Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 5, May-2016

Network Security issues in IVC

Rudrappa B. Gujanatti[1], Azilda Rodrigues[2], Rewati Bad[3], Arun Tigadi[4], Sachin Urbhinatti[5]

[1]Department of ECE, KLE Dr. MSSCET, Belgaum, India
[2]Department of ECE, KLE Dr. MSSCET, Belgaum, India
[3]Department of ECE, KLE Dr. MSSCET, Belgaum, India
[4]Department of ECE, KLE Dr. MSSCET, Belgaum, India
[5]Department of CSE, TKIET, Warnanagar, India

Abstract — Vehicular Ad-hoc Networks (VANETs) have unfolded recently as one of the most attractive topics for researchers and the automotive industries because of their tremendous potential to improve traffic safety, efficiency and other added services. However, the VANETs are themselves quite vulnerable against attacks that can directly lead to the corruption of networks and then provoke big losses of time, money, and even lives. This paper presents a survey of VANETs attacks and the solutions in carefully considering the other similar works as well as the updating of new attacks and categorizing them into different classes.

Keywords- Vehicular Ad -hoc Networks (VANETs), Security, Privacy, VANETs Attacks

I. INTRODUCTION

In vehicular networks, security has always been an issue which must be seriously considered and the design and implementation for security infrastructure must be carried out in such networks. An attacker can inject false and invalid traffic messages to distract drivers from choosing a specific route, or can use the network to determine a driver's identity or his location. On the other hand, by gaining unauthorized access in network, an attacker can gain the control of critical components of a vehicle that can cause irreparable damage to its passengers or the vehicle that is being used.

In VANET, one of the main challenges is to route the data efficiently from the source to the destination. Designing an efficient routing protocol for a VANET is a very tedious task. Also because of wireless medium it is vulnerable to several attacks. Security is mandatory since the operations of the network have been misled by the attackers, for the successful deployment of such technology.

There are several applications of the vehicular networks which have been discussed by manufacturers and also academics which will be leading to both time and money saving. There are numerous solutions and methods available in order to improve the efficiency, privacy and security of these networks. However, the security, has always been a major issue in vehicular networks which must be seriously taken into consideration and an effective and efficient security infrastructure has to be designed and implemented in these networks.

II. RADIO BANDS USED IN IVC

This section discusses the different frequency bands that can be made use of in IVC. The Bluetooth and Ultra-Wideband (UWB) technologies are explored in detail. It is possible for communicating vehicles to use both infrared and radio waves. For instance, 75 MHz is allotted in the 5.9 GHz band for dedicated short range communication (DSRC). It is also possible to use Bluetooth, which operates in the 2.4 GHz industry, science and medicine (ISM) band, to allow the communication between two vehicles. It is reliable up to a speed of 80 km/h and range of 80 m. However, it may take up to 3 secs to establish the communication. Also, as Bluetooth uses a master and slave setup, the master is likely to refuse a communication request. Moreover, the master may already be communicating with another slave, which could lower the communication rate.

An alternative to the use of Bluetooth is a radio frequency technique called UWB. Because UWB has a wideband nature it has been used in radar applications. The major advantages of UWB technology are high data rate, cost effective, and immunity to interference. On the other hand, it could also interfere with other possible radio services, for example, the Global Positioning System (GPS). As the bit error rate (BER) is low, the coded Gaussian pulses waveform is considered to be superior to monocycle pulses.

III. WAVE PROPOGATION SIMULATIONS IN IVC

This section analyzes different predictive models and techniques which can be utilized in Inter-Vehicular Communication. Direct and reflected waves are described, as well as multi-path components and ray tracing method.The 60 GHz band is used for inter-vehicle communication. Since a vehicle can communicate with other vehicles both in front and behind it, the line-of-power received in the LOS case, a 2-wave model can be used. The model consists of a direct wave and a wave that is reflected from the surface of the road. It determines the propagation loss on the path. The measurable distance between the sending and receiving antennas, as well as the height of the antennas, are variables considered in the model, but the non-uniformity of the road is not considered. This non-uniformity causes variations in the phase shift and the amplitude of the wave reflected from the road. This wave can be calculated by using a reflection coefficient which is determined from the complex refractive index of asphalt at 60 GHz (n=2-j0.05).

IV. MEDIUM ACCESS CONTROL (MAC) IN IVC

This section summarizes MAC protocol specifics as they are applied in IVC. The performance measurements have been reviewed, and several new concepts have been presented. An ad-hoc network between vehicles is suited well for vehicle communications than centralized service. Since information has to go from the vehicle to a nearby central base station and then back to another vehicle the centralized architecture proves to be not very efficient. Wireless connectivity between moving vehicles is provided by existing 802.11 compliant devices. Data rates of up to 54Mbps can be achieved effectively with 802.11a hardware.

Two vehicles with ORiNOCO IEEE 802.11b WLAN cards, and laptops running on Linux were used for these tests. An omni- directional antenna was mounted on the top of the cars to increase the range of the connectivity. The location and velocity of the cars also could be tracked using the GPS devices. One of the laptops is set as the sender of streaming User Datagram Protocol (UDP) packets, while the other is set up as the receiver. Each of the wireless cards are set to operate in broadcast ad-hoc mode. This mode disables MAC retransmissions. The sender then generates random bits in the UDP packets. For every second the GPS devices provide latitude, longitude, speed, and bearing.

V. SECURITY REQUIREMENTS

In order to have a dependable and secure vehicular network, a number of security requirements have to be considered. Some of these security requirements are the same for all networks but some are valid and specific to vehicular the networks only. Vehicular communications must be secured in all aspects with respect to the mentioned attacks and vulnerabilities. Here is a list of some general security requirements that must be taken into consideration in order to reduce vulnerabilities and attacks against VANETs.

As far as security requirements are concerned the applications of VANET are focusing on safety messaging, cooperative driving, toll application etc. Therefore, the integrity, liability of message and the liability of the user has to be protected and at the same time privacy has to be looked upon. A secure VANET system should satisfy following requirements.

5.1 Authentication

Despite the lack of confidentiality, network nodes must and have to be authenticated in order to be able to send the messages through the network. Before reacting to messages and events a vehicle must verify the legitimate sender and the messages sent by him, therefore there is a need for authentication. Without authentication, illegitimate and malicious users can introduce false messages into the network and confuse other vehicles by distributing false information. With authentication, the vehicles can simply drop the messages from unauthenticated.

5.2 Authorization

Authorization is a higher level implementation used by access control which itself is defined by network policies. Authorization describes the role of a node in the network which includes the types of messages a node can read or write in the network and the actions it is allowed to take and generally the protocols that it can execute.

5.3 Data Consistency

Along with authenticating the sender, the consistency of messages with similar ones regarding the time and the location must also be considered, because of false messages from legitimate senders are not impossible. It is immensely important for warning messages to meet the time and location constraints. A warning message has to be shown to the driver before it is very late to react and also before passing the corresponding geographic location of the warning.

5.4 Confidentiality

In Vehicular ad-hoc networks, the definition of confidentiality refers to “confidential communication”. In a group, none except the members in the group are able to decrypt the messages that are broadcasted to every member of group; and none except the dedicated receiver member is capable to decrypt the message devoted to it.

5.5 Integrity

It ensures that data or the messages that are delivered among nodes are not altered by attackers. This concept in VANETs commonly combines with the “authentication” concept to guarantee that: A node should be able to verify that a message is sent and signed by another node without being modified by anyone. In order to gain this property, Data Verification is required. Once the sender vehicle has been authenticated, the receiving vehicle performs a set of data verifications to check whether the current message contains the correct data or corrupted data.

5.6 Availability

The vehicular network should be available even if it is under an attack without affecting its performance. This concept of VANETs is not different from other kinds of networks but is not easy to ensure because of the mobility in high speed vehicles. The three main security requirements above, the following security aspects should be also satisfied in VANETs.

5.7 Privacy

The profile of the driver or a driver’s personal information must be maintained against unauthorized access. We must consider the two cases mentioned below: Communications between vehicles and RSUs: Privacy means that an eavesdropper is impossible to decide whether the two different messages come from the same vehicle. Communications between vehicles: Privacy means that determining whether the two different valid messages coming from the same vehicle source is intensely burdensome for everyone else except a legitimate component e.g, tracing manager.

5.8 Traceability and revocability

Although a vehicles genuine identity should be hidden from other vehicles, there still should be a component (e.g., Trace Manager) that has the ability to obtain vehicles real identities and to revoke them for future usage.

5.9 Non-repudiation

Drivers have to be reliably identified in case of accidents. A sender should have the mandatory responsibility in transmitting the messages for the investigation that will determine the correct sequence and the content of messages exchanged before the accident.

5.10 Real-time constraints

Since vehicles are able to move in randomly and quickly move out to a group of a VANET for a Short duration, the real-time constraints should be maintained.

VI. ATTACKS AND COUNTERMEASURES IN VANETs

In this paper, only the attacks perpetrated against VANETs communication are Considered. Physical problems (e.g., hardware tampering) are out of the scope of our research.

6.1 Sybil Attack

To perform this kind of attack, a vehicle declares to be several vehicles either at the same instant or in succession. This attack is extremely dangerous since a vehicle can claim to be in different positions at the same instant, thereby creating chaos and massive security risks in the network. The Sybil attack damages network topologies and the connections as well as the network bandwidth consumption. In Figure 1, an attacker A transmits a number of messages with different identities to the other vehicles. Thus the, other vehicles realize that there is currently a heavy traffic.

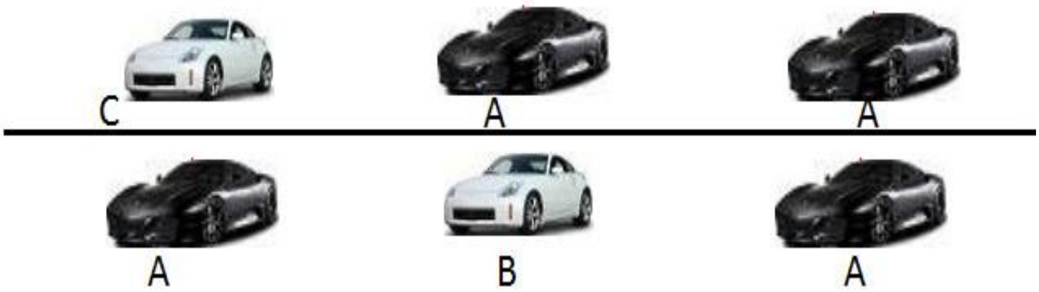

Figure 1. Sybil attack

In the traditional ad-hoc networks, there are three types of defenses against Sybil attacks introduced, namely registration, position verification, and radio resource testing. Registration itself is not enough to prevent Sybil attacks, as the malicious node has the possibility to register with multiple identities by non-technical means such as stealing. In addition, a stringent registration may lead to serious privacy troubles. In position verification, the position of nodes will be verified. The objective is to make certain that each physical node refers to one and only one identity.

The testing of the radio resource is based on the assumption that all physical entities are limited in resources. In order to verify that none of the neighbors is a Sybil identity, a node can assign each of its n neighbors a different channel on which it broadcasts certain messages. Then it further selects a channel randomly to listen. If its neighbor is legitimate, it will be able to receive the response from the corresponding channel. Otherwise, that must be a Sybil node. The detection rate arises if this test is repeatedly processed.

6.2 Bogus Information and Bush telegraph

The attacker executing the Bogus Information attack can be an outsider (i.e intruder) or an insider (legitimate user). The intension is to transmit incorrect or bogus information in the network for Personal advantage. For instance, an attacker may send a message announcing “Heavy traffic conditions” to the others in order to make its movement easier on the road.

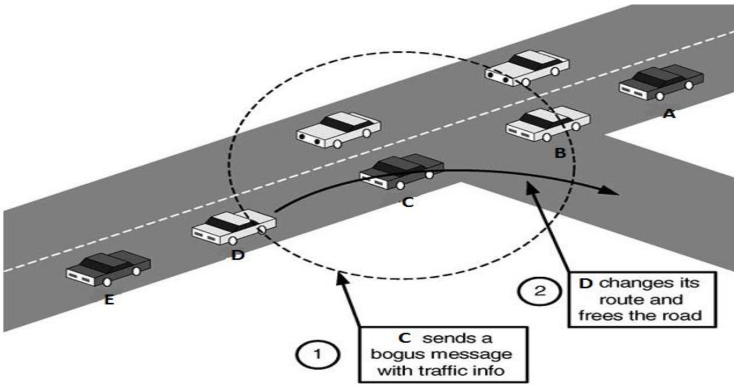
A
B
C
D
E
2
D changes its route and frees the road
1
C sends a bogus message with traffic info

Figure 2. Bogus information attack

Figure 2, demonstrates an example of bogus information attack, colluding attackers (A and C) spread false information to affect the decisions of other vehicles (D) and thus clear the way of attacker E.

ECDSA (Elliptic Curve Digital Signature Algorithm) is named as one of the solutions for this kind of attacks. The message authentication scheme made use of employs a hashing technique to keep messages better secured and to provide a strong authentication for the destination vehicles. Each vehicle consists of private key and public key. The public key is made available to all the vehicles in VANETs. It is mandatory for both the source and destination nodes to correspond to the elliptic curve Domain parameters. ECDSA is a variant of DSA (Digital Signature Algorithm). The source vehicle first hashes the message then, encrypts it by using a secured hash algorithm and private key, and sends the message to the vehicle at the destination. At the destination vehicle, the message is decrypted using the public key, which is the hash of the message. This scheme proves to be more secure on message authentications since hashing is a strong technique. Changes in messages will also bring change in the hash message, which makes it unique.

6.3 Denial of Service (DOS)

Denial of Service (DoS) is always one of the most serious level attacks in every network. The plot to perform are very diverse. The main objective is to prevent the authentic users to access the network services. In DoS attacks, the attackers may impart dummy messages to jam the channel and thus, reduce the efficiency and the performance of the network. A portion of or the total network is no longer available to legitimate users. Figure 3, indicates that a malicious black car creates a large number of fake identities and sends a fake message to the authorized car right behind it and even to a RSU to create a jam in the network.

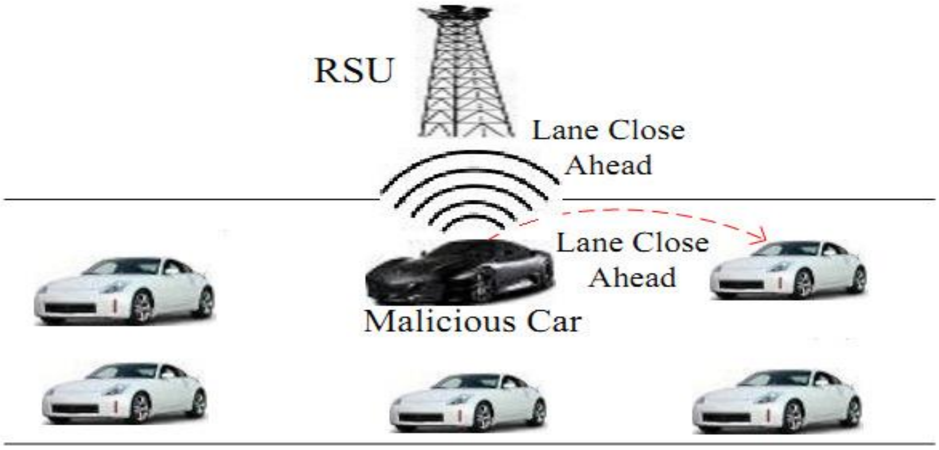

Figure 3. Denial Of Service (DOS) attack

The Distributed DoS (DDoS) is more acute problem than the DoS where a number of malicious cars attack on a legitimate car in a distributed pattern from different locations and timeslots. Figure 4 demonstrates that the three malicious black cars attack on the car A from different locations and different time so that A cannot communicate with the other vehicles.

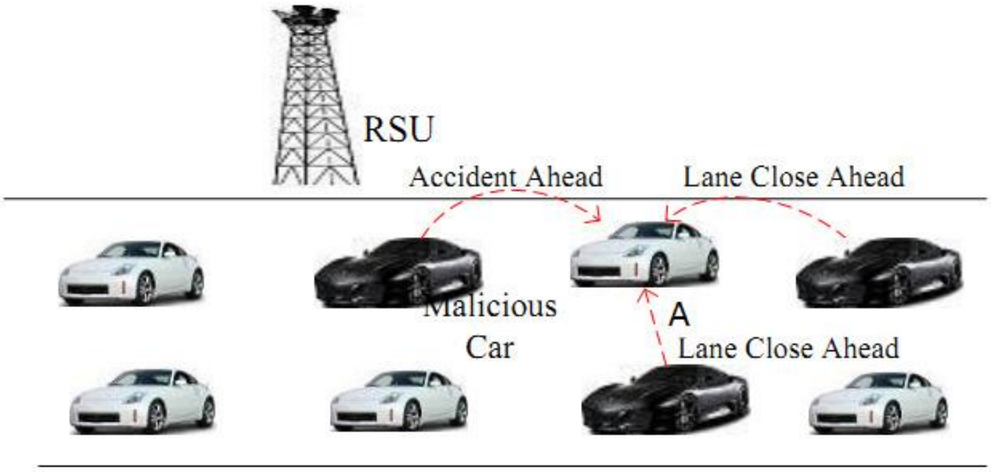

Figure 4. Distributed Denial Of Service (DDOS) attack

One of DoS attack solutions is based on the support of OnBoard Unit which is equipped in vehicles. There is a processing unit that has the task to suggest the OBU to the switch channel, or to use the frequency hopping technique or the multiple transceiver in the case of DoS attack. The work presents a distributed and a robust defense against DoS attacks where a malicious node creates a huge number of fake identities, i.e., the Internet Protocol (IP) addresses in order to disrupt the actual functioning of the data transfer between the two fast-moving vehicles. In the proposed approach, these fake identities are examined through the means of the consistent existing IP address information. All the vehicles exchange their beacon packets frequently to claim their presence and be aware of the neighbors. Each node periodically keeps and updates a record of the database by exchanging the information within community. If a node detects that in its own record that there are some similar IP addresses, these identical IP addresses are probable evidences of a DoS attack. The authors have developed a model for the DoS attack prevention called the IP-CHOCK that proves the significant strength in determining the location of the malicious nodes without the requirement of any secret information exchange or any special hardware support. Simulation results represent an encouraging detection rate that will be enhanced whenever the optimal numbers of nodes are created by the attackers.

6.4 Black hole attack

A black hole is an area where the network traffic is redirected. However, either there is no node in that area or the nodes present in that area turn down to take part in the network. In a black hole attack, a malicious node introduces itself for having the small distance to reach the destination node and thus, cheats the routing protocol. before checking the routing table firstly, this hostile node announces rapidly that it has a fresh route for the route request. In consequence, attacker node wins the deserve of answering to the route request and thus it is able to intercept the data packet or retain it. When the malicious route is successfully accomplished, it depends on the malicious node whether to drop or forward the packets to wherever it wants. Figure 5, illustrates an example where the node A wants to send data packets to node F but unaware of the way to F. Therefore, A begins the route discovery process. As a malicious node, D claims that it has effective route to F and acts that it must be next-node if A wants to send packets to F. Depending on the routing protocol (i.e e.g., Ad hoc On-demand Distance Vector (AODV) or Optimized Link State Routing (OLSR), an attacker frame its private method to fits in the data routes.

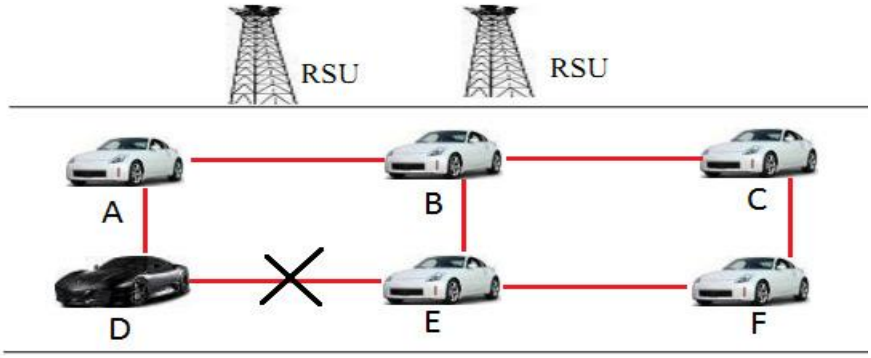

Figure 5. Black hole attack

We can use packet sequence numbers in a packet header as the solution, so that if any packet is lost, the destination can simply check it from the lost packet sequence number.

6.5 Man in the Middle Attack (MiMA)

As the name itself suggests, in this particular attack, malicious vehicle listen to the communications among two different vehicles, pretends to be each of them to reply the other and inject false information in between the vehicles. Figure 6, demonstrates a Man in the Middle attack scenario, in which the malicious vehicle C is eavesdropping the communication between the vehicles B and D as well as sending wrong information received from A to the vehicle E.

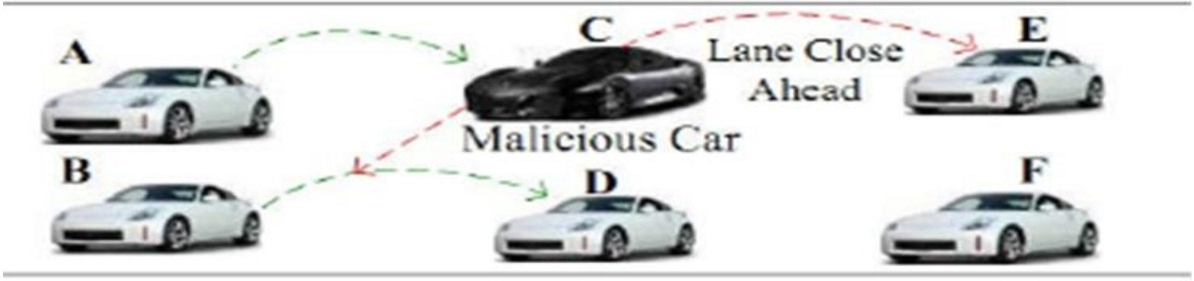

Figure 6. Man in the middle attack

In order to deal with this type of attacks, rational solutions are confidential communications (e.g., by powerful cryptography) to avoid an attacker from eavesdropping the communication among the others, data integrity verifications and a secure authentication (e.g., by hash functions) to avert messages modifications.

6.6 Malware and Spam

Malware and spam attacks are basically similar to viruses and spam messages, can cause serious disruptions in the typical VANETs operations. This kind of attack is normally executed by malicious insiders rather than outsiders. For example, an attacker sends a huge amount of spam messages in the network to consume the bandwidth and to raise the transmission latency. It is not a simple task to control such kind of behavior because of the lack of centralized administration and necessary infrastructure. Moreover, malwares are just like viruses that hamper the normal operation of the network. VANETs get infected usually when OnBoard Units (OBU) of vehicles and RoadSide Units (RSUs) perform software updates. The embedded anti-malware frameworks that are implemented are still a problematic issue in VANETs research community.

6.7 Illusion Attack

In the illusion attacks, the vehicles adversary deceives i.e the sensors on his car to produce false sensor readings and hence produce incorrect traffic information. In consequence, the corresponding system reaction is invoked and then incorrect traffic warning messages are transmitted to the neighbors. Thus, illusion condition is successfully created. In general, the behavior of the driver will depend on the traffic warning messages they have received. Caused by illusions, vehicles received the false traffic information received will most likely change their driving behaviors, correspondingly. Hence, the attacker can cause an accident, a traffic jam and therefore decrease the performance by manipulating the network topology of the network.

Traditional message integrity verification and the message authentication cannot totally prevent the illusion attacks as the sensors directly manipulates and confuses the sensors present on the vehicle to report false information. Plausibility Validation Network (PVN) is a security model which is implemented to secure the VANETs against the illusion attacks. PVN processes by accumulating raw sensors' data and verifying whether the accumulated data are plausible or not. Two different types of inputs are taken into account, first incoming data from antennas and data accumulated by sensors. An input data header will categorize the data. PVN basically has a typical rule database and a data-checking module, which aids to check the validity of input data and take necessary action respectively. A message is considered to be trustworthy if it passes all verifications. Or else , it is declared as an invalid message and is dropped automatically. PVN has a cooperation with various types of cryptography methods and defend against further attacks.

6.8 ID Disclosure

It aims to provide authentication, integrity, availability, confidentiality, and non-repudiation properties for VANETs, thus, detect and prevent misbehaviors (e.g., virus).The major advantages in this protocol for secure data transmission in VANET are, the lesser time consumption and the security assured for both outsider and insider attacks. In this attack, a node in the network imparts the identity of neighbors, tracks the current location of the target node, and then uses this data for a range of purposes i.e e.g., this is actually the way some car rental companies track their own cars. One of the well known scenarios of ID Disclosure is as follow: A global observer dispatches a "virus" to a few neighbors of the target node. Whenever attacked by the virus, these neighbors periodically report the locations and the ID of the target node. This attack violates the requirement concerning not only the authentication but also the privacy.

Authors propose a holistic protocol for secure data transmission and detecting the Misbehavior transmitted by the authorized users. In their submitted work, the vehicle should register with the nearby Road Side Unit (RSU). In Registration phase, the user submits the user name and the password to the RSU, then the RSU provides Registration ID to the user, which consists of the license number and also the vehicle registration number. Then RSU authenticates the vehicle by verifying the certificate that has been provided. If the authentication is failed, the data/node will be blocked to prevent further disruption. This type of protocol is holistic protocol which is concerning the whole rather than the individual.

VII. CONCLUSION

Due to recent improvements in connecting vehicles to external networks, genuine security mechanisms have to be developed in parallel in order to reduce the risk of malicious and unauthorized behavior in the vehicular network domain. Users need safety while commuting on road in future vehicular network and it could be possible by implementing VANET applications.

We study the requirements for the security and challenges to implement the security measure in the VANET. Different types of attacks and their related solutions are also discussed. We discuss some technologies which are used in the different solutions. Among all the requirements used authentication and privacy are the main issues in VANETs. However, confidentiality is not of importance in VANET because generally the packets on the network do not contain any confidential data.

REFERENCES

[1] Swapnil G. Despande," Classification of Security attack in Vehicular Ad hoc network: A survey", in International Journal of Emerging Trends & Technology in Computer Science (IGETTCS), Volume 2, Issue 2, pp 2-4, 2013.

[2] Vinh Hoa LA, Ana CAVALLI," SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR

AD HOC NETWORKS: A SURVEY", in International Journal in Ad hoc Networking Systems(IJANS), Volume 4, Issue 2, pp 6-16, 2014.