International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Advanced Security Attacks on Vehicular AD HOC Network (VANET)

Komal Singh, Sachin Sharma

Abstract: ***VANET is becoming an emergent technology in Intelligent Transportation Systems. Their main purpose is to provide road safety and improve driving experience for both drivers and passengers. Other unique features of VANET include dynamic topology, short connection period, high mobility of nodes, etc However, security and privacy becomes major issues when communicating in such open wireless environment. In this paper, along with VANET characteristics, we presented security requirements and challenges that need to be kept in mind while designing a security protocol. We defined all existing security attacks and privacy issues in VANET. We categorized these security attacks into different classes based on their properties and provided the comprehensive analysis on them.***

Keywords: Vehicular ad hoc networks, security, road side units (RSU).

I. INTRODUCTION

With the emergence of new concepts like Smart Cities, Intelligent Transportation System need to be developed to improve the quality of transportation system [1]. Its main objectives are to improve efficiency of traffic management system and to facilitate drivers and passengers by providing road safety applications, driver assistance to reduce traffic congestion and awareness about emergency warnings [2]. In order to do so, these vehicles need to communicate with each other and exchange road status information such as traffic pattern, unforeseen obstacles, etc. To accomplish this task, a special type of communication system is designed, known as Vehicular Ad hoc Network (VANET).

A VANET is a special type of wireless ad hoc network where communication is taking place among moving vehicles and roadside infrastructures and equipment's [3]. Vehicles communicate with each other by broadcasting messages containing information about road conditions, traffic conditions and about itself, for example, awareness information for the purpose of accident prevention, traffic information in order to avoid congestion or music sharing and network gaming to make driving more enjoyable. Drivers take desired action according to the content of the message. While these messages will help to improve the driving experience, they can also threaten the security of the network if altered and misused by any malicious user. Also, the attacker or malicious user can read messages containing personal information about the vehicle or the driver and misuse them for their own benefit. Thus, influences the protection of drivers which if not taken in concern might result in fatal consequences. Therefore, data transmitted over VANET has high need of security for proper functioning of these networks. These concerns may seem to be like those we come across in other wireless communication networks, however, they are not. It is very unusual and challenging to solve security issues in VANET because of the limitless network, varying speed of the vehicles, the exceptionally sporadic network between them. And leaving this ad hoc network unprotected opens the door for attackers to alter life-critical messages, broadcast false signals, or even block network signals altogether. The motivation behind this paper is to present a proper survey on security threats and attacks possible on intelligent vehicles and their networks. The rest of the paper is organized as follows: Section II provides an overview of VANET. Section III covers the security aspect of VANET. Section IV provides attacker model. Section V explains analysis of possible security attacks in VANET. Section VI concludes the paper.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Komal Singh*, Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India. Email: komalsingh.0492@gmail.com
Sachin Sharma, Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India. Email: sxsharma88@gmail.com

II. OVERVIEW OF VANET

In this section, we present the basic architecture of VANET including on-board unit, road side unit, and trusted authority and the types of communication possible among different units present within VANET.

A.Network Model

For establishing connection and communication among vehicles and road side infrastructures, VANET architecture requires following indispensable components [4]:

1. Vehicles equipped with:

- Electronic Control Unit (ECU): Present vehicles are equipped with a number of subsystems each having specific task such as Global Positioning System (GPS) to find current location of the vehicle, Electronic License Plate (ELP) to identify vehicles. To monitor, control and make communication possible among these subsystems, embedded computers known as ECU's are installed in each subsystem. Each ECU has a specific functionality, for example, one ECU is responsible for Handling driver's door functionality while one ECU is responsible for the radio system in the vehicle.

- On-Board Unit (OBU): OBU is a radio device equipped in every vehicle to provide a wireless medium for communication with RSUs and with other vehicles OBU. An OBU comprise of a processor for processing the collected data, storage device for storing information, a user interface, and network device which works as a gateway for wireless communication.
- Application Unit (AU): AU is a device installed within the vehicle is used to communicate with the network only by using the OBU.

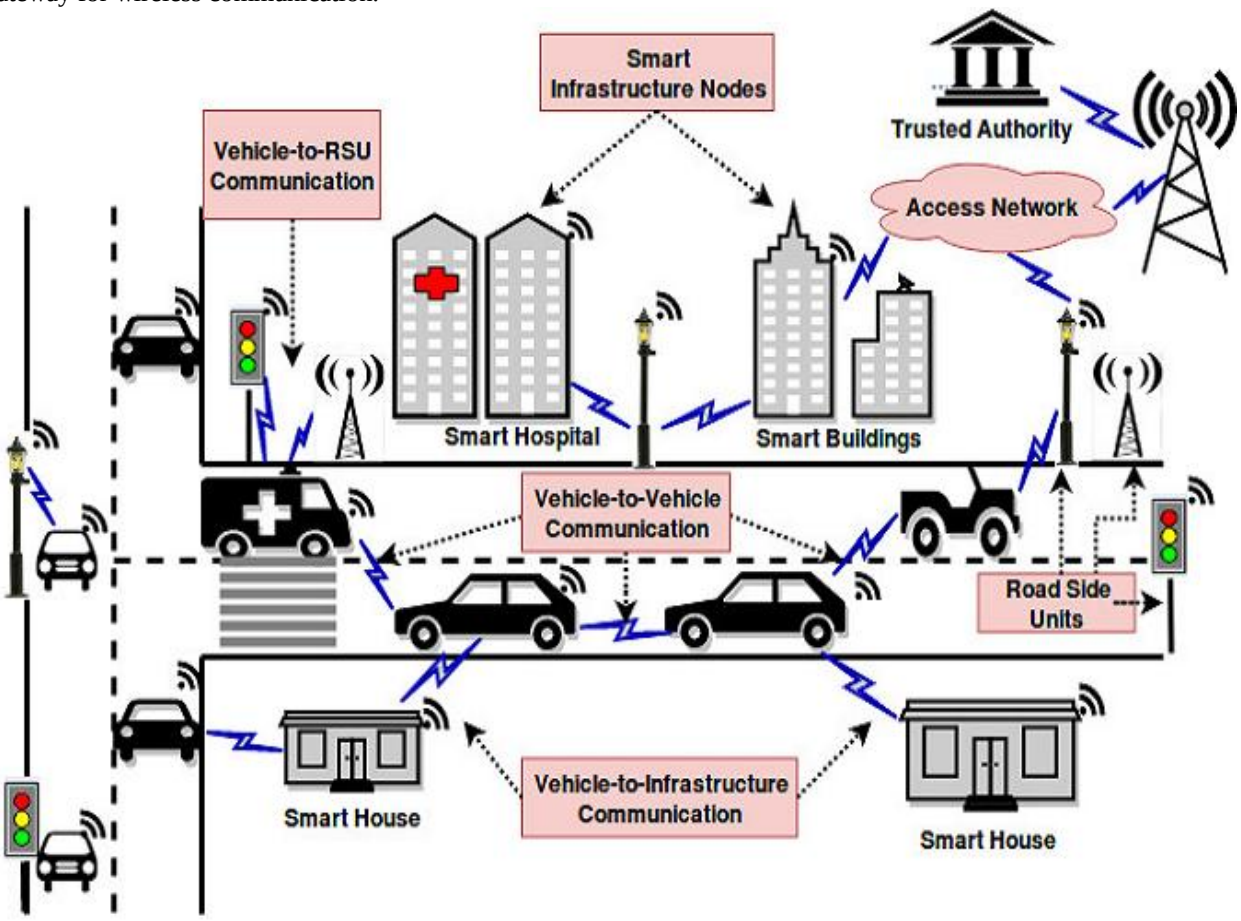

Fig. 1. VANET Architecture and Communication Techniques

2. Road Side Unit (RSU): RSUs are fixed network infrastructure placed along the roadside in such a manner that they can be sparsely distributed all over the network. They are equipped with network communication devices, hence are used as a router for communication between different nodes of the network. OBUs communicate wireless with RSUs using the DSRC protocol based on IEEE 802.11p [9]. The main functions of RSUs included:
(i) Providing Internet connectivity to OBUs for forming a network.
(ii) Checking authenticity of new vehicles entering the network.
(iii) Running safety applications like accident warning message or traffic condition report.

RSUs are quite vulnerable because they are easily exposed to attackers, so we must put minimal trust in RSUs.Trusted Authority (TA): TA is the automotive company (a third party service provider) whose responsibility is to provide security mechanism to the entire network. All the vehicles have to register themselves to TA for getting an authentication certificate for the usage of VANET services. TA stores the identities of these joined vehicles and will use it to reveal the real identity of vehicle in case of any malicious behavior. In addition, they also have full control over all RSUs. In reality, there are many TAs distributed all over the globe, each one of them is responsible for a specific geographical area.

3. Access Network: Wireless access network is required so that vehicles can communicate with each other as well as with RSUs and other infrastructures.

B. Communication Techniques

Different components of VANET architecture communicate with each other forming different types of communication techniques, i.e., intra-vehicle communication and inter-vehicle communication.

1. Intra-Vehicle Communication: Sensors and ECUs present with in a vehicle communicate with each other by sharing data among them, thus forming an intra-vehicle communication network [10]. This intra-vehicle network consists of 50-70 ECUs and uses a wireless gateway to communicate with external units. Common in-vehicle network types include Controller Area Network (CAN),

Local Interconnect Network (LIN), and Media Oriented System Transport (MOST), FlexRay.

2. Inter-Vehicle Communication: Vehicles communicate with each other and neighboring infrastructure nodes installed along the road side to share emergency warnings and traffic conditions, thus forming a inter-vehicle communication network.
3. Different types of inter-vehicle communication are formed depending on the type of node involved in communication i.e. Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Roadside Unit (V2R) as shown in Fig. 2. Fig. 3 shows how a warning message is transmitted in an inter vehicle communication network.

- Vehicle-to-Vehicle Communication: V2V communication takes place when vehicles communicate with each other directly in ad hoc mode, forming a single-hop or indirectly in a multi-hop mode where message is forwarded from one vehicle to another until it reaches its required destination vehicle. Single-hop V2V communication is used when broadcasting local safety warnings while non safety related messages are exchanged through multi-hop V2V communication. The goal of this communication is to exchange present road condition information such as emergencies, traffic conditions or accident warnings [11].
- Vehicle-to-Infrastructure Communication: In V2I or I2V communication [12], safety messages are communicated between vehicles and infrastructure on and alongside the road. This communication transforms infrastructure into smart infrastructure by incorporating algorithms in them and give them computational power. Messages received from a vehicle is fed as an input in these algorithms to perform calculations that results in production of warning or alert messages for drivers in advance. For example, (i) Smart Traffic Signal Systems broadcast the Signal Phase and Timing (SPAT) message to vehicles in order to convey them the current status of traffic signal at an intersection. A vehicle approaching the intersection uses this information to calculate their speed profile hence reduces stop-and-go driving as shown in Fig. 3. (ii) Smart street lights can also be used to transmit firmware updates and diagnostics requests to OBUs in vehicles.
- Vehicle-to-Roadside Communication: In order to access the services provided by a RSU, a vehicle first sends a connection request message to the nearest RSU. Vehicles use this message to authenticate them self with RSU, and in return RSU authenticates the validity of their own identity to the requesting vehicle. Once both are authenticated to each other, they start communicating each other via messages. Sometimes, RSU broadcasts safety or warning message related to the road condition to all the other vehicles in the network, forming a one hop broadcast. For example, RSU periodically broadcast a message containing the regulations regarding the speed limit. Whenever a vehicle violates the specified regulation, RSU broadcasts a auditory or visual warning message, requesting the driver to reduce speed. Hence maximum load for proper communication is given to RSU in this type of communication.

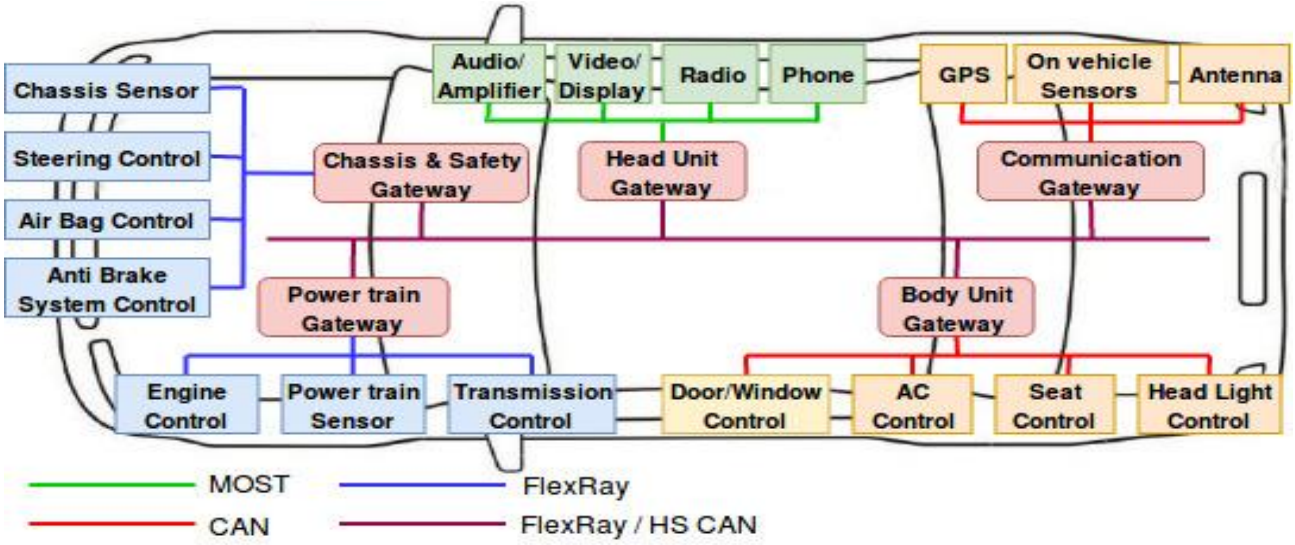

Fig. 2. Intra-vehicle Communication

III. SECURITY IN VANET

The main objectives of VANET is to provide early warning signals about road safety to drivers on road through frequent sharing of safety information about vehicles, road condition advisory and traffic. So this communicated information needs to be accurate, efficient and reliable. But due to ad hoc nature of VANET, a malicious user can get access to this data and leave this network prone to many attacks targeting violation of data privacy and confidentiality. Any successful attack can have catastrophic result like economical loss or loss of life. Hence it is essential to secure the transmitted information because it may affect the life of people on the road. But solving security issues in VANET are quite challenging because of the following VANET characteristics [4]:

- Real-time constraints: Real-time information is shared between vehicles in VANET. This information should reach the receiver in sufficient time for it to make decisions and take corresponding actions according to the information present in received message.
- High mobility of vehicles: Vehicles part of the VANET are normally in moving state all the time. Therefore, a little delay in message delivery can result in danger situation.

- Dynamic network topology: Due to high mobility of vehicles, the topology of VANET changes quickly. As a result, it becomes difficult to identify attackers vehicle leaving the VANET vulnerable.
- Scalable network size: Network size in VANET is not fixed because of the frequent instantaneous arrival and departure of vehicles in/from the network.
- Short connection period: Because of the mobility of nodes, connection between nodes remain only for a limited period of time up to few wireless nodes. Hence, it would be difficult to ensure the security of personal contacts in VANETs.

A.VANET Security Challenges

Above mentioned exclusive features of VANET not only provide services but also give rise to unique security challenges which can affect applying security methods in VANET. High dynamic environment of VANET gives opportunity to attackers to hide after modifying any vital information. It is challenging to make sure that the vital information cannot be modified by any attacker. In addition to this, use of wireless media also give attackers to breach the network from outside i.e. without being part of the network. Different authors provided a survey of these issues [5], [7]. Hence to conquer these challenges, we specified some requirements in the next section that need to be satisfied for becoming a secure VANET.

B. VANET Security Requirements

The safety and security information which is being shared among vehicles and RSUs is critical and should reach to the destination without any modifications. Therefore, some prerequisites must be defined and it should be paramount to address these requirements for the appropriate operation of the network. This subsection discusses these requirements in detail [9].

- Authentication: Authentication ensures that the received message is trust-able i.e. it is generated by a legitimated user. It is very necessary that the sender and the receiver node must verify the identity of each other and check authenticity of messages for a trustworthy transmission between them.
- Availability: Availability ensures that the services and applications provided by the network should be available to all authenticated (authorized) users at any time without affecting its performance even if it is under any malicious attack.
- Confidentiality: Confidentiality ensures that the content of transmitted message is not accessible by any unauthorized and illegitimate user. Only the dedicated receiver must be able to access the content of message.
- Integrity: Integrity depends on authentication. It ensures error detection i.e. the received information has not been altered or modified by an unauthorized user during its transmission between vehicles and RSUs either accidentally or intentionally. Alteration of message has to be done by authorized users only.
- Non Repudiation: Non-repudiation depends on authentication. It ensures the security mechanism where sender cannot deny that they are not sending messages. This requirement makes sure that the receiver receives a proof that a particular sender is accountable for that particular message.

Besides these main security requirements, the following security aspects should be also satisfied in VANETs:

- Privacy: The privacy of vehicles, owners and drivers must not be endangered by any unauthorized vehicle or user.
- Access control: Vehicles should have the capability of accessing available services offered by remote nodes.
- Trace-ability: Although a vehicle's real identity should be hidden from others, still there should be a component with the ability to obtain vehicles' real identities to revoke them for future use.
- Flexibility and efficiency: Flexibility in the security architecture and the system design is significant. Though it is essentially designed for traffic safety application that requires less time and bandwidth. This makes the channel efficiency crucial in its consequent low delay.

IV. ATTACKER MODEL

Different types of attacks are possible in VANET. Mainly, the impact of these attacks depends on the intentions of the attacker and the technique used to perform that attack. There may be several reasons for such malicious behavior, such as to get some confidential information about the system or to disturb the efficient working of the network. One cannot comprehend the behavior of attacker but can be classified based on some basic properties. Authors in [13] described an attacker model consisting of two levels. Authors in [5] suggested one more class of attackers known as adversaries. In this paper, we classified all the attackers based on four classes:

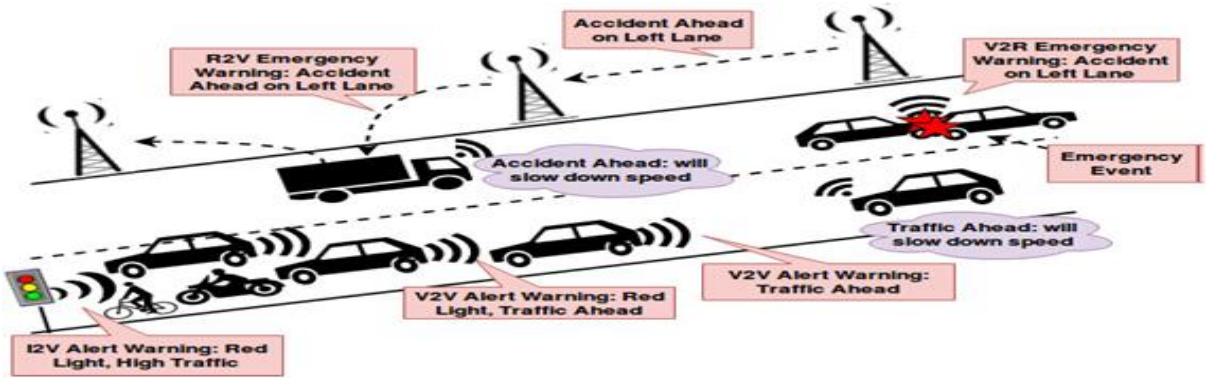

Fig. 3. Inter-vehicle Communication

Table-I: Advanced VANET security attacks

Attack Name	Attacker Type	Requirement Compromised	Communication Compromised	OSI Layer Affected
Bogus Information	Insider/Outsider, Active	Integrity, Confidentiality	V2V, V2I	Application
Bush Telegraph	Insider/ Outsider, Active	Integrity, Availability	V2V, V2I	Application
Broadcast Tampering	Insider, Active	Availability	V2V, V2I	Application
Message Tampering	Insider, Active	Authentication, Integrity	V2V, V2I	Application, Transport
Message Fabrication	Insider, Active, Malicious	Integrity	V2V, V2I	No layer violated
Message Suppression	Insider, Active, Malicious	Integrity, Authenticity	V2V, V2I	No layer violated
Spam	Insider	Availability	V2V	No layer violated
Black Hole	Insider, Active, Local, Malicious	Availability	V2V	Network
Gray Hole	Insider, Active, Local, Malicious	Availability	V2V	Network
Worm Hole	Insider, Malicious, Active/Passive	Availability, Confidentiality	V2V	Network
Rushing Attack	Insider, Malicious, Active/Passive	Availability, Confidentiality	V2V	Network
Illusion Attack	Insider, Active	Integrity	Intra Vehicle	-
Greedy Behavior	Insider, Active	Availability, Access Control	Intra, Inter Vehicle	MAC
Sybil Attack	Insider, Active	Confidentiality, Authentication, Availability	V2V	Network
Masquerading	Insider, Active	Integrity, Authentication	V2V	Network
Impersonation	Insider, Active	Integrity, Authentication, Non Repudiation	V2V	Network
ID Disclosure	Insider/ Outsider, Passive	Confidentiality	V2V, V2I	Network
Repudiation Attack	Insider, Active/Passive	Authentication, Non Repudiation	V2V, V2I	No layer violated
Brute Force Attack	Insider/Outsider, Active	Confidentiality, Authentication, Privacy, Anonymity	V2V	Network
Key/Certificate Replication	Insider, Active	Authorization, Authentication	V2I, V2V	Network, MAC
Hidden Vehicle Attack	Insider, Active	Availability	V2V, V2I	Application
GPS Spoofing	Insider, Active	Integrity, Availability, Authentication, Traceability	V2V	Network
Tunnel Attack	Insider	Availability	V2V	Network, MAC
Location Tracking	Insider/Outsider, Passive	Confidentiality	V2V	No layer violated
Jamming Attack	Insider/ Outsider, Active, Local, Malicious	Availability	V2V, V2I	MAC
SYN Flooding	Insider/ Outsider, Active, Local, Malicious	Availability	V2I	All layers
Distributed DoS Attack	Insider/ Outsider, Active, Local, Malicious	Availability	V2V, V2I	All layers
Eavesdropping	Passive	Integrity, Confidentiality	V2V	Network
Replay Attack	Insider, Active, Local, Malicious	Integrity, Confidentiality	V2V	Application
Man in the Middle Attack	Insider, Active, Malicious	Integrity, Confidentiality, Availability	V2V, V2I	All layers
Timing Attack	Insider, Active	Integrity, Availability	V2V, V2I	No layer violated
Session Hijacking	Insider/ Outsider, Active/ Passive	Confidentiality, Authentication	V2V, V2I	Transport

A. On the basis of Membership

Any authorized or unauthorized node can perform malicious activity in the network.

- Insider: An insider is an authorized member node of VANET network who have the privileged to communicate with other members of the network.
- Outsider: An outsider is not an authenticated user of the network. They are the intruders who try to enter in network either by impersonation or other attacks and have limited capacity to attack.

B. On the basis of Intentions

Any attack is associated with the intention of the attacker, i.e. main objective of the attacker behind that attack.

- Rational Attacker: These attackers seek personal benefit from the attacks and hence are more predictable.
- Malicious Attacker: These attackers have no personal benefit from attacks. Their only goal is to create chaos in proper network functionality.

C. On the basis of Activity

Whether an attacker is active and makes frequent changes to network or not, the attackers are classified as:

- Active Attacker: These types of attackers try to alter the network information and generate malicious packets and signals.
- Passive Attacker: These types of attackers do not alter the network information. They silently eavesdrop the network.

D. On the basis of Scope

How much the network will get affected depends on the scope of the attacker.

- Local: Local attackers have a specific scope of their attack range even if they compromise several entities.
- Extended: Extended attackers have several entities that are extended across the network.

V. SECURITY ATTACKS ANALYSIS

This section covers all existing attacks possible on VANET. These attacks can be categorized depending upon the type of information about the network and the vehicle used. Some attacks falsify the location of vehicles while some attacks falsify the messages that are being transmitted over the network. Also, the impact of these attacks depend on attackers intentions and their accessibility to the network such as an inside attacker can do more damage than an outsider. Many researchers classified these attacks based on the security requirement they are violating [4], [6], [8], [9]. While some researchers classified security attacks based on the OSI layer they target. In this paper, we provided our own classification based on type of information tampered. We classified existing attacks in to seven different criteria as described below. Attacks that come under these classes are also specified. Table I summarizes these attacks and provide analysis of how much damage they do to the network. Along with it, the table also provide the intentions of attacker for each type of advanced attacks in VANET.

A. Tampering position information

This class of attacks tampers location information which is being transmitted over the network. Using this class of attacks, attacker can hide itself after compromising the network.

- Hidden vehicle attack: In this attack, attacker vehicle cheats with positioning information. A vehicle broadcasting warnings message will listen for feedback from its neighbors and stop its broadcasts if it realizes that at least one of these neighbors is better positioned for warning other vehicles. Attacker vehicle deceive the accidental vehicle that it is in a best place to broadcast safety or warning message. But in actual, attacker will hide this safety message and will keep the accidental vehicle silence from broadcasting the safety or warning message.
- GPS Spoofing: In VANET, a location table is maintained in the GPS satellite which contains the vehicles identities and geographic location information of those vehicles. Attacker alters the location table of the GPS system by producing false GPS coordinates. These fake coordinates hide attackers position and deceive other vehicles that it is in some other position.
- Tunneling: GPS signals temporary disappears in tunnels which results in temporary loss of positioning information. Attacker exploits this weak spot by injecting false information into the vehicle's database once it leaves the tunnel and before it receives original position update.
- Location tracking: In this attack, attacker violates privacy of a node by trying to get confidential information about the driver. Attacker tracks the targeted vehicle node to find its position or route followed by that node.

B. Tampering routing information

This class of attacks targets routing information of nodes by exploiting the vulnerabilities of routing protocols. They disturbs routing process of a network either by dropping the packets or by forwarding these packets to an unintended user. Hence these attacks can result in Denial-of-Service attack. Following are the most common routing attacks in the VANET:

- Black hole attack: In this attack, a malicious node called as Black hole node, attracts the other nodes by making an illusion to them that it is having the shortest path to their destination node and thus, cheats the routing protocol. After attracting the nodes, when they start forwarding their packets to this malicious node, it depends on the malicious node whether to drop the packet or forward it to an unintended destination.
- Warm hole attack: This attack involves two or more attacker nodes. A tunnel is created to transmit packets from one end of the attacker node to the other attacker's node. Wormhole attacks disrupt the multi-cast and broadcast routing, thus, threaten the security of transmitting data packets.
- Gray hole attack: It is a variation of Black hole attack. In this attack, the malicious node behaves like a black hole node by agreeing to forward the packets, but sometimes it drops the packets for a while and then switches to its normal behavior.
- Rushing attack: This attack is used against on-demand ad hoc network routing protocols such as ARAN. This type of attack makes a malicious vehicle have a higher probability of finding routes due to its ability to send route requests more quickly than legitimate users.

C. Tampering technology

This class of attacks tampers the hardware such as sensors and ECUs to generate wrong information.

- Illusion attack: In this attack, the adversary deceives intentionally the sensors on his own car to produce wrong sensor readings. As a result, incorrect traffic information messages are broadcast in the network.
- Greedy behavior attack: Attacker attacks on the functionality of MAC (media access control) layer protocol to get more bandwidth on wireless medium and to minimize its waiting time.

D. Tampering identity

In this class of attack, a malicious node from inside or outside the network creates its fake identity or discloses the identity of nearby nodes. Attacker forges identity of other existing nodes and use them for further attacks.

Following are
the attacks that come under this category.

- Sybil attack: In this attack, attacker creates many forge identities and convince the real vehicles to change their route by creating an illusion of traffic jam.
- Masquerading: The attacker forges identity of a legitimate user which has already been registered and authenticated inside the network to broadcast false messages.
- Impersonation: The attacker obtains identity of legitimate user and spoof's MAC and IP of other users.
- ID disclosure: The attacker discloses itself using identity of a legitimate user. It tracks location of a target node and affect its neighbors by sending any malicious message.
- Key/Certificate replication: The attacker creates duplicate key and certificate of legitimate vehicle and use it as its own identification proof to show to Trusted Authority.
- Brute force attack: The attacker uses trial-and-error method to find confidential information like vehicle identification number, network security information.
- Repudiation attack: The attacker after sending any malicious information in the network denies the fact of sending message in case of any dispute.

E. Tampering message

This class of attacks target the information carried by the messages exchanged between network nodes.

- Bogus information: The attacker transmits bogus or incorrect information in the network to misguide other network users.
- Bush telegraph: The attacker appends tolerable error to the message at each intermediate node crossed to reach destination node. Since error is with in tolerance margins at each node, message will get accepted. When reaching to destination node, the overall accumulated error yield to bogus information.
- Message Tampering: The attacker falsifies transaction application request. After gaining access, the attacker can drop, modify or corrupt the messages exchanged in the network.
- Message Fabrication: The attacker broadcast false messages in order to gain priority in the network.
- Message suppression: The attacker drops some selective messages which may contain some safety related or some sensitive information.
- Broadcast tampering: The attacker broadcasts false safety condition messages which can compromise the whole network.
- Spam attack: The attacker transmits many spam messages in the network. Here, the purpose is to occupy network bandwidth as much as possible and increase transmission latency.

F. Denial of service

The purpose of DoS attacks is to prevent authenticated users from accessing the network services and resources. As a result, a part of or the total network may be no longer available to legitimate users and thus, reduces the efficiency and performance of the network.

- Jamming attack: The attacker jams the communication medium by sending a strong signal having frequency range equivalent to receiver's frequency range.
- SYN flooding attack: The attacker sends multiple SYN requests to target node for forming multiple connections. But the attacker never completes the 3-way handshake process for any of the sent request. As a result, target node denies to service further.
- Distributed DoS: Multiple attackers attack a single target in a distributed manner from different locations and different time slots.

G. Monitoring information

This class of attacks monitor the whole network. They listen all the communication messages passed in V2V and V2I. If any useful information is found they misuse it according to get benefit.

- Eavesdropping: The attacker eavesdrops the transmission channel in order to get access to security credentials or any confidential information.
- Man in the middle attack: The attacker node eavesdrops the communication channel established between two legitimate users. It then intercepts this communication by pretending to be each one of them and reply to the other by using false information.
- Replay attack: The attacker replays again and again previously received messages in order to confuse other nodes.
- Timing attack: In this attack, attacker forwards the received message after adding some time slots to create delay, hence violating real-time transmission of messages.
- Session hijacking: Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.

VI. CONCLUSION

Providing safety to road travelers is the main purpose of VANET. However, due to its unique characteristics providing security and privacy to travelers becomes a challenging issue. If an attacker changes the content of a safety message, then whole network can be compromised. In this paper, we first review the basic knowledge of VANETs. After then we presented a survey of all possible attacks by classifying them in to seven categories. We also explained the behavior of the attackers based on the attack they launched. We hope that our classification criteria and attacker's behavior for each criteria will allow researchers to find new mechanisms to prevent possible attacks.

REFERENCES

1. Djahel, Soufiene, Ronan Doolan, Gabriel-Miro Muntean, and John Murphy."A communications-oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches." IEEE Communications Surveys Tutorials 17, no. 1 (2014): 125-151.
2. Shukla, Sumit N., and Tushar A. Champaneria. "Survey of various data collection ways for smart transportation domain of smart city." In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 681-685. IEEE, 2017.
3. Hartenstein, Hannes, and L. P. Laberteaux. "A tutorial survey on vehicular ad hoc networks." IEEE Communications magazine 46, no. 6 (2008): 164- 171.

4. Lu, Zhaojun, Gang Qu, and Zhenglin Liu. ”A survey on recent advances in vehicular network security, trust, and privacy.” IEEE Transactions on Intelligent Transportation Systems 20, no. 2 (2018): 760-776.
5. Sharma, Bharati, Mayank Satya Prakash Sharma, and Ranjeet Singh Tomar. ”A Survey: Issues and Challenges of Vehicular Ad Hoc Networks (VANETs).” Available at SSRN 3363555 (2019).
6. [6]Kelarestaghi, Kaveh Bakhsh, Mahsa Foruhandeh, Kevin Heaslip, and Ryan Gerdes. ”Survey on Vehicular Ad Hoc Networks and Its Access Technologies Security Vulnerabilities and Countermeasures.” arXiv preprint arXiv:1903.01541 (2019).
7. Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. ”Survey on VANET security challenges and possible cryptographic solutions.” Vehicular Communications 1, no. 2 (2014): 53-66.
8. Haas, Roland E., Dietmar PF Mller, Prateek Bansal, Rahul Ghosh, and Srikrishna S. Bhat. ”Intrusion detection in connected cars.” In 2017 IEEE International Conference on Electro Information Technology (EIT), pp. 516-519. IEEE, 2017.
9. Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. ”Survey on VANET security challenges and possible cryptographic solutions.”Vehicular Communications 1, no. 2 (2014): 53-66.
10. Navet, Nicolas, and Franoise Simonot-Lion. In-vehicle communication networks-a historical perspective and review. University of Luxembourg,2013.
11. Dasuha, Laura Carolina, and Teddy Mantoro. ”Car to car communication in VANET using Co-operative Mobility Services of the Future (CoMoSeF).” In 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), pp. 349-353. IEEE.
12. Ometov, Aleksandr, and Sergey Bezzateev. ”Multi-factor authentication: A survey and challenges in V2X applications.” In 2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 129-136. IEEE, 2017.
13. Sumra, Irshad Ahmed, Halabi Bin Hasbullah, Iftikhar Ahmad, and Daniyal M. Alghazzawi. ”Classification of attacks in vehicular Ad hoc network (VANET).” International Information Institute (Tokyo) Information 16, no. 5 (2013): 2995.

AUTHORS PROFILE

Ms. Komal Singh is working as an Assistant Professor in Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India. She has completed her graduation from Graphic Era Deemed to be University, Dehradun and Post-graduation from National institute of technology Kurukshetra. Her area of interests include machine learning and network security

Dr. Sachin Sharma, Associate Dean, International Affairs and Associate Professor, Department of Computer Science and Engineering at Graphic Era Deemed to be University, Dehradun, UK, India. He is also Co-founder and Chief Technology officer (CTO) of IntelliNexus LLC, Arkansas, USA based company. He also worked as a Senior Systems Engineer at Belkin International, Inc., Irvine, California, USA for two years. He received his Philosophy of Doctorate (Ph.D.) degree in Engineering Science and Systems specialization in Systems Engineering from University of Arkansas at Little Rock, USA with 4.0 out 4.0 GPA and M.S. degree in Systems engineering from University of Arkansas at Little Rock with 4.0 out 4.0 GPA and He received his B.Tech. degree from SRM University, Chennai including two years at University of Arkansas at Little Rock, USA as an International Exchange Student. His research interests include wireless communication networks, IoT, Vehicular ad hoc networking and network security.