ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 5, MAY 2015, PP 280-283

# A Comprehensive Analysis on The Threats and Vulnerabilities in VANET Technology

V.Kumar, Shalni, S.Rani, R.P.Singh, G. C. Banerjee

**Abstract**— A VANET (Vehicular Ad-Hoc Network) [1] is a collection of mobile hosts forming a temporary network without the aid of any established infrastructure. This exibility in space and time induces new challenges towards the security needed to support secure wireless communications[2]. VANETs are being used to improve road safety and enable a wide variety of value-added services. A lots of work are done towards the VANET but the security[3] get less attention. In this project we will discuss the threats, attacks on VANET, and some mechanisms how to prevent from these attacks[4-5] which are helpful to keep the safe VANET technology.

**Index Terms**— VANET, Security, Threats, Broadcasting, DOS, Sybil

## 1 INTRODUCTION

Now a day's technology tries to reaches at its peak and we are aware of the technologies. Now a day's technology reaches on wheels means now vehicles are able to communicate to each other. In a simple "NETWORKS ARE ON WHEELS". One such network that has received a lot of interest in the last couple of years is the "VANET". VANET has become an active area of research, standardization, and development because it has tremendous potential to improve vehicle and road safety, traffic efficiency, and convenience as well as comfort to both drivers and passengers. VANET is a type of wireless communication which provides to support a large number of mobile applications on the road as well as it is designed with the goals of enhancing driving safety and providing passenger comfort. There are three main types of VANET: Vehicle to Vehicle (V-V), Vehicle to Infrastructure (V-I), Inter Roadside Communication (IRC).But similar to Ad-Hoc which is base technology of VANET, there is no specific protocols which owing good strategy. As we know reason of issues is most of Ad-Hoc protocols has suffered from energy consumption. Although it seems VANET has better situation because energy has not critical position as its predecessor.But security has a critical situation in VANET similar to Ad-Hoc. Using VANET is increasing and security architecture must be carefully designed especially when it becomes a worldwide VANET which give service million of vehicles on the road.

- *Vikash Kumar is currently pursuing Bachelor degree program in Computer Science and Eengineering Department at Bengal Institute Of Technology and Management,Santiniketan, India,PH-08642885571. E-mail: vickyvikash393@gmail .com*
- *Shalni is currently pursuing Bachelor degree program in Computer Science and Eengineering Department at Bengal Institute Of Technology and Management,Santiniketan, India,PH-09476350583. E-mail: shalnithakur375@gmail .com*
- *Suchita Rani is currently pursuing Bachelor degree program in Computer Science and Eengineering Department at Bengal Institute Of Technology and Management,Santiniketan, India,PH-0890048558. E-ranisuchita6@gmail .com*
- *Ravi Prakash Singh is currently pursuing Bachelor degree program in Computer Science and Eengineering Department at Bengal Institute Of Technology and Management,Santiniketan, India,PH-8926897300. E-mail: raviprakashsingh265@gmail .com*
- *Gurucharan Banerjee is currently working as an Assiatant Professor in-Computer Science and Engineering department at Bengal Institute Of Technology and Management,Santiniketan, India, PH-09434210838. E-mail: cse_jgec2006@yahoo.co.in*

## 2 PROBLEMS IN VANET

In VANET there are some problematic issues that most of them are about security. There are security issues in data integrity, privacy and confidentiality that inherited from the Ad-Hoc. In addition of these issues, there are some issues which can impact performance of VANET such as unpredictable temporary situation. The security of VANET is one of the most critical issues because of their transmission information is propagate in open access environments. It is important that all transmitted data cannot be eavesdropped or changed by malicious users. Moreover, the system must be able to detect these malicious users in addition of there is a problem which is legitimated users who do not emphasize their privacy. It seems these problems in VANET are difficult to solve because of increasing network size, speed of the vehicles, their geographical position, and the randomness of the connectivity between them.

## 3 SECURITY ANALYSIS IN VANET

### 3.1 Security objectives

Location information gathered by legitimate network nodes should correspond to actual node positions. This is coherently significant for measuring system volatility and realistic limitations. Location information is evaluated on the basis of received message reporting the location. Nodes should individually be responsible for providing their actual location details and impersonation must be impossible.Another vital requirement is that data and control packets should be free from loops and directed only to their actual target destination.

ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 5, MAY 2015, PP 280-283

Merely forwarding packets on short route paths towards target destination is not required due to volatile nature of the network.

Robustness of the system is necessary against a bus of communication services particularly aimed at resource depletion.

### 3.2 Security Requirement

Authentication: - It guarantees that an origin of communication is what it claims to be form. In absence of such assurance an attacker would fake a node, thus gaining unauthorized access to resource and critical information ultimately distorting the regular operations of the node.

Availability: - It guarantees that the services of system and network are available at all times everywhere throughout the network and are not derived to legitimate users authorized to access.

Confidentiality: - It ensures protection and safety of vital information from being subjected to unauthorized users or entities throughout the network area.

Integrity: - It is assurance that the messages in transmission is never altered or tampered while being transmitted from one end of network to another end by unwanted interception or interference.

Privacy: - It guarantees privacy and secure in the case of sensitive and critical information such as the identity of the driver, location of vehicle, route etc.

Access control: - Access to specific services provided by the infrastructure nodes, or different nodes, is decided locally by police. As a part of access management, authorization establishes whatever node is allowed to try and do in VANET.

Jamming: - The Jammer deliberately generates interfering transmission that prevents communication within their reception range. In the VANET scenario, attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power.

## 4 THREATS ON VANET

Because of the nature of open medium which used in VANET and lack of security in Ad-Hoc protocols, VANET is vulnerable against several attacks. Attackers by using these vulnerabilities can reduce performance of the network and because serious problem for legitimate users.Similar to other types of networks in VANET there are several threats which can impacts performance and security of it. But VANET has potential to expand the worldwide network such as the Internet. Therefore, threats of VANET became a serious issue and all providers, must adopt strong policy against them. Basically, attacks can be broadly categorized into three main groups.

### 4.1 Threats to Availability

The following threats are against the availability of V-V and V-R communications have been identified.

Black hole attacks: This threats is formed when nodes refuse to participate in the network or when an established VANET user drops out when the user drops out, all network traffics are redirected to a specific user which does not exist at all and result is data lost.

Malware: - Malware in VANET can cause distribution to VANET normal operation. Malwares may be injected into the network when the cars VANET unit and/or roadside station receives updates. Generally, malwares are more likely to be carried out by a malicious insider user rather than an outsider user.

Broadcasting tampering: - This type of threats is injecting false safety message into the network to cause serious problem.

Spamming:- Sending spam messages in VANET can cause increasing transmission latency and consuming VANET critical resources.

Greedy drivers: - Greedy drivers who will try to use network just for their own goals such as using resources more than regular users. These users make serious problem especially in hotspots because they cause overload problem for VANETs. This happens because the prediction of condition made by VANET turns out to be wrong and therefore the legitimate users encounter with delays service.

Dos (denial of service):- There are several attacks in the network world but one of the most important of these threats is DOS attacks. This group of attacks has potential of becoming main problem in networks which have limitation in resource such as VANET.

### 4.2 Threats to Authentication

Providing authenticity in VANET involves protecting legitimate users from attackers permeating into the network by using a false identity, identifying attacks that suppress, fabricate, alter or replay legitimate messages, revealing spoofed GPS signals, and impede the introduction of misinformation into the vehicular network. This group of attacks in VANET includes:

Masquerading: The attacker pretends to be another vehicle by using false information such as a massage fabrication, alternation, and replay.

Global positioning system (GPS) spoofing: In this attack, malicious user tries to deceive legitimate users that they think they are in a different location. This is possible by giving false GPS information to users. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than

those to generate by the genuine satellite.

Replay Attack: This attack happens when an attacker replay the transmission of earlier information to take advantage of the situation of the message at the time of sending.

Tunneling: The attacker connects two distant parts of the Ad-Hoc network using an extra communication channel and those nodes suppose that they are neighbors and send data using the tunnel. This attack gives the attacker ability of controlling his attacks outside the victim environment.

Sybil Attack: In this attack type, a node sends multiple messages to other nodes and each message contains a different fabricated source identity in such a way that the originator is not known. The basic goals of this attacker are to provide an illusion to other nodes by sending wrong messages and to enforce other nodes on the road to leave the road for the benefits of the attacker.

Massage Tampering: This type of attack is against message integrity. Generally in VANET, everyone within the same zone can listen to all the messages which other users is sending. Thus, malicious users can modify the contents of the message before receive it by real destination.

Id Disclosure: Disclose the identity information of users who are existence in the network. With this method of attack, attacker can track the current location of the real his target user.

Sensor Tampering: In this attack attackers deceive the vehicle's sensors with wrong information such as tampering with the GPS system or temperature sensors.

Brute Force: In VANET communication keys are used for encrypting data. Brute force attack is an exhaustive key search strategy by checking all possible key values. If the confidentiality of the keys is lost, the identity of the vehicle is lost. Integrity and authenticity of the node is also compromised.

Sinkhole Attack: In sinkhole attacks all the traffic from particular areas goes through the attacker node. Therefore, the attacker will have control over the traffic, enabling the occurrence of many other attacks, such as selective forwarding.

Illusion Attack: Illusion attack is a new security threat on VANET applications where the adversary intentionally deceives sensors on his/her own vehicle to produce wrong sensor readings. As a result, the corresponding system reaction is invoked and incorrect traffic warning messages are broadcasted to neighbors, creating on illusion condition must be achieved by the attacker to create the virtual traffic event. The first condition is to realize or create the pre requisite traffic situation on the road. Second, the false traffic warning messages should be generated and distributed by the attacker. The traditional message authentication and integrity check used in wireless networks are inadequate against the illusion.

### 4.3 Threats to Confidentiality

Confidentiality of messages exchanged between the users of a typical VANET is vulnerable with malicious techniques such as eavesdropping and also collecting location information available through the broadcast messages. In the case of eavesdropping attacker can collect information about exist users without their permission and use the information at a time.

## 5 Prevention from Attacks

By using some mechanism we try to solve the problems related to attacks on VANET. Some mechanisms are discussed below:

DOS: Sharing of private key between only access point and the vehicle which prevents vehicle from exhausting its resources and also avoiding delay in request.

Sybil Attack: Use of an eye to OBU co-ordination mechanism where in one matches the GPS co-ordinates received from nearly vehicles to the real position seen and heard. By this way malicious can be isolated.

Worm Hole Attack: VARS system has been proposed which is a completely distributed approach depending on reputation making use of direct and indirect trust. It is also based upon opinion piggybacking to enable confidence decision on event messages.

## 6 Conclusion

VANETs are the promising approach to provide safety and other applications to the drivers as well as passengers. It becomes a key component of the intelligent transport system. A lot of works have been done towards it but security got less attention. In this project we have to discuss about the VANET and its technical and security challenges. We have also discussed some major attacks and solutions that can be implemented against these attacks. Among these attacks Illusion attack is a serious threat that assists an attacker to hijack a car to have a clean getaway after a theft or robbery. Our future work is to purpose a solution to detect Illusion attack.

## References

[1] G Chandrasekaran, VANETs: The Networking Platform for Future Vehicular Application". Rutgers University, pp. 45-51, may,2007.

[2] Monika, Sanjay Batish and Amardeep Singh," Border-node based Movement Aware Routing Protocol", International Journal of Computer Science and Informatics ISSN (PRINT): 2231 -5292, Vol-1, Iss-4, 2012.

[3] Rakesh Kumar, 2Mayank Dave," A Comparative Study of Various Routing Protocols in VANET",IJCSI International Journal of Computer Science Is-

sues, Vol. 8, Issue 4, No 1, July 2011.

[4] K. Jayasudha," Hierarchical Clustering Based Greedy Routing in Vehicular Ad Hoc Networks", European Journal of Scientific Research ISSN 1450-216X Vol.67 No.4 (2012), pp. 580-594 © Euro Journals Publishing, Inc. 2012.

[5] K. Lakshmi[1], K.Thilagam[2], K. Rama[3], A.Jeevarathinam[4], S. Manju Priya[5]," Comparison of Three Greedy Routing Algorithms for Efficient Packet Forwarding in VANET", IJCTA|JAN-FEB 2012.