Review of Potential Security Attacks in VANET

[1]MUHAMMAD ANWAR SHAHID, [2]DR. ARUNITA JAEKEL, [3]DR. CHRISTIE EZEIFE, [4]QASIM AL-AJMI, [5]IKJOT SAINI
[1,2,3,5]Department of Computer Science, University of Windsor, ON, Canada
{shahi116, arunita, cezeife, saini11s} @uwindsor.ca
[4]Faculty of Computer Science and MIS, Oman College of Management and Technology, Barka, Oman
qasim.alajmi@omancollege.edu.om

***Abstract*—Vehicular Ad hoc Networks (VANETs) is a special branch of ad hoc network which consists of cars as network nodes, Road-side units (RSU) and On-Board Unit(OBU). Basic purpose of VANETs is to provide efficient routing and better safety for drivers and passengers. This emerging technology is gaining more and more popularity as car accidents are increasing in the world. In this self-oriented network, security and privacy is so crucial. In this paper, we review the potential threats to Availability, Confidentiality, Authentication and Integrity in VANETs and, we also compare the type of potential attacks and its solutions.**

Keywords—VANETs, security, Adhoc Newtwork, Wireless.

I. INTRODUCTION

VANET attracts the manufacturers and the researchers in the wireless networks due to the growing number of the applications designed for the safety of passengers by the new communication systems called ITS(Intelligent Transport System). VANETs are adhoc networks, highly dynamic, with little access to the network, infrastructure and offering multiple services. Road activities are increasing in the world day by day. It provides us the platform to think more about road safety and better movement of vehicles on the road. Vehicular adhoc network or VANET is an efficient solution to provide better road safety and other applications to drivers and passengers. Vehicular Ad hoc Networks (VANETs) is a special branch of ad hoc network which consists of cars as network nodes, Road-side units (RSU) and On-Board Unit(OBU).

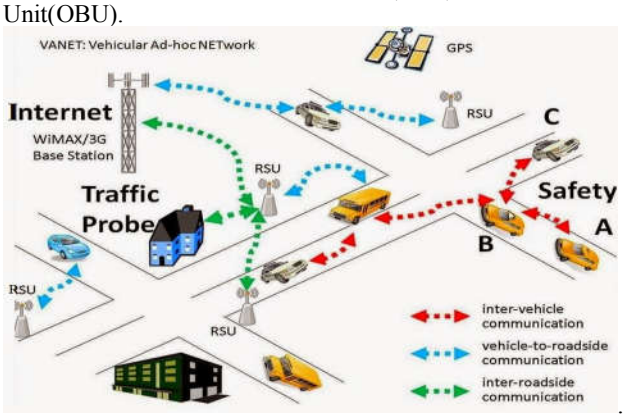

Fig. 1: Formation of VANET on the road[1]

VANETs also provide promising solution to traffic control problem. In VANET, every car serves as a network node which can communicate with other nodes as well as with road-side unit/Infrastructure or RSUs. Basic purpose of VANETs is to provide efficient routing and better safety for drivers and passengers. This emerging technology is gaining more and more popularity as car accidents are increasing in the world. In short communication, VANETs can be between vehicle to Vehicle(V2V), Vehicle to Infrastructure(V2I) or Infrastructure to Infrastructure(I2I) as described in Fig. 1.

Because of rapid and fast movement of cars, VANETs form highly changing network topology[2]. VANET is highly supporting and, in favor of implementing Intelligent Transportation System (ITS)[3]. Other applications of VANET include sharing messages, picture and videos, parking and toll collection services, collision avoidance, safe driving and traffic control.

The rest of the paper is organized as follows: Section II presents characteristics of VANETs. Section III presents details of security in VANETs. Section IV presents recent security proposal in VANETs. Section V describes more about future direction in securing vehicular network. Finally, in VI, we conclude our work.

II. CHRACTERISTICS OF VANET

A. High Mobility and Rapidly Changing Network

As shown in Figure 1, each car is equipped with On-board unit or OBU which connects with other OBU or RSU. vehicles on the road move so fast with high speed and change their position instantly. It is very difficult to predict the position and hence, lead to privacy issues. The fast speed of vehicles also create rapidly changing network. VANET topology depends on infrastructure of roads and position of vehicles[4].

B. Network Size and Exchange of Information

Network size in VANET has no geographical boundaries. It can consist of town, cities, provinces or even countries. Information exchange in this rapid network is so frequent because it gets signals from other vehicles as well as RSUs. Accurate and timely conveyed information can only reduce the risk on the road. VANET provide such platform where drivers can get information on time and avoid accidents[4]. There is no specific duration where vehicles can stay connected. They can be in network for limited time or for long time. Some vehicles can join others or some other vehicles can exit the network any time.

C. Processing Power and Energy

Network nodes or vehicles in VANET come with installed batteries and thus, they do not have issues with power and energy. This power is more than enough to run complex authentication algorithms and calculations[5].

D. Physical Location and Position

Network nodes in VANET are well oriented by their location and position because most of the cars have GPS installed[3].

In later sections we will discuss security in VANET, security architecture, different security attacks in VANET and comparison of the available solution. In the end we will provide the future research issues in security of VANET.

III. SECURITY IN VANETS

In wireless communication, security is at utmost priority because of exchange of information and authentication setup. VANET also should ensure security in terms of availability, confidentiality, authentication and integrity because risks attached to vehicles and people cannot compromised. Authentication is related to valid and authentic origin of sender or receiver. Availability discusses the proper processing of each message so that it should reach the destination on-time. Any delay in the message can provide nothing to the receiver. Confidentiality handles the rules associated to use different assets like OBU, RSU etc. Integrity can be done by using digital signature so that no change exist in the delivered message[6]. In V2V communication, the exchanged information(emergency message, safety messages etc.) through wireless channels requires a secure environments to avoid attacks on V2V network. Such attacks include i. injection of erroneous messages containing false information to cause an accident or to redirect the traffic in a way to release the used route. ii. the revelation of the identity and the geographical position of the other vehicles. For example, a car rental company that wants to follow its own vehicles in an illegitimate manner. iii. the unauthorised access where the malicious entities access the network services without having the rights and privileges. iv. the usurpation of the identity of a nodes(spoofing and impersonation) where the attacker tries to impersonate another node in order to receive messages or to get privileges that are not granted to him. v. the denial of services(DoS) which make the resources and the services unavailable to the users in the network either by jamming or "Sleep Deprivation". In this context, secure communications requires the implementation of certain mechanisms to achieve the security requirements.

A. Security Architecture

There are so many security architectures for VANET. They are developed by different countries or entities like USA, Europe, ETSI and NHTSA. IEEE 1609.x and 802.11p are also being used as standards. Recently IEEE established a standard security architecture for VANET. It is called WAVE (Wireless Access in Vehicular Environment) architecture. In figure 2. we can see that WAVE is a layered architecture for devices complying IEEE 802.11 to operate on Dedicated Short Range Communication (DSRC) band which is operating on 5.9GHz band. The 1609.2 standard defines the infrastructure based on PKI for keys and certificates management.

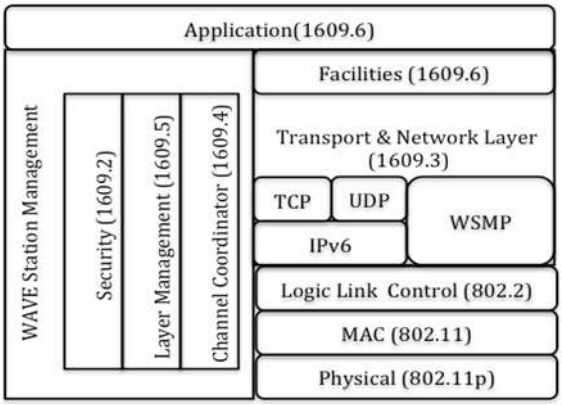

Fig. 2: WAVE Architecture [IEEE 1609.0-2013]

Symmetric encryption AES-CCM(Advanced Encryption Standard Counter with Cipher Block Chaining Message) , asymmetric signature ECDSA (Elliptic Curve Digital Signature algorithm), and asymmetric encryption ECIES(Elliptic Curve Integrated Encryption Scheme) are used for key distribution and the safety messages formats.

B. Classification of Security Attacks in VANETs

VANETs are vulnerable to different attacks and threats. It is very important to classify security attacks because VANETs involves humans and humans cannot expose to risks. Main classification of these attacks are related to Availability, Confidentiality, Authentication and Integrity[7]. Now we will explain each one with different potential attacks.

Availability: to ensure the access of the authorised entities to the network resources with adequate quality of service. Potential security attacks are Denial of Service(DoS), Jamming, Broadcast Tempering, Malware, Spamming and Black Hole Attack.

Confidentiality: to ensure that only the authorised parties can access the data transmitted through the network. It can be vulnerable to Eavesdropping, Information Gathering, Traffic Analysis etc.

Authentication: to allow network members to ensure the proper identity of the members with whom they communicate. It involves attacks like Replay, GPS spoofing, Position Faking, Masquerade, Tunneling, Key/Certificate Replication, Message Tempering etc.

Non-Repudiation: to ensure that issuer cannot deny being the issuer of the message. It can be vulnerable to loss of events traceability.

Integrity: to ensure that exchanged data is not altered either intentionally or accidently. It allows the recipients to detect the data manipulation performed by unauthorised entities and discard the corresponding packets. It can be vulnerable to Message Suppression, Message Alteration, Message Fabrication, Masquerade, Replay.

C. Classification of Attackers in VANETs

Attackers in VANETs are gaining too much popularity among researchers because of sensitive and high mobility of network nodes. It is very much important to classify the attackers in VANETs to handle all the attacks as per their nature/type[5]. Main classifications of attackers are as under:

Insider: It can be any authenticated node which can harm the network or node. He can have access to public key.

Outsider: These are intruder nodes with limited resources to harm the network assets

Malicious: These attackers do not harm the network for personal benefits but exploit it for the loss of cost and services.

Rational: These attackers provide damage to the assets for personal benefits and are predictable.

Active: These type of attackers can have access to signals and can broadcast packets or signals.

Passive: They can indulge in eavesdropping the wireless channel.

IV. Recent Security proposals in VANET

This section describes the recent proposals which are aimed to increase security in VANETs.

A. Using Cryptography

[8] proposed a comparison of cryptographical solution to different attacks in vehicular networks. Table 1 shows this comparison in detail. Symmetric encryption is used to produce an effective delay and RSUs are used for authentication and key distribution. In [9] a decentralized lightweight authentication scheme for V2V is given to protect valid users in VANETs for malicious attacks based on the concept of transitive trust relationships. Thus the amount of their cryptographic calculation is less than in existing schhemes.

Table 1 shows security attacks and cryptographic solution

Type of Attacks	**Security Aspect**	**Cryptographic Solution**
Eavesdropping	Confidentiality	Symmetric encryption of secure messages
Denial of Service	Availability	Digital Signature
Jamming	Availability	Frequency hopping technique
Traffic Analysis	Confidentiality	Securing Traffic Pattern
Message Tempering	Integrity	Similarity algorithm, integrity matrics
Impersonation	Authentication	Variable MAC and IP addresses
Unlawful Tracking	Privacy	Set of anonymous key changes, certified Authority
Brute Force	Confidentiality	Strong encryption and key generation algorithm
Fake Position	Authentication	Using signature with GPS
Sybil Attack	Availability	Deploy central validation authority

A non-interactive authentication scheme is presented in [10], providing privacy among drivers in V2V communication networks; Drivers may change their own set of public keys frequently without control from TTP(Third Trusted Party). [7] shows an efficient and robust pseudonym-based authentication, with mechanisms that reduce the security overhead for safety beaconing. Vehicle on-board units generate their own pseudonyms. Security architecture in V2V and V2I coomunication is so essential to protect privacy of the participants and be very efficient in terms of computing capabilities and communication bandwidth using asymmetric and symmetric cryptography.

B. Trust Grouping Framework(TGF)

Nodes in vehicular network should be aware of each other so that they can know what's happening on the road. This can be done by sending and receiving accurate messages. To meet these requirements researchers have developed symmetric and asymmetric cryptographic techniques. According to this approach[9], a hardware can implement hybrid (symmetric and asymmetric) cryptography module for safe communication among nodes. This framework consists of 4 components: message dispatcher, Group Entity, Group Communication and TPM as shown in figure 3.

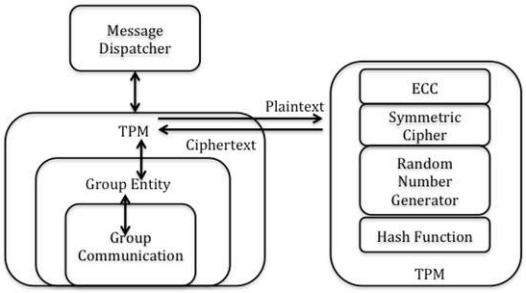

Fig. 3 TGF framework in VANET[9]

In this figure TPM is the trusted Platform Module. It is a hardware chip which is installed in smart car for secure communication.

C. User Privacy Security System

The basic requirement in security of vehicular network consist of availability, confidentiality, authentication and integrity. Furthermore, privacy also is an important component of security because it gives piece of mind to user being exposed or tracked by attackers. [10] proposed an identity based security system for VANET that can effectively solve the conflicts between privacy and tractability.

This figure shows the interactions between different entities and arrows show the direction of flow/communication. This system can definitely preserve user privacy because of cryptography solution. Security in vehicular network is becoming more and more significant because of its importance and interest of stakeholders. To secure this network, so many solutions have been proposed in the past.

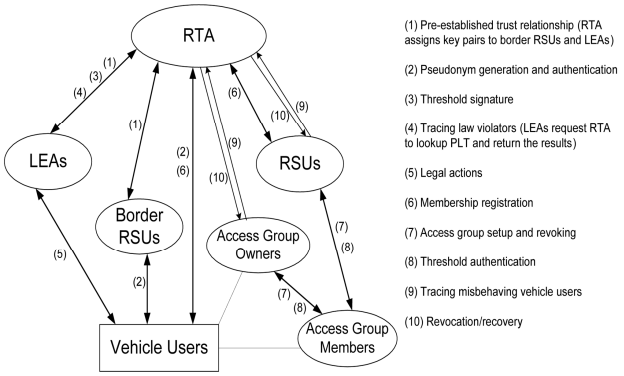

Fig. 4 shows Identity Based Security System for VANET[10][11]

Some solution provide security to hardware, some solution secure data only and some other solution provide software security. For example Authentication technique uses encryption along with digital signature/certificates and hash function but one of the disadvantage is the complication to authenticate the entity. Another technique of security is to use public key infrastructure where private key is kept with encrypted message but in vehicular network, malicious vehicle can have access to public key of the sender vehicle. These disadvantages are considered as the gateway to conduct further research in security in VANETs.

D. Group Based Authentication

[10] proposed a solution for authentication. In PKI(Public Key Infrastructure) scheme with absence of vehicular groups as shown is Fig. 5, there are delays due to many return to the RSU to verify the certificate or to authenticate the sender which cause an exhaustion of the RSU resources. In this solution, there is no return to RSU unless the GL only needs to do. They introduced group based V2V authentication and communication for safety message dissemination; a security architecture for V2V communication that ensure integrity, confidentiality, anonymity, authenticity and non-repudiation.

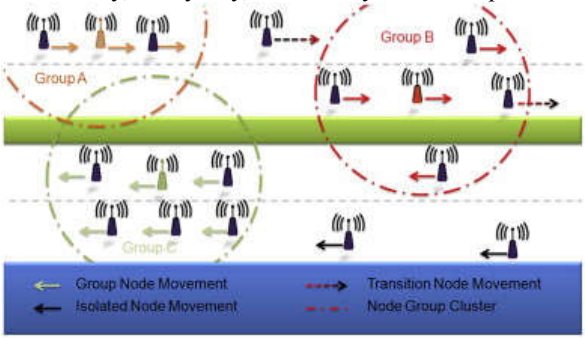

Fig. 5: Vehicular groups [12]

They proposed a solution that mitigated the drawback of the previously proposed schemes such as periodic use of an indispensible part of RSU resources for authentication and verification, limited anonymity, multi-hop communication, dissemination delay. This proposal combines symmetric and asymmetric encryption: AES-CCM and ECDSA(256bit) for digital signature on forming vehicular groups with unique key each, in addition to an offline periodical generation of the private and public keys. This solution is considered as an attempt to minimize the delays due to the PKI infrastructure for the dissemination of "Safety Messages" in V2V applications because of the dissemination time constraints≤100ms.

V. Future Directions for Security Issues in VANET

Many issues in vehicular network and its security are still open and need further research. These issues can include: certificate revocation, self organized network, trust and verification of data, privacy assurance, Antimalware and Intrusion Detection System, Efficiency of Cryptographic Solutions, trustworthy nodes, Key distribution and Standardization of security architecture.

VI. Conclusion

Vehicular adhoc network is the future of vehicles, drivers and passengers. There is a need of more research in this area because of its importance and risks involved for human beings. We formulated a comprehensive survey which can be utilized as a start-up in doing research in VANETs.

References

[1] Yadav, K.A. and Vijayakumar, P., 2016. VANET and its Security Aspects: A Review. *Indian Journal of Science and Technology*, *9*(44).

[2] Hasrouny, H., Samhat, A.E., Bassil, C. and Laouiti, A., 2017. VANet security challenges and solutions: A survey. *Vehicular Communications*.

[3] Engoulou, R.G., Bellaïche, M., Pierre, S. and Quintero, A., 2014. VANET security surveys. *Computer Communications*, *44*, pp.1-13.

[4] Raw, R.S., Kumar, M. and Singh, N., 2013. Security challenges, issues and their solutions for VANET. *International Journal of Network Security & Its Applications*, *5*(5), p.95.

[5] Lim, K. and Manivannan, D., 2016. An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. *Vehicular Communications*, *4*, pp.30-37.

[6] Samara, G., Al-Salihy, W.A. and Sures, R., 2010, September. Security analysis of vehicular ad hoc nerworks (VANET). In *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on* (pp. 55-60). IEEE.

[7] Mejri, M.N., Ben-Othman, J. and Hamdi, M., 2014. Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications*, *1*(2), pp.53-66.

[8] Wagan, A.A., Mughal, B.M. and Hasbullah, H., 2010, February. VANET security framework for trusted grouping using TPM hardware. In *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on* (pp. 309-312). IEEE.

[9] Sun, J., Zhang, C., Zhang, Y. and Fang, Y., 2010. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems*, *21*(9), pp.1227-1239.

[10] Hasrouny, H., Bassil, C., Samhat, A.E. and Laouiti, A., 2015, April. Group-based authentication in V2V communications. In *Digital Information and Communication Technology and its Applications (DICTAP), 2015 Fifth International Conference on*(pp. 173-177). IEEE

[11] Sun, J., Zhang, C., Zhang, Y. and Fang, Y., 2010. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems*, *21*(9), pp.1227-1239.

[12] Lloret, J., Canovas, A., Catalá, A. and Garcia, M., 2013. Group-based protocol and mobility model for VANETs to offer internet access. *Journal of Network and Computer Applications*, *36*(3), pp.10