Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 53-59
ISSN: 2395-0196

A Documentary Research For Avoiding BLACKHOLE And SYBIL Attacks In VANET

Anil Pal[1], Bright Keswani[2], Dinesh Goyal[3]
[1]Research Scholar, Suresh Gyan Vihar University,
[2]Professor, Suresh Gyan Vihar University, Department of CSE
[3]Professor, Department of CSE, Poornima Institute of Engineering & Technology

Abstract

The creation of VANET is obviously a great benefit to road driving safety and traffic management. However, the design of VANET brings a series of emerging challenges, especially in terms of security and privacy. As an implementation of Mobile Ad Hoc Network (MANET), VANET inherits all known and unknown security vulnerabilities. It is obviously a critical task to develop a suite of carefully designed security mechanisms for achieving security and conditional privacy preservation in a VANET. Until recently, however, security and privacy issues of VANETs have been subject to little attention, which has formed a major barrier that prevents many car manufacturers from employing the state-of-the-art wireless communication devices. Security and routing are two critical concerns for the designers of VANETs.

Keywords: VANET, Sybil Attack, Black hole attack

1.0 Introduction: VANET is a mobile ad hoc network that provides communication between nearby vehicles. And the communication between the vehicle and nearby fixed equipment (usually called roadside equipment). The main goal of VANET is to provide passengers with safety and comfort. To this end, a special electronic device will be placed in each car, which will provide passengers with an Ad-Hoc network connection.[1] The main goal of VANET is providing safety assurance and comfort for passengers. Each vehicle installed with VANET device will be a node in the Ad-hoc network and can accept & transmit other messages through the wireless network. Collision alert message, Road signal arms and in place traffic view will give the driver necessary tool to decide the best path along the way. VANET or Intelligent Vehicular Ad-Hoc Networking provides an intellectual way of using vehicular Networking. With the sharp increase of vehicles on roads in the recent years, driving becomes more challenging and dangerous. The main idea behind this research is to help manufacturers that are about to make a big step in the computer industry and also in the car industry.[2] The long term goal is to create a form of communication between vehicles that helps the person driving the car. Initiatives of analyzing the costs of such a major step have been substantial in the past years and one of the most important aspects of the deployment of such a network is the strong analysis of the security aspect. Using VANETs vehicles will increase their awareness of the environment and therefore contributing to a safer and more efficient traffic[3].The main purpose of VANET is to provide security-related information, traffic management and infotainment services. Simple and effective security mechanism is the main problem of deploying VANET in public places [9].The main goal of VANET is to provide passengers with safety and comfort. Each vehicle equipped with VANET equipment will be a node in the Ad-hoc network, and can receive and transmit other messages through the wireless network. Collision warning messages, road signal

arms and on-site traffic views will provide drivers with the necessary tools to decide the best path along the way. VANET or smart car Ad-Hoc network provides a smart way to use car network. In recent years, with the rapid increase of vehicles on the road, driving has become more challenging and dangerous.

2.0 Literature Review: Different researchers have analyzed VANET security issues, needs and priorities with the different perspective. In this article, the author discusses the security attacks that SDN-based VANET should face in the future, and studies how SDN will exert its advantages in establishing new countermeasures. SDN-based VANET encourages us to deal with the limitations and difficulties of traditional VANET. It handles the general system through a single wireless controller, thereby helping us to reduce the general burden of the system. Although SDN-based VANET provides us with some benefits in applications and services, they also have some important challenges to be solved. In this research, we discussed and explained the challenges, applications and future development directions of SDN-based VANET. Finally, we provide the conclusions of the entire study.[4] The author proposes a Sybil node detection technology based on a timestamp mechanism. In this work, the time stamp is the only certificate that RSU provides to all vehicles on the road in VANET. In the proposed node discovery and data transmission work, they used the Ad-hoc On-Demand Distance Vector (AODV) routing protocol and timestamp as the hash function of the public key, and used it to detect Sybil nodes implemented by the NS2 simulator.[5] In the current era of technical challenges for data transmission, it is urgent to determine the main components and tools used to transmit and receive vehicle object data. In the past few decades, the Vehicle Ad Hoc Network (VANET) has become one of the most popular research areas. Vehicles are connected spontaneously in a wireless environment called VANET, which is a sub-part of MANET. Due to frequent changes in the topology, it is very difficult to make VANET safe. In this research article, we observed that there are many security challenges, and further research must be conducted to make VANET more secure. Extensive discussion about VANET components, security issues and challenges, key analysis of attacks and their solutions[6] In this article, the author elaborated on specific attacks on VANET and showed a comparison of different security technologies related to VANET security. In this article, we have discussed between different security technologies, such as distributed key management, effective conditional privacy protection, reputation checking, plausibility checking, and clustering and key distribution. Based on the given comparison, clustering and key distribution have more advantages compared to other available solutions.[7] In this article, the author discusses the security of ad hoc networks and different types of attacks in mobile ad hoc networks. The author discusses network security from the perspective of confidentiality vector, integrity vector and availability vector. Different types of attacks are discussed, such as active, passive and advanced attacks in self-organizing networks. This article only focuses on different types of attacks and their adverse effects on the network.[8]

3.0 VANET Attacks: Here discussion is done with different thirteen types of VANET attacks. Different types of attack and its effect is shown in Table 1.1, which will be followed by detailing

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 53-59
ISSN: 2395-0196

of different VANET attacks.[9]

Attack Name	**Active / Passive**	**Security Requirement**	**Impact on Network**
(DOS) Attack	Active	Availability	High
(DDOS) Attack	Active	Availability	High
Sybil Attack	Active	Authentication	Medium
Node Impersonation Attack	Active	Integrity	Medium
Eavesdropping	Passive	Confidentiality	Medium
Masquerading	Active	Authentication	High
Global Positioning System(GPS) Spoofing	Active	Authentication, Traceability	Medium
Brute force Attack	Active	Confidentiality, Privacy and anonymity	High
Pranksters	Active	Integrity	High
Application Attack on safety and Non Safety messages	Active	Availability, Integrity	High
Worm Hole attack	Active	Availability	High
Gray Hole attack	Active	Availability	High
Black Hole attack	Active	Availability	High

Table 1.1: Different VANET Attacks

3.1 Sybil Attack: In the Sybil attack, malicious nodes will create multiple node identities, which will spread wrong information in the VANET network. In this type of attack, data is broadcast with a forged identity. The attacker OBU performs this type of attack on another legitimate OBU to obtain different benefits. In this attack, the attacker vehicle creates multiple identities and sends messages to legitimate users as if there is more traffic on the selected road, so please change the route. The attacker will create an illusion, and similar types of messages will be sent to the same vehicle. Now, the legitimate user will receive the same type of message, and due to this illusion, it will fill in that the message was sent by another sender and believe that the vehicle will change its route. This decision is beneficial to the attacker, and now the attacker's vehicle will get a clear route on the selected itinerary. This type of attack will also be used to

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 53-59
ISSN: 2395-0196

redirect users to the wrong location. Figure 1 represents a Sybil attack, where the attacker car C is creating multiple identities and sending messages about heavy road traffic to other users. Therefore, by obtaining such information, car B and car D will choose other alternative paths, and now car C will get a free road[10]

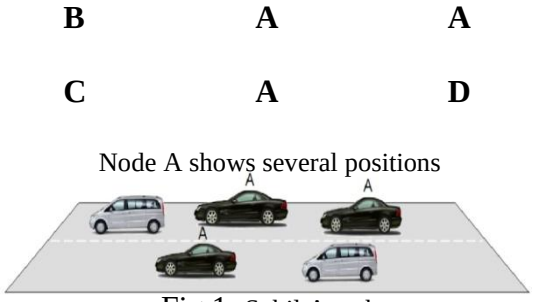

Fig 1: Sybil Attack

3.2 Black hole attack: This is a routing attack in which the attacker shows the shortest path to the interested sender node to attract another node of the network to send data packets through it. After obtaining the data packet, discard it. Figure 2 illustrates an example in which Car-A wants to send packets to Car E and Car G, but neither of them has any routing details. Therefore, car A initiates the route discovery process and forwards RREQ to car B and car H. As a malicious node, Car H will claim that it has the shortest route to Car E and Car G. According to the available replies, Car A sends all messages to Car H and becomes a victim of the black hole attack.[11]

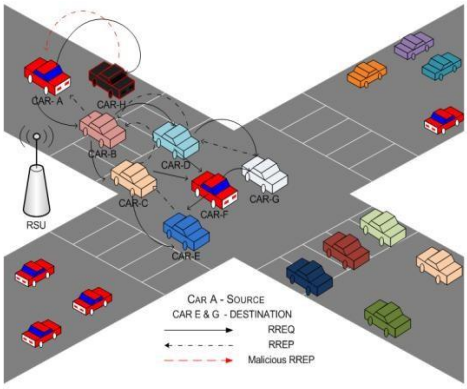

Figure 2: Black Hole attack

Due to the high mobility of vehicles, routing in VANET is a difficult and challenging task. Malicious nodes may discard, block or modify messages, and spread damaged or updated routing information within the network, which may cause some or all of the network traffic to be redirected. This requires designing a secure framework to manage the authenticity and reliability of messages. The malicious node silently discards the message and produces a black hole effect. A black hole is an area that can be created by a single node or multiple nodes, mistakenly

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 53-59
ISSN: 2395-0196

redirecting network traffic to this area. Figure illustrates an example where Car-A wants to send packets to Car-E and Car-G, but neither of them has any routing details. Therefore, Car-A initiates the route discovery process and forwards RREQ to Car-B and Car-H. As a malicious node, Car-H will claim that it is the shortest path to Car-E and Car-G. Based on the available replies, Car-A sends all messages to Car-H and becomes a victim of the black hole attack.

4.0 Objectives of this research: The major objectives of this research are-

1. Study of existing models of VANET.
2. Analysis and finding problems with existing secure framework for VANET.
3. Identify and Analysis of different attack possible in existing security model for VANET
4. Design of New Secure Framework for avoiding Blackhole & Sybil Attack over VANET.
5. Performance and result Analysis of Proposed & Existing framework over VANET.

5.0 Proposed model and method for secure the VANET network: The aim of this research is to improve the performance and scalability issues of employing public key cryptosystems to support secure services for VANETs. For investigation we use the network simulator NS-2 to simulating the current WLAN hardware with the Ad hoc Network. The connectivity tests have shown that it is a realistic option to use ad hoc networks for vehicular communication. But our limitations also have drawn out that several security improvements and extensions would lead to much better performance, especially for message integrity. In a life critical situation like an accident a particular vehicle can communicate with other vehicle and infra to inform them that there is an accident occurred in a particular way or path. The architecture of VANET is shown in fig 3 given below-

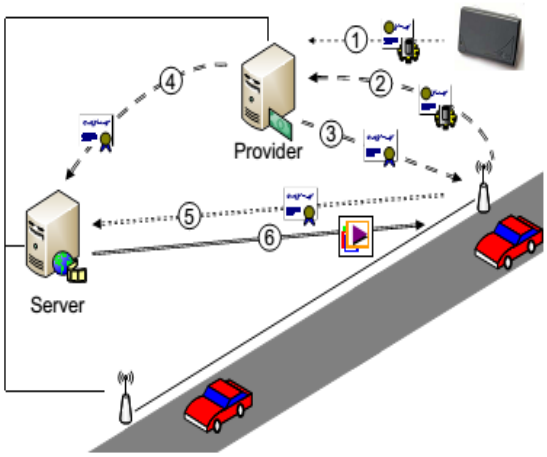

Figure 3: Architecture of VANET

(1) User registers device with certificate provider and RSU
(2) User sends service request
(3) Certificate Provider issues temporary credentials

(4) Provider informs server and RSU about temporary credentials
(5) User requests service using temporary credentials
(6) Server delivers content.

6.0 Conclusion: Solving security and privacy issues is a prerequisite for any VANET-based vehicle application. In summary, developing a well-designed security mechanism to achieve security and conditional privacy protection in VANET is obviously a vital task. However, until recently, the security and privacy issues of VANET have received little attention, which has become a major obstacle preventing many car manufacturers from using the latest wireless communication equipment. Security and routing are two key issues for VANET designers. This work recommends research to determine the challenges encountered in VANET security, study existing frameworks and models, design and analyze new frameworks to solve the problems encountered by previous frameworks and models, and propose the development of a new method to ensure VANET security.

References:

[1] Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA
[2] Harsch, C., Festag, A., & Papadimitratos, P. (2007). Secure position-based routing for VANETs. In Proceedings of IEEE 66th vehicular technology conference (VTC-2007), fall 2007 (pp. 26–30), September 2007.
[3] Gerlach, M. (2006). Full paper: assessing and improving privacy in VANETs. www.network-on-wheels.de/downloads/ escar2006gerlach.pdf (accessed: May 29, 2010).
[4] Muhammad Arif et al. "ISDN-based VANET, Security Attacks, Applications and Challenges", Applied Science 2020, 10, 3217; doi: 10.3390/app10093217
[5] Syed Mohd Faisal and Taskeen Zaidi, "VANET Sybil Attack Detection Based on Timestamp", International Journal of Cyber Security, Volume 22, Issue 3, PP.397-408, May 2020 (DOI: 10.6633 / IJNS .202005 22(3).05)
[6] Taskeen Zaidi, "Overview: Various Attacks in VANET", ICCCA Conference Paper • July 2019, DOI: 10.1109/CCAA.2018.877753
[7] Amandeep Singh, Sandeep Kad, "Review of Various Security Technologies of VANET", Procedia Computer Science, Volume 78, 2016, Pages 284-290, ISSN 1877-0509.
[8] Mohan V. Pawar, J. Anuradha, Network Security and Types of Attacks in the Network, Procedia Computer Science, Volume 48, 2015, Pages 503-506, ISSN 1877-0509.
[9] Bassem Mokhtar, Mohamed Azab, "Investigation of Security Issues in Vehicle Self-Organizing Networks", Alexander Engineering Journal, Vol. 54, No. 4, 2015, pp. 1115-1126, ISSN 1110-0168.
[10] A. D. Patel and K. Chawda, "Black Hole and Gray Hole Attacks in MANET", International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, 2014, pages 1-6.
[11] D. Manivannan, Shafika Showkat Moni, Sherali Zeadally, "Secure Identity Verification and Privacy Protection Technology in Vehicle Private Network (VANET)", in Vehicle Communication 25 (2020) 100247

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 53-59
ISSN: 2395-0196