQ from source node and RREP from destination node. Here some rules are specified for identifying destructive behavior of nodes. These rules identify the malicious node using rules and eliminate them in MANET.

In our proposed mechanism, we use medical emergency application, there we introduce a Malicious Node Identification Mechanism which includes the modification of AODV routing protocol that identifies various attacks like Sybil attack, Wormhole attack and Black hole attack. For identifying Sybil attack, we use Signal Print based Sybil classification [6] which classifies the true RSSI values and false RSSI observation on packet transmission while RSSI signal is identified at RSU. False observations are verified based on its IP address and MAC address at DMV (Department of Motor Vehicle). For identifying the Wormhole attacks and Black hole attacks we modify the AODV routing process by identify the lifetime of every node and we allow the route redundancy process in [4] which solves the link breakages and packet loss in during packet transmission. For protecting the network from severe attacks we introduce AES-Blowfish Cryptographic mechanism. The contribution of our proposed work is,

- Malicious Node Identification Routing mechanism is introduced that works against Black hole attack, Sybil attack and Wormhole attack.

- Protection Mechanism is introduced that includes key management to preventing our VANET from various attacks.

The rest of the paper is as follows: Section 2 describes about the literature survey, Section 3 says about the problem that occurs on VANET for safe communication between the vehicles, Section 4 describes our proposed work in our paper which includes malicious node identification mechanism and Protection mechanism, Section 5 evaluates our proposed process by comparing with existing system and finally Section 6 concludes our paper.

2. Literature Survey

Researchers such as Vrushali Kelatkar and Prof. Pravin Dere proposed an overview of Light weight Sybil detection on MANET [7]. In MANET, an attacker attains several identities and they use only one time at a time or all identities are used simultaneously. Here the lightweight scheme describes a sensing of new identities of Sybil attackers without using any trusted third party such as additional hardware like GPS, directional antenna. Every received RSS value is passed to add new RSS function with its time of reception and address of transmitter. If the address is not in RSS table which means that it is a mingled node and it is compared with upper bound threshold. If the result is superior or equal to threshold then node is added to malicious node otherwise it is added to RSS table and link list is created for that specific address for storing the received RSS along with its time of reception in it.

In paper [8], authors suggested a detection and prevention of Sybil attack based on MAC address in MANET. Initially sender node broadcast a RREQ packet to a destination and it receives the RREP message along with MAC address and logical (IP) address. Sender node maintains a table that checks malicious node. Here if a node with same physical address with different logical address is considered as a Sybil attacker. After identification of sender node a new alternative path is chosen for safe packet transmission.

Authors like Khaled Rabieh, Mohamed M. E. A. Mahmoud, Terry N. Guo, and Mohamed Younis. This paper is focus on sybil attack which is severe when a vehicle colludes with other vehicles that must use valid credentials for authenticating sybil vehicles [9]. Here authors proposed a cross-layer scheme which enables RSU s for identifying sybil vehicles in the VANET, this schemes is based on verifying vehicles locations. A challenging packet is sent to that specific claimed vehicle location based on directional antenna. If the vehicle at corresponding location it sends immediate response packet otherwise the specific node is a suspicion of sybil attack. The cross-layer design is performed by composing challenge packet at MAC layer and directing PHY layer to send it to specific layer. For securing the challenge and response packets, hash function and public key cryptography are used. Overhead is occurred when challenging packet is sent to all vehicles at a time; to solve this we send a challenge packet when there is a suspicion of Sybil attack in the network.

Authors such as Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty proposed a lightweight and scalable protocol for detecting sybil attacks [10]. In this method, malicious user can be pretending to multiple other vehicles which are in distributed manner. This can easily identified by distributed manner through passive overhearing by a set of fixed nodes called road side boxes (RSBs). The detection of sybil attacks does not require any other vehicles and privacy is preserved all times in the networks. In this paper, the RSB is securely connected to DMV via a backhaul wired network, where DMV plays a role of certificate authority (CA) and it has capability to manage ownership, vehicle registration and other administrative policies. DMV helps to hide vehicle s unique identity which provides a pool of pseudonyms of vehicles. For preventing a vehicle, multiple pseudonyms assigned to a hashed common value because multiple pseudonym directs to sybil attack.

In paper [11], researchers such as Kenza Mekliche, Dr. Samira Moussaoui proposed an approach which uses infrastructures and localization of nodes for detecting sybil attacks. Here the cooperation between adjacent RSU s to find the location of suspicious nodes and it measures a distinguishability degree between positions of malicious nodes. the sybil detection is done in two levels: 1) the first level is done on road side where they overhear the vehicles communication measure positions of each vehicle based on adjacent RSUs. If degree of distinguishability is over a threshold then RSU reports suspicious vehicles to DMV. 2) this detection level is done by DMV, it generates fine grained hash of the suspicious vehicles that separate between actual attack and false positive.

Authors like Mahdi Nouri, Somayeh Abazari Aghdam, Sajjad Abazari Aghdam suggested a collaborative techniques for detecting wormhole attack in the network [12]. Here they introduced five kinds of wormhole attacks and its clusters are introduced. Two collaborative techniques for intrusion detection in MANET is introduced they are 1) Initial detection is designed for detection of malicious nodes on neighborhood of nodes in which each pair of nodes are within radio range of each other. 2) This detection method is also designed for detection of malicious nodes in neighborhood nodes, but here each pair of nodes may not be in the radio range i.e. there is a node among them which all nodes are in one-hop vicinity.

In paper [13], authors suggested an algorithm for detecting and recovering wormhole attack in MANET. Here they use path tracing algorithm which uses two specific parameters such as Hop Count and RTT (Delay). These parameters are calculated by sender node when it receives RREP packet from neighborhood nodes. When a sender node broadcast RREQ packets, here intermediates node forwards packets with hop count, add its own time and increase time stamp values and further broadcast RREQ message. After receiving the RREP packets, source node compares delay/hop count. The resulting value is compared with threshold value; if it is too large then RREP packet is discarded. Then alternative path is chose for packet transmission.

Researchers such as Khaleel Mershad and Hassan Artail presented a framework for secure and efficient data transmission and acquisition on VANET [14]. This introduces a system which takes advantages of RSUs which are connected with internet and provide various types of information to VANET users. Here a novel security and privacy information in this system is introduced and performance is evaluated using NS2 software. Authors in [15], proposed some key management techniques in Wireless Sensor Networks. This technique introduces a novel approach for cryptography which guarantees the data security. A secure communication is provided based on pair-wise key and it allows refreshment process for those keys which occurred successfully and also it has the ability of keys revocation.

In paper [16], authors like S. Balasubramani, S.K. Rani and K. Suja Rajeswari reviewed some security attacks and its mechanism in VANET and MANET. Here they analyze the common security attacks and their exploitation in various layers which are used for secure transmission.

3. Problem Definition

VANET is a recent technology that allows vehicles to communicate on the road side with the help of Road Side Unit. Due to infrastructureless network, VANET faces many problems in terms of security whereas several critical attacks like Sybil attack, Black hole attack and Wormhole attack degrades the performance of network [1]. Many algorithm and mechanism are introduced in the network which solves the problem and it results in performance degradation like higher delay, packet loss, breakage of link during routing. Commonly wireless networks are more vulnerable to sybil attacks, a defensive sybil detection mechanism is introduced in MANET, which consumes more energy for the packet transmission in the network [6].

Black hole attack and Wormhole attack are vulnerable to the VANET; a new routing algorithm is introduced safe for packet transmission which avoids black hole attack by monitoring the nodes behavior in MANET [5]. Here behavior of node is identified by specifying rules that denotes the malicious behavior. Wormhole attack is identified by route aggregation process and allows RTT for the packets that to be send. Both processes have disadvantages that node s lifetime and route lifetime is not considered which results in less route reliability, packet loss and link breakages.

4. Proposed System

4.1 Overview

VANET is a developing network which is also a subgroup of MANET. It allows communication between vehicles on the road side for improving traffic and safety applications. In our proposed system, we use medical emergency application; there we

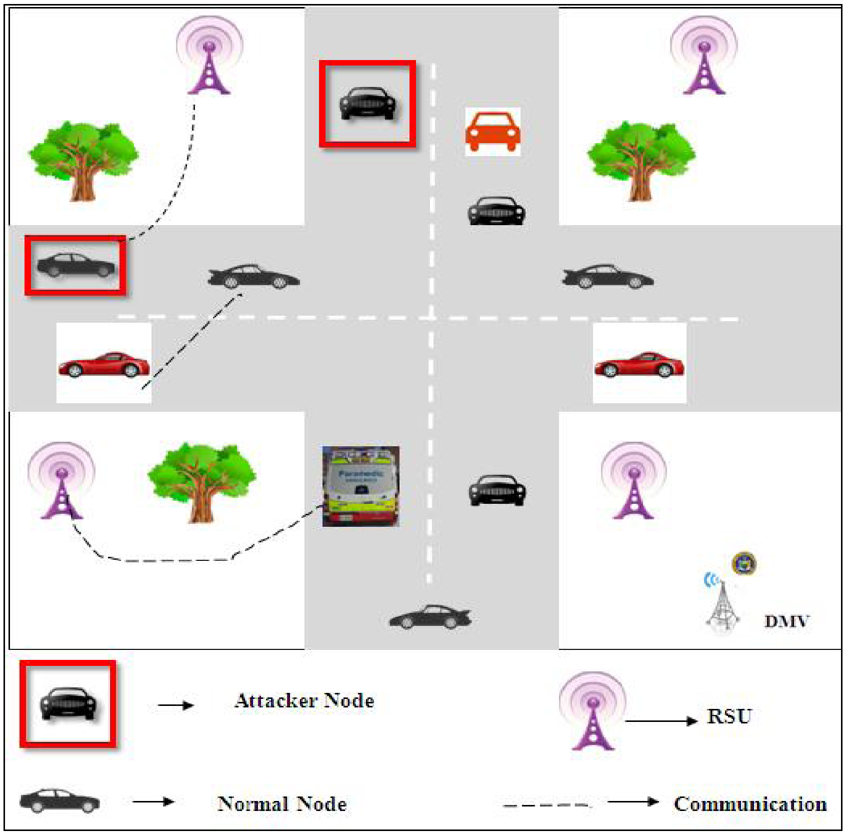


Figure 2. Architecture of Proposed Process

introduced a Malicious Node Identification Routing mechanism that includes identification of three different attacks such as Black hole attack, Sybil attack and Wormhole attack. This identification mechanism uses modified AODV routing protocol for the packet transmission in the VANET. Our algorithm provides attack free routes for packet transmission from sender to destination. This algorithm gives best performance in terms of delay, Throughput, packet loss and packet delivery ratio (PDR). For protecting the network from several attacks we introduce a secure Protection mechanism that includes key management process in the network.

Figure 2 describes the diagrammatic representation of our proposed system. This architecture has 4 Road Side Units, 1 DMV sector.

4.2 Malicious Node Identification Routing Mechanism

Routing is defined as the process in which it selects best path for packet transmission from source to destination. Our proposed mechanism includes a modified AODV routing algorithm that which provide safe transmission of packets in the network. There are three different scenarios for identifying attacker nodes such as Sybil attack, Wormhole Attack and Black hole attack in the network.

4.2.1 Identification of Sybil Attack

In our proposed mechanism sybil attack is identified using both trusted authorities and untrusted authorities. Initially sender sends RREQ packets to their neighbor nodes. Here RSU observes RSSI (Received Signal Strength Indicator) values of all nodes that get the packets of sender node and we get the reply packets with MAC address from neighbor nodes. After observing the RSSI values of nodes in the network, a signalprint based sybil classification method [6] is used for classifying the true RSSI and false RSSI. At the end of classification, we move false RSSI values to the Department of Motor Vehicle Sector, for the accurate identification of sybil attacker.

DMV sector consists of all information about the specific vehicle on the corresponding area. The false RSSI values are verified in the DMV sector based on its MAC address and Logical address (IP address). If a node has same MAC address with different IP address then it is considered as a sybil attacker node else it is a normal node in the network. After finding the sybil we generate the alarm signal in the network.

4.2.2 Identification of Wormhole Attack

In our routing algorithm we need to identify wormhole attackers by detecting the link lifetime of two nodes, route reliability and route redundancy from source to destination. Here we identify the link lifetime because nodes in the VANET moves at high speed their communication gets broken if a nodes moves out of coverage. Initially sender nodes discover routes to find destination by broadcasting RREQ packets to its 1-hop neighbors. If a destination is identified, it sends RREP to sender node on specific path based on first received RREQ packet. Here when source node broadcasts packet, it starts to calculate Round Trip Time (RTT). Destination node sends RREP to Sender node within some given time. RTT is calculated for every possible route from source to destination.

After getting possible routes, we need to calculate link lifetime [17] between two nodes,

$$LLT_i = min(LC_i, N_{i-1}, N_i) \tag{1}$$

Here LLT_i represents the lifetime of link, LC_i represents the connection time between two connected nodes they are N_{i-1} and N_i. Then we list the possible routes with same *RTT*, and some relay nodes that broadcasts *RREQ* at 1-hop neighbors. At this time we allow route aggregation, this allows to all nodes for participating in the network.

Source starts to count *RTT* is calculated for each route when *RREQ* is send through next 1-hop members. *RREP* is received to source at specific time; source stamps calculated *RTT* of its routes or route. Finally all routes with link lifetime are listed with number of hops and *RTT.*

4.2.3 Identification of Black Hole Attack

In our proposed mechanism, we improve the AODV routing for identifying black hole attacks and provide reliable route for secure packet transmission. Black hole attack is identified by initial request message which is send by source node to the neighbor nodes for finding destination node. After identification of destination node, it send reply message to the source node.

```
=====================================
Pseudo Code: Malicious Node Identification Routing
Mechanism
=====================================
Input: RREQ from S, Route= {a … z}, HC [route] = 0,
Timer [route] = 0
Output: Identifying Black hole attack, Sybil Attack and
Wormhole attack
Begin
Step 1: S → RREQ to $I_N$
Step 2: S ← RREP from $I_N$

////// identifying Wormhole attack
        If ($1^{st}$ RREP → S)
                HC [route] = HC [route] + 1
                Timer [route] = start (timer)
                Route = Route +1
        End if
        For (route)
        If (RREP != D)
                RREQ to 1-hop $I_N$
                HC [route] = HC [route] + 1
                If (next HC and route are same)
                  Agg.add = Aggregate (route)
                  Next.route [route] = route + Agg.add
                  Calculate LLT using equation [1]
                End-if
        End-if
        If (RREP == D)
                S = RREP.D + HC [route] + route
                Stop timer [route], S ← RREP
                S waits for 2 * 2 * $RREP_1$
                S creates list for routes
        End If
Step 3: Choose $B_{path}$
Step 4: Call Step 5

////// identifying Black hole attack

Step 5: if (LLT is high)
        Check $B_{path}$ using R
       End-if
Step 6: if ($B_{path}$ is error)
        Goto 3
      Else
        Transmit M, S → D
        Call Step 8
Step 7: End If

////// identifying Sybil attack

Step 8: $I_N$ observes RSSI of RREQ
Step 9: Each $I_N$ creates SET
Step 10: Classify SET
Step 11: SET→ RSU
Step 12: RSU forwards DMV
Step 13: if (RSSI == true)
          $I_N$ joins
        Else
          Create A1
        End-if
End
=====================================
```

Figure 3. Malicious Node Identification Routing Mechanism

When receiving all RREP to the source node, it notifies the behavior of nodes to identify black hole attacks in the network. Based on rules in [5], we can identify black hole attacker in route. Here we calculate the link lifetime (equation 1) for every path from source to destination.

Finally a path is selected without black hole attacker and higher lifetime of route between source and destination. Then packet is transmission takes place.

Our Malicious Node Identification Routing mechanism indentifies three types of attacks for secure transmission of packets. Figure 3 describes the pseudo code for our proposed routing mechanism.

The above algorithm describes the routing mechanism of our proposed work, here S is the source node, D is the destination node, RREQ is the route request and RREP is the route reply, IN is the intermediate nodes, SET is the subset list of nodes, HC is the hop count, timer is used for RTT, RSSI (Received Signal Strength Indicator) for every nodes, AGG is the aggregation routes, LLT is the link lifetime of routes, Bpath is the best path among various routes from source to destination; R is the rules from [5] for identifying black hole attacks, Route is the set of path from source to destination, M is the message that is to be transmitted. Figure 4 displays the pictorial representation of Routing mechanism.

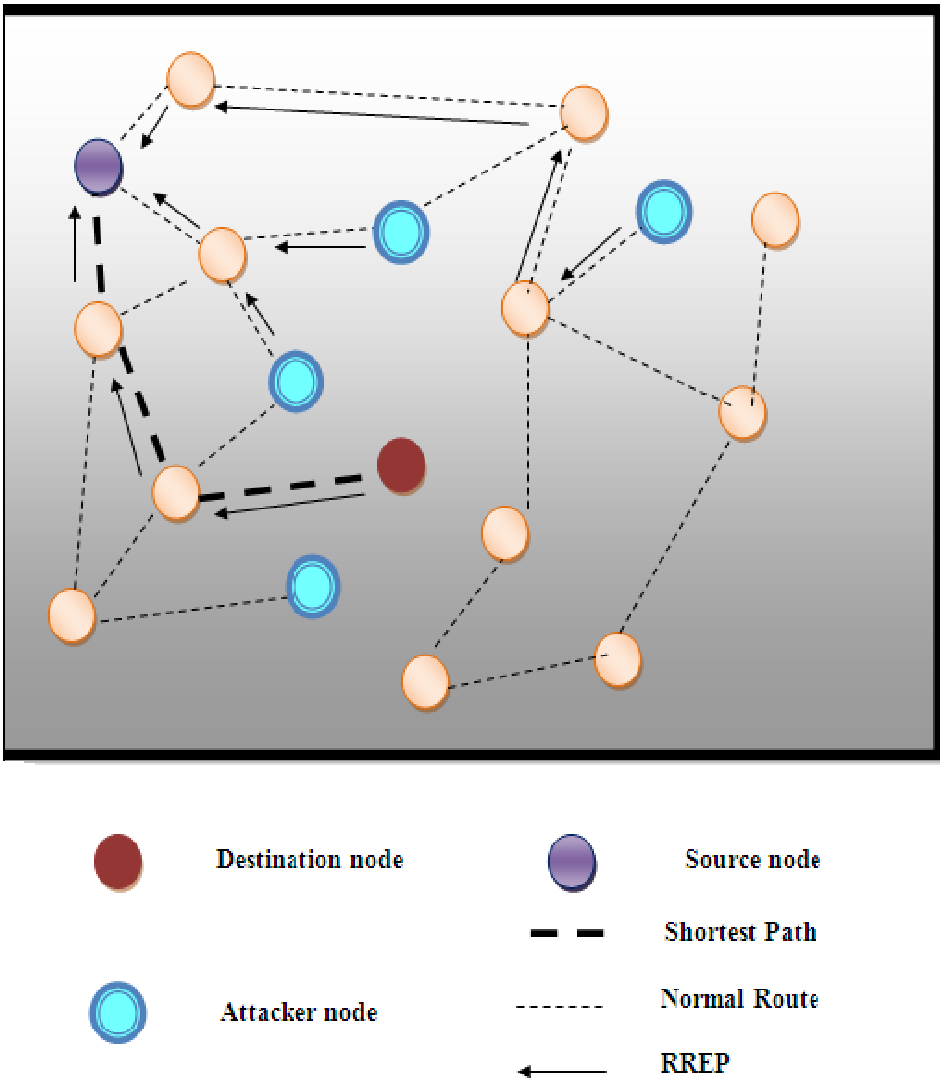


Figure 4. Routing Mechanism

4.3 Protection Mechanism

Security plays a major role in an ad-hoc network to provide safe and secure communication. The security goals are authentication, integrity, robustness, confidentiality, non-reputation and anonymity. In protection mechanism, we focus on securing the VANETs from several critical attacks such as Black hole attack, Wormhole attack and Sybil attacks. To provide data confidentiality, encryption is only used for allowing honest users for reading and processing the data which are transmitted. Asymmetric algorithms such as Elliptical Curve Cryptographic algorithm are mostly preferred for packet transmission in the network; it generates private key and public key, which has higher security. According to our proposed system, DMV sector generates asymmetric keys for vehicles in the networks that distribute them when keys are generated. The DMV sector does a key management process which avoids the attacks in the network, by having the key table. This Key table contains RSS values, MAC address and logical address and their private keys of every vehicle. During Vehicle-to-Vehicle Communication and Vehicle-to-Infrastructure in the network, keys are verified.

If any vehicle enters in a VANET, it must register in a DMV sector and it gets an asymmetric key for secure communication in the network. DMV sector maintains a key management process, by recollecting all keys from every vehicle in the network and updates the new key for every vehicle at every slot K. In our routing mechanism, any vehicle suspect any malicious node in the

```
==================================
Pseudo code: Protection Mechanism
==================================
Input: Message (M)
Output: Providing secure communication

Begin
    Step 1: $V_i \rightarrow$ DMV
    Step 2: $K_i$ Generation
    Step 3: Distribute $K_i$ to all $V_i$
    Step 4: $V_1 \rightarrow$ M
    Step 5: M $\rightarrow$(Req) $V_2$
    Step 6: $V_2 \rightarrow$(Req) RSU
    Step 7: RSU $\rightarrow$(Req) DMV
    Step 8: DMV $\rightarrow$ (Rep) RSU
    Step 9: RSU $\rightarrow$ (Rep) $V_2$
    Step 10: if (Rep is Valid)
                    $V_2 \rightarrow$(Rep) $V_1$
             Else
                    $V_2$ cancels it Rep
    Step 11: RSU generates A to $V_i$ and $RSU_i$

    ////// Revocation process

    Step 12: DMV recollects $K_i$
    Step 13: if (key table)
                  Generate new $K_i$
                  Update $K_i$
                  Distribute $K_i$
        Else
                  Cancel authentication to $V_i$
                  A $\rightarrow$ $RSU_i$
                  Generate new $K_i$
                  Update $K_i$
                  Distribute $K_i$
End
==================================
```

Figure 5. Protection Mechanism

network, it moves a warning message to other vehicles and again an warning signal is generated by the RSU to other RSUs. Here revocation process takes place, any malicious user have valid key, then DMV sector cancels the valid key and announces to RSU. Then every vehicle in the network cancels their connection to the specific vehicle.

If any vehicle suspects the malicious behavior of node (i.e. malicious behaving node (Sender node) sends message to another vehicle (Receiver Node)), then it sends a message to RSU followed by DMV sector. DMV sector check the keys of the malicious node, if it is valid node, it sends a message to RSU and RSU forwards message to receiver node. Then it can continue it communication else an invalid message is received to the receiver node.

Figure 5 describes the pseudo code for protection mechanism. K_i is the private keys for every vehicle, V_i represents the vehicles, M is the Message from sender vehicle (V_1), Req represents the request message from V_1 to RSU and to DMV and Rep is the reply message from DMV to RSU and to V_1. A is the alarm signal that generated when malicious user communicates with other vehicle.

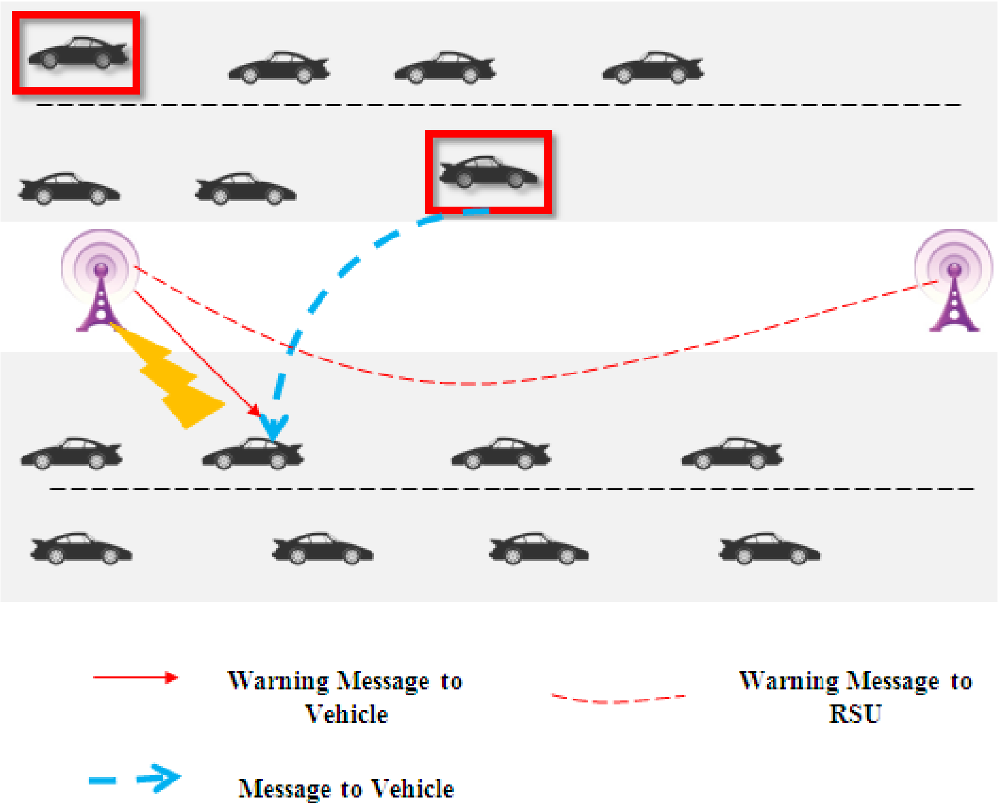


Figure 6. Protection Mechanism

Figure 6 describes the protection mechanism in our paper. In this diagram, a malicious node sends a message to normal node. Here normal node needs to check the sender is normal node or malicious node, so it sends a message to RSU, RSU sends a message by checking in the DMV Sector whether it is a valid node or invalid node. If normal node receives valid message then it continues its communication else it cancels its communication with malicious node. Then RSU sends a warning signal to all vehicles and to all RSU in the network.

5. Performance Evaluation

In this section, to know the performance of our proposed mechanism, we need compare our mechanism with existing system. Our proposed mechanism introduces an extended AODV routing named Malicious Node Identification routing which identifies malicious behaving nodes such as Sybil attackers, Wormhole attackers and Black hole attackers in the network. For comparison, we compare some of the parameters such as End-to-End Delay, Packet Delivery Ratio, Packet loss, Misdetection rate, Detection rate and Throughput. Here the existing system such as AODV protocol [5], ISDNAODV [5] for removing black hole attacks in the network; AODV++ [19] for removing the wormhole attacks in the network; SCID [20] for removing the sybil attack in the network. We improved and integrated all above existing system in a single routing mechanism that identifies Black hole attacks, Sybil attacks and Wormhole attacks in VANET. We explain existing systems working procedure in briefly are as follows:

- **AODV Protocol**

Ad-hoc On-demand Distance Vector (AODV) Protocol is a reactive routing protocol which is used for an on-demand dynamic routing process. In this routing source node doesn t have any direct route to the destination node. Due to these reasons, source node initiates the route discovery process by broadcasting a route request (RREQ) packet to it s the intermediate nodes, when intermediate nodes receives RREQ packets that has specific route to destination node then it generates the route reply (RREP) packet to the source node. Here RREP is generated when it is itself a destination node. The advantage of this AODV protocol is that it minimizes the Routing table.

- **ISDNAODV Protocol**

ISDNAODV is an improvement of AODV protocol which allows sender node to notify the behavior of intermediate nodes while transmitting the RREQ packets in the network. Here some rules are introduced for monitoring the behavior of intermediate nodes while transmitting RREQ packet. This results in better performance for identifying the black hole attacks in the network.

- **AODV++ Protocol**

This protocol is also a improvement to the AODV protocol that detects and avoids wormhole attacks in the network. Here geographical leashes are used which allows to know the geographical own location and it must have the synchronized clocks. Then it is followed by a HEAP for the safety of the control packets and traffic packets. This helps in packet authentication schemes in ad-hoc network and also it is used by modifying the HMAC based encryption algorithms.

- **SCID Protocol**

This protocol is used for detecting the sybil attacks based on the improvement of the AODV routing protocol named Secondary ID (SCID). This protocol introduces a new field named SCID. This is maintained in order to identify the unique node. In this extended AODV routing protocol, every packet format has the sequence number with SCID. When any malicious node has the sequence number of other node, it can be identified by the unique sequence number.

5.1 Simulation Results

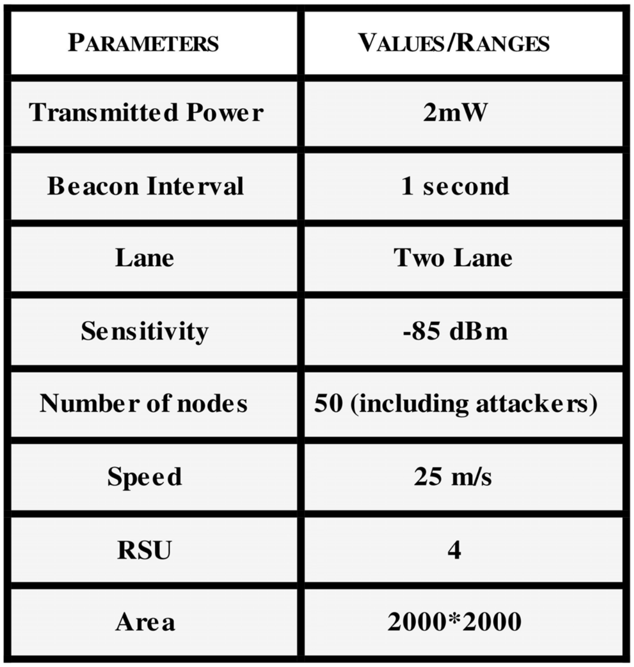
We perform our proposed experiment on OMNeT++ simulation framework. This simulation tools provide us to work with new algorithms and mechanisms. We consider some of the parameters on OMNeT++ Simulation which are shown in the table 1.

In our proposed experiment, the parameters are as follows, our simulation area is about 2000 * 2000, and there we use 50 nodes which include attackers (Sybil, Black hole and Wormhole). Here all nodes are mobile in nature and it moves in a speed of 25 m/s. In our simulation process, we include a pre-simulation step with SUMO setup that includes road map extraction, creating road network; it can allows conversion of routes and traffic flows; it can also creates obstacles on the road map. In the coding part, we C++ coding for the components. Here we use 4 Road Side Units (RSU) separately.

5.2 Performance Metrics

We consider some of the metrics in our proposed system, which proves our results efficiently on OMNeT++ Simulation that between existing system and proposed mechanism. Here we list the metrics such as,

- End-to-End Delay
- Energy
- Packet delivery ratio
- Throughput



Parameters	Values/Ranges
Transmitted Power	2mW
Beacon Interval	1 second
Lane	Two Lane
Sensitivity	-85 dBm
Number of nodes	50 (including attackers)
Speed	25 m/s
RSU	4
Area	2000*2000

Table 1. Simulation parameters

- Detection rate
- Misdetection rate

These parameters are explained in sub-section and they are graphically represented in the next section.

5.2.1 End-to-End Delay

End-to-End Delay plays a major role in routing process that specifies average time taken for a packet for transmission across a network from source to destination. The delay occurs during the route discovery process.

The End-to-End Delay is calculated by,

$$\text{End-to-End Delay} = \frac{\sum(\mathit{Arrive\ time} - \mathit{Send\ time})}{\sum(\mathit{Number\ of\ Connections})}$$

5.2.2 Packet Delivery Ratio

Packet Delivery Ratio (PDR) is defined as the ratio of number of delivered packets from source node to destination node. This describes the level of delivered data to destination.

$$\text{Packet Delivery Ratio} = \frac{\sum(\mathit{Number\ of\ packet\ receive})}{\sum(\mathit{Number\ of\ packet\ send})}$$

5.2.3 Throughput

Throughput is defined as the rate at which processing of something. Throughput in network is a measure of how many number of units of information is processed by a system at a given time i.e. bits per second (bps). It is degraded by various factors such as behavior of end-user, physical medium and available processing of power.

5.2.4 Energy

In our proposed mechanism, we use link lifetime that identifies the lifetime of links for efficient packet transmission. Here if the link of nodes breaks it results in packet loss and if the energy consumption is low then our network gains higher lifetime.

5.2.5 Misdetection Rate

Misdetection rate is defined as the percentage of honest nodes incorrectly denoted and classified as malicious node. Here Specificity is denoted as number of honest nodes which are correctly identified. Here the misdetection rate is calculated as,

$$\text{Specificity} = \frac{Number\ of\ Honest\ Nodes\ identified\ Correctly}{Total\ Number\ of\ Honest\ Nodes}$$

Misdetection rate = 1 – Specificity.

5.2.6 Detection Rate

Detection rate is defined as the percentage of malicious node detected and its classification. Here the detection rate is calculated as,

$$\text{Detection Rate} = \frac{Number\ of\ Malicious\ Nodes\ Detected\ Correctly}{Total\ Number\ of\ Malicious\ Nodes}$$

5.3 Comparative Analysis

In this section, we compare our proposed mechanism with other existing algorithms and mechanisms while concentrating on the performance metrics.

5.3.1 Energy Consumption

Our proposed routing mechanism consumes less energy. Here initially we select route with higher link lifetime for packet transmission. Figure 7 describes the comparison of proposed Malicious Node Identification Routing mechanism with existing AODV routing. In graphical representation x-axis describes the speed of nodes in terms of m/s with the attackers and y-axis describes the energy consumed in joules.

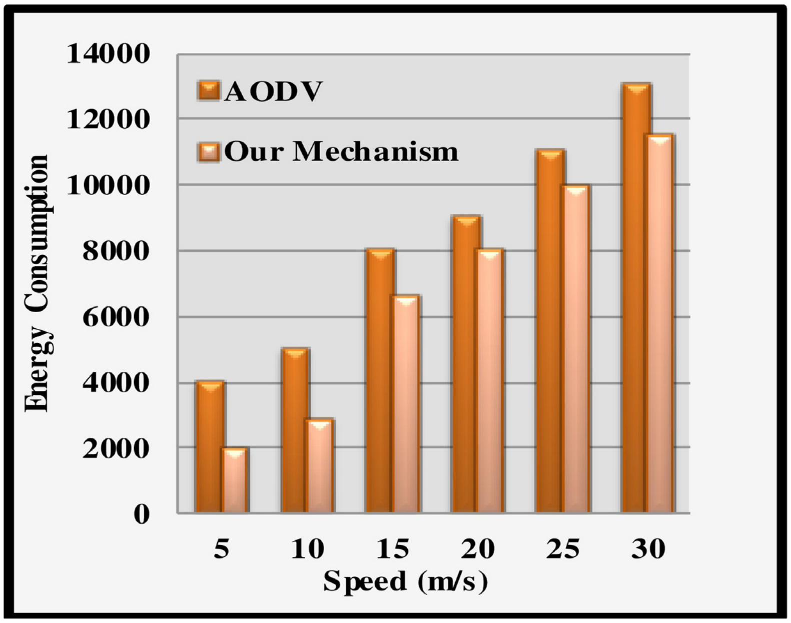


Figure 7. Energy Consumption

5.3.2 End-to-End Delay

Fig 8 displays the graphical representation of End-to-End delay performance in our Malicious Node Identification Routing mechanism. In this graph, x-axis represents the number of nodes in the network and y-axis represents the end-to-end delay in milliseconds. Our proposed routing mechanism is compared with AODV++ routing for wormhole attack, ISDNAODV routing for black hole attack and MAODV routing for sybil attack, to display the results with has better performance.

5.3.3 Throughput

Figure 9 describes the graphical representation of Throughput performance in our Malicious Node Identification Routing mechanism. In the graph x-axis represents the number of nodes and y-axis represents the number of bits in MBPS. Our proposed routing mechanism is compared with AODV++ routing for wormhole attack, ISDNAODV routing for black hole attack and MAODV routing for sybil attack, to display the results with has better performance.

5.3.4 Packet Delivery Ratio

Figure 10 displays the graphical representation of Packet Delivery Ratio (PDR) performance in our Malicious Node Identification Routing mechanism. In the graph x-axis represents the number of nodes and y-axis represents the percentage of PDR. To achieve best performance in PDR, Our proposed routing mechanism is compared with AODV++ routing for wormhole attack, ISDNAODV routing for black hole attack and MAODV routing for sybil attack, that displays the results with has better performance.

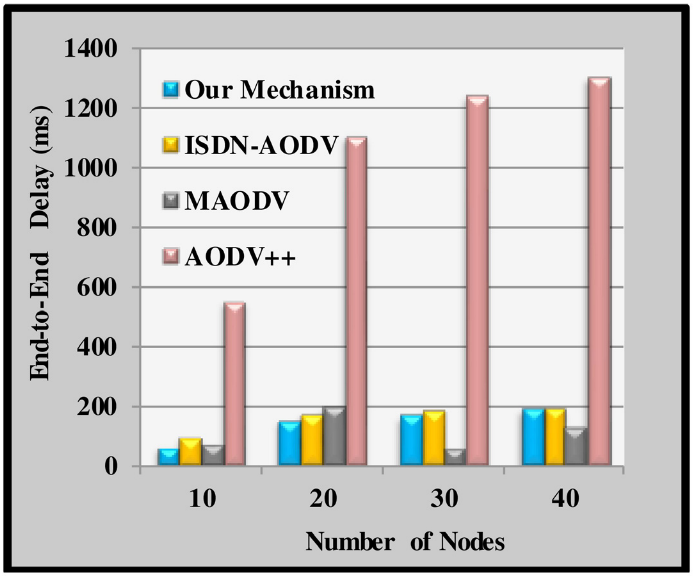


Figure 8. Performance of End-to-End Delay

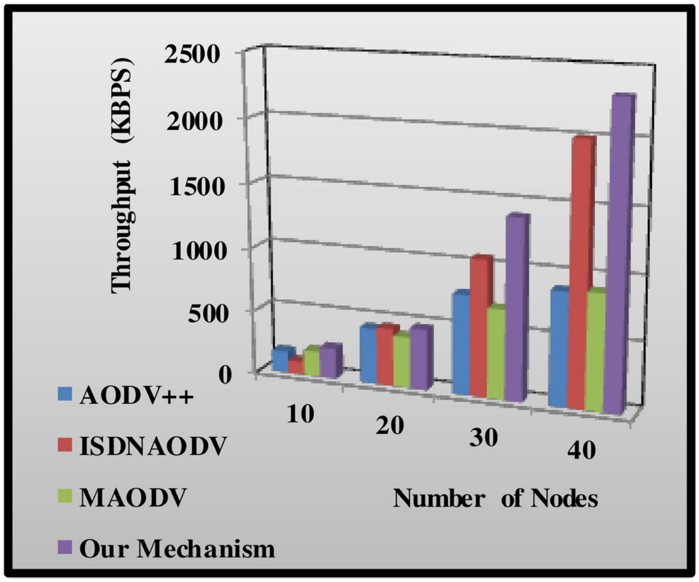


Figure 9. Performance of Throughput

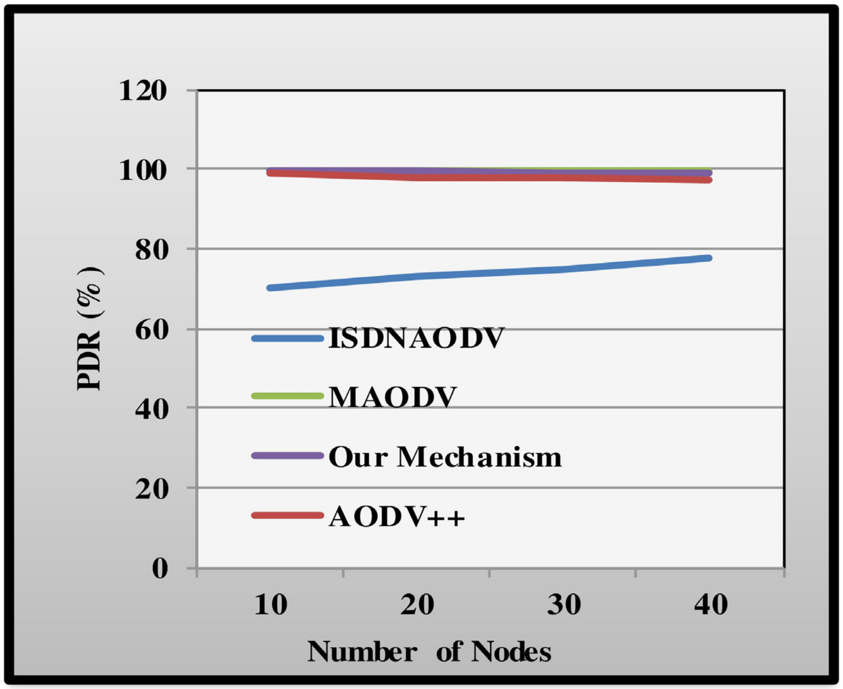


Figure 10. Performance of Packet Delivery Ratio

5.3.5 Detection Rate

Figure 11 displays the graphical representation of detection rate of malicious nodes in the network. To know the performance of in terms of detection rate of Black hole attackers, Wormhole attacker and Sybil attackers, our proposed routing algorithm is compared with normal AODV routing.

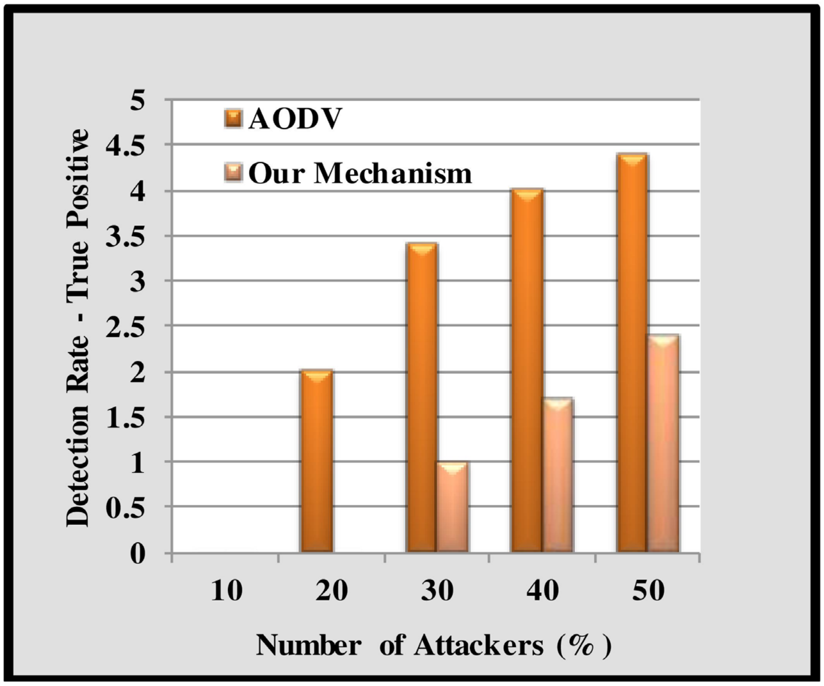


Figure 11. Performance of Detection rate

5.3.6 Misdetection Rate

Figure 12 displays the graphical representation of Misdetection rate of honest nodes in the network. To know the performance of in terms of misdetection rate, our proposed routing algorithm is compared with normal AODV routing, which provides best results.

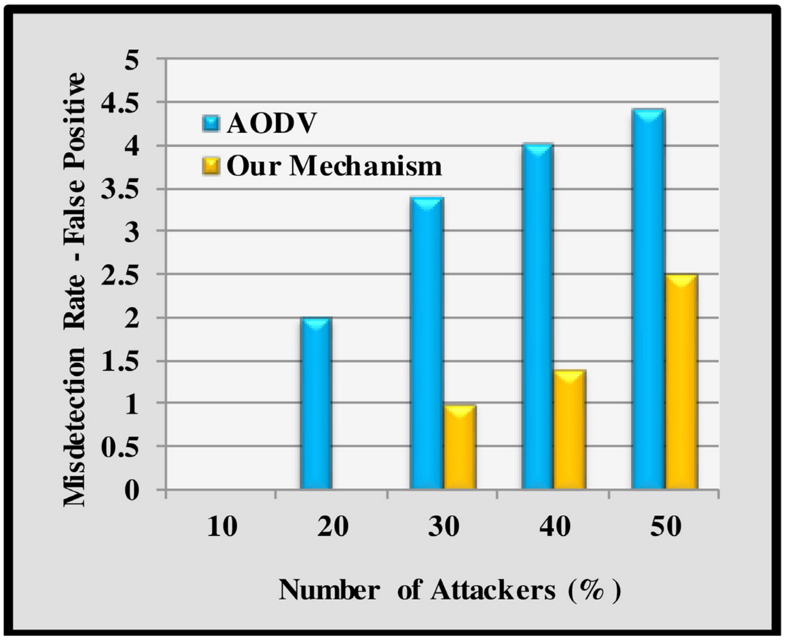


Figure 12. Performance of Misdetection rate

6. Conclusion

VANET is an emerging ad-hoc network which provides efficient communication between two vehicles. In recent years many researchers noticed that, it has capacity to improve higher communication and safety measures, and they pointed out that VANET facing many problems mainly in terms of security. There are more number of vulnerable security threads arising in the VANET, such as Sybil attack, Wormhole attack and Black hole attack. To detect these kinds of attacks we proposed a *Malicious Node Identification Routing Mechanism* which includes AODV protocol. This Routing mechanism includes three different scenarios for identifies these attacks in the network. For prevent the networks from various attacks, we introduce a *Protection Mechanism* that uses an asymmetric algorithm and it allows a key management based on key revocation process in the network.

Our proposed mechanism is implemented using OMNeT++ simulation tool that uses SUMO Setup for providing effective results. Our routing mechanism provides best results in terms of End-to-End Delay, Packet Delivery ratio (PDR), Throughput, etc. In our future work, we improve our routing process that detect and protect VANET from more vulnerable attacks like gray hole attack, Brute force attack, sink hole attack etc.

References

[1] Balmahoon, R., Peplow, R. Vehicular Ad-Hoc Networks: An Introduction to Privacy.

[2] TRIKI, Bayrem., REKHIS, Slim., CHAMMEM, Mohamed., BOUDRIGA, Noureddine. (2013). A Privacy Preserving Solution for the Protection Against Sybil Attacks in Vehicular Ad Hoc Networks, IEEE.

[3] RAWAT, AJAY., SHARMA, SANTOSH., SUSHIL, RAMA. (2012). VANET: Security Attacks and Its Possible Solutions, *Journal of Information and Operations Management*, 3 (1) 301-304, Available online at http://www.bioinfo.in/contents.php?id=55

[4] Shin, Soo-Young., Eddy Hartono Halim, (2012). Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation, IEEE.

[5] Shahabi, Sina., Ghazvini, Mahdieh., Bakhtiarian, Mehdi. (2015). A modified algorithm to improve security and performance of AODV protocol against black hole attack, Springer Science+Business Media New York.

[6] Liu, Yue., David, R., Bild, Robert, P.. Dick, Z. Morley Mao, and Dan S. Wallach (2015). The Mason Test: A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities, *IEEE Transactions on Mobile Computing*, 1536-1233. IEEE

[7] Kelatkar, Vrushali., Dere, Pravin (2015). Lightweight Sybil Attack DetectionTechnique, An Overview, *IJCSMC,* 4 (11), (November), 173 – 180.

[8] Pareek, Anamika., Sharm, Mayank. (2015). Detection and Prevention of Sybil Attack in MANET using MAC Address, *International Journal of Computer Applications* 122 (21) (July).

[9] Rabieh, Khaled., Mohamed, M. E. A. Mahmoud, Terry, N., Guo, Younis, Mohamed. (2015). Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs, IEEE ICC 2015 - *Communication and Information Systems Security Symposium*

[10] Zhou, Tong., Romit Roy Choudhury, Ning, Peng., Chakrabarty, Krishnendu. (2011). P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks, *IEEE Journal on Selected areas in Communications*, 29 (3) (March).

[11] Mekliche, Kenza., Moussaoui, Samira. (2013). *L-P2DSA: Location-based Privacy-Preserving Detection of Sybil Attacks,*

[12] Nouri, Mahdi., Somayeh Abazari Aghdam, Sajjad Abazari Aghdam, Collaborative Techniques for Detecting Wormhole Attack in MANETs.

[13] Sorathiya, Darshana., Rathod, Haresh. (2015). Algorithm to Detect and Recover Wormhole Attack in MANETs, *International Journal of Computer Applications* 124 (14).

[14] Mershad, Khaleel., Artail, Hassan. A Framework for Secure and Efficient Data Acquisition in Vehicular Ad hoc Networks, *IEEE TRANSACTIONS ON* .

[15] Khawla Naji Shnaikat, Ayman Ahmed AlQudah. (2014). KEY MANAGEMENT TECHNIQUES IN WIRELESS SENSOR NETWORKS, *International Journal of Network Security & Its Applications* (IJNSA) 6 (6).

[16] Balasubramani, S., Rani, S. K., Suja Rajeswari, K. Review on Security Attacks and Mechanism in VANET and MANET.

[17] Priyadharshini, C., Tamilarasi, M., ThamaraiRubini, K. (2012). Predicting Route Lifetime for Maximizing Network Lifetime in MANET, *ACS-International Journal in Computational Intelligence*, 3 (1) March.

[18] Hwang, Ren-Junn., Hsiao, Yu-Kai., Liu, Yen-Fu. (2011). Secure Communication Scheme of VANET with Privacy Preserving, *In*: IEEE 17th International Conference on Parallel and Distributed Systems.

[19] Safi, Seyed Mohammad., Movaghar, Ali., Mohammadizadeh, Misagh(2009). A Novel Approach for Avoiding Wormhole Attacks in VANET.

[20] Navneet, Gill, Rakesh. (2013). Sybil Attack Detection and Prevention Using AODV in VANET, *IJCSMS International Journal of Computer Science & Management Studies*, 13 (7) (September)