JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-4, Issue-10 E-ISSN: 2347-2693

VANET and its Security Issues- A Review

Varinderjit Singh[1*], Karan Mahajan[2]

Department of Computer Computer Science and Engineering,
Global Institute of Management & Emerging Technologies, Amritsar (PUNJAB)

Available online at: www.ijcseonline.org

Received: 23/Sep/2016 Revised: 02/Oct/2016 Accepted: 17/Oct/2016 Published: 31/Oct/2016

***Abstract*—Vehicular Adhoc Networks (VANETs) are gaining growing interest and research efforts over recent years for it offers enhanced safety and enriched travel comfort. However, security concerns that are either general seen in adhoc networks or unique to VANET present great challenges. This review paper presents the basics of VANET which includes architecture of VANET, its applications and its characteristics. The major consideration of this paper is on security, so security requirements and issues related to security are also presented in this paper. This paper also provides information about types of attackers and types of attacks in VANET.**

***Keywords*- MANET, VANET, Key management**

I. INTRODUCTION

The need for communication when the deployment of any fixed infrastructure is impossible and the advancement of computer and wireless communication technologies has led to the development of Mobile Ad hoc Networks(MANETs). This category of wireless networks does not rely on any fixed infrastructure, this make their deployment very easy. In addition, nodes in MANET are enhanced with routing functionalities to provide multi-hop communications. These specific features have allowed the expansion of their use in different application domains. During the last years, a great interest was awarded to the deployment of MANETs to improve road safety, then, Vehicular Ad hoc Networks have emerged. [1]

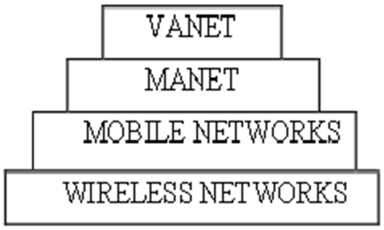


Fig. 1- Hierarchy of Networks [1]

Vehicular Ad hoc Networks (VANETs) are a subclass of MANETs. They are a promising approach for the Intelligent Transportation System (ITS). VANET is a set of vehicles moving on the road, equipped with communication capabilities among one another and with Road Side Units using wireless technologies such as Wi-Fi or WiMAX. The number of possible applications of VANETs is expanding. In addition to safety applications, vehicles are foreseen to support entertainment applications such as peer-to peer applications and Internet connectivity applications. However, these advantages create other challenges in terms of attacks on security since information is distributed in open access environments. Approaches designed for MANETs are not suitable for VANET because they do not consider the high mobility constraints. Protocols designed for VANETs must take into consideration QoS requirements which are important for VANET safety, emergency and multimedia services. QoS parameters such as throughput, latency, jitter, packet loss are key requirements in VANETs.

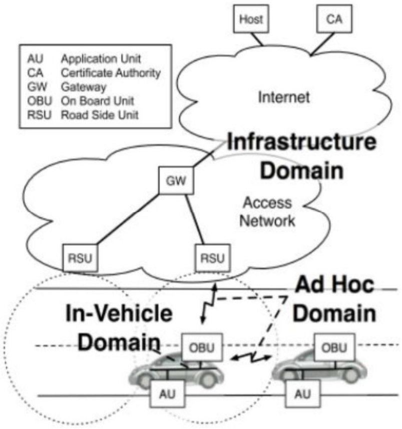


Fig. 2- VANET system Architecture [2]

II. VANETS APPLICATIONS

VANETs represent an opportunity to develop application that improves the transportation sector and the traffic condition through collaborative systems. According to the functionality, the applications are classified in three primary categories which are safety application, efficiency application n and infotainment application:

A. Safety Application

The main goal is to increase public safety and protect the loss of life. The main characteristic of this application is that safety data should be delivered to the intended receivers within the bounded time.

*B.*Efficiency and Infotainment Application

These both applications are non-critical safety application.
In this intended to focus only on non-critical safety application.

Category	Sub classification	Vehicular application
Safety application	Collision Avoidance	• Cooperative collision warning. • Safe distance notification. • Hazardous intersection message.
	Road sign Notification	• Curve speed warning. • Cooperative violation warning.
	Incident Management	• Emergency vehicle notification. • Post-crash notification.
Efficiency application	Traffic Management	• Intelligent traffic flow. • Roadways planning. • Congested road notification.
	Traffic Monitoring	• Road condition sensing. • Vehicles and fleet trafficking.
Infotainment application	Contextual Information	• Commercial service announcement. • Parking assistance.
	Entertainment	• Media content download

a- Vehicular Application Classification [2]

III. Characteristics of VANET

VANET is an application of MANET but it has its own distinct characteristics, the characteristics of VANETs are basically a mixture of wireless medium characteristics. The characteristics are: Vehicular network have some special type of behavior and characteristics, which distinguishing them from other types of network. As compare to other networks vehicular network have unique and interesting features as follow:

A. Unlimited transmission power

In the ad-hoc devices power issues is main constrain but in the case of this network nodes/vehicle provide continuous and sufficient power to computing and communication devices for doing other task.

B. Computational capacity very high

Operating vehicles can have very significant computing capacity which done by sensor and circuit in the vehicle with sufficient energy, communication and sensing capabilities.

C. Predictable mobility

In the mobile ad-hoc network where the vehicle mobility is very hard to predict, vehicles have very predictable movements that are limited to roadways. Roadways information is often available from positioning systems and map based technologies such as GPS. It can give brief about the vehicle average speed with according to some distance, current speed of the vehicle and path of the future position of vehicle can also be finding them.

D. High Mobility

Vehicular networks operate extremely dynamic and their configurations. If take the example of highway where relatively speed of up to 190-230 Km/h may occur while density 1-2 vehicle in 1 Km on other side where relative speed up to 65-70 Km/h and in rush hours especially very high density of nodes.

E. Partitioned network

Vehicular network will be frequently divided and dynamic nature of traffic may result in large inter vehicle gaps in sparsely populated scenarios in several unusual clusters of nodes.

F. Network topology and connectivity

In the vehicular network scenarios are vary from location to location. When vehicle move and change their position constantly in the dynamic scenarios. As the link between the nodes connect and disconnect very often because of network topology changes frequently. As the network is connected is hugely depend upon the two factors which are the range of wireless links and the fraction of participant vehicles, where only a fraction of vehicle on the road could be equipped with wireless interfaces [3].

IV. VANET Model

In VANET there are different units involved in the deployment. Although majority is nodes (Vehicles), there are other units or entities that keep the basic operations functioning in the network. Due to the large and complex system model, it has been categorized into four sub models namely: Driver and Vehicle Model, Traffic Flow Model, Communication Model, and application Model.

A. Driver and Vehicle Model

This shows the behavior of a single vehicle. In this model two factors are considered such as: different driving styles and the vehicle characteristics.

B. Traffic Flow Model

This model depicts the interaction between vehicles, drivers, and the infrastructure to develop a good road network.

C. Communication Model

This shows the flow of data or information between or among the road users.

D. Application Model

This point out the usefulness in the behavior and quality of cooperative VANET applications.Fig.3 illustrated the VANET units and entities that make up the VANET model, and it is explained in detail section below. There are two different environments generally researched in VANET namely; Infrastructure and Ad-Hoc environment.

E. Infrastructure Environment

In this environment, units or entities can be interconnected permanently. Inside this environment mainly contains the entities that mange traffic and also gives access to external services. Manufactures are known to be inside this environment of the VANET model; because during manufacturing they identify each vehicle uniquely. Legal authority is also in this environment of VANET model; putting aside the different regulations that binds countries, vehicles registration and offence reporting is ensured. The Trusted Third Party (TTP) are also in this environment. They offer various services such as time stamping and credential management. Manufactures and the Authority are related to (TTP) because the services are needed, example; issuing of electronic credentials. Service providers are also in this environment, because they give out services that can be accessed via the VANET, such services are‟ Location Based Services (LBS) or Digital Video Broadcasting (DVB) etc.

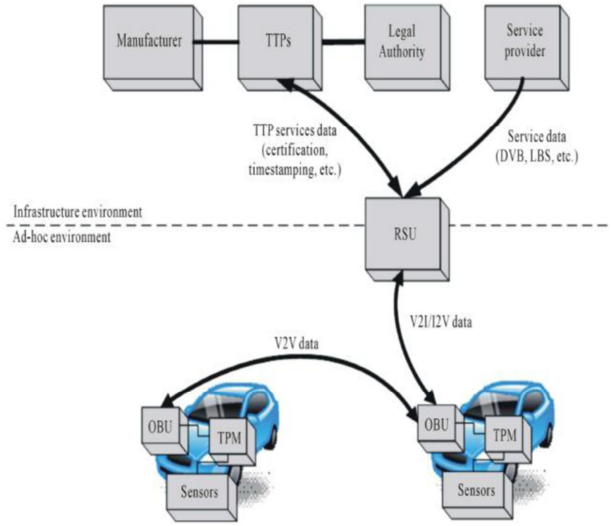


Fig. 3- VANET Units and entities [4]

V. SECURITY CHALLENGES IN VANETS

The challenges of security must be considered during the design of VANET architectures, security protocols, cryptographic, algorithms etc. The following are the some security challenges in VANET.

A. Real time constraint

VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used.

B. Data consistency liability

VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence correlation among the received data from different node on particular information may avoid this type of inconsistency.

C. Low tolerance for error

Some of the protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time and small error in probabilistic algorithm may cause harm.

D. Key Distribution

All the VANET security mechanisms which are implemented its dependent on keys. The messages have to be encrypted and decrypt at receiver end either with same key or different key. Also different manufacturer can install keys in different ways and in public key infrastructure trust on CA become major issue. Thus the distribution of keys among vehicles is a major challenge in designing a security protocols.

E. Incentives

Manufactures they have to build applications that consumer likes most. Very few of the consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET.

VI. SECURITY REQUIREMENTS IN VANET

There are several important requirements to achieve security in VANETs, which are discusses as follows:

A. Authentication

Vehicles should respond only to the message transmitted by legitimate member of network, authentication ensures that the message is generated by the legitimate user. Thus, it is very important to authenticate the sender of a message.

B. Data Verification

A regular verification of data is required to check whether the message contains the correct or corrupted data.

C. Privacy

The profile or a driver„s personal details must be maintained against unauthorized access.

D. Non-Repudiation
A sender must not deny that he/she does not transmit the message whenever an investigation or identity of a vehicle is required. For eg. After sending the message, the vehicle should not deny having sent the message this is called sender non-repudiation. Also after receiving a message, the vehicle should not deny having received the message this is called receiver non-repudiation.

E. Availability
The network should be available even if it under an attack without affecting its performance. For eg. The services provided by the RSU should be available to the vehicles whenever it is required.

F. Data Integrity
It ensures that data or messages received are exactly the same sent by the authorized node without any modification, deletion or replay. This concept in VANETs often combines with the concept ―authentication‖ to guarantee that a should be able to verify that a message is indeed sent and signed by another node without begin modified by attacker.

VII. DIFFERENT TYPES OF ATTACKERS IN VANETS

Attackers play an important role in the VANET by launching the different types of attacks, which may create a problem for the user as well as the network. Attackers can be classified based on scope, behavior of the attack as follow:

A. Active attackers
The attackers can generate message containing wrong information or do not forward the received message.

B. Passive attackers
Passive attacker does not generate the message and they do not participate in the communication process of the network. Attackers eavesdrop only on the wireless channel.

C. Insider Attackers
The insider attacker is a member node who can communicate with the other member of the network and have details knowledge of network. When they have all the information about the configuration than it is easy to launch attack and create more problem.

D. Outsider Attackers
These attackers who is not authenticate to directly communicate with the other member of the network and create a very fewer problems as compare to insider attackers.

E. Malicious Attackers
This attacker uses a various method to damage member of the network and these attackers are not personally benefits from attack.

F. Rational Attackers
The rational attackers seek for their own benefits from the attack.

G. Local Attackers
These attackers send off an attack with a limited scope for a particular area.

H. Extended Attackers
Attacker broadens its scope by controlling several entities that are scattered across the network.

VIII. ISSUES OF VEHECULAR NETWORKS

VANET suffer from various attacks; these attacks are discussed in the following subsections:

A. Denial of Service Attack
DoS attacks can be carried out by network insiders and outsiders and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. Flooding the control channel with high volumes of artificially generated messages, the network‟s nodes, onboard units and roadside units cannot sufficiently process the surplus data.

B. Broadcast Tampering
An inside attacker may inject false safety messages into the network to cause damage, such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosen route.

C. Malware
The introduction of malware, such as viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks are more likely to be carried out by a rogue insider rather than an outsider and may be introduced into the network when the onboard units and roadside units receive software and firmware updates.

D. Spamming
The presence of spam messages on VANETs elevates the risk of increased transmission latency. Spamming is made more difficult to control because of the absence of a basic infrastructure and centralized administration.

E. Black Hole Attack

A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the node drops out, all routes it participated in are broken leading to a failure to propagate messages.

F. Masquerading

Masquerading attacks are easy to perform on VANETs as all that is required for an attacker to join the network is a functioning onboard unit. By posing as legitimate vehicles in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false messages.

G. Replay Attack

In a replay attack the attacker re-injects previously received packets back into the network, poisoning a node"s location table by replaying beacons. VANETs operating in the WAVE framework are protected from replay attacks but to continue protection an accurate source of time must be maintained as this is used to keep a cache of recently received messages, against which new messages can be compared.

H. Global Positioning System (GPS) Spoofing

The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite.

I. Tunneling

An attacker exploits the momentary loss of positioning information when a vehicle enters a tunnel and before it receives the authentic positioning information the attacker injects false data into the onboard unit.

J. Position Faking

Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.

K. Message Tampering

A threat to authenticity can result from an attacker modifying the messages exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forge responses.

L. Message Suppression/ Fabrication/ Alteration

In this case an attacker either physically disables inter-vehicle communication or modifies the application to prevent it from sending to, or responding from application beacons.

M. Key and/or Certificate Replication

Closely related to broadcast tampering is key management and/or certificate replication where an attacker could undermine the system by duplicating a vehicle"s identity across several other vehicles. The objective of such an attack would be to confuse authorities and prevent identification of vehicles in hit-and-run events.

N. Sybil Attack

Since periodic safety messages are single hop broadcasts, the focus has been mostly on securing the application layer. For example, the IEEE 1609.2 standard does not consider the protection of multi-hop routing. However, when the network operation is not secured, an attacker can potentially partition the network and make delivery of event-driven safety messages impossible. [5]

There are five different classes of attacks and every class is expected to provide a better perspective for the VANETs security A. Monitoring Attacks: In this attack tracking of the vehicles come in this class. The attacker just monitors the whole network, listen to the communication between V2V and V2I. If they find any related information then pass this information to the concern person (example- if the polices are planning to perform some operation against the criminal and they communicate each other„s and guide about the exits location of the operation. Attackers will listen to all the communication and inform to the criminal about the operation). Every vehicle has its own unique ID and attacker disclose the identity of the other vehicles in the network by using this unique ID the attacker can track the location of required vehicles. B Social Attack: All unmoral message (social attack) are lies on this class, it is a kind of emotional and social attack. Purpose of these kinds of messages is to indirectly create a problem in the network, any user show angry behavior when they receive such kind of messages.

IX. KEY MANAGEMENT TECHNIQUES

Vehicular ad hoc network is commonly used network among the vehicles in a centralized way. This network is built in order to send and receive messages from the vehicles which are present in the network. The main issue of the VANET is maintenance of the system and revocation of malicious vehicles. Therefore the various management keys have been framed to overcome the above said problems. These are:

A. Distributed Key Management Frame

A distributed key management framework based on group signature to provision privacy in vehicular ad hoc network (VANETs). All of the existing group signature schemes in VANETs are based on a centralized key management which preloads keys to vehicle. In this framework, since keys are distributed and the distributed keys are connected to the centralized sever [2] [3]. Sending and receiving messages ends up in delay in delivering the messages security related issue in hacking the packet data and the message authentication is distance biased This technology uses the below said techniques for this framework.

1. Centralized server (or) centralized authenticator.

2. Extra protocols for beyond the range.

3. Group authentication.

Centralized server

Centralized server are centralized authenticator will be the roadside connected with the key distributor. Extra protocols for beyond the range: Extra protocol may be added for sending and receiving messages beyond the range. Group authentication: Group authenticator is done for the connected keys with the group leader.

B. Shared Key Management Framework

The author proposed the shared key management technique that has various advantages over the distributed key management system. In this framework RSU is not responsible because the key is shared among them, when a vehicle approaches another vehicle [3]. It‟s getting connected to the vehicle automatically without the help of RSU. But message is send from one vehicle to another vehicle needs the help of RSU. The centralized server is not required, since the keys are shared group authentication is not necessary for transferring the information because the key them self shared the information. In this method there is no necessity for extra protocol for the authentication beyond the range why because every participating key is given priority message authentication [6].

CONCLUSION

There are different techniques that can detect the attack but Security expert or forensic investigator analyzes the network traffic using the empirical knowledge. There is no rule to perfectly distinguish attack from network traffic. Thus, there is need of more efficient attack detection system which will analyze the network traffic and provide a security to the VANET network by detecting various attacks.

REFERENCES

[1] Diyar Khairi M S, Amine Berqia, “Survey on QoS and Security in Vehicular Ad hoc Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, 2015, pp. 42-52.

[2] Praveen G Salagar, Shrikant S Tangade,” A SURVEY ON SECURITY IN VANET‟‟, International Journal For Technological Research In Engineering, Volume 2, Issue 7,2015, pp. 1397- 1402

[3] Jaydeep P. Kateshiya, Anup Prakash Singh, “Review To Detect and Isolate Malicious Vehicle in VANET”, International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 2, 2015, pp.127-132

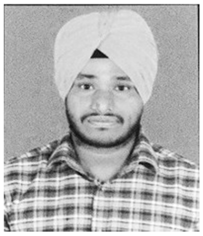
[4] Arif Sari, Onder Onursal, Murat Akkaya, “Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)”, Int. J. Communications, Network and System Sciences, Vol. 8, 2015,pp.552-566

[5] Komal B. Sahare, DR. L.G.Malik, “ Review - Technique for Detection of Attack in VANET”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, 2014, pp.580-584.

[6] Rashmi Raiya, Shubham Gandhi, “ Survey of Various Security Techniques in VANET”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, 2014, pp. 431-433.

[7] Divya Chadha, Reena, “Vehicular Ad hoc Network (VANETs): A Review”, International Journal of Innovative Research in Computer and Communication Engineering, 2015.

AUTHORS PROFILE



Er. Varinderjit Singh is doing his M.Tech in Computer Science and Engineering from Global Institute Of Management And Emerging Technologies, Amritsar, PUNJAB. This paper is published as a Review paper of his M-Tech Dissertation. He is doing his thesis in VANET to enhancing the scalability and privacy of IVC.

Er. Karan Mahajan has done his M.Tech in Computer Science and Engineering from Lovely Professional University, Jalandhar, PUNJAB. He is working as the Assistant Professor in Global Institute Of Management And Emerging Technologies, Amritsar, PUNJAB and he has four year teaching experience. His area of interst Cloud Computing, Mobile Computing and VANET