International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2018/49390 Volume 5, Issue 2, March – April (2018)

RESEARCH ARTICLE

MNP: Malicious Node Prevention in Vehicular Ad Hoc Networks

Syed Rameem Zahra
School of Computer Science & Engineering, SMVD University, J&K, India
rameemzahra@gmail.com

Published online: 26 April 2018

Abstract – Today, traffic security has become an obligation rather than a necessity. Hence to secure the traffic, provide comfort to the driver and the passengers, ensure safety of the pedestrians, infrastructure as well as the one's sitting inside the cars, Intelligent Transport System (ITS) was created. The base of ITS is formed by a class of networks called as VANET. The VANETs make communication between vehicles and vehicle to infrastructure possible. They vary from other Ad-hoc network because of their rare characteristics. VANETs are the networks which lack centralized control and infrastructure, in which the nodes are highly mobile, topology is extremely dynamic and the links are volatile. Consequently, VANET security is threatened- the network is vulnerable to number of mischief. The easiest of all the attacks on VANETs is that on the availability – the Black-hole attack. This attack is carried out by the malicious nodes which can even be the authentic users of the network, implying that the security procedures involving encryption and authentication will not help. Therefore, to secure the VANETs against this common type of attack, we have proposed an algorithm MNP- Malicious Node Prevention. MNP improves DMV (Detection of Malicious Vehicle algorithm) as well as DMN (Detection of Malicious Nodes algorithm) in a way that MNP simply prevents the malicious nodes from participating in the packet forwarding while as both DMV & DMN first identify the malicious nodes and then remove them. This way, DMV as well as DMN cause the loss of many data packets which may be important. Hence MNP greatly improves the performance of the network when under malicious attack.

Index Terms – ITS, VANET, Black hole attack, MNP, DMV, DMN.

1. INTRODUCTION

VANETs are the class of networks which can be thought of as the children of other class of networks called MANETs. In VANETs, the nodes are the moving cars which have become intelligent systems, and thus often called smart vehicle. These smart vehicles are also incorporated with radio communication interfaces and these vehicles communicate with each other using wireless local area network (WLAN) technologies. In a VANET, there are 2 types of entities: on board units (OBU's) and road side units (RSU's). OBU's are mounted onto the vehicles and are radio devices while as RSU's constitute the common infrastructure. For the purpose of connecting these smart vehicles to RSU's, OBU's make use of dedicated short range communication. One more important feature of VANETs is that the vehicles which act as the communicating nodes remain uninformed about each other's presence [1] and that simultaneously VANETs are the self-organizing networks.

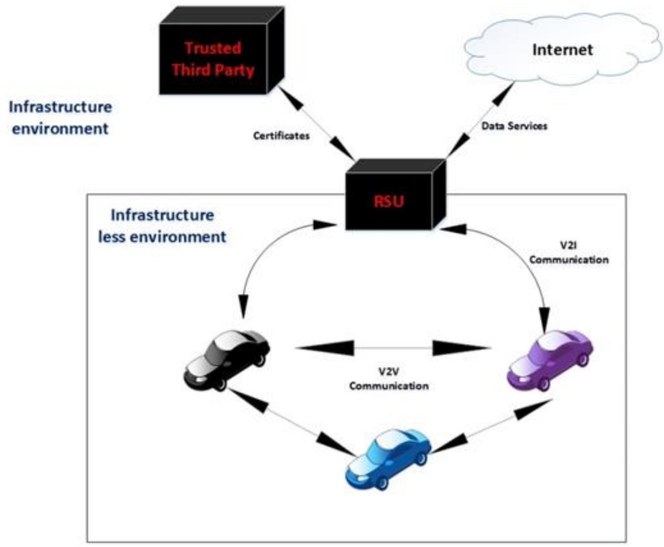

Figure 1 VANET Components

From the figure – 1 it is clear that in VANET we can have either vehicle to vehicle communication or vehicle to infrastructure communication [2].

1.1. Vehicle to vehicle communication (V2V)

When the cars communicate with each other in infrastructure-less mode (also called Ad hoc mode) [3] it is called vehicle to vehicle communication (V2V). In this category, the vehicles exchange information such as traffic conditions, road accidents etc. When a smart car makes use of vehicle to vehicle communication in a situation of danger, it sends useful messages/warnings to other vehicles recommending them not to come in that region. V2V communication can be of 2 types via: single-hop or multi-hop. The type of V2V communication which occurs will depend on the relative location of the sender-receiver pair i.e. a car will send safety messages/warnings using single hop V2V communication while as multi-hop V2V communication will be employed to broadcast the other type of messages i.e. the non-safety messages.

1.2. Vehicle to infrastructure communication (V2I)

This type of communication is used to broadcast information between RSU's and vehicles as well as for the transfer of important information like safety measures to be taken by the drivers or the passengers or the condition of road at the moment [3]. In this type of communication, the vehicles give information to RSU's. The RSU's are connected to the public networks such as the Internet, so they put the information on the Internet. The vehicle – RSU links are more secure, require more bandwidth than the former V2V type of communication. The V2I communication therefore converts the infrastructure elements into 'intelligent infrastructure and elements' by the unification of special algorithms which detect the dangerous or risky situations prior to their occurrence by deciphering the information or data which they receive. This results in the generation of specific warnings which are given to the drivers so that they take the safety measures. All these warnings help in avoiding the clashes between the vehicles in addition to providing mobility, safety and environment related advantages.

Also, the main components of VANETs are the vehicles (that have OBU's fitted inside) and the RSU's. In ITS, the nodes (e.g. a smart vehicle) necessarily need to have the following components via: Sensors, Cameras, On board computers, GPS (Global Positioning System), Event data recorders, Omni directional antennas [4].

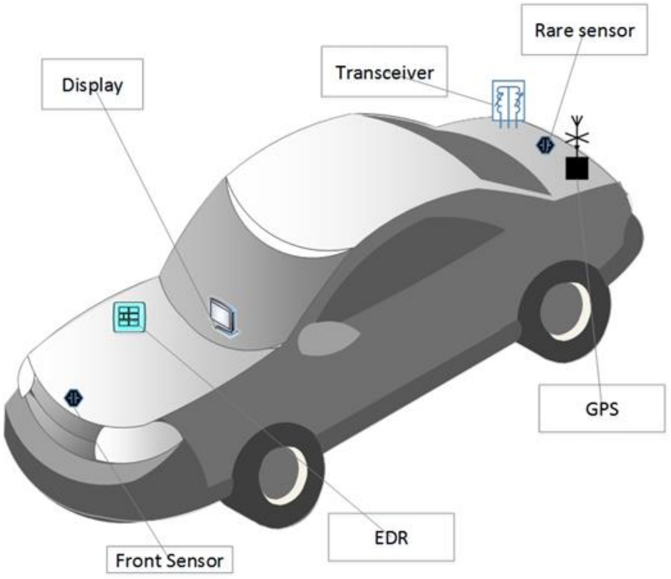

Figure 2 Smart Vehicle

The sensors can be of various types (Radars – both front and reverse). The function of these sensors is to receive the important information which otherwise is possible for the driver to obtain. Also, they provide information regarding the various obstacles which may be present there in the environment.

The smart vehicle is also studded with GPS, which is extremely helpful in locating the vehicle and in providing help in driving. If a vehicle for example, faces an accident, V2I communication takes place giving information about the accident location to RSU (vehicles make use of GPS present in its OBU). RSU puts the information on Internet and hence the help can be expected at the accident location within seconds. This will definitely be helpful in reducing the harm caused by accidents.

Event data recorder (a component of OBU – present inside the smart vehicle) is a computing device which works in the same way as the black box of an aircraft (contains every detail – a record of every spoken word, every activity performed).

The Omni-directional antennas are used for the easy access of wireless channels Moreover, the components which may be useful for security concerns as per [5] include: ELP (electronic license plate) or ECN (electronic chassis number). These 2 differ from the traditional license plates in that they give an electronic identity to the vehicle which can be used by the traffic police or any other authority [6]. Figure 2 shows the various elements which can be combined together in order to transform an ordinary vehicle into a smart vehicle.

The RSU acts as an interface (the connecting entity) between the infrastructure-less and infrastructure based parts.

2. STATE OF ART & LITERATURE

It is said that necessity is the mother of invention. There was a time when one would have to wait for some minutes of time to see a car on the road, but today there are traffic jams which long for hours (owing to large number of cars on roads), consequently the roads have become extremely dangerous- the number of accidents on roads are high and thus traffic security becomes an obligation rather than a necessity. For this reason, there was an invention of intelligent transport systems (ITS) [7] in which you automate the cars to a huge extent so that the probability of accidents is reduced substantially. The main motive of ITS is to give solutions to the gigantic problems like traffic congestion and safety of passengers. Also it has been proven time and again that the incorporation of information technology improves things hence, because of ITS the comfort of drivers as well as their driving condition (pertaining to the environment) are improving.

The quick implementation of any new technology depends upon how much standardized and normalized communications and information technologies are. When standardization is applied to VANETs, it affects almost all 7 layers of OSI (open system interconnection) model. Studies showed that often "Dedicated Short Range Communication (DSRC)" [8], "Wireless Access in Vehicular Environments (WAVE)" or "IEEE 802. 11p" [9] are used to define the entire stack of protocol for standards employed with VANETs. As per [10, 11] 75 MHz the DSRC band is split between 7 channels each of 10 MHz numbered as 178, 172, 174, 176, 180, 182, 184. Out of these channels 178 is used as the 'control channel' and the rest of the 6 are employed as the 'service channels'. WAVE [12] & 802.11p [13] has been added to the family of 802.11.

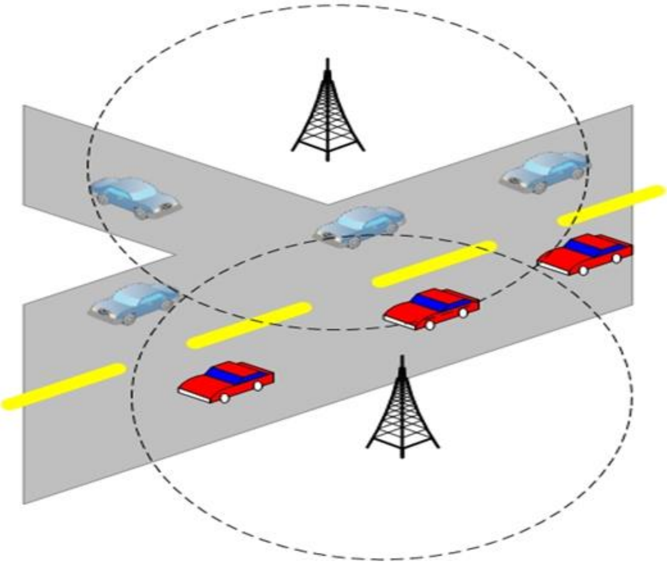

Figure 3 WLAN Architecture

VANET is a child class of a bigger class of networks called as MANETs. MANETs are ad hoc networks and hence take no centralized control, nodes depend on each other for the routing services. However, there are fundamental differences between MANETs and VANETs, which include: Higher Mobility [14], rapid Topology Change [15], limited Bandwidth, Smaller Network Diameter [16], large scale [17] etc.

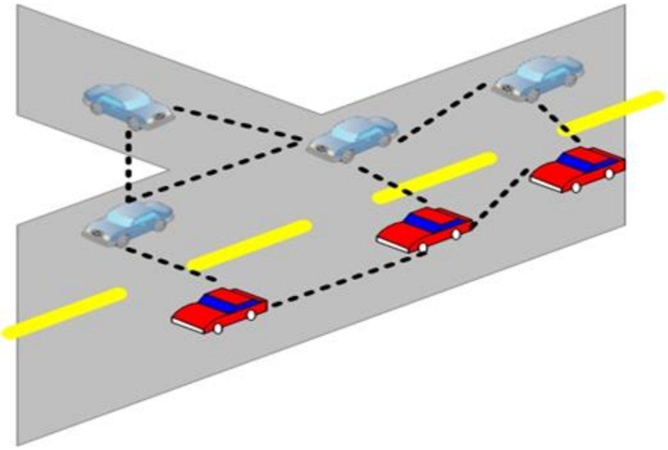

Figure 4 Ad Hoc Architecture

The characteristic feature of ad hoc networks is that they do not rely on any infrastructure for the purposes of communication and distribution of information. The same can be said about the vehicular ad hoc networks whose architecture can be classified along 3 directions [15], shown in figure – 3 to 5.

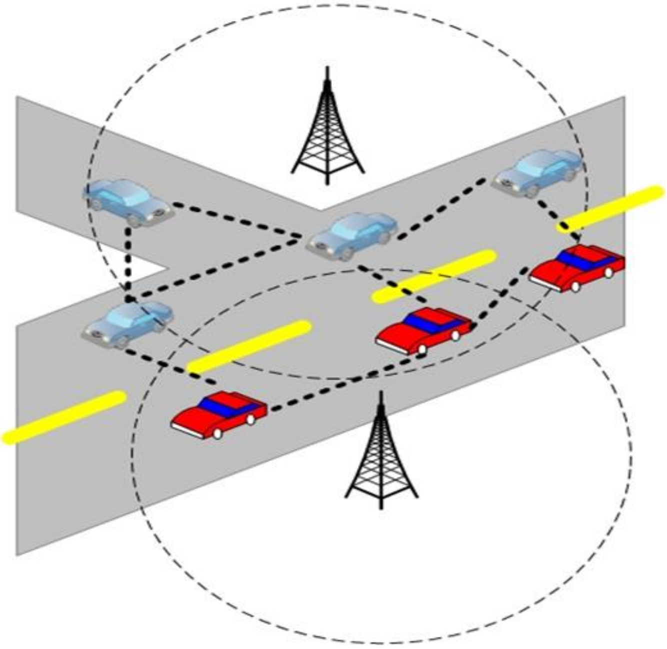

Figure 5 Hybrid Architecture

Three main applications of VANETs are: Road safety applications, applications for a driver assistance and passenger comfort applications. VANETs offer great applications from the viewpoint of comfort and safety which the other networks can't provide. The applications of VANETs range from safety to infotainment, from comfort to value added applications. While [26] classifies VANET applications into two categories: safety and infotainment, [27] categorized VANET applications into: Road safety applications, Traffic efficiency applications and value-added applications. [28] Makes the classification of VANET applications based on the equipment of VANET which is involved via: passenger, driver, infrastructure or vehicle.

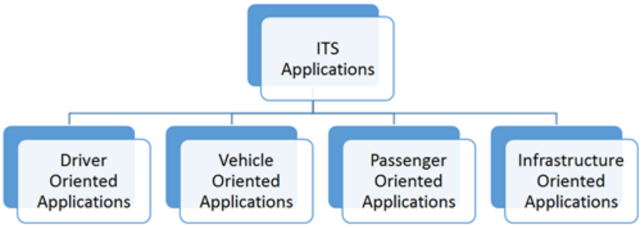
ITS Applications
Driver Oriented Applications
Vehicle Oriented Applications
Passenger Oriented Applications
Infrastructure Oriented Applications

Figure 6 ITS Applications

2.1. VANET Routing Protocols

There are routed protocols and routing protocols. The routed protocols like IP, IPX, and APPLE TALK are those with the help of which data can be routed. Routing protocols are those which are used only between the routers. Routing protocols are used by routers for building and maintaining routing tables. In

VANETs routing protocols are divided along six directions [18, 19].

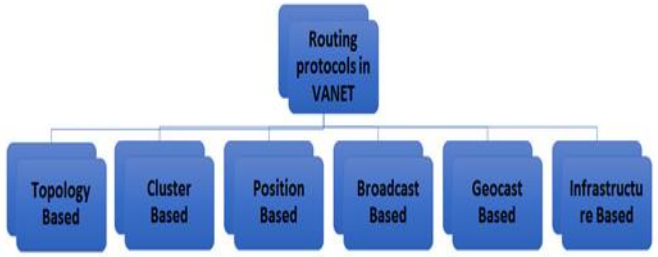

Figure 7 Routing protocols for VANET

Routing protocols based on Topology: These protocols find the routes and create routing tables before sending the packets. There is one disadvantage of the topology based routing protocols – they do not work well when the node count exceed hundred [19]. They are classified into three types: Proactive routing protocols: OLSR [20], FSR [18], DSDV [21]; Reactive routing protocols: DSR [20], AODV [22]; Hybrid routing protocols: ZRP, HARP [18]

Routing protocols based on position: These routing protocols make use of data made available by the positioning systems such as "Global Positioning System (GPS)" and hence there is no need to create routing tables between source and destination. So far "greedy Perimeter Stateless Routing (GPSR)" [23] is the most popular among all the position based routing protocols. It employs a combination of greedy routing (type of routing where in the data packets are always pushed to the hop which is graphically nearest to the destination) and face routing. VGPR, GPSR [23], MIBR [18] are included in this category.

Routing protocols based on clustering: A virtual infrastructure is created in the cluster-based routing by the vehicles which cluster together and hence provide scalability. Every cluster has a single cluster-head whose job is to manage functions relating to either the things within the cluster or between 2 clusters. CBLR, CBR, HCB, CBDRP [18] belong to this category of routing protocols.

Routing protocols based on broadcasting: This one is the most frequently used protocols in VANETs. In these protocols, a mechanism of flooding is used to broadcast the important messages such as those related to weather, emergency, traffic etc. to the entire network. The flooding works as follows: The message gets broadcasted from every node to every other node in the neighborhood excluding the one interface from which the node itself got the message (so as not to get trapped in an infinite loop). In this way, the entire network gets the message. EAEP, DV-CAST, SRB [18] are examples of broadcast routing protocols.

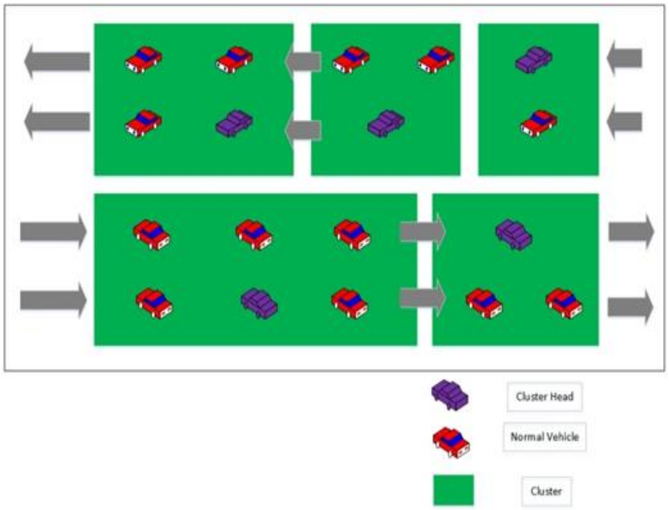

Figure 8 Cluster Based Routing

Routing protocols based on Geo-casting: The main aim here is to send the message from its originator to all the nodes which lie near the source of the message i.e. in the Zone of Relevance (ZOR) [24]. This is particularly useful in VANET applications for example, the vehicle in ITS finds itself caught in an accident, so it will like to send alarms/alerts only to other vehicles which are in its vicinity or the zone of relevance. Sending messages to all other nodes would only result in the creation of hue and cry atmosphere. ROVER, DTSG [25] belongs here.

Routing protocols based on infrastructure: Those routing protocols which are actually used for infrastructure based networks and are modified for use in VANETs. RAR, SADV [18] are examples of this type.

2.2. Challenges in VANET

Although VANETs have many advantages for drivers and passengers in particular and the humans, infrastructure on road in general, there are various challenges which require attention via: Time constraints, scale of the network, mobility of nodes and volatility [29].

2.2.1. Time constraints

In VANET, a node must be able to send a message/warning within a specific time interval because a warning that relates to safety has no meaning if it reaches the required party after a certain deadline e.g. if there is an emergency and the node is incapable of sending the warning immediately, then the consequences may be fatal. Again, the driver who gets the message must get enough time to respond. To come up with the time constraints, the authentication of the messages too has to be very fast, which is a challenge.

2.2.2. High node mobility

High node mobility gives rise to many challenges such as: Firstly, the traditional techniques of authentication cannot be applied to nodes- A handshake protocol cannot be applied to VANET nodes because there is a possibility of one-time communication between some nodes. Secondly, the cars in VANETs need schemes like that of mobility management in order to provide them with the easy and seamless communication facility in situations where these cars change their point of attachment with the network.

2.2.3. Volatility

It refers to the short interval time connections which are shared between the 2 vehicles in VANETs. The connectivity time period is short in VANET owing to their high mobility– sometimes the connected vehicles may even move in opposite directions. Let us consider a scenario where the range of transmission of each node is 250 meters, it means that if the spacing between the 2 vehicles is less than 250 meters, then there would be a link between them. Now, if these 2 cars are moving in opposite direction at the speed of 60 mph , then the link will last for a mere 10 second duration [15].

2.3. VANET Security Challenges

2.3.1. Attack on Availability

Availability is one of the most important security requirements of the network. It says that the network is functional. One of the easiest victims of attacks in VANETs is the availability because the medium of communication is air, the nodes are moving fast, the topology is extremely dynamic so it is not difficult for an attacker to put the availability on stake. For example, denial of service (DOS) attack brings the network down and hence makes VANET unavailable [4, 31].

2.3.2. Denial of Services attack (DOS)

The main motive of this attack is to render the VANET unavailable for use legitimate users. It can be carried out by the internal or external corrupt nodes [32]. The malicious nodes send a lot of control messages on the medium of communication, thereby rendering it unavailable to authorized users [33].

Since huge numbers of Control messages are sent, the RSU’s and OBU’s can’t handle them because of their memory and computational constraints, the result is that VANET is brought down. Important examples of DOS are black hole attack, jamming, greedy behavior etc.

2.3.3. Black hole attack

In Black Hole attack a malicious node always replies the source with the shortest route even if it doesn’t have any path to reach the destination. The source gets tempted to route all the data packets via the malicious node ‘M’. ‘M’ on receiving them either drops them or sends to other malicious nodes. That is, Data is sent on the path to destination which actually doesn't exist, thereby causing data loss [33].

2.3.4. Jamming attack:

This attack is launched at the physical level. It involves disruption of the communication channel by a signal transmission [36]. This attack results in lowering of signal-to-noise Ratio at the receiving end.

2.3.5. Greedy behavior attack

This type of attack puts into compromise the services provided by the MAC layer. A greedy node (malicious node in case of VANETs) just wants to get faster access to the medium and therefore doesn’t respect the method used for accessing the channel. This way it punishes honest nodes [37].

2.3.6. Attack on Authenticity and identification

Authentication is one of the most important criteria for security. One of the first precautions that are taken in right real life scenario is that of authentication so as to make sure that only recognized/legitimate nodes/people enter a gathering. In VANETs, the authentication of both inside and outside vehicles is a must [32]. Important examples of such attacks are Sybil attack and impersonation attack which are discussed below:

2.3.7. Sybil attack

First discussed in [38] Sybil attack is that in which the attacker node feigns numerous identities at one time. This attack has drastic consequences on VANET.

2.3.8. Impersonation attack

For the authentication purpose, every vehicle in VANET is given a unique identification (ID) to distinguish it from the rest of the vehicles. In this type of attack, the malicious entity uses the ID of the legitimate user and executes its job of putting the security at compromise and of damaging the network.

2.3.9. Attack on confidentiality

With confidentiality comes trust. This makes sure that only the authorized users get the information or data [33]. This is very important because there can be no compromise on the privacy of confidential data. If so happens then the security of every organization will be at stake. In VANETs, if there is no procedure/mechanism to ensure confidentiality then a every message that is exchanged is vulnerable to attacks [32].

At the same time, it should be noted that if in a VANET such messages are exchanged which are not sensitive or do not contain critical information then as per [7] confidentiality is not necessary. Eavesdropping attack is one of the most discussed attacks on confidentiality, it is defined below:

2.3.10. Eavesdropping attack

A form of passive attack in which the attacker silently listens to the communication medium extracting all the local data which might be useful for vehicle tracking activity. Eavesdropping does not affect the network, but highly puts the confidentiality in compromise.

2.3.11. Attack on integrity and data trust

Integrity of data is always important. Every source wants the receiver to receive what it actually sent and not the modified version of it. In VANETs, vehicle to vehicle (V2V) communications are more vulnerable to integrity attacks then vehicle to infrastructure communications (V2I). If sensors present in the vehicles are Manipulated then the integrity attacks get facilitated [34]. Masquerading is an example of such attack.

2.3.12. Masquerading attack

The attacker remains in hiding by covering its actual face by a mask (ID of authentic user) and then attacks the network by sending false messages while the others think that the messages are coming from an authentic source.

2.3.13. Attack on non-repudiation/accountability

In security of computer networks, non-repudiation refers to the inability of the sender or the receiver to deny that they actually sent or received the message in case when they did [35]. In other words, non-repudiation of source proves that particular source actually sent the message while as non-repudiation of destination proves that a particular destination actually received the message.

2.3.14. Loss of event track-ability

Here the attacker is the legitimate source or destination which after respectively sending or receiving the message denies of doing so. Such attacks have not been discussed in any document so far from the VANET perspective.

3. RELATED WORK

Intelligent transportation systems are best studied using vehicular Ad hoc networks (VANETs) [40]. [41] Was the first in literature to discuss the detection of malicious nodes/vehicles which depicted an abnormal behavior of the type that they dropped/duplicated data packets. Vehicles forming the VANET communicate using DSRC and the communication takes place either between vehicle and vehicle or between vehicle and infrastructure. VANETs also contain numerous trusted third-parties which are called as certification authorities (CA's) whose job is to monitor the vehicles which fall in their areas (example district, country) [42] for their identities et cetera. It is very crucial that the messages generated by the source reach the destination in intact form without any alterations. However, because of several reasons as discussed in previous section, VANETs are highly vulnerable to being attacked by attackers. The aim of attackers differ e.g. an attacker may sniff (eavesdrop) communications which take place, it may even drop, modify or add illegitimate packets into the network [43] to achieve its goal. One solution to this problem as per [41] is that the vehicles work together to achieve security. This clearly asks for proper mechanisms of security, protocols and facilities so as to reduce and to get rid of attacker's effect. Till today, only a few attacker detection schemes are available at the application layer. [44] Created a detection system which makes use of time-stamps, components that are trustworthy and assigned messages to detect the malicious nodes. [44] Then goes further to revoke the certificates of the vehicles which are detected to be misbehaving. However the performance of [44] reduces slightly when the vehicle speed is very high. For [44] misbehavior is when a particular node is behaving in a different way than the average behavior of other nodes, but this is not a very good definition of misbehavior because that way [44] will call a car that has crashed misbehaving since its behavior will be far different than the other cars. In this case, the crashed car is not misbehaving [45]. In regard to after-crashing notification applications, [45, 46] propose and analyze Misbehavior Detection Scheme (MDS). [47] Introduced a mechanism to detect the malicious data flowing in the vehicular ad hoc networks. In [47] multiple entities observe the same event. However the trust of this scheme cannot be ascertained in the situations such as high-speed of the vehicles, changing network topology. Apart from these, there are many algorithms that are proposed to achieve security and for detecting attackers in VANET. The papers [48-53] employed the use of digital signatures and encryption keys for securing the messages. Also [54] improves cooperation among VANET nodes by making use of dynamic trust tokens. The shortcoming of [54] is that it has made an assumption that every vehicle has successor nodes in its range of transmission, but at the same time the transmission rate is calculated using the static method. Moreover [55] has analyzed the existing ways for securing ad hoc routing in vehicular ad hoc networks. Again, few static, dynamic explanations for honest establishment are audited and compared in [56].

The author in [41] gives a scheme to detect the misbehavior which it calls "Detection of Malicious Vehicles (DMV)". In order to detect malicious vehicles, it makes use of trust values and annotates each vehicle with its distrust value. To calculate the trust value, [41] makes some vehicles as verifiers (the trustworthy ones) which operate in an independent manner. The verifier verifies only the vehicles which fall in its cluster (vehicles are organized into clusters and one of the vehicles is made the cluster head and other vehicle is made the spare cluster head). In case, cluster head faces some problems, back-up cluster head is the most trustworthy vehicle in that cluster after him. Every vehicle gets monitored by some of its neighbors which are working as verifiers. The job of verifier is to monitor the nodes in its cluster for any abnormal behavior like duplicating/dropping packets, when verifier sees such a behavior it increases the distrust value of that node. After that, verifier sends the ID of this abnormally behaving node to certificate authority (Note that a certificate authority (CA) is an authority which manages the id's, keys and other credentials of nodes falling in a particular region), if the distrust value has gone above threshold (sigma sign). In [41] every node constructs and maintains 2 lists, one list consisting of normal nodes-which forward messages without dropping/duplicating them, while the other list consists of Malicious nodes- which drop or duplicate messages (blacklist). The certificate authorities broadcast their fundamental blacklist to all the cluster heads on a periodic basis. The cluster heads in turn send the list to the vehicles falling in their regions. However, the entire approach of [41] has used all trustworthy nodes as the verifiers which lead to reduced utilization of network resources, that puts un-required pressure on vehicles, therefore [57] uses only selected trustworthy nodes as verifiers and not all, only the selected trustworthy nodes monitor other nodes. This leads to better utilization of network resources and hence better performance.

For this purpose, [57] uses node centric approach. In node centric approach, an unauthentic node is isolated from the network by verifying the security credentials, digital signatures and other security related data (used to authenticate a node in the network). Node centric scheme is only concerned about the nodes of network and not the data that is being transmitted by them. For implementing this approach, it has used the concept of trusted certificate authorities, which are responsible for managing the complete network. These certificate authorities gather information from verifiers, calculates new distrust values for all the nodes and if the distrust value of any node falls below threshold (node is malicious) then it also informs all other nodes of network about this malicious node. The information related to malicious nodes is given to each cluster head in network, which creates a black list. When a node wishes to transmit data to a specific destination, it first checks whether any node between source and destination is in blacklist or not. If yes, then it drops this path and discovers another path for data transfer between source and destination. For the selection of verifiers for a particular vehicle relaying data between source and destination, it has calculated decision parameter for each node eligible for verifier. The decision parameter for a node depends on load, distrust value and distance between the verifier node and the verified node.

3.1. Critical Analysis

There is much higher complexity and resource wastage in DMV & DMN approaches, because each time the verifiers have to continuously monitor other nodes which will increase their burden and can also affect their own data transfer performance. Also the system completely depends on cluster heads and certificate authorities for dropping the malicious nodes from network, if any one of these fails or stops working, then the complete security mechanism comes down. Also, DMV & DMN approaches first allow the malicious nodes to drop initial packets, by which they then identify these malicious nodes (by monitoring the number of packets dropped by a node), and then isolate them from the network, but during this entire process many initial packets are lost.

So, for this purpose a preventive algorithm against black hole attack for VANET has been proposed and will be discussed in upcoming sections.

4. PROPOSED SYSTEM

The primary security requirement in any network is availability because it says that the network is working and functional. Putting this availability of VANET at stake is very easy owing to the unique characteristics of these classes of network like dynamically changing topology, quickly moving vehicles, absence of centralized monitoring body. There are various threats to this availability, most important one being the denial of service (which includes black hole attack, wormhole attack, jamming attack etc.), were a legitimate user/vehicle can also launch such attacks which makes these attacks more difficult to detect using cryptographic techniques. There are certain techniques proposed (as discussed earlier) which are able to detect malicious nodes in VANET, but these techniques are not fullyable to eliminate the effect of such attackers. These techniques continuously monitors the data traffic transmitted, forwarded and received by the network nodes, and then detect Black hole nodes by measuring the number of data packets dropped, but during this process some of the data packets are being lost. So to prevent VANET completely from such attacks a different approach is needed, which can eliminate these attackers from the network and reduce the effect of Black hole nodes. To do this a Malicious Node Prevention (MNP) technique is proposed which prevents VANET from malicious nodes and reduces the effect of malicious nodes to greater extent.

4.1. Malicious Node Prevention (MNP) Algorithm

In the preceding sections, all the available solutions to the Black hole problem in VANET were presented. All these solutions detect the malicious nodes during data transfer phase due to which some of the packets are lost. Also the complexity of these solutions is higher. To overcome these problems, a prevention algorithm (MNP) is presented. The algorithm used in MNP automatically creates two lists: Blacklist and white-list. All the black hole nodes detected by MNP algorithm are placed in Blacklist, and rest of nodes are placed in White-list. During data transfer phase, the packets are forwarded only to those nodes which lie in the White-list. Also, MNP algorithm works well when the underlying routing protocol is AODV.

For creating the Blacklist, we have made an assumption that no node present in the network has a routing table with it initially (when no node has yet transferred any data to another node in the network). So, initially only destination is allowed to send reply (in the form of RREP packets) to the source (which has sent RREQ packet to particular destination). Since, VANET has no centralized monitoring body in the network. Each node has the responsibility of detecting the abnormal behavior of other nodes. Thus, every node in the network is accountable for checking whether it has received RREP packet from destination or not. If a node receives RREP packet from an intermediate node (that is not the destination), then the RREP is discarded and the node sending RREP is placed in Blacklist. Every black hole node will send RREP to source, claiming that it has got the shortest path to reach the destination, but it is assumed that no node has route to destination initially in the network. Thus all the black hole nodes will be placed in the Blacklist and their RREP packets will be discarded, while the non-malicious nodes will be placed in White-list. Due to this process all the malicious nodes in the network will be detected initially and no data packet will be lost in data transfer phase. Once both the lists are complete, then one can receive RREP packets from intermediate node, which claim that they have shortest path to destination, but the condition is that the intermediate nodes sending RREP should not be among the Blacklisted nodes. Moreover, when a new node steps into the network, it is again checked for the abnormal behavior. The newly entered node is neither in Blacklist nor in White-list, so if this node sends RREP to any source node in the network (claiming that it also has shortest path to destination), then again it will be placed in Blacklist, because it is evident that this node has recently joined the network and will not have any shortest path to destination. The complete procedure of detecting a malicious node in VANET is shown in figure – 9.

The figure – 9 describes complete procedure of MNP approach for detecting malicious nodes in network. This procedure will be followed by all nodes in the network whenever they receive an RREP packet from other nodes in the network. By following this procedure, only White-listed node will be used for data forwarding from source to destination, thereby eliminating the malicious nodes from network. The process of detecting and annihilating the malicious nodes from network is explained thoroughly in following steps/phases:

4.2. Initial Route discovery

When a VANET gets deployed and the very first node starts route discovery process for determining shortest route from source to destination, the process RREQ flooding is initiated. In RREQ flooding process, the source node produces RREQ packets, which is then flooded to all the neighboring nodes, the neighboring nodes flood these RREQ packets to further nodes present in the network, and the process continues. Each node checks if it is the destination (for which the RREQ is sent), if not, then the node forwards RREQ to its neighbors (except the one who sent this packet) and preserves reverse path for sending RREP to source. If the node receiving RREQ packet happens to be the destination, then this destination sends RREP packet to source through the reverse path. Due to this initial route discovery process all the nodes in the network are able to formulate shortest paths to all other nodes in the network. So, before this process no node in the network has the shortest path to any other node. During initial route discovery process if any node sends RREP to source, claiming that it has shortest path to destination, then that node is labeled as malicious and is placed in Blacklist, and all other nodes are placed in White-list.

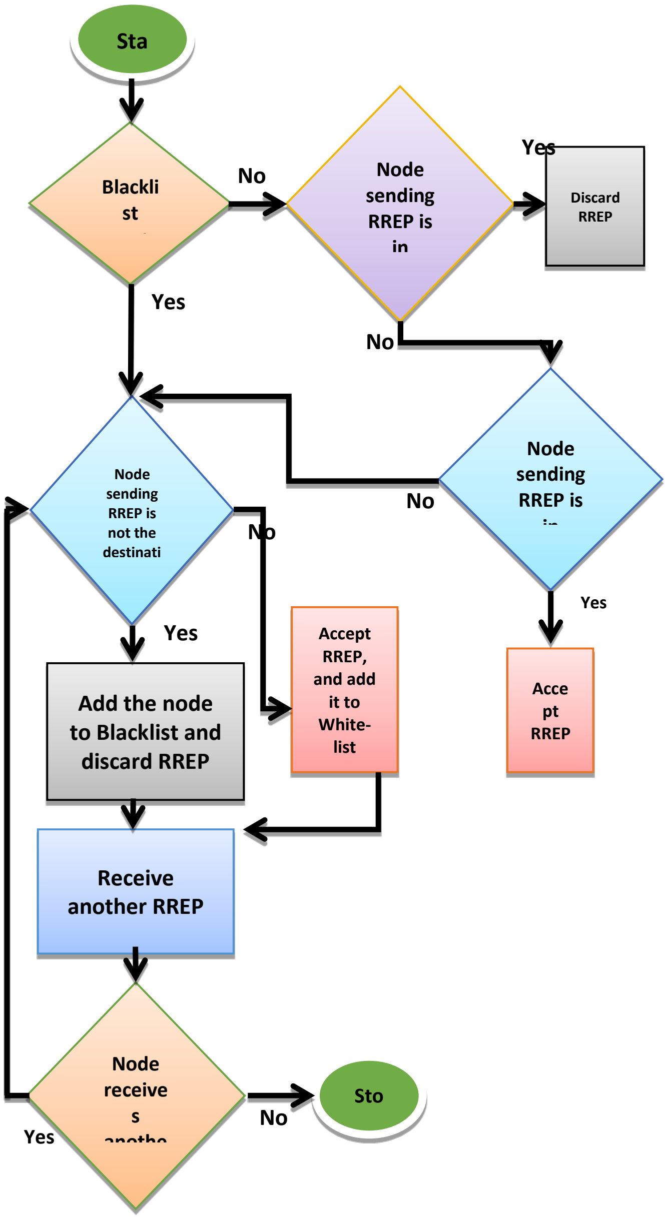

Figure 9 MNP Procedure

4.3. Data transfer phase

Once the initial route discovery phase is completed, all the nodes of network are classified into Blacklisted and White-listed nodes. Thus, whenever a source node has to transfer data to destination, it will only forward data through those nodes which are in White-list. Hence, it is in initial Route discovery phase when all the malicious nodes are detected. Also, in VANET the nodes are dynamic, i.e. the network nodes are at constant motion, which can alter the routes formed in initial route discovery phase. To deal with this problem AODV always initiates route discovery whenever a node has to send data to another node in a network and during this route discovery, again only those nodes will be included in new routes which are in White-list and not those in Blacklist.

4.4. Network Monitoring

Suppose if a new node has entered in the network after initial route discovery phase. This new node will neither be in Blacklist nor in White-list, so for such node we have to follow the same procedure, as followed in initial route discovery process, and have to classify the new node in Blacklist or White-list and then include it in the network. If the new node sends RREP packet (claiming that it has shortest path to destination) immediately after joining the network against some RREQ packet received by it then it is to be placed in Blacklist, because the node has recently joined the network and it is quite clear that such node is not aware of any route to other nodes in network. Also, if any White-listed node leaves the network, then it has to clear all the entries in its routing table and re-create its routing table when it enters the network again. Thus, the network needs to be monitored continuously by other White-listed nodes.

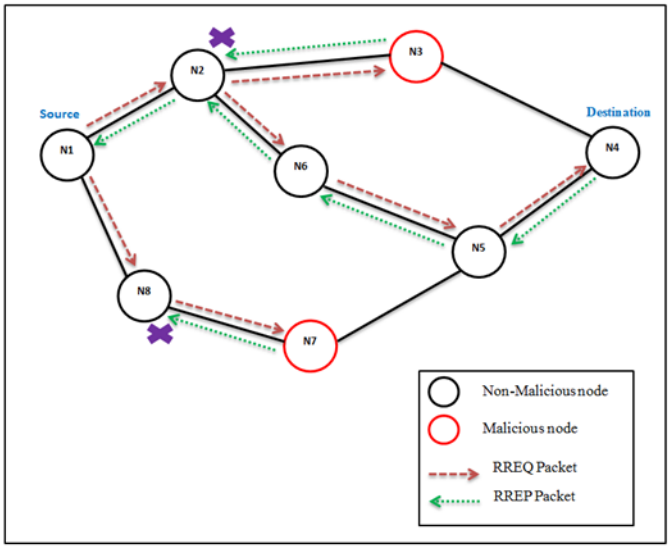

Figure 10 Detection of Malicious node during Initial Route discovery

In figure – 10 the source node (N1) has to transmit data packets to node N4, for this it floods RREQ packets into the network for determining the shortest path from N1 to N4. During the flooding process when a Non-malicious node receives a RREQ packet, it initially checks whether it is the destination for received RREQ packet, if yes then it will accept it and sends RREP packet to source. But if the receiving node is not the destination, then it will forward the RREQ packets to their neighbors (because initially no node has shortest path to destination). So, node N2, N6, N5 and N8 forwards RREQ packets to their neighbors. On the contrary to this, when a malicious node receives RREQ packets, it immediately accepts RREQ packet and sends RREP packet to the node which sent RREQ packet to this node, claiming that it has shortest path to destination. So, node N3 and N7 (which in our example are malicious nodes) will send RREP packets to nodes N2 and N8 respectively. On receiving the RREP packets by N2 and N8, they will check whether the nodes N3 and N7 were the destination nodes for RREQ packets sent by N2 and N8, if not, N2 and N8 will discard the RREP packet and place nodes N3 and N7 in Black-list. When a Non-malicious node receives RREP packet from destination, it forwards the RREP packet to source through reverse path and each node is informed that this packet has been generated by the destination node (which is done by preserving the address of destination node in reverse path). Therefore, in our example nodes N5, N6 and N2 will forward the RREP packet to its source node (N1) and due to this Initial Route discovery process each Non-malicious node has shortest route to another nodes in the network and these routes are free of malicious nodes.

Thus it is evident from the above example that the malicious nodes are being detected and eliminated from the network initially before any data transfer takes place between the nodes. Also when a new node/vehicle enters the network it is first tested for malicious behavior and is again eliminated (if the node is malicious). Due to this technique the network is prevented from malicious nodes and the effect of such nodes is reduced to larger extend.

5. EXPERIMENTAL EVALUATION

The proposed approach for preventing the malicious nodes in VANET has been implemented using Network Simulator – 2 (NS2) and SUMO. NS2 is an open source network simulator which uses C++ (at backend) and OTCL (at front-end) to construct and configure networking components. Also SUMO is an open source discrete time vehicular traffic generator package, so using SUMO a realistic scenario of traffic has been generated and data packets are then being transmitted between different nodes of network. A complete configuration of the network topology, number of lanes, number of vehicles, maximum and minimum speed of vehicles and simulation time are provided as input to SUMO, which then simulates the complete scenario and finally outputs the complete TCL file.

The TCL file is then executed in NS2 for further analysis. The basic AODV routing protocol is being supplied by NS2 package, which is then modified to prevent the malicious attacks in VANET. The modification is done at backend using C++ language. The performance of proposed Malicious Node Prevention (MNP) algorithm is computed using parameters like packet delivery ratio, throughput and end to end delay, which are defined as:

Average Throughput: It is described as "the successful rate of messages which is being transmitted per second over a communication channel". The unit of measurement for average throughput is bits per second. Thus, we have:

Average Throughput = (Total Received Packets / (Stop Time – Start Time))(8/1000).*

Average End to End delay: It is defined as "the average time taken for a packet to be transmitted from source to destination". If in a network some of the packets get dropped during transmission process, then this parameter cannot be used for performance measurement for such networks. This is computed by taking average of end to end delays of all the packets transmitted in the network by different nodes.

Packet delivery ratio: It may be explained as "the ratio of number of data packets received at the receiver to that of the number of data packets transmitted by transmitter". It is calculated as:

Packet delivery ratio = (data Packets received by destination / data Packets transmitted by source)

We have constructed VANET using 41 nodes/vehicles and 4 RSU's (Road Side Units) which are placed in such a way that they help in efficient and quick forwarding of data packets between nodes. Each node has variable speed with which they move from one point to another and ranges from 20 m/sec to 70 m/sec. The basic routing protocol used to route data packets from one node to another is AODV. The simulation is run for 50 seconds with CBR type of data traffic between the nodes with a packet size of 512 bytes and has used 802.11 MAC layer protocol. To comprehend the effect of malicious nodes in the network, the Black hole attack is being implemented and the malicious nodes are chosen randomly. We vary the number of malicious nodes from 2 to 12 in order to get different readings of performance parameters. The complete simulation parameters are presented in table – 1.

Simulator	NS-2 (2.35)
Mobility Generator	Sumo (version – 2.92)
Number of Nodes	41
Number of RSU	4
Simulation time	50 seconds
Traffic type	CBR
Routing Protocols	AODV
Packet Size	512 bytes
Antenna type	Omni-directional
MAC type	802.11 MAC layer
Malicious Behaviors	Black hole
Number of Malicious Nodes	2, 4, 6, 8, 12
Mobility	Variable (20 m/s to 70 m/s)

Table 1 Simulation Parameters Used

In the simulation process, first we have implemented Black hole attack in VANET and effect of such attack is noted and is presented in figure 11, 12. The black hole nodes are chosen such a way that they will drop the maximum number of packets in the network. Once the Black hole attack is completely implemented in the network and the network performance is being calculated, then we implement the MNP technique to prevent the malicious attacks in VANET. Then again the effect of malicious nodes over the performance of network is calculated (in presence of MNP technique). To compare the performance of proposed approach (MNP) for preventing the malicious nodes in VANET, we have compared it with Detection of Malicious Vehicle (DMV) & Detection of Malicious Node (DMN) schemes and the results are given in figures 13 to 15.

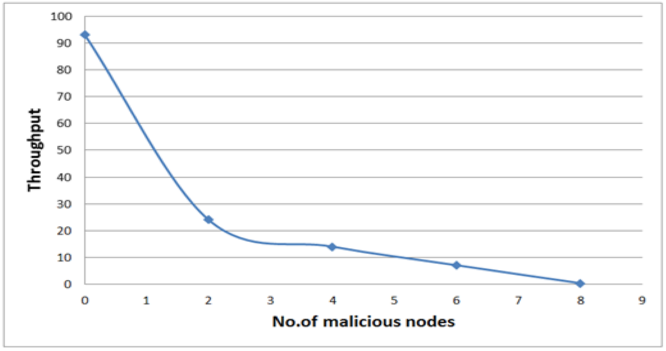

Figure 11 Effect of Malicious nodes on throughput of different nodes in VANET (without the implementation of any detection or prevention scheme)

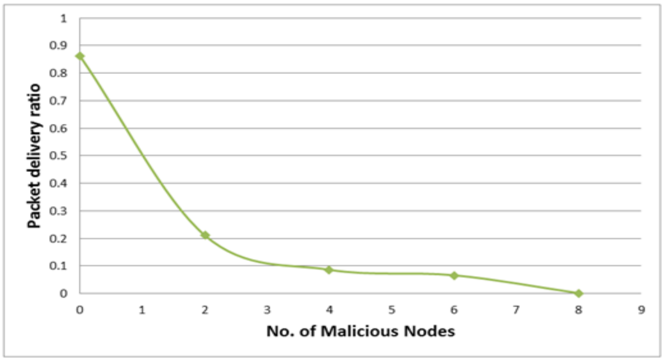

Figure 12 Effect of Malicious nodes on average Packet delivery ratio of different nodes in VANET (without the implementation of any detection or prevention scheme)

As shown in the figure 11 and 12 as the number of malicious nodes increase, the average packet delivery ratio and throughput of different nodes decrease drastically and when the number of malicious nodes reach to 8, almost all the data packets are dropped. This shows that how immensely the malicious nodes can affect the performance of VANET. To overcome this problem a MNP technique is then implemented with similar malicious nodes in the network and the performance of such network is calculated (presented in figure 13 to 15) which is compared with the performance of DMV & DMN techniques.

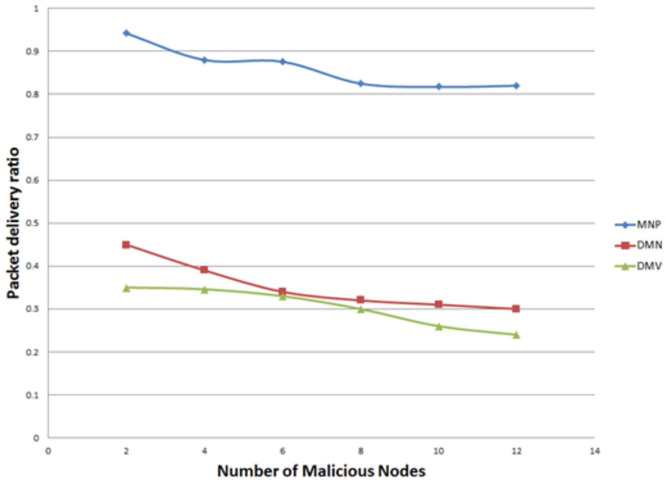

Figure 13 Packet delivery ratio comparison of Malicious Node Prevention (MNP), Detection of Malicious Vehicle (DMV) & Detection of Malicious Node (DMN) schemes in presence of malicious nodes in VANET

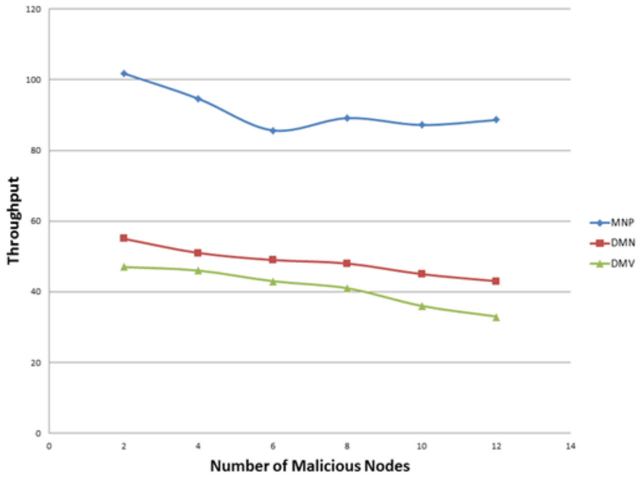

Figure 14 Average Throughput comparison of Malicious Node Prevention (MNP), Detection of Malicious Vehicle (DMV) & Detection of Malicious Node (DMN) schemes in presence of malicious nodes in VANET

Figure 13 shows that as the number of malicious nodes increase in the network the packet delivery ratio (using MNP technique) almost remains constant and in comparison to DMV & DMN techniques, it is much higher. This shows that negligible number of packets are being dropped by malicious nodes in the network. In other words we can say that there is no effect of malicious nodes on the network performance in presence of MNP technique. Also figure 14 shows that the average throughput of network nodes slightly decreases as the number of malicious nodes increase in the network, but again the average throughput of node in presence of MNP technique is much more than that of DMV & DMN techniques. This again proves that the proposed MNP technique performs better than DMV &DNM techniques for eliminating the effect of malicious nodes in VANET. The figure 15 shows that MNP has higher end to end delay in comparison to DMV & DMN approaches and this delay increases as the number of malicious nodes increase. The explanation to this anomaly is that each time when a node has to send data packets to another node in a network it initiates route discovery process and each node which receives RREP from another node it first has to check whether the nodes is in blacklist or in white-list during route discovery mechanism and accordingly reject or accept the RREP packet. If the node is found malicious, then it has to calculate another route which does not contain malicious nodes in it. It is this deferral due to which the MNP technique has higher end to end delay.

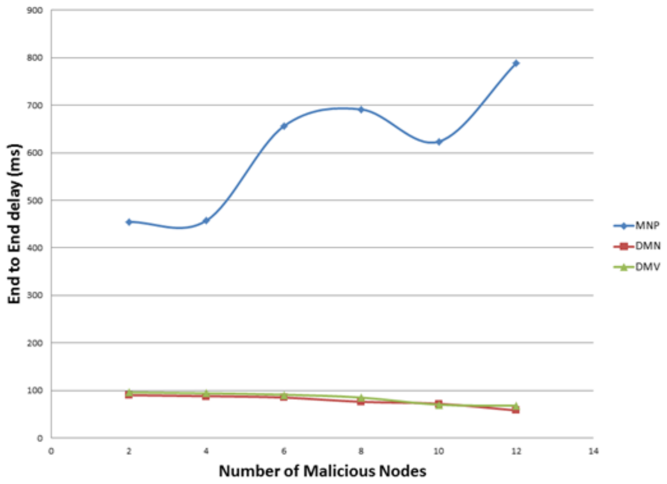

Figure 15 Average End to End delay comparison of Malicious Node Prevention (MNP), Detection of Malicious Vehicle (DMV) & Detection of Malicious Node (DMN) schemes in presence of malicious nodes in VANET

Finally, we can say that even though MNP has higher end to end delay than DMV & DMN schemes, but MNP performs better than both DMV & DMN when taking average packet delivery ratio and throughput into consideration, which shows that MNP prevents VANET from malicious nodes to larger extend.

6. CONCLUSION AND FUTURE WORK

This work encloses an exhaustive review of the state of art of security in VANETs, after discussing a count number of VANET aspects such as applications and architecture of VANETs, their special characteristics, important routing protocols used in VANETs. Moreover, the various VANET standards were presented. The fundamental security concerns related to VANETs have been drawn out. It was concluded that in order to alleviate the cruel effects of attacks on availability (especially the black-hole attack) a preventive mechanism was needed. Consequently, we devised MNP (Malicious Node Prevention) algorithm. This algorithm prevents the initial loss of the packets by the malicious nodes during the data transfer phase (as is allowed by other techniques in literature such as DMV and DMN) prior to sending the data packets through them. Therefore MNP greatly reduces the data loss during the Black-hole attack. The simulation results clearly depict that MNP works extremely well during the attack. It keeps the packet delivery ratio almost constant when the number of malicious nodes in the network increase. With MNP only an infinitesimal amount of data packets are dropped. The PDR is much better than DMV &DMN. The results also indicate that the end to end delay is the higher in MNP technique as compared to the DMV &DMN techniques proposed earlier. Moreover, the throughput of the network during the attack is far better, when MNP is employed instead of DMV &DMN.

For the purpose of taking our research a step ahead, we will work on how to reduce the overall end-end delay while using MNP approach. We can also consider the scenarios involving complex traffic or limited resources. Again, the proposed technique can be deployed in real time which will help us to evaluate its performance better and also will give us the opportunities to figure out the extensions which can be made.

REFERENCES

[1] Richard Gilles Engoulou, Martine Bellaiche, Samuel Pierre, Alejandro Quintero, “VANET security surveys”, in: computer communications Elsevier, 1- 13, 2014.

[2] O. Trullols, M. Fiore, C. Casetti, C.-F.Chiasserini, J.M. BarceloOrdinas, “Planning roadside infrastructure for information dissemination in intelligent transportation systems”, Comput. Commun.33 (4) 432–442, 2010.

[3] S.S. Kaushik, “Review of different approaches for privacy scheme in VANETs”, Int. J. 5 ISSN 2231-1963, 2012.

[4] A.Stampoulis, Z.Chai, “A Survey of Security in Vehicular Networks”, Project CPSC 534,2007.

[5] J.-P. Hubaux, S. Capkun, J. Luo, “The security and privacy of smart vehicles”, IEEE Secur.Priv. 2 (3) 49–55, 2004.

[6] C.Wei, Y,Jianding, L. Xiangjun, “The design of electronic license plate recognition terminal system based on nRF24LE1”, in : 2012 Fifth International Symposium on Computational Intelligence and Design (ISCID), pp. 127-129, 2012.

[7] M. J.-P. Hubaux, S. Capkun, J. Luo, “The security and privacy of smart vehicles”, IEEE, J.-P.Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur.15 (1) 39–68, 2007.

[8] Qing Xu, Tony Mak, Jeff Ko, Raja Sengupta “Vehicle-to-Vehicle Safety Messaging in DSRC” ACM 1-58113-922-5/04/0010, October 1, 2004.

[9] I.C. Society, “802.11p– IEEE standard for information technology – local- and metropolitan area networks – specific requirements – part 11”: Wireless LAN medium access control, (mac) and physical layer (phy) specifications amendment 6: wireless access in vehicular environments, 2010.

[10] DSRC, Dsrc, http://grouper.ieee.org/groups/scc32/dsrc/.

[11] ETSI, European Telecommunications Standards Institute (ETSI), http://www. etsi.org.

[12] ITS, ITS standards fact sheets of IEEE, http://www.standards.its.dot.gov/ factsheets/factsheet/80, seen, April 19, 2014.

[13] L. Miao, K. Djouani, B.J. van Wyk, Y. Hamam, “Evaluation and enhancement of IEEE 802.11 p standard: a survey”, Mob. Comput.1 (1) 2012.

[14] G.Jyoti, M.S.Gaur, in: S, Auerbach (Ed.), “Security of Self-organising Networks MANET, WSN, WMN, VANET”, CRC Press, 2010.

[15] Y.wang, F.Li, “Vehicular Ad Hoc Networks”, Springer-Verlag, London, 2009.

[16] H. Hartenstein , Kennith P. Laberteaux, “A tutorial survey on vehicular ad hoc networks”, IEEE commun. Mag., 2008.

[17] SalehYousefi ,MahmoodSiadatMousavi, MahmoodFathy, “Vehicular Ad Hoc Networks (VANETs) : Challenges and Perspectives”, in : International conference on ITS Telecommunications Proceedings, pp. 1151- 1155, 2006.

[18] J. Kakarla, S. Siva Sathya, B.G. Laxmi, B. Ramesh Babu, “A survey on routing protocols and its issues in VANET”, Int. J. Comput. Appl. 28 (4) ISSN 0975-8887, 2011 .

[19] L.K. Qabajeh, M.L.M. Kiah, M.M. Qabajeh, “A scalable and secure position-based routing protocols for ad-hoc networks”, Malays. J. Comput. Sci. 22 (2) 99–120, 2009.

[20] F.D. Rango, J.-C. Cano, M. Fotino, C. Calafate, P. Manzoni, S. Marano, “OLSR vs DSR: a comparative analysis of proactive and reactive mechanisms from an en- ergetic point of view in wireless ad hoc networks”, Comput. Commun.31 (16) 3843–3854, 2008.

[21] Philippe Jacquet, Paul Muhlethaler, Thomas Clausen, AnisLaouiti, Amir Qayyum, Laurent Viennot, “Optimized link state routing protocol for ad hoc net- works”, in: Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings.IEEE International, IEEE, pp. 62–68, 2001.

[22] M. Osman, “The performance of aodv routing protocol based on dropped packet and throughput metrics: a simulation and comparative study for VANET”, Int. J. Manag. Inform. Technol. 4 (2) 265–279, 2013.

[23] B. Karp and H.T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks”, in Proceedings of the ACM/IEEE International Conference on MobileComputing and Networking (MobiCom), 2000.

[24] R. Jain, A. Puri, R. Sengupta, “Geographical routing using partial information for wireless ad hoc networks”, IEEE Pers. Commun. 8 (1) 48–57, 2001.

[25] H. Rahbar, K. Naik, A. Nayak, “Dtsg: dynamic time-stable geo-cast routing in vehicular ad hoc networks”, in: 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), IEEE, pp. 1–7, 2010.

[26] S.-Y. Wang, C.-C.Lin, K.-C.Liu, W.-J. Hong, “On multi-hop forwarding over wbss-based IEEE 802.11 (p)/1609 networks”, in: IEEE 20th International Sympo- sium on Personal, Indoor and Mobile Radio Communications, 2009, IEEE, pp. 3040–3044, 2009.

[27] L. Miao, K. Djouani, B.J. van Wyk, Y. Hamam, “Evaluation and enhancement of IEEE 802.11 p standard: a survey”, Mob. Comput.1 (1), 2012.

[28] B. Ducourthial, F. El Ali, et al., “Architecture pour communication vehicular-infrastructure”, in: CFIP, 2009.

[29] J.T.Isaac, S. Zeadally, J.S. Camara, “Security attacks and solutions for vehicular ad hoc networks”, IET commun, 4 894-903, 2010-04-30.

[30] V.S. Yadav, S. Misra, M. Afaque, "Security of Wireless and Self-Organising Networks: Security in Vehicular Ad hoc Networks", CRC Press, pp.227-250, 2010.

[31] M Raya, P. Papadimitratos, J.P. Hubaux, "Securing vehicular communications, IEEE wireless", Commun, 13 8-15, 2006.

[32] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges", Telecommun. Syst. 50 (4) 217–241, 2012.

[33] A. Dhamgaye, N. Chavhan, "Survey on security challenges in VANET", Int. J. Com- put. Sci. 2 88–96, ISSN 2277-5420, 2013.

[34] J.M. d. Fuentes, A.I. González-Tablas, A. Ribagorda, "Overview of security issuesin vehicular ad-hoc networks", in: Maria Manuela Cruz-Cunha, Fernando Moreira (Eds.), Handbook of Research on Mobility and Computing, IGI Global, 2010.

[35] B. Schneier, "Applied Cryptographic protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., 1996.

[36] R. Minhas, M. Tilal, "Effects of jamming on IEEE 802.11 p systems", Chalmers University of Technology, 2010.

[37] A. Hamieh, J. Ben-Othman, A. Gueroui, F. Naït-Abdesselam, "Detecting greedy behaviors by linear regression in wireless ad hoc networks", in: IEEE Interna- tional Conference on Communications, ICC'09, IEEE, pp. 1–6, 2009.

[38] J.R. Douceur, "The sybil attack", in: Peer-to-Peer Systems, Springer, pp. 251–260, 2002.

[39] M.S. Al-kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)", in: 6th International Conference on Signal Processing and Commu- nication Systems (ICSPCS), IEEE, pp. 1–9, 2012.

[40] Nadeem T, Shankar P "A comparative study of data dissemination models for VANETs", IEEE Mob Ubiquitous SystNetwServ: 1–10, 2006.

[41] AmenehDaeinabi, Akbar Ghaffarpour Rahbar "Detection of malicious vehicles (DMV) through monitoring in vehicular Ad-hoc Networks" in : Springer, pp 325-338, 2013 .

[42] Abdulhamid H, Tepe KE, Abdel-Raheem E "Performance of DSRC systems using conventional channel estimation at high velocities", Int J Electron Commun: 556–561, 2007.

[43] Picconi F, Ravi N, Gruteser M, Iftode L "Probabilistic validation of aggregated data in Vehicular Ad Hoc Networks", International Conference on Mobile Computing and Networking, Los Angeles, CA, USA: 76–85, 2006.

[44] Raya M, Papadimitratos P, Aad I, Jungels D, Hubaux JP "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks", IEEE J Sel Areas Commun 25(8):1557–1568, 2007.

[45] Ghosh M, Varghese A, Gupta "A Distributed misbehaviour detection in VANETs", IEEE WirelCommun Network Conf: 2909-2914, 2009.

[46] Ghosh M, Varghese A, Kherani AA, Gupta A, Muthaiah SN "Detecting misbehaviour in VANET with integrated root cause analysis", Elsevier AD Hoc Networks 8:778-790, 2010.

[47] Gelle P, Grren D, Staddon J "Detection and correcting malicious data in VANETs", in Proc VANETS'04: 29–37, 2004.

[48] Guo J, Baugh JP, Wang SH "A group signature based secure and privacy-preserving vehicular communication framework", Mob NetwVeh Environments: 103–108, 2007.

[49] Li ChT, Hwang MSh, Chu YP, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc network", ComputCommun 31(12):2803–2814, 2008.

[50] Raya M, Hubaux JP, "The security of vehicular ad hoc networks", J ComputSecur Spec Issue Secur Ad Hoc Sensor Netw 15(1):39–68, 2007.

[51] Wang NW, Hauang YM, Chen WM, "A novel secure communication scheme in vehicular ad hoc networks", ComputCommun 31(12):2827–2837, 2008.

[52] Wua B, Wua J, Fernandeza EB, Ilyasa M, Magliveras S, "Secure and efficient key management in mobile ad hoc networks", J NetwComputAppl 30:937–954, 2007.

[53] Yan G, Olariu S, Weigle MC, "Providing VANET security through active position", ComputCommun 31(12):2883–2897, 2008.

[54] Wang Z, Chigan CH, "Countermeasure uncooperative behaviors with dynamic trust-token in VANETs", Proc IEEE IntConfCommun: 3959–3964, 2007.

[55] Wex P, Breuer J, Held A, Leinmuller T, Delgrossi L, "Trust issues for Vehicular Ad-Hoc Networks", VTC.2008: 2800–2804, 2008.

[56] Fonseca E, Festag A, "A survey of existing approaches for secure Ad Hoc routing and their applicability to VANETS", Technical Report NLE-PR, NEC Network Laboratories, 2006.

[57] Uzma Khan, Shikha Agarwal, Sanjay Silakari, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks", in: Elsevier, pp 965-972, 2015.

Author

Syed Rameem Zahra received the B.Tech. degree in Computer Science and Engineering from university of Kashmir, Srinagar, J&K, India, and the M.Tech. degree in Computer Science and Engineering from SMVDU, katra, J&K, india. She is currently pursuing the Ph.D degree with the department of Computer Science and Engineering, National Institute of Technology Srinagar, J&K, India. Her area of research is database systems, Wireless sensor networks, VANETs and IOT security.