Timestamp Based Detection of Sybil Attack in VANET

Syed Mohd Faisal and Taskeen Zaidi
(Corresponding author: Taskeen Zaidi)

Department of Computer Science and Engineering, Shri Ramswaroop Memorial University
Village Hadauri, Post Tindola, Lucknow - Deva Road, Barabanki, Uttar Pradesh 225003, India
(Email: taskeenzaidi867@gmail.com)

(Received July 24, 2019; Revised and Accepted Dec. 15, 2019; First Online Feb. 28, 2020)

Abstract

VANET is a subset of MANET in which communication among the vehicles may be done using vehicle -to- vehicle or roadside infrastructure. But there may be chances of attacks in VANET due to mobility of nodes and random change in topology. One of the prominent attack is Sybil attack in which attacker creates multiple false identities to disturb the functionality of VANET. In literature many solution have been proposed for detection and protection of vehicles from Sybil attack. In the current work, authors have proposed a Sybil node detection technique based on timestamp mechanism. In this work timestamp is a unique certificate provided by RSU to all vehicles on the road in VANET. In the proposed work for node discovery and data transmission, we used Ad-hoc On Demand Distance Vector (AODV) Routing protocol and timestamp as a hash function of public key and for detection of the Sybil node implemented through NS2 simulator.

Keywords: Network Security; NS2; NS3; Sybil; VANET

1 Introduction

With the recent development in network topologies and trends, VANET receives a lot of interest of researcher and scientists.

Vehicular Ad-hoc Network (VANET) is a shade of Mobile Adhoc Network, which has potential to improve passenger safety by means of communication among vehicles [10]. Mobile Ad-hoc Network (MANET) provides communication between stand by devices, these devices either have slow movement or no movement on the contrary VANET establish and cater communication betwixt swift moving vehicles [20]. Apart from this, their are several other differences between MANET and VANET which were listed in Table 1.

Each year exponential number of vehicles were running on roads, in course of time, definitely, it will grow drastically. It will cause traffic on the roads that fritter away time, money, petroleum products and many more. Government is investing more money to construct more and more roads and destroying landscape for the reason that existing roads are not in a condition to support generated traffic. Their is a solution of all these problems *i.e.* VANET. VANET provides communication between vehicles that helps to improve traffic on the roads. Prior to, vehicles obtain traffic information of route and driver takes decision based on that information.

VANET is a way to enforce Intelligent Transport System (ITS) based on IEEE 802.11p standard for the Wireless Access for Vehicle Environment (WAVE).

VANET allows vehicles to seamlessly connect in a region, where no existing infrastructure is available. VANET system aims at providing platform for various services that can improve passenger's safety and efficiency, driver assistance, infotainment, transportation regulation *etc.* In order to provide these services VANET require accurate and timely (no delay) data transmission. Information is transmitted in between Vehicles (mobile nodes) and some nearby stable Road Side Units (RSU).

VANET connects those vehicles that were in range of 100 to 500 meters and if a vehicle is not in that range, it will not connect with other vehicles. Figure 1 shows the complete architecture of VANET.

Primarily VANET supports two types of communication *i.e.*

1) Vehicle-to-Vehicle (V2V) Communication;
2) Vehicle-to-Infrastructure (V2I) Communication.

Vehicle-to-Vehicle (V2V) communication do not require any infrastructure for communication, it creates a self-network. The range of this network is up to 500 meters from the geographical position of initiator vehicle. Vehicle in that range can communicate using On Board Unit (OBU) with other vehicles of the network sans availing the benefit of VANET. In V2V, vehicle share information about safety messages, vehicle identities and information about malicious vehicle. On contrary, Vehicle-to-Infrastructure (V2I) communication relies totally on the preset infrastructure *i.e.* Road Side Unit (RSU). In

Table 1: Comparison of MANET with VANET

SN	Parameters	MANET	VANET
1.	Node Mobility	Low	High
2.	Node Density	Low	High
3.	Change in Network Topology	Slow	Frequently
4.	Energy Constraints	Medium	Low
5.	Moving pattern of Nodes	Random	Constrained by Road
6.	Range	100m	Upto 500m
7.	Node Speed	Low(6km/hr)	Medium-High(20-100Km/hr)
8.	Scalability	Average	High
9.	Bandwidth	Hundred Kbps	Thousand Kbps
10.	QoS	Low	High

V2I communication RSU communicate with Vehicles and transmit network management message, road condition, nearby hotel, internet access. Figure 1: Architecture of VANET shows the broader picture of VANET and services provided by it.

As we know that movement of vehicles are very fast in VANET so the intensity of connection and disconnection of vehicles are very high and due to that topologies keeps changing. Meanwhile, there is a favorable chance for attacker to attack on the network when the topologies change. Therefore, security is also a major concern in VANET, it is necessary to figure out the chances of attack and eliminate them.

Firstly, VANET is a wireless network so it inherits all the security threats of wireless network. Secondly, movement of vehicles are high in VANET so for the efficient communication vehicles keeps switching between topologies because of that there is a great chance of attack at the time of handoff.

Various forms of forging attacks were implemented and designed by authors [7]. The attacks were analysed through vehicles speed, number of collisions and percentage of delivered packets. Rana *et al.* [21]. modified PKI for message authentication, integrity and privacy. A coordination based algorithm designed for dynamic network for information flow and vehicle security is maintained by a unique signature method [2]. Grover *et al.* [6] used neighborhood list to detect and identify Sybil node. This scheme specifies that if neighboring node is watching a malicious node for a longer duration of time then this node will be identified as a Sybil node but the drawback of this scheme was that it was very complex and time consuming. A survey routing protocols for VANET has been done by authors [9] on unicast, multicast, geocast, mobicast and broadcast protocols. A navigation based system for VANET is proposed for the guidance of drivers in real-time manner. The system is useful for computation of better route in real road based scenario [1]. A system model was proposed by authors [25] using dynamic certificate generation technique to restrict and identify the Sybil node. It was analyzed by authors [14] that in VANET vehicles communicated through RSU using central server and road side servers. The communication may be Vehicle to Vehicle (V2V) or Vehicle to Roadside (V2R).

Authors [23] proposed a shared key management technique which has advantage over distributed key management system. In this framework the vehicles may be inter connected automatically without using RSU. The message transmission is done by RSU. Emergency Electronic Brake Lights System was proposed by authors [3] which warns the vehicles on the road about weather condition and V2V communication is used to propagate the alert messages to the vehicles. A distributed and localized approach was proposed by authors [30] for the detection of Sybil nodes on roads. Two algorithms were proposed for position verification and detection of Sybil attacks by observing signal strength. Simulation was performed to analyze the proposed scheme. Authors [8] have proposed a Sybil node detection method using electro acoustic position using context aware switching technique. Simulation has been done to analyze the accuracy of proposed scheme. A physical layer authentication scheme was proposed by authors [29] to detect Sybil attack in indoor and urban environment. Hypothesis was proposed to detect the Sybil nodes for narrowband and broadband wireless system. The performance was depicted through network analyzer tool. NS2 is a networking tool used for simulation purpose for wired and wireless networks [13, 18].It is an open source simulator used for networking research and has support protocols like TCP, FTP, UDP, HTTPS, DSR and AODV. It uses TCL as an scripting language and C++ and OTCL language.

2 Background

Because of the communication in wireless environment, VANET is exposed to various attacks and threats as shown in Figure 2. Following are the necessities required to ensure security in VANET [11, 15].

Authentication.

Authentication framework is vital to identify as it ensures that the participants in the network is as same

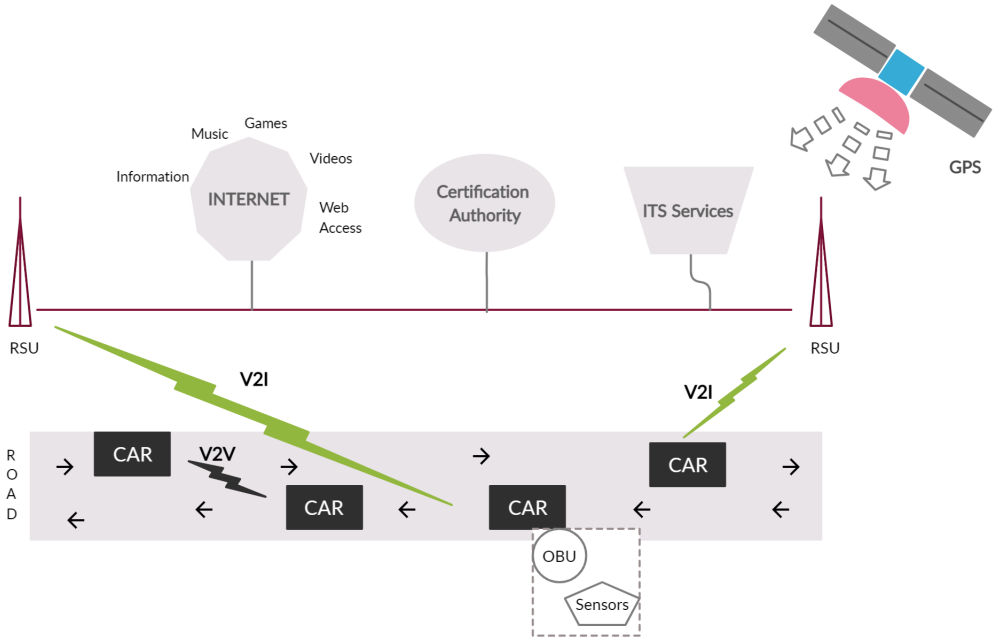

Figure 1: Architecture of VANET

as it claim to be. It also certifies that authenticated vehicle gain all the privilege provided by VANET.

Integrity.
Integrity of the messages should be preserved *i.e.* transmitted messages are prohibited to alter in the transmission medium [19].

Availablity.
Network resources should be available even in the time of failure and in the presence of malicious node. Availability of the network is directly related to all the other security attributes. Even in the worst case, network should be available and run efficiently.

Confidentiality.
Confidentiality is not to share private information with adversaries. Not every message in the network needs to preserve confidentiality but messages containing information like session key, payment data, OTP needs to be secure and guard confidentiality. Requirement of confidentiality is needed when transmitting some data or when multiple node comes in-group communication. In both the cases if confidentiality breaks then malicious vehicle may take maximum privilege of the network or may damage the network integrity and availability.

Non-Repudiation.
Non-Repudiation assures that someone cannot deny the validity of something. Typically nonrepudiation refers that sender of the message cannot deny the authenticity of their signature on a message. It is important to resolve dispute about who transmitted this message.

Privacy.
Most of the information about the nodes are broadcasted publicly in VANET so it is necessary to maintain privacy. Communication in the network should be anonymous and message sent by authorized vehicle should be protected in the presence of unauthorized observer *i.e.* authenticated nodes/vehicles have right to access personal information [17]. Contrarily adversaries may collect and analyze information, fix up a trap and harm the user.

Scalability.
Scalability refers to the capacity of a network to manage the growing vehicles and network. Scalability often refers to the stability of the network so that network performance will be not disrupted or degraded even in the worst case.

3 Classification of Attackers

In this section, we classified the attackers based on its behaviour, nature and efficiency. Efficiency of all attacks depends on the capacity of attackers [16, 22, 28]. Therefore, before discussing attacks it is essential to know about the type of attackers as shown in Figure 3.

Active vs. Passive.
Some attackers do not transmit or receive any message on the network, though they eavesdrop on the wireless network to gain knowledge about the pattern and frequency of the data transmission and use this earful information in future. These attacks are done by Passive Attackers, on the contrary, Active

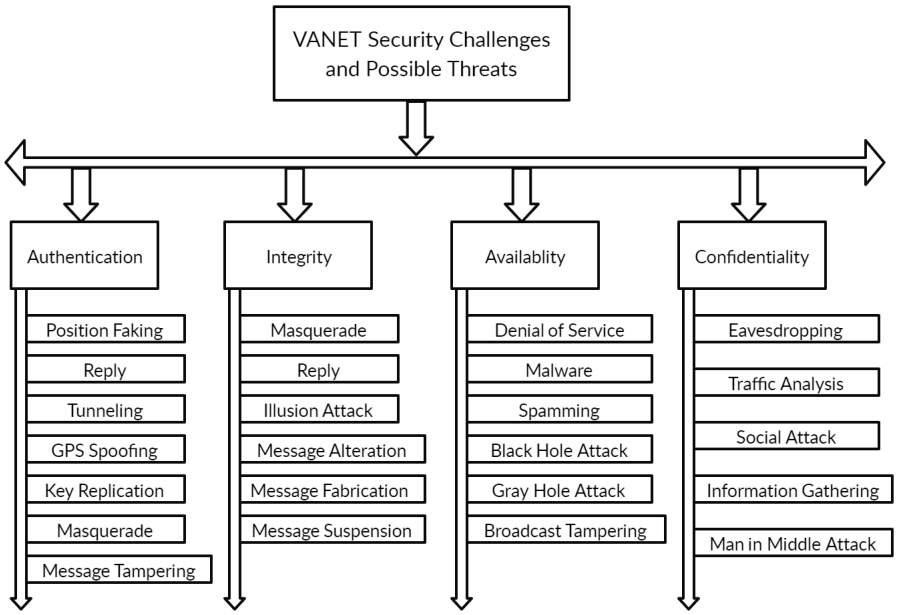

Figure 2: VANET Security Challenges and possible attacks

Attackers alter the information it receives, generate false signals, do not forward received packets, apply modification in data stream to disrupt the efficiency of the network or to gain access of unauthorized services.

Insider vs. Outsider.
An attacker may be an authorized member of the network who has all the knowledge and access of the network, such attackers are known as Insider. While Outside Attackers (outsiders) are intruders, who do not have access to communicate directly to the insiders and can launch attacks of less variegation.

Malicious vs. Rational.
Not all attacks are launched to seek personal benefits; some attacks are launched to disrupt the performance of network and to create hurdle for the members of the network, these attackers are known as Malicious Attackers. On the other hand, Rational Attackers seeks personal benefits; attackers launch these attacks intentionally for specific node or for specific network.

Local vs Extended.
Local Attackers launch attack of limited scope and in limited control region/area. Whereas, attackers of extended class controls several entities, which are distributed across whole network. Extended class attackers have potential to degrade the performance of the network or shut down the entire network.

4 Sybil Attack

VANET works on wireless environment, due to which it is vulnerable to many types of the security attacks. Because of the unique nature of VANET, it adds additional vulnerability and complexity in order to create a secure network. There were many threats possible on VANET but in this paper, we will focus on Sybil Attack as it is the root cause of many attacks and security threats. Sybil attack was first introduced and illustrated by Douceur in context to Peer-to-Peer Network [7, 26].

Sybil attack is a threat against security of a network. As malicious vehicle, impersonate multiple legitimate identities by forging new identity or by stealing identities from vehicles of the network. Attackers steal identities of other vehicles by eavesdrop broadcasting messages, as the vehicle are highly mobile in nature, density of network changes dynamically, network topology also changes dynamically so vehicles continue to communicate with other in order to update their routing tables. Attackers take the advantage of these properties and impose Sybil attack over the vehicles of the network and create the illusion of presence of multiple legitimate vehicles in the network. In the Figure 4, victim vehicle (green node) is surrounded by multiple Sybil vehicle (black nodes) that can block all the transactions by performing attack it receives access over the vehicle.

Sybil vehicle have potential to influence the functioning of the services of VANET like update routing table, voting, fair resource allocation, misbehavior detection, data aggregation, *etc.* By imposing Sybil attack, attacker takes over the control of network and may inflict other attacks such as black hole attack, timing attack, denial of service attack, impersonation attack and others.

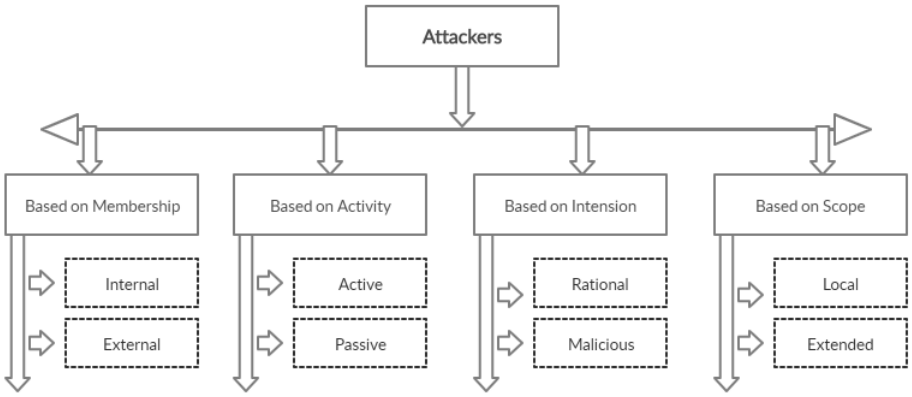

Figure 3: Attackers classification

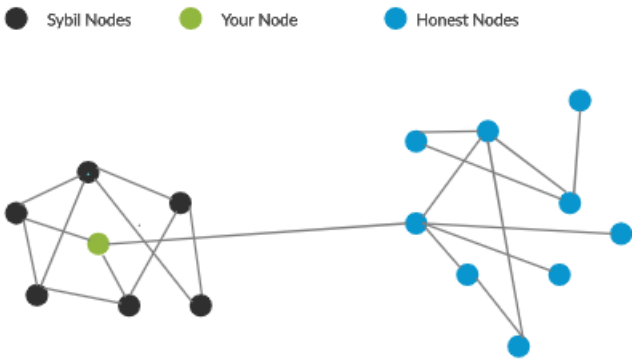

Figure 4: Sybil attack

For Example: Suppose a vehicle on highway significantly reduced its speed and broadcast a warning message. Recipients of the message will reply it and further broadcast that message. However if there are Sybil vehicles, then those Sybil vehicles can deny to reply and broadcast (DOS attack). This can invert the proper functioning of the network and create a massive pileup on the highway and serge loss of life. In addition, Sybil vehicle in network can impose any attack on the vehicle or network.

5 Analysis of Defence Mechanism

We know that there is no logical central authority for the efficient functioning of VANET, many protocols award unique identity to vehicles and then apply security rules and measures to defend from Sybil attack [5]. Although researchers proposed different mechanism to secure network from Sybil Attack:

1) Resource testing method;
2) Position verification method;
3) Domain specific;
4) Trusted devices;
5) Trusted certification method;
6) Neighbor list method.

5.1 Resource Testing Method

This method is used to detect Sybil attack. Resource testing method test vehicle resources, *i.e.* radio resource, memory resource, identification resource and computational resource. It is assumed that every vehicle is equipped with limited computational resources. In this method, a typical puzzle is distributed to the vehicle of the network in order to check the computational ability of vehicles. A Sybil attacker vehicle also receives the puzzle for computation but because of handling multiple identities with limited computational resources, it is impossible for Sybil vehicle to perform additional computation. This approach is based on assumption that every vehicle has same and limited computational resources but there is a chance that Sybil vehicle may have additional computational resources. Therefore, this method is not suitable for the detection of Sybil attacker.

5.2 Position Verification Method

Sybil attack detection using position verification method is based on the fact that a vehicle can present only on one position at a time. In this method physical location of any vehicle is to be verified before the data transmission. Network transmits a request message to all the vehicles of the network. All vehicles on the network are bound to respond that message; here Sybil vehicle also transmits their position coordinates. As network receives exactly same geographical coordinates from multiple vehicles which reflects that a particular vehicle is behaving like a Sybil vehicle and after the detection of Sybil vehicles network takes necessary action for the elimination of Sybil vehicle from the network.

5.3 Domain Specific

Some researches proposed Sybil attack detection in light of domain. Proposed Sybil attack detection mechanism is based on the location/geographical position of vehicles. If an attacker vehicle having single device and attacker starts performing Sybil attack then all the Sybil vehicles move together in specifically same fashion with same speed in a specific domain. In this way, network track down the trajectory and pattern of the Sybil vehicles and generate alert signal. However, this method is sufficient to track the Sybil vehicles having unary device but this method is not efficient against malicious vehicles having multiple devices.

5.4 Trusted Devices

In this method, trusted devices are combined with trusted Certificates, the binding of hardware with vehicles restrict vehicles to obtain multiple false keys. This method is sufficient to secure the network from Sybil attack, but it pushed an overhead of installation of extra hardware in vehicles, another issue is that there is no such efficient mechanism that restricts vehicle from obtaining multiple trusted devices except the manual interaction.

5.5 Trusted Certification

Trusted Certification is the most commonly used solution for the prevention of Sybil attack due to its ease of implementation and potential to remove Sybil attack from the network. In this method, a third party certification authority is responsible for issuing identities and Centralized authority assigns these identities to vehicles. Centralized authority also ensures the uniqueness of certificate for every vehicle. There is no such mechanism for issuing unique identities to every vehicle; it is to be done manually. There is no big deal in issuing certificate but it creates a bottleneck in large scale system, another issue is to manage a database for used, unused, lost and stolen identities. Because of these issues, it is difficult to implement this mechanism although this mechanism is efficient and removes the headache of installation of new hardware in vehicles.

5.6 Neighbor List Method

Author proposes a new method for the detection of Sybil vehicle using list of neighbor vehicle. This approach is based on assumption that if a vehicle is observing same neighbor vehicles simultaneously for long duration of time, that means there must be a Sybil vehicle. In order to obtain information about neighbor vehicles, every vehicle keeps exchanging their information with neighbors and vehicle create list of neighbor vehicles. This scheme is complex as after every time interval (T1, T2, T3..) vehicles share list of neighbor vehicle to detect Sybil vehicle. Here intersection operation is performed on the list of neighbor vehicles generated at different intervals and mark suspected vehicles *i.e.* particular vehicle is neighbor vehicle for seamlessly long duration of time. This approach put an extra overload by sharing list of neighbor vehicles but sill fails to detect Sybil vehicle in some cases.

Case 1: Suppose a vehicle in a network refuses to share a list of neighbor vehicle.

Case 2: Sybil vehicle claims itself as not a neighbor vehicle of any vehicle. In both the cases, intersection operation failed to detect suspected vehicles, as there is no mechanism that bound vehicles not to perform these malicious activities [4, 27].

6 Comparative Study

6.1 Resource Testing Mechanism

Resource Testing Mechanismwas not sufficient to detect and prevent Sybil attack, as it is restricted to identify fake identities and in some case it fails when attacker will equip its vehicle with extra computational equipment.

6.2 Position Verification

Position Verification mechanism requires extra hardware instead, there is no such guarantee that all the vehicles are legitimate. Any attacker vehicle may change its geographical coordinates and forward that information, in that case there is no such mechanism to identify and track down the actual geographical coordinates of vehicles.

6.3 Domain Specific

Domain Specific is a better technique to detect attacker vehicles although it gets restricted and generates falsie result in case when vehicle creates its replica.

6.4 Trusted Devices

Trusted Devices requires installation of extra hardware that increases the cost of vehicles but there is no central authority, which makes sure that every vehicle is equipped with only one trusted device. By the reason there are several chances of a vehicle, equipped with multiple trusted devices and in that scenario Trusted Device mechanism fails to detect and eliminate Sybil vehicles.

6.5 Trusted Certification

Trusted Certification mechanism requires a huge amount of data transmission in order to validate a vehicle. This mechanism blindly relies on the third party who is issuing certificate to vehicles moreover if Sybil attacker directly attacks over the certification authority then the whole system shuts down, consequently attacker can gain full privilege of the VANET. Another issue is this, that there

is no proper mechanism to identify lost and stolen certificates, because of this, identification of false certificate requires a good amount of computation power and time.

6.6 Neighbor List Method

Neighbor List Method was not sufficient when Sybil vehicles refused to participate or transmit false data to the leader vehicle. Another issue was that Neighbor list method requires a lot of computation power and by the time there are great chances for an attacker to commit an attack, disrupt the whole system and leave the network.

7 The Proposed Schema

In this section, we proposed a method to detect Sybil attack. Proposed schema used timestamp mechanism for the detection of Sybil vehicle in VANET. This mechanism is ideal for less number or average number of vehicles. As we know there were number of limitations in VANET *i.e.* confidentiality, integrity, repudiation *etc.* Therefore, the proposed mechanism is designed keeping all these issues in knowledge.

Way for the detection and elimination of Sybil vehicle, we used timestamp mechanism. Time Stamp is a unique certificate, which is provided by Road Side Unit (RSU) to all the vehicles on the road that want to take privilege of VANET. Time stamp is a unique identity but here we assume time stamp as a Hash Function of Public key and for the sake of security, only RSU know the Hash key and has authority to generate, assign time stamp to requesting vehicles.

It is to be assume that

1) Certification Authority (CA) assigns some unique public key to manufacturers and manufacturers assign these keys to vehicles, which is hard-coded into vehicles communication device. In this way, every vehicle receives a registered unique public key.

2) It is impossible for a vehicle to pass from multiple RSU at same time.

Taking these assumptions in knowledge, we start our workflow for the detection of Sybil attack and later we will provide pseudo code of our proposed mechanism.

Vehicular Ad-hoc Network is a secure network *i.e.* without complete authentication and verification, vehicles are not allowed to access VANET services. For the initial authentication purpose, vehicles transmit its public key (Pki) to RSU, as vehicles enter into VANET environment.

RSU authenticate public key from Certification Authority (CA): As Certification Authority has a list of all keys issued to vehicles. If Certification Authority sends an acknowledgement (ACK) to RSU then RSU will generate Time stamp (hash function of requesting vehicle public key) and issue a Time stamp to vehicle. On the flip side if Certification Authority issue Negative Acknowledgement (NAK) to RSU, then RSU wont issue Time Stamp and block the request for specific period of time, still if RSU continuously receives request message from same public key then RSU mark requesting public key as suspected key, generate an alert message and broadcast that public key as suspected key.

As soon as vehicle receives Time Stamp issued by RSU, vehicles get license to access VANET services and communicate with other vehicles. For the communication VANET vehicles are bound to insert its own Time stamp into message packet and update hop count.

Table 2: List of Timestamp assigned

S.No	Public Key	Timestamp (hash function of Public key)
1	ck1213n	dkjj1152cmwchb
2	zzaj132	bbdcdc55155njd
3	.....	.....
.	.....	.....

When any vehicle receives the requesting packet, it finds out for the destination into its routing table and responds if destination is found otherwise intermediate vehicle/this vehicle decreases the hop count, update its timestamp, public key into message packet and flood the packet into network. As soon as destination is found, destination vehicle inserts its own time stamp into message packet and revert the message to the source vehicle. By the time, search packet is on the network source vehicle wait for respond only for time interval t (varies with protocol) if source vehicle will not receive the respond within time, it will rebroadcast the request message. On the other hand if source vehicle receives the respond (that enclose vehicle id and time stamp of all intermediate vehicles) it will forward vehicle id and time stamp of destination vehicle to RSU. As we saw earlier only RSU keeps mapping public key of requesting vehicle so it maintains the table of time stamp assigned to corresponding public key. As soon as RSU receives Public Key and Time stamp from source vehicle it will look for its table of assigned time stamp to respective public key as shown in Table 2. If timestamp is same as assigned by RSU to corresponding public key, RSU forward acknowledgement packet to source vehicle and source vehicle start transmitting message via same intermediate vehicles. If RSU send negative acknowledgement then source vehicle discard the message packet and again flood fresh request query for the destination.

When destination receives the message from the source vehicle, it will not directly accept that message packets although destination vehicle forward the list of source vehicle and intermediate vehicles public keys with their corresponding time stamp to RSU, if all the time stamps are

valid as assigned by RSU then RSU forward the acknowledgement to destination consequently destination vehicle receives/process all the messages.

Assuming that while matching, RSU founds any timestamp which would not assigned by any RSU to specific public key or RSU founds similar public key with multiple timestamps or vice versa in all these cases RSU forwards negative acknowledgement to Destination vehicle, mark that public key as Sybil Vehicle, generate alert and forward the updated list of Sybil Vehicles to neighbor RSU. Destination vehicle discard all the messages and forward the request for the retransmission of messages.

By using this mechanism we validate all the vehicles involve in communication *i.e.* source, intermediate and destination vehicles and eradicate all the malicious vehicles meanwhile we authenticate the integrity and confidentiality of the messages send and received. At end we identified the Sybil vehicles and block the vehicles for the future perspective.

Suppose a vehicle ($V_i = S_0$) wants to communicate with other vehicle ($V_j = DS_1$), then source vehicle (V_i) search for destination in its routing table. For an instance, destination (DS_1) founds then source vehicle (V_i) authenticate the validity of Destination vehicle through RSU if RSU forward Acknowledgement (ACK) then Source vehicle encrypt the request message and transmit the message to Destination vehicle (DS_1). If destination not found, then source vehicle (V_i) appends its public key (Pk_i), Time stamp (T_i), Hop Count (HC), Destination address in request message and rebroadcast the request message to neighbor vehicles. Neighbor vehicle checks its routing table, if there is an entry of destination vehicle (DS_1) or neighbor vehicle itself is a destination vehicle then in both the case respective vehicle replies to Source Vehicle (V_i) about the path otherwise neighbor vehicle append its public key (Pk_k), Time stamp (T_k), decrease the hop count value and broadcast again to its neighbor vehicle. This process continues until destination is not found or value of hop count becomes zero.

As destination vehicle (DS_1) receives the request message, decrypt the packet using its private key and start the request packet authentication process. As we know every request packet contains public key and timestamp of all intermediate vehicles, so destination vehicle transfers list of public keys and time stamps to RSU. As RSU issued time stamp to vehicles, so it maintains a data base of time stamp issued to public key of vehicles. RSU compares the list of time stamp and public key forwarded by destination vehicle with its own time stamp issued to respective public keys. If RSU found all legal timestamp issued to public key, it replies Acknowledgement (ACK) to destination vehicle (DS_1). Moreover, in case RSU founds some illegal/wrong time stamp over corresponding public key, RSU replies Negative Acknowledgement (NAK) to destination (DS_1) and mark the public key as Sybil vehicle, add the malicious public key in list of suspected vehicle, generate alert and transmit the updated list of suspected vehicle to all their neighbors. If Destination vehicle receives NAK (form RSU), then it discards the request message and request for the retransmission of that message.

Only when destination vehicle (DS_1) receives the Acknowledgement (ACK) message form RSU, then destination receives the message and process that message sent by source vehicle.

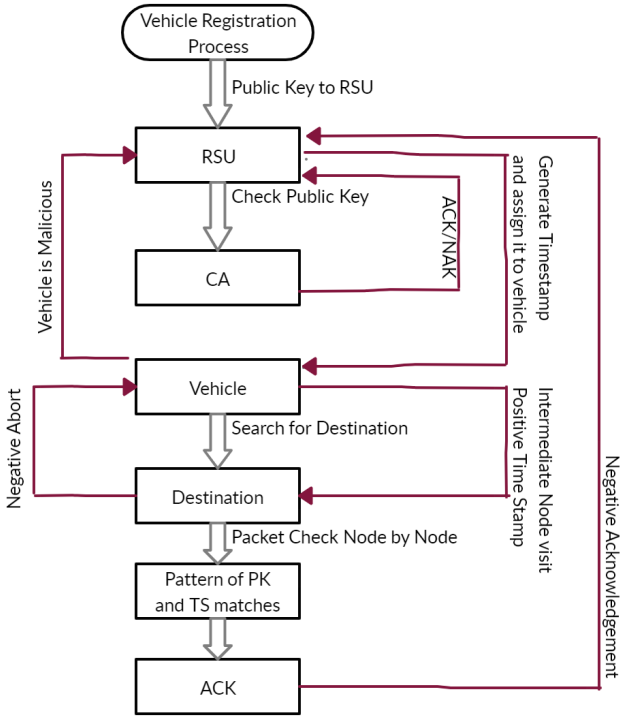

Figure 5: Flowchart of Proposed algorithm

7.1 Update Time Stamp

For the communication in VANET, vehicles are bound to have time stamp so as vehicles enters into VANET environment RSU issues time stamp over its public key and RSU update the database of time stamp issued. Usually vehicles are in mobile fashion and passes from multiple RSUs but it not possible to pass from multiple RSUs at a time interval. When a new vehicle crosses a RSU, vehicle forward its public key to RSU, RSU authenticate the public key from Certification Authority (CA), if RSU receives ACK from CA then RSU generates hash function from public key and forward the hash function as assigned time stamp to the requesting vehicle. Otherwise, RSU generate an alert and mark the public key as suspected vehicle. Suppose that a previously registered vehicle crosses new-RSU in such case vehicle forward time stamp and public key to new-RSU, as we know neighbor RSUs have list of timestamp issued over public key. Thus new-RSU authenticate the time stamp issued by previous-RSU and this authentication will take place via neighbor

RSUs, if authentication is successful then new-RSU issues new time stamp and assigns new time stamp to requesting vehicle, in the mean while new-RSU update the list time stamp issued and forward the list of updated time stamp to neighbor-RSUs. In the same way, every vehicle gets authenticated and receive updated time stamp. This process is also helpful in rectifying Sybil vehicle as this process issues only one time stamp to authenticated public key so when Sybil vehicle insult false public key, RSU generate an alert and mark the public key/ vehicle as suspected public key/vehicle.

Figure 5 shows the flowchart of proposed algorithm for the detection and elimination of Sybil vehicle.

7.2 Algorithm

Table 3 shows the pseudonym of notations used in Algorithm 1.

Table 3: Notations used in this paper

S.No	Notation	Comments
1.	V_i	ith vehicle
2.	RSU_j	jth RSU
3.	ACK	Acknowledgement message
4.	NAK	Negative Acknowledgment
5.	Pk_i	Public Key of Vehicle i
6.	S_0	Source Vehicle
7.	DS_1	Address of Destination Vehicle
8.	RT	Routing Table
9.	T_i	Time Stamp of Vehicle i
10.	HC	Hop Count
11.	PKT	Message Packet
12.	&&	Logical AND
13.	11	Logical OR

8 Simulation Results

Network Simulator 2 (NS2) is the most widely used simulator tool in academics and industry in order to perform real time analysis.

For the simulation purpose, we use Network Simulator 2 as this is the one of the most powerful simulator tool to carryout network experiments. NS2 was developed in year 2000 to analyze the performance of Congestion Control Network in TCP [31]. Still NS2 is a powerful tool used to simulate and analyze the performance of network based on various parameters *i.e.* packet loss, throughput, delay and many others. NS2 is a product of NS and it is object oriented, event driven simulator supporting C++ and TCL/OTCL languages [12, 24].

In order to detect Sybil vehicle we implement the proposed algorithm over Network Simulator 2 (NS2). For vehicle discovery and data transmission, we use Ad-Hoc On-demand Distance Vector Routing Protocol (AODV).

Algorithm 1 Working of Proposed Methodology

1: Begin
2: for i=1 to p
3: $s_i \varepsilon V$
4: **if** $V_i \varepsilon VANET(Servics)$ **then**
5: $V_i -> RSU_j(Pk_i)$
6: $RSU_j -> CA(Pk_i)$
7: **else if** $CA -> RSU_j(Pk_i) : ACK$ **then**
8: RSU_j issues Timestamp (T_i) to V_i
9: **else if** $CA -> RSU_j(Pk_i) : NAK$ **then**
10: RSU_j marks vehicle as Sybil and generates alert.
11: **end if**
12: **if** $V_i = S_0$ **then**
13: look for destination.
14: Goto Step 17.
15: **end if**
16: Repeat Step 34 while DS_1 *not found* && $HC == 0$
17: **if** $DS_1 \varepsilon RT(S_0)$ **then**
18: $PKT = Pk_i \ Ti \ DS_1 \ HC$
19: Message PKT send to DS_1
20: **else if** while (HC =! 0) **then**
21: forward request message to neighbor for DS_1
22: **else if** $V_k \ DS_1 \ || \ DS_1 \ \varepsilon \ RT(V_k)$ **then**
23: reply $PKT = Pk_iT_iDS_1HC, Pk_rT_r \cdots Pk_kT_k$
24: **else**
25: forward request message to neighbor for DS1
26: $S_i - > RSU_k(Pk_j, T_j)$
27: **end if**
28: **if** $RSU_k - > S_i(ACK)$ **then**
29: Destination Identified and Secure: Start data Transmission
30: **else**
31: $RSU_k -> S_i(NCK)$
32: Destination Identified but not Secure: Discard Packet: Forward fresh search packet for Destination
33: **end if**
34: **if** $PKT \varepsilon DS_1$ **then**
35: for $i = 1$ to $i = z$
36: **if** $(Pk\_i, \ Ti \ == \ RSU_i(Pk\_i, \ Ti))$ **then**
37: $RSU_j -> DS_1(ACK)$
38: **end if**
39: **else**
40: $RSU_j -> DS_1(NAK)$
41: **end if**
42: **if** RSU_j *send* $ACK(DS_1)$ **then**
43: goto Step 17
44: **else if** $RSU_j -> DS_1(NAK)$ **then**
45: i. Sybil vehicle is detected.
46: a. mark vehicle as Sybil vehicle.
47: b. generate alert in network.
48: ii. Request sends to destination vehicle for the retransmission of request message.
49: **end if**
50: End

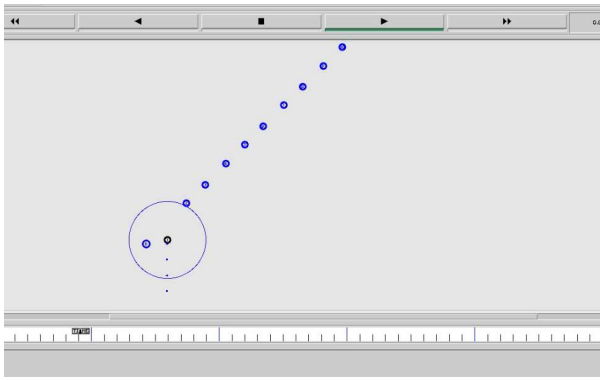

Figure 6: Detection of Sybil vehicle in VANET

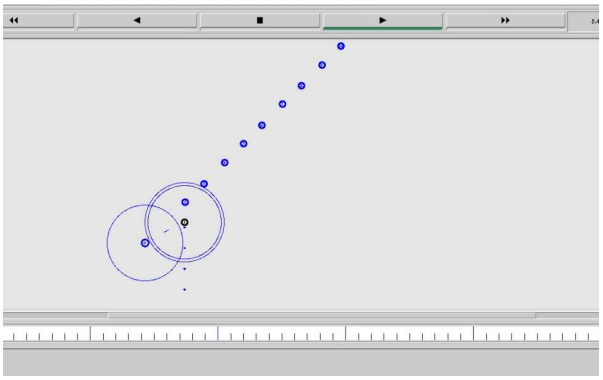

Figure 7: Detection of sybil vehicle in VANET

Where every non-falsie vehicle follows AODV protocol whereas falsie vehicle violates the principle of AODV Protocol and perform malicious behavior in network. Our work is based on real time traffic as explained earlier for that NS is most suitable simulator to implement that.

First of all we have deployed network on NS3 simulation tool. We have injected Sybil vehicle 1 in the network. We have implemented network of 15 vehicles as shown in Figure 6. We have applied AODV algorithm for routing of packets from source to destination. In VANET each vehicle has a unique address to participate in routing and there is no central authority to verify vehicles. Malicious vehicles may use different address for Route request (RREQ) and Route reply (RREP). In this work author have identified and detected vehicle 1 as malicious using proposed time stamp based algorithm in VANTE as shown in Figures 6-10.

In the proposed work RSU issued time stamp to all the vehicles and maintain a data base of time stamp issued to public key of vehicles. RSU compares the list of time stamp and public key forwarded by destination vehicle with its own time stamp issued to respective public keys. If RSU found all legal timestamp issued to public key, it replies Acknowledgement (ACK) to destination vehicle (DS_1).

Moreover, in case RSU found some illegal/wrong time stamp over corresponding public key, RSU replies Negative Acknowledgement (NAK).

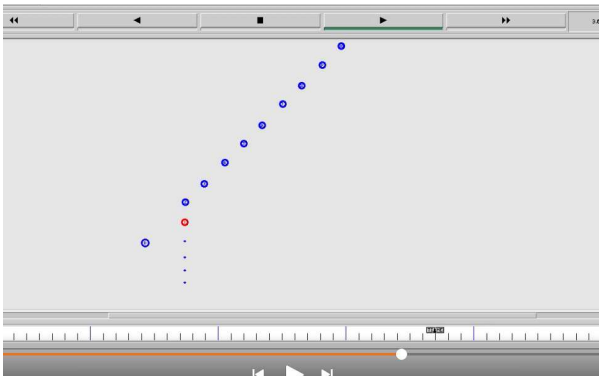

Figure 8: Detection of sybil vehicle in VANET

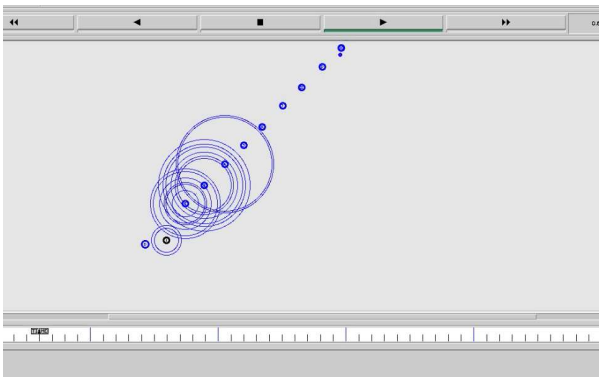

Figure 9: Detection of sybil vehicle in VANET

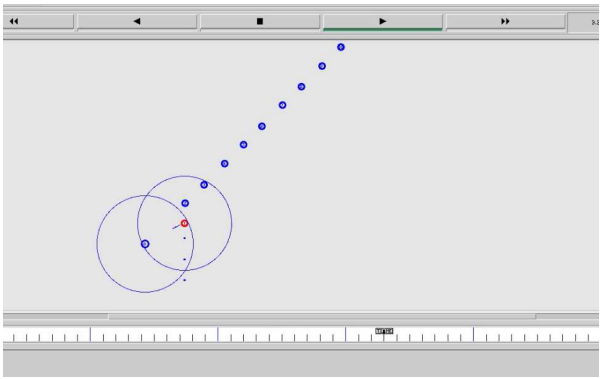

Figure 10: Detection of sybil vehicle in VANET

9 Future Work

In future work we would like to extend our work and create a network where it will be impossible to perform Sybil attack. In addition, we would like to design algorithms and examine our work for more than one Sybil vehicle and perform simulation over real time traffic model. In our future work, we will also try to build an automatic model to establish reliable relationship among components of VANET.

Acknowledgments

This study was supported by Shri Ramswaroop Memorial University of Lucknow, Uttar Pradesh, India. I would like to express my special thanks to my supervisor (Dr.Taskeen Zaidi) without her support this research paper would not be possible.

References

[1] T. W. Chim, S. Yiu, L. C. K. Hui and V. O. K. Li, "VSPN: VANET-based secure and privacy preserving navigation," in *IEEE Transactions on Computers*, vol. 63, no. 2, pp. 510–524, Feb. 2014.

[2] A. Daeinabi, A. G. Rahbar, "An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks," *Computers & Electrical Engineering*, vol. 40, no. 2, pp. 517–529, Feb. 2014.

[3] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and challenges in intelligent vehicle area networks," *Communications of the ACM*, vol. 55, no. 2, pp. 90–100, Feb. 2012.

[4] S. M. Faisal, A. K. Vajpayee, "Extended zone routing protocol," *International Journal of Computer Sciences and Engineering*, vol. 5, no. 5, May 2017.

[5] J. Farooq, M. S. Alouini, *et al.*, "A stochastic geometry model for multi-hop highway vehicular communication," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 2276-2291, 2016.

[6] J. Grover, M. S. Gaur, V. Laxmi and N. K. Prajapati, "A sybil attack detection approach using neighboring vehicles in VANET," in *Proceedings of the 4th International Conference on Security of Information and Networks*, pp. 151-158, 2011.

[7] J. Grover and V. Laxmi and M. S. Gaur, "Attack models and infrastructure support detection mechanism for position forging attack in vehicular adhoc networks," *CSI Transactions on ICT*, vol. 1, no. 3, pp. 261–279, Sep. 2013.

[8] S. Han, D. Ban, W. Park and M. Gerla, "Localization of sybil nodes with electro-acoustic positioning in VANETs," in *IEEE Global Communications Conference*, pp. 1-6, 2017.

[9] J. P. Hubaux, J. Luo , S. Capkun, "The security and privacy of smart vehicles," *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 49-55, 2004.

[10] M. Inam, Z. Li, A. Ali, and A. Zahoor, "A novel protocol for vehicle cluster formation and vehicle head selection in vehicular ad-hoc networks," *International Journal of Electronics and Information Engineering*, vol. 10, no. 2, pp. 103–119, 2019.

[11] M. Ivanov, F. Brännström, A. G. i Amat, P. Popovski, "Broadcast coded slotted ALOHA: A finite frame length analysis," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 651-662, 2016.

[12] J. P. Jeyaraj and M. Haenggi, "Reliability analysis of V2V communications on orthogonal street systems," *IEEE Global Communications Conference*, pp. 1-6, 2017.

[13] Z. Jianhong, X. Min and L. Liying, "On the security of a secure batch verification with group testing for VANET," *International Journal of Network Security*, vol. 16, no. 4, pp. 313–320, July 2014.

[14] M. Khabazian, S. Aissa and M. Mehmat-Ali, "Performance model of safety message broadcast in vehicular ad hoc network," *IEEE Transactions On Intelligent Transportation Systems*, vol. 14, no. 1, pp. 380–387, Mar. 2013.

[15] T. Kimura and H. Saito, "Theoretical interference analysis of inter-vehicular communication at intersection with power control," in *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM'16)*, pp. 3–10, 2016.

[16] X. Liu, X. Zhang, M. Jia, L. Fan, W. Lu, X. Zhai, "5g-based green broadband com-munication system design with simultaneous wireless information and power transfer," *Physical Communication*, vol. 28, pp. 130-137, 2018.

[17] Z. Na, X. Li, X. Liu, *et al.*, "Subcarrier allocation based simultaneous wireless information and power transfer for multiuser OFDM systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, pp. 148, 2017.

[18] S. Park, B. Aslam, D. Turgut and C. C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support," in *IEEE Military Communications Conference*, pp. 1-7, 2009.

[19] A. Rakhshan and H. Pishro-Nik, "Improving safety on highways by customizing vehicular ad hoc networks," in *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2017-2026, Mar. 2017.

[20] A. Rana, D. Sharma, "Mobile ad-hoc clustering using inclusive particle swarm optimization algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 1-8, 2018.

[21] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, vol. 25, no. 8, pp. 1557–1568, 2007.

[22] D. Sam, C. Velanganni, T. E. Evangelin, "A vehicle control system using a time synchronized Hybrid VANET to reduce road accidents caused by human error," *Vehicular Communications*, vol. 6, pp. 17-28, Oct. 2016.

[23] G. Samara, W. A. H. Al-Salihy and R. Sures, "Efficient certificate management in VANET," *The 2nd International Conference on Future Computer and Communication*, vol. 3, pp. 750-754, 2010.

[24] P. Sarkar, C. Kar, B. Sen and K. Sharma, "Sensitivity analysis on AODV with Wormhole attack," *The 2nd International Conference on Next Generation Computing Technologies (NGCT'16)*, pp. 803-807, 2016.

[25] A. K. Sharma, S. K. Saroj, S. K. Chauhan and S. K. Saini, "Sybil attack prevention and detection in vehicular ad hoc network," in *International Conference on Computing, Communication and Automation (ICCCA'16)*, pp. 594-599, 2016.

[26] P. K. Singh, S. Sharma, S. K. Nandi, S. Nandi, "Multipath TCP for V2I communication in SDN controlled small cell deployment of smart city," *Vehicular Communications*, vol. 15, pp. 1-15, 2019.

[27] A. Tassi, M. Egan, R. J. Piechocki and A. Nix, "Modeling and design of millimeter-wave networks for highway vehicular communication," in *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10676-10691, Dec. 2017.

[28] United States Department of Transportation, National Highway Traffic Safety Administration, Traffic safety facts, 2015. (`https:\//crashstats.nhtsa.dot.gov/\#/DocumentTypeList\\/11`)

[29] L. Xiao, L. J. Greenstein, N. B. Mandayam and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," in *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 492-503, Sep. 2009.

[30] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," in *Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS'06)*, pp. 1-8, 2006.

[31] T. Zaidi and S. Faisal, "An overview: Various attacks in VANET," *The 4th International Conference on Computing Communication and Automation (ICCCA'18)*, pp. 1-6, 2018.

Biography

Syed Mohd Faisal is a research scholar in department of Computer Science and Engineering at Shri Ramswaroop Memorial University, Lucknow, India. Syed Mohd Faisal is also working as Assistant Professor in Department of Computer Application at Integral University. His area of interest is Wireless sensor Network, Computer Networks and Cloud Computing.

Dr. Taskeen Zaidi is working as an Assistant Professor in department of Computer Science and Engineering at Shri Ramswaroop Memorial University. Her area of interests is Software engg., Cloud Computing, Distributed computing and Ad-hoc networks.