Vehicular Ad-hoc Networks and Associated Risks

P Aishwarya Naidu[*1], Satvik Vats[*2],Pooja Chadha[*3], Rajeshwari K[#4]

[*]*B.E Student, Department of Information Science and Engineering, B.M.S College of Engineering, Bangalore, India*

[#]*Assistant Professor, Department of Information Science and Engineering, B.M.S College of Engineering, Bangalore, India*

Abstract — *We are transforming into a new era of technology in which everything around us is 'smart', be it our home appliances, our work related gadgets or even our cities, everything is turning into an interactive and connected collection of technologically advanced devices, where each and everything is managed such that the resources are used in a sustainable way and our needs are also fulfilled. The transportation or vehicular movement of people or goods is one such necessity that has created a lot of chaos in our cities. Our travel infrastructure is not able to cope up with the expansion in the vehicular traffic on roads as it should have been. Thus, leading to a complete mismanagement of traffic which ultimately adds to the suffering of people in form of loss of life and property due to road accidents, adverse environmental impacts in form of increased emissions from vehicles in congested traffic and it also causes a complete failure of public transport systems in the cities. It is due to this failure of public transport systems that a strong need for a technologically innovative solution focused on vehicle management is needed. Vehicular ad hoc networks (VANET) is one such solution which provides us with a dedicated network interconnecting vehicle to one another and to the roads is being developed and researched across the globe to make our vehicles 'smart' and ready for the new 'smart' world that we have dreamt of. Although, VANETs are extremely useful and are the need of the hour, there are a few risks associated with them. This paper outlines the security and privacy threats associated with these networks that need to be taken care of before placing any such system in use.*

Keywords — *Vehicular ad hoc networks, Wireless, Security, Attacks*

I. INTRODUCTION

The Intelligent Transport Systems (ITS) is the need of the 'smart' world that humans are trying to form as the advancement of technology has led to new discoveries of driverless or automated vehicles but the infrastructure on which they rely to operate or commute remains the same and rather a limited resource. Hence, the management of traffic remains a top priority and concern in order to accommodate all the pre-existing as well as new vehicles that are technologically advanced on the same infrastructure. Vehicular ad hoc network (VANET) is a network that has vehicles and road side units (RSUs) working as its nodes in the dedicated network, whereas the nodes in Cellular and WLAN/LAN networks are our mobile devices, access points and routers placed in the network. VANETs are structurally and principally similar to Mobile Ad hoc Networks (MANET) as they are also a router-less network with mobile nodes. The role of IoT in today's world cannot be ignored as now a days more and more vehicles are becoming IoT enabled but when talking about vehicles they have different needs and different constraints, therefore, enabling IoT technology in vehicles alone cannot fulfil our requirements of smart traffic management using ITS and that of providing a safer travel or commute to people. In VANETs each node participates in the task of forwarding the data packets and the routing decisions are made dynamically depending upon the vehicle's position and RSU position. The routing protocols used in VANETs can be reactive routing protocols that make routing decisions in real-time as vehicles move from one place to another and according to traffic management norms specified.

With the increasing traffic that our roads are witnessing today, they seem to have been already exhausted and not only this, it also has led to an enormous increase in unfortunate cases of road accidents and associated deaths, injuries and loss of property as well. These mishaps reveal a noticeable pattern in their occurrence as most of it is happening in the places where the traffic is comparatively less technologically managed or controlled. This vulnerability can be observed as there is no Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) communication happening that can predict the upcoming danger based on congestion levels and road advisement in case of uneven roads or terrain. Due to this VANETs seem to be playing a key role in future Intelligent Transportation Systems (ITS). Going by records it is evident that approximately 1.35 million people die in road accidents each year across the world. This data comes at a time when more and more money is being spent on infrastructure development of countries and major cities in them which is focused on increasing road cover, making expressways and ring roads. This scenario suggests that increasing the road infrastructure alone cannot solve and satisfy the safety needs of passengers and vehicles. It also implies that the need of a technical solution is needed and VANET is a promising solution to this, as it is innovative and effective for management of vehicular traffic. All the nodes in VANET will be connected to each other, enabling vehicles to send and receive data from each other and from the road side units (RSUs). This data could be used by regulating authorities in real time to manage the traffic movement.

One big advantage comes in the form of the ease with which VANETs can be used to manage the public transport system in our cities. As we know that despite the huge investments and arrangements made in our public transport systems in metropolitan cities, the system seems inefficient and insufficient. Primarily because the available resources are not managed at real time according to the passenger loads on different routes and timings. The buses when connected to each other and to RSUs through VANETs can share real time traffic data and also bus timing at different stops on a route can be fixed and passengers can access that information about bus schedule. In this way the same number of buses can be utilised sustainably and solve the mobility issue by increasing availability and decreasing congestion that leads to discomfort in public transport.

Everyone is aware of the state of our natural resources be it land, air or water. Environmental degradation is one of the major concerns of citizens and governments across the globe. Unfortunately, the ever-increasing traffic and its chaotic management has contributed a fair amount in this degradation. Especially in noise and air pollution, as they contribute to the elevation of particulate matters like nitrogen oxides and ozone. Having a dedicated network like VANET that has a network in which the vehicles themselves are acting as nodes and routing the information dynamically will help to control vehicular movement according to the air pollution level and congestion on different roads.

Now we are able to accept that VANETs are an innovative and useful technology that needs to be researched upon. It's architectural features needs to be researched upon as it has to address a lot of challenges like managing the real time constraints as the nodes here are continuously moving and sharing data with one another, other challenge is that of the network system's tolerance towards any kind of functional or non-functional errors because it will be deployed in the critical traffic management systems in which any error could lead to a serious mishap. Apart from these challenges the VANETs also face the challenge of maintaining data consistency liability. They are also vulnerable to different types of cyber security attacks like impersonation in which a malicious node in the network would try to appear and function as an authenticated node/vehicle. Location tracking can also be done putting at risk the driver's privacy and data. Similarly, VANETs also need to have a defence mechanism against the routing attacks by compromising the routing protocols in the network layer as this may lead to disruption in the routing process and the data packets may lose their path and not reach their actual destination. Eavesdropping, session hijacking and Denial of Service attacks are some of the other attacks that VANETs are vulnerable to. Thus, it is important to assess the associated risks of implementing and using VANETs so that they can be resolved or a mitigation strategy for avoiding them can be formulated.

II. LITERATURE REVIEW

In [1], the authors provide a summary of state of the art of VANETs. The basic architecture and state of the art such as characteristics, standardization, protocols, projects and applications of these systems are outlined. The architecture of VANETs includes various components. The vehicles are equipped with an On Board Unit (OBU) which is mounted on the vehicle as shown in Fig. 1. The unit of infrastructure located on the road is called the Road Side Unit (RSU). There exist two kinds of communication in VANETs.

1.Vehicle to Vehicle (V2V) is an ad hoc communication mode in which messages are exchanged directly between close range vehicles or indirectly using multiple hops.

2.Vehicle to Infrastructure (V2I) is the communication between vehicles and network infrastructure such as the Road Side Unit (RSU). In this mode, a vehicle makes a connection with the RSU to connect to external networks such as the Internet. This type of communication is hard to attack and also requires more bandwidth.

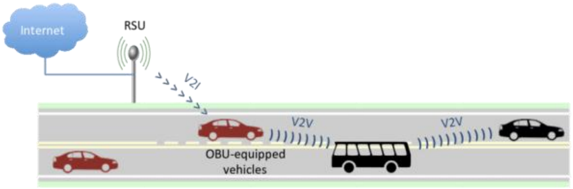

Fig. 1.VANET System Architecture [2]

Some of the standard protocol stacks dealing with vehicular communication include DSRC, WAVE and IEEE 802.11p. WAVE IEEE 1609 defines an architecture for VANET environment to operate and establish V2V and V2I communications using a standard set of protocols, interfaces and services which also define the security of exchanging messages. The WAVE IEEE 1609 standards family includes standards such as Resource Manager, Networking Services, Multi-Channel Operations, Layer Management to name a few [3]. The security challenges of VANETs are presented whilst also defining the entities directly involved which are: the driver, OBU, RSU, third parties and the attacker. Since VANETs communicate using wireless medium, it has many drawbacks when it comes to security such as eavesdropping, jamming and interference. The architecture of vehicular networks involves all seven layers of the OSI model, thereby making it vulnerable at almost every level from physical to application layer. The security attacks are classified from a cryptographic standpoint since the proposed solutions are based on cryptographic techniques such as encryption/decryption, symmetric cryptography, asymmetric cryptography, PKI, digital certificates and time stamping. The solutions are compared and studied to evaluate their efficiency. The authors finally express that it is important to look into new cryptographic techniques such as homomorphic encryption and ID-based cryptography to overcome the weakness of the present system.

In [4], authors bring up a great concern on the security aspects of VANETs. The article mentions that a wireless network of intelligent vehicles can make travel safer and efficient, but it also raises a question on whether hackers can exploit the system to cause accidents. Security in VANETs is essential because it affects the lives of people. It is crucial that the information communicated in VANETs cannot be deleted, modified or tampered by an attacker. Any security breach can cause huge problems. The main factors which are the basis of security breaches in VANETs are: the use of wireless medium, high mobility and its dynamic network topology [1]. It's highly dynamic environment pertaining to the frequent arrival and departure of cares, and short connection periods, makes it a difficult task to come up with a complete security solution. The literature [4] mentions the DoS attacks at the link layer and on the network layer. Since the system depends on a cooperative channel sharing mechanism, it exposes the network to DoS attacks at the data link layer. The wireless medium makes the system vulnerable due to interference, limited bandwidth and anonymity. Attackers can jam the wireless medium or exhaust the limited bandwidth which can achieve denial of service. DoS attacks also threaten the system at the network layer. If a message in VANET cannot be propagated directly, it is delivered by a multi-hop mechanism similar to a router. The reliance on hopping through unknown nodes presents a threat of DoS attacks. Attackers could hack the nodes or impersonate or legitimate nodes. The malicious nodes could fail to forward the messages, delay propagation or even alter the integrity of the messages.

The authors in [5] talk about different forms of DoS attacks and techniques. The authors provide classification based on the various mechanisms of the attack such as scope of the attack, number of attackers, purpose of the attack and the OSI layers in which the DoS attack happens. The attacks discussed include SYN flooding, wormhole attack, blackhole attack and grayhole attack etc. It also lists the various algorithms which can be used to detect and prevent DoS attacks. The literature mentions that DoS attacks are one of the most dangerous attacks because they interrupt the services for a legitimate node or block them from accessing any network resources which leads to isolating the node. This results in degradation and denial of service. Due to this, there is a reduction in throughput which ultimately leads to unavailability of service.

Preservation of commuter's location privacy is discussed by authors in [6]. Authors present a state-of-the-art survey on using mix zones to prevent misuse of location information that is shared over the VANETs. They identify the On Board Unit, Road Side Unit (RSU) and Third Party (TP) providing connectivity, as the three basic parts of VANETs that when put together, form the whole architecture. They have emphasized on the use of a temporary secret name by nodes in the networks, that are the vehicles on roads and this name has to be different from real node id, also it should keep changing so that attackers are not able to guess it. This unique id that will be used by vehicles are known as pseudonyms, but they alone cannot ensure safety from the attackers who would try to know the previous and current location of vehicles connected through VANETs, as the pseudonyms will have linkability. This shortcoming gives rise to the mix zones that are basically a specific region over the roads upon entering those regions the vehicles will change their pseudonyms in a coordinated way such that acquiring pseudonyms in it will ensure unlinkability as shown in Fig. 2. In order to achieve unlinkability the mix zones will implement dummy events in them, anonymization and obscuration of nodes etc. Just a care has to be taken that the vehicles should not enter and exit the mix zone at the same time in a coordinated way instead they should enter and exit it in a random manner.

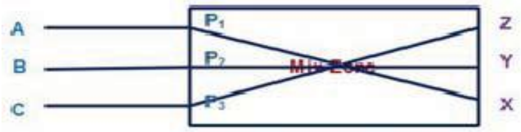

Fig. 2. Mix- Zone Model [6]

There are other risks associated with VANET in addition to security. These challenges are present due to the architecture and the very nature of the system itself. These challenges are presented by authors in [7] which include time constraints, scale of the network, high mobility and volatility. The nodes in the network have to transmit important messages in an accepted time limit especially when it comes to emergency messages related to safety. However, this is a difficult task considering all the messages must first be authenticated for security reasons which increases the delivery time of the messages. Network scale is another issue to consider. VANET is about to become the biggest ad hoc network in the world since there are millions of vehicles on the road. There has to be some global authority who will govern the network and is in charge of managing identity as well as distributing the private and public keys for security reasons. The authors have also presented various security requirements, threats, attacker profiles and attack characteristics [7].

In [8], the authors proposed an algorithm for detection and prevention of Sybil attacks in VANETs. A node is classified as genuine or not with the help of a public key which is given to every registered node. Using PKI (Public Key Infrastructure), key management strategy is used to identify targeted nodes at routing time. If the node has its own public and private keys it is known to be a legitimate node or targeted node otherwise. To detect sybil threats, cryptographic hash functions are also used. Safety analysis of work proposed by authors shows that it is secure against multiple recorded attacks and offers additional security features such as mutual authentication, RSU confidentiality. The number of packets transmitted between the endpoints in the suggested method is 325 for a simulation period of 50ms, while the number of packets transmitted in sybil attack is 220.

In [9], authors talk about how an unauthorized user can hijack a session by duplicating MAC address at link layer and TCP sequence number at the transport layer which leads to packet delay and network congestion. These authors present a machine learning algorithm to discover malicious nodes in the VANET system. The Roadside Unit of a session behaves as a Central Head which observes the traffic flowing through all the nodes. If the traffic is found out to be more than 1 then it is considered to be a malicious node and a warning message is sent out to all the nodes of the session. A new session is then started excluding the malicious node. Information about the malicious node is transferred to other RSU in the network. The authors simulated the model using Network Simulator NS-2 and the simulation results showed less delay and throughput.

In [11], the authors have proposed an algorithm to prevent the security threats on VANETs. They have focused mainly on avoiding DDoS attacks and Sybil attacks on the VANETs by selecting a routing protocol that has the highest receive rate of data packets between the nodes/vehicles. The comparison was made with the help of a simulation tool called Simulation of Urban Mobility (SUMO) that generated a real time scenario including roads, vehicles, traffic lights and pedestrians. Simulation results showed that Dynamic Source Routing (DRS) algorithm had better throughput when compared to other protocols like Destination-Sequenced Distance-Vector (DSDV), Optimized Link State Routing Protocol (OLSR) and Ad hoc On-Demand Distance Vector (AODV). This state of the art work analysed different research works in the VANET security domain and categorised the solution presented in them by either being detective or preventive towards the security risks addressed in them. It can be deduced that where on one hand most of the state-of-the-art works have emphasised on methods that are detective measures, i.e. once any such security attack happens, whereas the methods for prevention or risk reduction of the same attacks were less when compared to preventive measures.

In [12], the authors proposed an algorithm to detect multiple malicious nodes in contrast to the existing algorithms that detect a single malicious node at a time. In the proposed work, the nodes communicate via RSU which stores information about their locations and checks the frequency and velocity of each node. If the frequency and velocity is found to be more than a specified range then the node is tracked and all the messages sent by the node are stopped to avoid DoS attack. The node is removed from the network and is not allowed to send any more packets. The simulation was done in NS-2 with different numbers of nodes and multiple parameters were considered. The proposed work gave better results than the existing algorithm in terms of packet loss ratio, lifetime of network and network throughput.

In [14], the authors talk about a new security measure for vehicular cloud computing. The existing security measures verified only the key given by the user but not their identity which is not enough for ensuring security. Authors proposed a security mechanism which involves UBP (User Behaviour Profiling) and DT (Decoy Technology) over fog computing systems. Whenever an attacker tries to get a hold of user data through the network, the protocol automatically creates a decoy file of the same name and scrambles information in such a way that it appears original as the intended file and gives it to the attacker. Serving decoy files misleads intruders to think they extracted valuable information [15]. System was analysed by trying it on 50 vehicles and using UBP and DT together gave better results than them being used separately.

In [16], the authors talk about a model to detect sybil attacks. Attacks in which a node obtains several false identities and sends messages through those identities into the network which can lead to DoS are called sybil attacks. Authors suggested a model based on public key infrastructure. Encryption and decryption algorithms on combinations of public keys and RSU time stamps were used for secure communication in VANET. By using a public key encryption mechanism, sharing via a public key infrastructure algorithm in the real-time environment and receiving real-time certificates of authentication from authority is difficult. The proposed model was successful in detecting if any node attempted to interrupt the communication between two or more vehicular nodes.

III. SECURITY IN VANET

It is important to analyse the security aspects in VANETs as the development of mitigation strategies for such vulnerabilities is crucial for deployment of VANETs in its purpose of enabling V2V and V2I communication over an area. These possible security attacks have to be analysed in detail to develop a VANET architecture that has methods that are capable of detection as well as prevention of the security risks. In this work of analysing security in VANETs the first step is to know all the entities of VANET that are either affected by or themselves affect any risk factor or vulnerability present in the architecture. Then according to these entities, the security requirements of the network are formulated. Knowing the attackers, attack characteristics and the attacks themselves is as important as knowing the associated entities and security requirements of the architecture. Thus, in the following sections we put forward the entities, security requirements, attacker profiles, attack characteristics and the attacks respectively.

A. *Entities*

The entities involved from a security standpoint are presented in Table 1.

TABLE I
SECURITY ENTITIES

Entities	**Description**
The Driver	The driver is a significant entity in VANET security because it is always present and makes important decisions based on the information received. If any attack occurs, the driver is the one most affected.
The Vehicle (OBU)	The vehicle, which has the OBU mounted on it, is one type of node present in the system. In a security system, we can differentiate between two kinds of vehicles: normal vehicles and malicious vehicles.
Road Side Unit (RSU)	RSU is another type of node present in the system. Similar to OBU, we can distinguish two kinds of RSU: normal RSU and malicious RSU.
Third Parties	Third parties include trusted (or semi-trusted) third parties such as the law enforcement, transport regulators, vehicle manufacturers, traffic police. Every third party has their own respective public private keypairs.
The Attacker	Attacker is a single or group of unauthorized nodes intending to perform malicious activities to disrupt the system to achieve its goal

B. Security Requirements

Before talking about the security attacks of the system, it is important to understand the security requirements. Whenever a security requirement is compromised or not followed, it leads to a possible threat. The main requirements for VANET security are given below.

1) Availability**:** For a system to be useful, it must be available to its authorized users. Availability is a crucial requirement for vehicular networks. It ensures that the network is fully functional and that the information required is available to those who need it when they need it. The user’s lives are at risk if essential information such as road safety information is not delivered when needed. Disruption of system availability for even a short time can lead to catastrophes. Due to its immense importance, availability is one of the biggest targets for attackers.

2) Authentication: It is essential to authenticate all the users in the network before letting them access its services since it controls the level of authorization of the vehicles. Authorization is a mechanism which determines the privileges or level of access a particular user is allowed. Ensuring authentication in VANETs protects the legitimate nodes from outsider or insider attackers who are intruding in the network under a false identity. Therefore, having information about the transmitting node such as its identity and other properties such as location is useful.

3) Data Integrity: Integrity ensures that the exchanged data in the system has not been tampered with during transmission. It helps to protect the information in the messages against modifications, additions or deletions. The message received must match the message that was sent. In VANETs, integrity is mainly compromised in V2V communications since they are fragile in comparison to V2I communications.

4) Confidentiality: When there is communication between two entities, outsiders should not be able to access this confidential information. The data should only be read by the authorized parties. If not, sensitive information such as the user's location or routes might be collected. Confidentiality in VANETs depends on the application. If the message is safety related which does not contain any sensitive information, then there is no need for it to be confidential. But for other applications such as toll payments or user personalized data such as maps information need to be kept confidential by encrypting them.

5) Accountability: Accountability in security means the state of being able to verify the sender and the receiver entities who claim to have sent or received a message. This makes it infeasible for the entities involved in a communication to deny having participated in the event. This creates undeniable evidence for an event or action. It can be used to resolve disputes that might occur. Malicious users will not be able to deny their actions. Another word for accountability is non-repudiation.

6) Access control**:** Access control defines the rights and privileges of the nodes in the network. There are some sensitive communications in the network which must only be accessible to those from the law enforcement or police. It must not be accessible to any other nodes in the system. This requirement makes sure that unauthorized nodes are prevented from communications they have no access right over.

C. Attacker Profile

Defining the capacities of the attacker is another important task before describing the attacks itself. The attacker's characteristics can help us understand his intentions and how to handle the attack. In this section we present the four dimensions in defining the attacker profile [10].

***1) Outside vs Insider*:** An outsider is someone who is not part of the network. They are not authenticated to the network which limits the type of attacks they can perform. However, eavesdropping is one of the attacks which an outside can perform to collect information of the drivers for future attacks. An outsider can also jam the network or initiate a DoS attack by flooding bogus messages. VANETs can also be attacked by insiders. This presents a grave danger because insiders are authenticated users of the network which gives them more access compared to outsiders. An insider can either be a fully authenticated user of the network or a third party who holds a certified public key. It is very easy for an insider to initiate an attack. They also have to power to cause greater damages.

***2) Malicious vs Rational*:** A malicious attacker gains no personal benefit from attacking the system. They do not have a specific target nor do they seek a specific result. Their only goal is to harm the users of the network and cause the maximum amount of damage. They may employ any means necessary to bring down the system with any regards to cost or consequences. This makes them unpredictable. A rational attacker has a specific target and personal benefit. This makes their actions more predictable.

3) *Active vs Passive*: An active attacker attempts to alter or modify the information being transmitted. They generate packets or modify them. Usually these attackers have authorization in the network. A passive attacker simply observes the information or messages being transmitted. They do not interfere. The legitimate users of the network have no idea that their information is being observed. While this does not harm the system or its users, it can be used to gather information for future attacks. Generally, passive attackers are outsiders.

***4) Local vs Extended*:** An attacker can be distinguished in the scope of his attack. A local attacker has control of one or more nodes within a short range. An extended attacker has control over nodes scattered all over this network.

D. Attack Characteristics

In order to understand and build a powerful security system for VANET, it is important to understand the characteristics of the attacks that might take place. The attack characteristics [13] are listed below.

***1) Nature*:** The nature of the attack tells how malicious nodes are harming other nodes in the network. This helps us make out what kind of attack is being carried out. For example, a node might give false information about their identity or location or speed. This nature of the attack can be used to trace it to GPS spoofing

***2) Target*:** The target of the attack depends on the distance between the malicious node and the victim node. It can either be local or projected. When the target is local, the malicious and victim nodes are within short range. It is easy for the malicious node to convince and give false data when the target is local. If the target is projected, it means that the victim node is in an extended radius. When the distance is long, malicious nodes will need help from other nodes to convince the victim node about the accuracy of the information. Malicious nodes will also need help from allies to convince the normal nodes that their information is legit because in VANETs, vehicles do not use information from a single source to take any decision and action.

***3) Scope*:** The scope of an attack can either be limited or extended. It tells us about the extent of the damages of the attack. If only a small area was successfully attacked or the number of victims is low, it is referred to as a limited attack. If the attack area is huge, it is considered to be an extended attack. Although, a limited attack can be propagated to a large area and cause an extended attack because it is challenging to prevent such propagations.

***4) Impact*:** The impact of the attack tells us the level of the attack damage as well as the level of capacity in overcoming the attack. There are 3 possible cases: i) detected and corrected, ii) detected and uncorrected, and iii) undetected and uncorrected.

E. Attacks

The various attacks that are possible in VANET are presented below.

1) *Denial of Service*: The malicious nodes in VANETs may try to attack the network so that the legitimate nodes would be unable to connect to the network and the already connected nodes would not be able to participate in V2V and V2I communications. Using algorithms that monitor the network congestion in VANETs and report any suspicious node that is transmitting data at a rate higher than usual can be used to prevent DoS attacks by detaching that node from the network. Emerging technologies like big data analytics can also be incorporated in algorithms designed to detect and prevent DoS attacks in VANET [11].

2) ***Jamming***: It is the act of intentionally disrupting the communication medium by transmitting a signal. This causes the Signal to Noise Ratio (SNR) to reduce. It is called interference when it is done unintentionally.

3) ***Greedy behaviour attack***: This attack happens at the MAC layer. The attacking node does not respect the access method and greedily tries to use the media which prevents other nodes from connecting and using the services. Greedy behaviour cannot be detected by the upper layers' mechanisms as it is independent and hidden to them.

4) ***Blackhole attack*****:** This blackhole attack, apt to its name, describes a security threat in which the malicious node discards the packet instead of relaying them according to the routing protocol. The effects the routing tables and blocks the recipient node from receiving packets.

5) ***Grayhole attack***: Grayhole attack is a variant of the blackhole attack in which only certain packets that belong to a specific application are prone to packet loss.

6) ***Sybil attack***: In this type of attack, the attacker node claims multiple identities at once. This gives an attacker the power to damage the system applications by creating an illusion of traffic congestion.

7) ***GPS spoofing***: Location or position information is of utmost importance in a VANET. It has to be accurate. GPS spoofing consists of providing neighbouring nodes with false position or location information.

8) ***Node impersonation***: In a node impersonation attack, a malicious node pretends to be a legitimate node in the network by obtaining their identification.

9) ***Tunnelling***: In this attack, attackers use the network to create a private connection (tunnel) between two distant parts of the VANET.

10) ***Eavesdropping***: It is an attack in which the attacker listens to the transmission. It is easy to do in a wireless network like VANET. It is a passive attack, so the victim is not even aware of it.

11) ***Key and certificate replication***: The attacker replicates the key or certificate which is used as a proof of identity. By the usage of duplicate keys and or certificates, the authorities have a difficult time in identifying vehicles, particularly during disputes.

12) ***Masquerading attack***: In a masquerading attack, the attacker uses a valid identity of a legitimate node and tries to form a blackhole or fabricate false messages that seem to be transmitted from a genuine node.

13) ***Replay attack***: It is a form of network attack in which it repeatedly broadcasts a message already sent. Non-legitimate users can perform replay attacks.

14) ***Message tampering or suppression***: In this attack, the message is altered. The message is modified or deleted or a new message is created by the attacker to achieve their goal.

15) ***Loss of events traceability***: This kind of attack removes any sort of traces which subsequently means that the attacker cannot be held responsible for their next actions as they can simply deny their involvement. Other attacks can assist this attack beforehand such as the Sybil attack.

16) ***Brute force attack***: Brute force attack performs an exhaustive search of all the possible confidential keys in the hopes of getting one of them right. It is a time consuming as well as resource intensive task. In VANETs, brute force can be used to crack encrypted keys or for the authentication process.

17) ***Man in the middle attack***: As the name indicates, in this attack the malicious node is inserted between the sender and the receiver. The victim nodes believe they are in direct connection but the attacker is in the middle and controls the entire communication.

18) ***Attack on location privacy***: An individual's location or his/her location history is considered confidential information and failure to preserve this information from malicious individuals is considered as a breach in the privacy of that individual. This is one of the attacks that the vehicles interacting in VANETs are vulnerable to [6], as they are constantly exchanging data packets with other nodes/vehicles and RSUs through the OBUs mounted on them. Using deceptive names for nodes instead of the real names and changing it constantly is one of the mitigation strategies. The mix-zone methods described in [6] would also ensure preservation of driver's location data.

The summarisation of different types of attacks that VANETs are vulnerable to and the security requirements that are being compromised by these attacks are presented in Table 2. From Table 2, it is evident that the availability of the network and its services, and authentication of the nodes are compromised in most of the possible attacks in comparison to integrity and confidentiality of the nodes.

TABLE 2
LIST OF ATTACKS

Attacks	**Security Requirements Compromised**
Denial of Service	Availability
Jamming	Availability
Greedy behaviour attack	Availability
Blackhole attack	Availability
Grayhole attack	Availability
Sybil attack	Authentication Availability
GPS spoofing	Authentication
Node impersonation	Authentication Integrity Accountability
Tunnelling	Authentication
Key and certificate	Confidentiality

replication	Authentication
Eavesdropping	Authentication
Masquerading attack	Authentication
Replay attack	Authentication Integrity
Message tampering or suppression	Availability Integrity Accountability
Loss of events traceability	Accountability
Brute force attack	Confidentiality
Man in the middle attack	Authentication Confidentiality Integrity
Attack on location privacy	Confidentiality

IV. CONCLUSIONS

The emergence of VANET has led to a revolution in the domain of ad-hoc networks being used for traffic management by enabling V2V and V2I communications. The very characteristics that are unique to VANETs have also exposed the network to vulnerabilities in the form of security and privacy related threats. VANETs provide various kinds of applications ranging from safety applications, commercial applications to even convenience applications for the commuters on the VANET enabled roads. The challenging features of VANETs, like the large-scale mobility of millions of vehicles on the roads and these vehicles themselves being the nodes of the ad-hoc network, results in a network that has a constantly changing and diverse topology. The ad-hoc network being vulnerable to various security related threats as a result of its features and characteristics needs a detailed analysis of the possible threats and vulnerabilities present in the system in order to develop mitigation strategies to ensure a seamless connectivity in the network. This paper deals with the review of various security related threats and possible strategies to mitigate those threats and vulnerabilities.

ACKNOWLEDGMENT

We wish to acknowledge Dr.M Dakshayini (Professor &Head-Department Information Science and Engineering, B.M.S College of Engineering Bangalore) for her support and guidance in carrying out the research work. We are also grateful to our institute ‘B.M.S College of Engineering’ for providing access to valuable resources to carry out this work.

REFERENCES

[1] Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. "*Survey on VANET security challenges and possible cryptographic solutions*." Vehicular Communications 1.2 (2014): 53-66.

[2] Ligo, Alexandre, et al. "*Comparison between benefits and costs of offload of mobile Internet traffic via vehicular networks*." TPRC, 2015.

[3] ITS, ITS. "*standards fact sheets of IEEE*." IEEE Standards 1609 (2014).

[4] Blum, Jeremy, and Azim Eskandarian. "*The threat of intelligent collisions*." IT professional6.1 (2004): 24-29.

[5] Ahmed, Wedad, and Mourad Elhadef. "*DoS Attacks and Countermeasures in VANETs*." Advanced Multimedia and Ubiquitous Engineering. Springer, Singapore, 2018. 333-341.

[6] Kalaiarasi, C., N. Sreenath, and A. Amuthan. "*Location Privacy Preservation in VANET using Mix Zones–A survey.*" 2019 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2019.

[7] Engoulou, Richard Gilles, et al. "*VANET security surveys*." Computer Communications 44 (2014): 1-13.

[8] Syed, Salman Ali, and B. V. V. S. Prasad. "*Merged technique to prevent SYBIL Attacks in VANETs.*" 2019 International Conference on Computer and Information Sciences (ICCIS). IEEE, 2019.

[9] Jeevitha R. and N. Sudha Bhuvaneswari. "*Malicious node detection in VANET Session Hijacking Attack*." 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE, 2019.

[10] Raya, Maxim, and Jean-Pierre Hubaux. "*Securing vehicular ad hoc networks*." Journal of computer security 15.1 (2007): 39-68.

[11] Naveen R, N.S.V Chaitanya, Nikhil Srinivas M. and Dr. Nandhini Vineeth. "*A Survey on Detection and Prevention of SecurityAttacks in VANET*." 2019 Grenze International Journal of Engineering and Technology, Special Issue.

[12] S. Kumar and K. S. Mann, "*Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs*," 2019 International Conference on Automation, Computational and Technology Management (ICACTM)

[13] Golle, Philippe, Dan Greene, and Jessica Staddon. "*Detecting and correcting malicious data in VANETs*." Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. 2004.

[14] Bousselham, Mhidi, Nabil Benamar, and Adnane Addaim. "*A New Security Mechanism for Vehicular Cloud Computing Using Fog Computing System*." 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS). IEEE, 2019.

[15] M. Mukherjee et al., "*Security and Privacy in Fog Computing: Challenges*," in IEEE Access, vol. 5, 2017.

[16] Soni, Mukesh, and Anuj Jain. "*Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks*." 2018 Second International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2018.

[17] S.Ranjithkumar, N. Thillaiarasu ”*A Survey of Secure Routing Protocols of Mobile AdHoc Network*” SSRG International Journal of Computer Science and Engineering, volume 2 issue 2 February 2015.