Journal of Advances and Scholarly Researches in Allied Education
Vol. 15, Issue No. 7, September-2018, ISSN 2230-7540

A Survey on VANET Security Attacks and Cryptographic Solutions

Ramil Gupta*

Department of Computer Science and Engineering, Baba Farid College of Engineering and Technology, Bathinda, India

Abstratct – Vehicular ad-hoc network (VANET) is being broadly used and considered important among the emerging technologies that guarantee broad range of applications in the field of military, medical, home and environment. Upcoming research in the area of Vehicular ad-hoc network technology has introduced a new part in the world of wireless communication. For communication, VANETs use inter-communication technologies such as GPS, digital maps, digital short range communication, in-built communication system to reduce traffic congestion and accidents on roads. VANET can be used for communication purpose where vehicles can exchange the information with other vehicles and roadside units. The data can be emergency messages or some entertainment related messages. Safety becomes one of the most important issues in VANET. To ensure security, cryptographic solutions are used.

----------X----------

INTRODUCTION

Rapid advances in wireless technologies provide opportunities to utilize the technologies for advanced vehicle safety applications. Vehicular accidents kill millions of people across the globe. Statistical studies reveal that about 1.3 million people die of traffic accidents per year, which can be avoided with sufficient Safety warning. Safety is a dominating factor in designing any vehicular automation system.

VANET uses moving vehicles as nodes and allows them to connect to each other through a wireless network with features such as predictable mobility, rapid changing topology, high computational ability and variable network density, supporting the Intelligent Transportation System (ITS)[Toor et al., 2008]. A number of novel problems are associated with VANET` because of the unique characteristics of the network. The routing protocols make communications possible in an ad hoc network. When it comes to communications, security is another factor that has to be taken into consideration. As important it is to know how security can be provided to a network, it is also important to know how security can be breached and what the security attacks can be. Due to unique characteristics such as high mobility, dynamic topology, short connection duration and frequent disconnections, unique security challenges rise in VANETs.

RELATED WORK:

In A Security and Privacy Review of VANETs, Qu et al., 2015 suggests that with increasing stringent security requirements such as less verification time, less computational load and less reliance on temper-proof hardware, the technologies involved in the solution of VANETs security and privacy become much more complex. In addition, security and privacy preserving should be achieved at the same time which brings to light the tradeoff between security and privacy. On the other hand, privacy preserving methods are reviewed, and the tradeoff between security and privacy is discussed. Finally an outlook is provided on how to detect and revoke malicious nodes more efficiently and challenges that have yet been solved. In An Efficient Identity-Based Conditional Privacy Preserving Authentication Scheme for Vehicular Ad Hoc Networks, He et al., 2015 suggest that the conditional privacy-preserving authentication (CPPA) scheme is suitable for solving security and privacy-preserving problems in VANETs because it supports both mutual authentication and privacy protection simultaneously. To achieve better performance and reduce computational complexity of information processing the design of a CPPA scheme does not use bilinear paring. The suggested CPPA schemes yields a better performance in terms of computation and communication cost. A CPPA scheme is proposed for VANETs that do not use bilinear paring and it is demonstrated that it could support both the mutual authentication and the privacy protection simultaneously. The proposed CPPA scheme

retains most of the benefits obtained with the previously proposed CPPA schemes. In Maria Elsa Mathew et al. have presented a recent classification of VANETs attacks and a category set of their possible solutions. Also, A. Rawat et al. presented some attacks targeting VANETs and their related solutions. Furthermore, VANETs are an example of mobile ad hoc networks (MANETs) which means they not only inherit all the known and unknown security weaknesses associated with MANETs but due to the unique features of these types of networks, such as the high mobility of the nodes and the large scale of the network, VANETs are more challenging. Therefore, a novel mechanism to guarantee the primary security requirements, such as authentication, integrity and non-repudiation needs to be developed before VANETs can be practically launched.

SECURITY REQUIREMENTS:

Safety in VANETs is of utmost concern because human lives are constantly at stake. Information about the vehicles within the network must be exchanged on time and most importantly in a secure way. The deployment of a comprehensive security system for VANETs is very challenging in practice. The vulnerabilities can cause small to severe problems in the network and also pose potential security threats which can deteriorate the functionality. A security breach of VANET is often critical and hazardous. Security requirements are the measures that define the basic needs to make a network secure. The important requirements to achieve security in VANETs are discussed as follows:

1. **Authentication**: All the nodes in the network should respond only to the messages transmitted by legitimate [Schwartz et al., 2012] members of the network. This will ensure that the critical information is being is exchanged securely. Therefore, to authenticate the sender of a message is very important.

2. **Data Verification**: The vehicular data has to be verified. Once the sender node is authenticated, the receiving vehicle performs data verification [Kumar, Dave, 2012] to check whether the message contains correct data.

3. **Availability**: The network has to be available at all the times of its functionality. Even if it is under an attack, it should be using alternative mechanisms to guarantee availability without affecting its performance.

4. **Data Integrity:** It ensures that data or messages are not altered by attackers. Data integrity [Raya et al., 2012] helps to protect the information against alteration and modification. Otherwise, users are directly affected by the altered emergency data.

5. **Non-Repudiation:** A sender must not deny a message transmission whenever an investigation or identity of a vehicle is required.

6. **Privacy:** The profile or a driver's personal information must be maintained against unauthorized access.

7. **Real-time Constraints**: Since in a VANET, vehicles are connected for a very short duration, real-time constraints should be maintained.

VANET SECURITY ATTACKS:

The routing protocols make communications possible in an ad hoc network. When it comes to communications, security is another factor that has to be taken into consideration. Before getting to know how security can be provided to a network, it is important to know how security can be breached and what can be the security attacks. Due to unique characteristics such as high mobility, dynamic topology, short connection duration and frequent disconnections, unique security challenges rise in VANETs. The unique features bring security issues such as trust group formation, position detection and protection as well as certificate management.

To get better protection from attackers we must have the knowledge about the attacks in VANETs against security requirements. Attacks on different security requirement are given below:

(I) **Impersonation:** In impersonate attack attacker assumes the identity and privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network. This type of attack is performed by active attackers. They may be insider or outsiders. This attack is multilayer attack means attacker can exploit either network layer, application layer or transport layer vulnerability.

(II) **Session hijacking:** Most authentication process is done at the start of the session. Therefore, it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.

(III) **Identity revealing**: Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.

(IV) **Location tracking**: The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.

(V) **Denial of Service:** DOS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node. DoS attacks can be carried out in many ways [Murthy et al., 2011].

(VI) **Black hole attack:** In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.

(VII) **Worm hole attack:** In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole [Stampoulis, Chai, 2010]. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.

(VIII) **Gray hole attack:** This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. This selection can be of two types, a malicious node can drop the packet of UDP whereas the TCP packet is forwarded or the malicious node can drop the packet on the basis of probabilistic distribution.

CRYPTOGRAPHIC SOLUTIONS:

Modern cryptography provides security for all the security requirements like confidentiality, authenticity, integrity, non-repudiation etc. To fulfill these security requirements various techniques like encryption, decryption, key generation, digital signatures and certificate management have to be followed. Usually the VANET structure uses the Public Key Infrastructure (PKI). The PKI uses a cryptographic pair of public and private key for secure data exchange in the network. For the encryption and decryption of messages a suitable algorithm is followed. Digital Signatures are used to enhance the VANET security, designed to provide an electronic counterpart to handwritten messages. However, one security mechanism cannot fulfill all the security requirements. Therefore, security schemes use a combination of digital signature algorithms. The algorithms are classified into two classes:

- Symmetric Cryptography
- Asymmetric Cryptography

Symmetric Cryptography: The most important part in symmetric key encryption is that the encrypt key is the same as the decrypt key. This means that if you either the key for encryption/decryption you have the key for both. But this becomes a drawback for the symmetric cryptography, because if the key for encryption is exposed to the intruder, the key for decryption also gets known. Therefore, it becomes easy for the system to get compromised.

Asymmetric Cryptography: Better known as Public key cryptography, uses two different set of keys for encryption and decryption. Each user has a set of two keys, one private and other public. The private key is kept as a secret and the public key is made public. It is made known to the other users. If a message is encrypted with the public key, only using the private key can that message be decrypted.

CONCLUSION:

VANETS are designed to make the transportation system an intelligent by enhancing user safety and to provide services for user comfort. However, the wireless networks attract attackers who pose a threat to user security. But as the security vulnerabilities have increased, with the advancements in technology security solutions have also been incorporated. For various security attacks counter cryptographic solutions have come forth.

REFERENCES

Chen W., 2008. A survey and challenges in routing and data dissemination in vehiclular ad-hoc networks. *Wireless Communications and Mobile computing,* 11(7), pp. 787-795.

Fengzhong Qu, Zhihui Wu, Fei-Yue Wang and Woong Cho, 2016. A Security and Privacy Review of VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 16(6), pp. 1-25.

Debiao He, Sherali Zeadally, Baowen Xu and Xinyi Huang, 2015. Anonymous authentication for wireless body area networks with

provable security. *IEEE Transactions on information forensics and security*, 10(12), pp. 1-12.

Preeti Sachan, Pabitra Mohan Khilar, 2011. Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism. *International Journal of Network Security & Its Applications (IJNSA),* 3(5), pp. 229-241.

Javed, M., Ngo, D. & Khan, J., 2014. A multi-hop broadcast protocol design for emergency warning notification in highway VANETs. *EURASIP, Journal on Wireless Communications and Networking*, 1, pp. 1-15.

Sommer, C., German, R. and Dressler, F., 2011. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. *IEEE Transactions on Mobile Computing*, *10*(1), pp.3-15.

Kumar, R. & Dave, M., 2012. A Review of Various VANET Data Dissemination. *International Journal of u-and e- Service, Science and Technology,* 5, pp. 27-44.

Li, D., Huang, H., Li, X., Li, M. and Tang, F., 2007. A distance-based directional broadcast protocol for urban vehicular ad hoc network. *In Wireless Communications, Networking and Mobile Computing WiCom,* Shanghai, China. pp. 1520-1523.

Liu, R., Luo, T., Zhang, L., Li, J. and Fang, S., 2012. A forwarding acknowledgement based multi-hop broadcast algorithm in vehicular ad hoc networks. *International Conference on Computer Science and Network Technology (ICCSNT),* Changchun, China, pp. 1258-1262.

Corresponding Author

Ramil Gupta*

Department of Computer Science and Engineering, Baba Farid College of Engineering and Technology, Bathinda, India

E-Mail – ramilgupta.bfcet@gmail.com