Manuscript Number: SNDC-21-9029

Type: Research Article

Received date: February 04, 2021; **Accepted date:** February 18, 2021; **Published date:** February 24, 2021

A VANET Protection Survey: Issues, Threats and Solutions

Abhishek Gupta*

Department of Computer Science and Engineering, Chandigarh Engineering College, Landran Mohali, India

****Address for Correspondence:*** *Gupta Abhishek, Department of Computer Science and Engineering, Chandigarh Engineering College, Landran Mohali, India*; *Email: guptaabhishek11581@gmail.com; abhishek.4186@cgc.edu.in*

Abstract

Vehicle Ad-hoc Network (VANET) is a non-infrastructure system. It provides improvements in safety technologies and makes driving easier. The network helps vehicles to share their data for traffic analysis and security purposes. With the development of modern technology and smart cities worldwide, the VANET sector has expanded. VANET provides a self-aware framework that can greatly impact on improving traffic related services and reducing accidents in the road. The information shared in this network is time-limited which requires a well-built and fast network connection. VANET, due to its wireless ad-hoc nature, fulfils this requirement, albeit with security concerns. The most dynamic connections of this network, sensitive information sharing and time sensitivity make it an attractive area for aggressors This study describes the literature survey on VANET with the main focus on security issues and the challenges coupled with it. VANET, architecture, security fundamentals, attack types, and characteristics of probable attacks on VANET are discussed in this paper.

Keywords: VANET • Architecture of VANET • Sybil • ARAN • SEAD

Introduction

Now a day, the heavy volume of traffic in the road influences the security and proficiency of traffic condition. “Around 1.5 million individuals were killed in 2017 because of accidents on the road”. Traffic security on the road has been the difficult issue in rush hour to handle. One conceivable path is to provide the vehicle related data to the vehicles with the goal which they can utilize to broke down the road traffic conditions. It tends to be accomplished by exchange the data of traffic condition among vehicles. Every vehicle is movable object in nature, consequently a mobile network is required which can act without any infrastructure support. With advances in the field of microelectronics, it is now possible to connect node and network devices to a single unit and wireless interconnection, i.e., ad hoc networks. This network was developed as a mobile ad hoc network [1].

VANET (Vehicle Ad Hoc Network) is a type of mobile ad hoc network. It is a self-contained system that can be built by integrating vehicles with web access for drivers and passengers, with the aim of improving web security and traffic management. In VANET, the communication is built up by exchanging the data about the street and movement conditions to avoid road accidents and efficient result of traffic [2-5].Communication can be provided in VANET in different ways. There is a complete wireless ad hoc network, where there is a vehicle to operate without any help of infrastructure. Another is the correspondence between roadside units (RSUs), fixed infrastructure and the vehicle. Every node in VANET is furnished with two sorts of components which are On-Board Unit and Application Unit (AU). On Board Unit is equipped with communicational capability whereas Application Unit implements the program making OBU‘s communicational abilities. A Road Side Unit can be linked to the infrastructure network which in turn associated to the internet. “OBU consist of a Resource Command Processor (RCP), and resources comprise a read/write memory used to pile up and retrieve information, a user interface, a specific interface to tie to other OBUs and a network device for minute range wireless communication based on IEEE 802.11p [6-9] radio technology Figure 1.”

The rest of the paper is structured as follows: Second section explains the security constraints of VANET, the security requirements of the system, and the challenges associated with security of VANET. Third section specifically focuses on assaulter and their types, attacks types on VANET, and preventive measures. Fourth section focuses on probable solutions to various attacks. Finally, Section five concludes the paper.

VANET Security Requirements

Due to the extremely changing topology, security of any network such as VANET is a real challenge. The issues of security are a significant test of VANETs and have to pay attention before deployment of any applications dependent on such kinds of systems. To know how vital security is, try to imagine that a security message initiated by a VANET system has been altered, deferred, or rejected due to any type of attack that caused by an attacker. As such, severe issues could happen such as injuries, deaths, damage of property etc.

Security Goals

The aim of network security is to keep safe the information from being hacked or modified. Network security can be analysed by following three goals-

Keep the privacy of data.
Preserve the reliability of data.
Keep the data available for authorized users all the time.

1. Keep the privacy of data: Privacy of data means confidentiality with the purpose to avoid the illegal expose of information. It includes the safety of data, providing access for those who are permissible to see it while prohibiting others from accessing the contents. It avoids essential information from getting into the hands of wrong folks while making sure that the right persons can have access to it [10-12]. Encryption of data is a good example to confirm secrecy.

2 Preserve the reliability of data: Preserving of data means to maintain the integrity of data. Integrity refers to the approaches for ensuring that information is unaffected, accurate and protected from unapproved client alteration.

3. Keep the data available for authorized users all the time: This security goal if achieved makes the data to authorized users all the time It means availability of data can be achieved through this goal. It is the assurance of trustworthy and consistent access to our delicate information by approved individuals.

Attacks in VANCET, classification and protective measures

In a network, there are many types of attacks, mainly on the network of vehicles. The impact of these attacks on the system depends mainly on the intent of the invaders behind it. The oscillator can perform malicious activity for a number of reasons, to get access of the system amenities for which he is not a legitimate user**,** for accessing the system's confidential data or disrupting the network's efficient functioning. Classifications of attackers on the basis of functionalities are described as [2].

Classification of attackers based on Association: Any recognized or unrecognized node can execute suspicious action in the network .Membership function exceptionally influences the effect of the assault and its prevention. On this the attackers can be classified as:

- **Internal Assailant:** They are the nodes that are authorized to perform suspicious activity only for their own personal benefit or to interrupt the network. These types of assailant have larger impact than the external ones.

- **External Assailant:** In this type attackers are the intruders who try to gain the access of the network either by masquerade or some other type of attacks.

Classification of attacks based on Activity: Based on the activities of attackers i.e. whether an attacker makes modifications to network or not, the assaulter can be classified as:

- **Active Attacker:** The assaulter in this type tries to harm or change the network related information and generates malicious packets and signals. Attacks by attackers in this type are more effective than that made by the other one i.e. passive type of attackers.
- **Passive Attackers:** In this the attackers do not modify the network data and information. They just quietly observe the network and use the information for their own benefit.

Classification of attacks based on Intensions: Any attack that is allied with the intension of the attacker, i.e. main objective of the attacker behind that attack. Following are the different types of attackers based on this:

- **Rational Assaulters:** In this the assaulters seek his own benefit from the attacks and therefore are easy to predict.
- **Malicious Assaulters:** The assaulters in this type of attack do not gain individual benefit. The main objective is to just to build problems in smooth working of network so that the data transfer can be affected.

VANET functions over the information that is life critical and is very sensitive in nature. So this type of information looks eye-catching to attackers; and the network serves as a fertile area for such malignant aggressors. VANET networks can be classified in five different classes as follows [7].

Network Attacks: These are the most severe type of attacks. The entire network will get affected from this. These are the direct attacks over smooth working of network and nodes. Sybil, DoS are some examples of attacks that lie in this class.

Application Attack: These types of attacks are mainly concerned with the information being shared and with the application being served. Eavesdropping, Bogus data are the example attack that lies in this class.

Social Attacks: The sort of assaults that create emotional disparity in other drivers come into this category. In this type of attacks unethical messages are sent to vehicles that distract the driver and may results into driving disruption that may lead to accidents.

Timing Attacks: Timing attacks do modification in the time slots of messages with the purpose to add some kind of delay in data transmission.

Monitoring Attacks: In these attacks, attacker silently examines the entire system and can perform malicious activities based on those observations. All passive type of attacks belongs to this class. Session hijacking and masquerade can also be considered in this type Table 1.

This is not an effective measure as in VANET node can have additional computational resource. The second approach has assumption that 'there is only one radio in each node' and 'a radio can send or receive only on one channel at a time'. So Sybil node working over different channel gets identified [10].

Impersonation: In a replication attack, the attacker refers to himself as an authoritative node. The purpose of these attacks is to harass the network or gain access to network privileges. These attacks are made possible by identity theft or false character possession. Fraud attacks can be prevented using the Trust Authority (TA) and Public Key Infrastructure (PKI) [11]. TA knows the true identity of all nodes. Whenever a vehicle contacts a new RSU, it first verifies its identity through the TA and then the vehicle shares the key.

Bogus Information: An attacker sends the wrong information to the network for personal gain. For example, a malicious node may send misinformation of heavy traffic due to an accident on the road and makes its route clear. Hashing and asymmetric cryptography is used for their handling.

Denial of Service attacks: DoS attacks have serious impact in any network. These attacks make the victim node unavailable to other legitimate user. This can be performed by Jamming, SYN flooding or distributed DoS attacks. Prevention to these attacks can be done through IP-CHOCK model. In this OBU analyze and update the IP information and on finding any duplicate IP it identifies the chances of DoS attacks [12].

Routing Attacks: These attacks exploit the shortcomings of routing protocols and their weaknesses. Major attacks in this category:

Blackhole Attack:
In these types of attacks, the attack node sends a duplicate route with the minimum hop count to the source, and when the source node transfers the data packet to that route, the attacking node drops the packets.

Grayhole Attacks: This is similar to a black hole attack, because it includes dropping packets, but it only throws the selected packet and has the attacker's need and purpose.

Wormhole Attack: The attacking nodes i.e. nodes are evolved to make tunnels receive the packets at one side and tunnel it to the other side of the network. Due to this tunnelling, route hop count containing the compromised node decreased and hence the route attracts packets toward it.

Eavesdropping: This is a threat to confidentiality and is often occurred. The main objective of these attacks is getting confidential and sensitive data for which attacker is not a legitimate person. These attacks fall in category of passive attacks where attacker silently sense the channel and get the information and further use that information for his own benefit. These attacks can be prevented by encryption of sensitive and confidential data.

Location Trailing: These attacks directly target the privacy. In this attack position or path followed by the vehicle is illegally trailed to trace the vehicle and to get private information about the driver. For prevention of such attacks ID-based security systems can be used [13].

Replay Attacks: In these attacks the attacker imitates itself as legitimate user or as RSU and replay the transmission of a previously captured packet. Replay attacks target the authenticity and confidentiality of the system. By using timestamps and global clock for all the nodes, system can be prevented from these attacks.

Session Hijacking: In this attack the attacker get the unique Session Identifier (SID) assigned for each new session and through that get the control over the session. Network layer session hijacking has an advantage that at network layer only one time authentication is performed. After generation and assignment of the SID, no authentication is done and hence this attack takes advantage of this feature. Encryption, dual authentication, random SID generation etc are some preventive measures for these types of attacks [14].

Timing Attacks: In this attack the malicious node when receive any data packet, it just not forward it but it alter the timeslot of the packet to create delay. As a result of it neighbor of the compromised node get the message after the time they suppose to receive it. Since information traversed in the network may be a sensitive information, especially in VANET information are time critical, so any latency can result into major accidents and casualty and serious traffic issues. Use of cryptographic solution such as TPM (Trusted Platform Module) can be used to prevent such attacks [15].

Table 2 represents the summarized view of attacks, attack class, their preventive measures in the basis of properties violated.

VANET securit solution

VANET has been suspected of a variety of attacks as discussed so far. Various research works has been done to provide security measures in VANET. In this section some of the work related to security solution for VANET security is discussed.

ARAN: This routing protocol, named as Authenticated Routing for Ad-hoc Network (ARAN), is a security standard based on the AODV protocol [16]. In this manner, a third party providing authentication certificates signed to the nodes is involved. In this process, each node on the network side is required to transfer the request certificate to the CA. The CA's public key is known to all authorized nodes. Asymmetric cryptography is used as a technique to identify authentic safeguards.
ARAN basically has 5 steps [17-18];

- Certification
- Authenticated Route Discovery
- Authenticated Route Setup
- Route Maintenance
- Key Revocation

Route authentication process is done at each step, through addition of sign and certificate of each intermediate node, so Impersonation problems are solved by this protocol.

SEAD: Secure and Efficient Ad hoc Distance vector protocol this routing protocol works on the DSDV. It uses a one-way hash function for the validation process. This protocol protects against incorrect routing. Destination-serial number is used in this system to ensure that the route is realistic. The hashing mechanism is implemented at each intermediate node to ensure the authenticity of the routes.

Ariadne: This protocol is based on the on-demand routing protocol DSR [19]. This protocol performs very efficiently the use of symmetric cryptographic operations. Max and one-way hash functions can be used for authentication and redistributed between nodes using shared keys. Broadcast authentication technology Tesla is the source of this protocol. Tesla time period is used in the root discovery and authentication process

SAODV: The purpose of this protocol is to incorporate security measures into the AODV protocol [20]. All messages are digitally signed to achieve authenticity, and the hop compute-based hash function is used to protect the network. In this method, the path is not sent by the intermediate node, even though the path is known. This problem can be solved by double signature but it increases the complexity of the system.

A-SAODV: SAODV extends to A-SAODV as an experimental feature of positive answer decision. In this, each intermediate node can decide whether to forward the source node based on the length of the queue [21].

One Time Cookie: Cookies are assigned to each session in session management. The One Time Cookie Protocol gave us the concept of OTC (One Time Cookie) [20] to protect the network from network hijacking. The OTC generates the token for each request, and the token is added to the token requesting to use the HMAC to avoid using the token.

ECDSA: Elliptical Curve Digital Signature Algorithm [21], as the name suggests this algorithm use digital signature. With hash function and asymmetric cryptographic operations authenticity and security is provided in this system. Both the sender and receiver need to be agreed upon elliptical curve domain parameters.

RobSAD: Strong Method for Sibyl Attack Detection [17] The main concept behind this method is that two different vehicles do not have the same speed pattern and are driven by different drivers, because each has its own. Drives according to convenience and need. The Sybil node is identified by two or more nodes searching the trajectory of the same speed Table 3.

Holistic Protocol: This protocol defines the authentication technique by registering vehicle by RSU [3]. In registration phase vehicle send Hello message to RSU then in response RSU prepares Registration id (consisting licence number and vehicle registration number) and send to vehicle. Further the authentication is done through certificate provided by RSU. If the node is authenticated then only data is shared with it otherwise the node is blocked.

Conclusion

VANET needs a safe and protected environment as a platform for the exchange of information. Due to its extremely dynamic environment, wireless medium of communication and constantly changing topology, VANET offers incredibly broad scope of assaults. VANET related security problems and concerns have a very high impact on effective system functionality. Today due to its enhancing features of providing quick, stable and comfort driving, VANET is being widely deployed. The hot topics related to current scenario are VANET, feature of VANET, need for protection in VANET. In this paper, we conducted a literature survey of different types of attacks, their preventive steps, type of assaulters and some current security solutions for VANET attacks.