Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.129 – 134

A Survey on Security in VANET

Amanpreet[1], Richa Gupta[2]

[1]Department of Computer Science and Engineering, Haryana Engineering College, Jagadhri, Haryana, India
[2]Department of Computer Science and Engineering, Haryana Engineering College, Jagadhri, Haryana, India
[1] aman15preet@gmail.com, [2] Reechaaggarwal8@gmail.com

Abstract*— Vehicular ad hoc networks (VANETs) are getting a lot of consideration these days due to the various applications and possible benefits they offer for their future users. Safety information exchange allows important applications, such as the alerting drivers during crossroads traversing and track merging, and thus, plays an important role in VANET applications. In a VANET, vehicles will depend on the reliability of received data for deciding when to present alerts to drivers. The communication between two vehicles, vehicle to roadside unit is done through wireless communication. That is why security is an important alarming area for vehicular network application. For authentication purpose large amount of bandwidth is consumed and the performance gets affected. In VANET there are some serious network attacks such as Sybil attack are possible. In this paper light is thrown on the previous researches done in this area and researches are compared.

I. Introduction

VANET is abbreviated form of vehicular adhoc network. It is a form of Mobile Adhoc Networks (MANETs), which provides communication between vehicles on road, and nearby fixed units called Road Side Units (RSUs). As given in the figure 1 every node i.e., either a vehicle or RSU communicates with any other node in single hop or multi hop. VANETs are designed with the goals of making driving more safe and comfortable. VANET includes the below mentioned communications:

- Inter-Vehicular Communication
- Vehicle-to-RSU Communication
- Inter RSU Communication.

The channel used for the communication in VANET is DRSC i.e Dedicated Short-Range Communications. DSRC/WAVE supports inter vehicular and vehicle-to-RSU communications in Intelligent Transportation Systems (ITS). DSRC systems eliminate the drawbacks in the wireless infrastructure by providing very less latency, geographically local, high data rate, and high mobility communications. IEEE 802.11p is an improved version of the IEEE 802.11 standard to provide Wireless Access in Vehicular Environments (WAVE). It provides enhancements for 802.11 and supports Intelligent Transportation Systems applications. This includes exchange of data between highly mobile vehicles and between the vehicles and the RSU in the ITS band of 5.9 GHz . IEEE 1609 is a higher layer advanced standard based on the IEEE 802.11p.

1.2 CHARACTERSTICS OF VANET:

VANETs has following characteristics:

- High mobility support
- Almost unbounded network size

© 2016, IJCSMC All Rights Reserved

- Time-sensitive packet transfer
- Accurate positioning of nodes
- Negligible power related problems
- Deployment in direction of road
- Large connection range and large amount of nodes possible

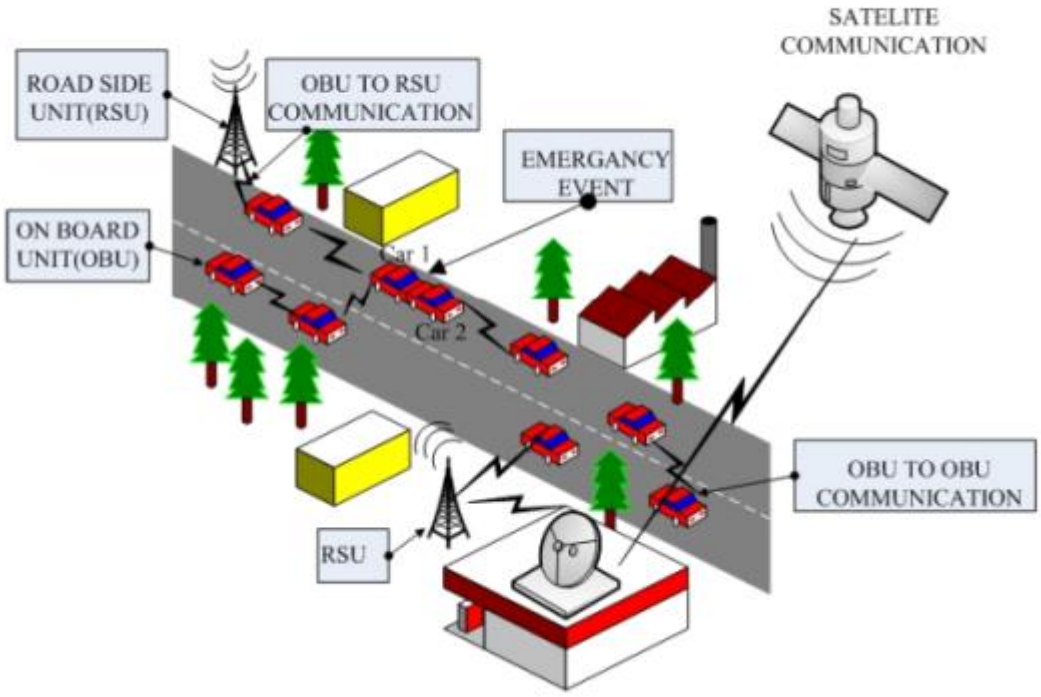

Figure 1 : VANET Architecture

1.3 VARIOUS ATTACKS IN VANET

- **Denial of Service attack**: This attack is said to have occured when the attacker takes control of a vehicles resources or hinders the communication channel used by the Network, this prevents important information from arriving. It also increases the problem for the driver, if it has to depend on the network information.
- **Message Suppression Attack:** An attacker selectively drops few packets from the network, dropped packets may hold important information for the receiver, the attacker suppresses these pack. The motive of such an attacker is not to allow registration and insurance authorities to know about collisions involving his vehicle and/or to prevent delivery of collision reports to roadside units.
- **Fabrication Attack:** this attack occurs when attacker transits false information into the network, the information could be corrupted or the transmitter could hide its original identity. This attack includes, warnings, fabricate messages , Identities ,certificates,.
- **Alteration Attack**: This attack is said to occur when attacker changes an existing data. It has many forms like delaying the transmission of the data, replaying previous transmission, or changing the actual data transmitted.
- **Replay Attack:** This attack is said to have occurred when an attacker replays the earlier transmission to take benefit of the situation at time of sending of the message..
- **Sybil Attack:** Sybil attack is the attack where an attacker creates a large number of false names, and behaves like it is more than a hundred vehicles, to show other vehicles that there is congestion or jam ahead, and thus forcing them to take alternate route.
- **Eavesdropping:** is a very prominent attack against VANETs confidentiality. In this attack attackers can be in form of a vehicle (stopped or moving) or in form of a false RSU. Their aim is to get unauthorized access to confidential information. As confidentiality is must in group communications, techniques should be established to handle such scenarios.

© 2016, IJCSMC All Rights Reserved

1.4 SECURTY SERVICES IN VANET

Security is an important topic for VANET'S. To ensure a secure network, one needs to consider the following attributes to measure security:

- **Availability:** The availability copes with the network services for all nodes and includes bandwidth and connectivity . In order to solve the availability problem, prevention as well as detection techniques involving group signatures scheme have been introduced. The scheme focuses on the availability of exchange of messages between vehicles and RSUs. When any attack leads network unavailability, the proposed method still prevails due to interconnection using private and public keys between RSUs and vehicles.
- **Confidentiality:** These techniques provide the confidentiality in the communication. The most popular technique "false names" are used to protect privacy in VANETS. Each node is given multiple key pairs along with encryption. Messages are encrypted using various pseudo and these pseudo have no link to the vehicle node but relevant authority concerned to it. Vehicle needs to obtain new pseudo from RSU before the previous pseudo expires.
- **Authentication:** Authentication is the checking of identity between vehicles and RSUs and the validation of data during the information exchange. Public or private keys with CA are proposed to establish connection between the nodes and password is used to access the RSUs and AS in authentication method.
- **Integrity**: Data integrity is the guarantee that the data received by nodes is the same as the data which has been generated during the exchange of messages. To protect the reliability of the message, digital signature which is incorporated with password access are used.

Non-Repudiation: It states that sending and receiving the message cannot disagree with ever sending and receiving the message such as accident messages. In some fields, non-repudiation is referred to as auditability where nodes can prove of message being receive and sent respectively.

II. LITERATURE REVIEW

Chih-Hsun Chou et. al. (2008), Ghassan Samara et. al(2010) analyzed that while current solutions to achieve secure VANET, to protect the network from opponents and attacks are still not enough, trying to reach a acceptable level, for the driver and manufacturer to accomplish safety of time and infotainment. The need for a strong VANET networks is sturdily dependent on their safety and privacy features, which are discussed in the paper. The author analyzed and talked about various types of security problems and challenges of VANET and also discussed a set of solutions open to solve these challenges and problems.

Mina Rahbari et. al(2011) Vehicular communications play a substantial role in providing safety transportation with help of safety message exchange. several solutions have been proposed for securing safety messages. Protocols which are based on a fixed key infrastructure are more well-organized in execution and maintain stronger security in contrast with dynamic structures. The paper shows a method based on a fixed key infrastructure for detection of Sybil attack. This attack, puts a great blow on performance of the network. The proposed method, with an cryptography mechanism to detect Sybil attack. lastly, using Mat lab simulator the results of this advance are reviewed, it has low delay for detection of Sybil attack, because nearly all operations are done in Certification Authority, so this proposed scheme is a efficient method for detection of Sybil attack.

Mushtak Y. Gadkari et. al(2012) Since the last few years VANET have expected increased attention as the probable technology to enhance active and protective safety on the road, as well as travel ease. Several unexpected grievous situations are encountered on road networks every day, many of which may lead to blockage and safety hazards. If vehicles could be provided with information about such incidents or traffic situation in advance, the quality of driving can be enhanced considerably in terms of time, stretch, and safety. One of the major challenges in Vehicular ad hoc network is of searching and maintaining an valuable route for transporting data information. safety and privacy are very important in vehicular communications for successful approval and deployment of such a expertise. The vehicular security application should be carefully tested before it is deployed in a real world to use. Simulator tool has been favored over outdoor research because it simple, effortless and inexpensive. VANET requires that a traffic and network simulator should be used collectively to execute this test. In the paper, the author makes an effort for identifying major issues and challenges linked with different vanet protocols, safety and simulation gear

Maria Elsa Mathew et. al(2013) discussed that value-added applications such as online fee services, geographical location recognition, etc. in VANET, develop driving safety, passenger ease, offer great business opportunity, and magnetize more and more attention in our daily life. VANETs join vehicles into a vast mobile adhoc network to share information on a better scale. By enabling the vehicles to be in touch with their neighbors and giving out their driving states, VANETs avoid accidents caused by lane changing, emergency

© 2016, IJCSMC All Rights Reserved

braking, etc. The characteristics of VANET create both challenges and opportunities in achieving safety goals. The a variety of attacks in VANETs are the Sybil attack, DOS attack, mischievous and damaged nodes, sinkhole attack, spoofing, traffic investigation attack, position attack. Providing security to VANET is main in terms of providing user ambiguity, verification, reliability, and privacy of data. In the paper, a complete survey on the problems and vulnerabilities in VANETs are explored and analyzed in detail. The compromised security goals are recognized for each risk. The presented solutions for these threats are also discussed in the paper.

Y.Bevish Jinila et. al(2014) Authentication of safety messages in Vehicular Ad hoc Networks (VANET) plays a major role. The time taken for signature generation and verification should be very less, to provide a secure and comfortable transportation to the node. many signature generation and verification schemes are proposed in the literatures. The author focuses on the usage of Cha Cheon's ID based signature scheme for authentication in vehicular networks. Experimental calculations show that the signature scheme incurs less signature size, less delay and less overhead in transmission when compared to the existing schemes.

Ali Akbar Pouyan et. al(2014) To become an advanced technology that provide safety on the roads, vehicular ad hoc network (VANET) requires strong security architecture. Strong architecture should protect vanet from different types of attacks and protect privacy of drivers. One of the major attack against ad-hoc networks is Sybil attack in which attacker creates multiple identities belonging to other vehicles or replica identities. Attacker uses them to gain an excessively large control in the network leading to accidents or delay in services for the driver of node using only single physical device. The paper presents a case study of various selective methods for Sybil attack detection in networks and their advantages and disadvantages for real implementation.

Rohini Avinash Nere et. al(2015) Vanet is a type of adhoc network which has a lot of scope. If efforts of scholars and technology of automobile industry work combined in this area they can reduce accidents occurring on roads .Vanet is network in which vehicles are considered as Nodes and these nodes communicate with each other as well as road side units on the road. The paper presents real time examples of vanet. There are large no of accidents happening at the intersection. Major motive is to avoid accidents at intersection by introducing RSU in the system.

Soyoung Park et. al proposed timestamp series approach in his paper to protect against Sybil attack in a vehicular ad hoc network (VANET) based on RSU support. The approach targets the initial deployment stage of VANET when basic RSU support infrastructure is accessible and a small fraction of vehicles have network communication capability. Unlike previously proposed schemes that need a devoted vehicular public key infrastructure to officially state individual vehicles, in our approach RSUs are the only machinery issuing the certificates. Due to the differences speed among vehicles, it is uncommon to have two vehicles crossing multiple RSUs at exactly the same time. By using this spatial and temporal relation between vehicles and RSUs, two messages will be considered as Sybil attack issued by one vehicle if they have the same timestamp series issued by RSUs. The timestamp series advance needs neither vehicular-based public-key infrastructure nor Internet reachable RSUs, which makes it an cost-effective solution suitable for the initial stage of VANET

TABLE 1. COMPARATIVE ANALYSIS OF SECURITY ISSUES IN VANET

YEAR	AUTHOR	FEATURES	MERITS	CONCLUSION	FUTURE SCOPE
2010	Ghassan Samara	Discussed current proposed solutions like group signature, use of Certificate authority, use of ECC to reduce overhead	Detailed discussion on present solutions available	VANET is a promising technology but has high chance of attacks	Propose new solutions for securer VANET
2011	Mina Rahbari	method based on fixed key infrastructure for detection of Sybil attack, in the vehicular ad hoc network, uses an cryptography mechanism to detect Sybil attack	method has low delay for detection Sybil attack, most operations are done in Certification Authority, efficient method.	Execution time of the algorithm is low, because most operations is done in Certification Authority	improve the method to detect Sybil attack

© 2016, IJCSMC All Rights Reserved

2012	Mushtak Y. Gadkari	Overview of various routing protocols, attacks and simulators in VANET	Comparison of Simulators in tabular form for better understanding	Surveyed and compared various routing protocols and simulators	_
2013	Maria Elsa Mathew	Survey on threats and vulnerabilities in VANET	Solution to all major threats has been discussed	Illusion attack is a major threat to security	Propose a solution to illusion attack
2014	Y. Bevish Jinila	Cha Cheon's ID based signature scheme	Scheme has less signature size, less delay, less overhead	Proposed scheme is suitable for use in VANET	Combining proposed scheme with pseudo IDs to generate privacy preserving authentication protocol
2014	Ali Akbar Pouyan	Case study of various methods for Sybil attack detection and their advantages and disadvantages in implementation.	Elaborate analysis of defence mechanisms	.Authentication methods are more reliable and useful for message integrity and position verification methods are easy for implementation	To develop suitable methods to balance all the needs of network
2015	Rohini Avinash Nere	studied real time examples of vanet..Motive is to prevent accidents at intersection by introducing Intersection RSU in the system		proposed a method that is based on the minimum waiting time principle to decrease no of accidents occurring at the intersection of roads.	Work on other challenges that affect delivery ratio of broadcasting
_	Soyoung Park	propose a timestamp series approach to protect against Sybil attack in a vehicular ad hoc network (VANET) based on roadside unit support.	targets the initial deployment stage of VANET when RSU support infrastructure is available	Sybil attack can be easily detected if traffic messages have similar timestamps	Compare and analyze this approach for various factors

III. CONCLUSIONS

In this paper we have discussed the security and authentication in Vehicular Network and also analyzed the previous security and authentication mechanism work. There are many attacks that pivot on the issue of identity. In this paper, we have presented an overview of work related to the Sybil attack, in which one node appears as many different identities. Although we lack an efficient, general solution for large systems, there are many solutions that can prevent the attack in several domains.

REFERENCES

[1] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Security Analysis of Vehicular Ad Hoc Networks (VANET)", International Conference on Network Applications, Protocols and Service,2010

[2] Mina Rahbari, Mohammad Ali Jabreil Jamali, "Efficient Detection Of Sybil Attack Based On Cryptography In Vanet", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

© 2016, IJCSMC All Rights Reserved

[3] Mushtak Y. Gadkari, Nitin B. Sambre," VANET: Routing Protocols, Security Issues and Simulation Tools", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 28-38

[4] Maria Elsa Mathew and Arun Raj Kumar P,"Threat Analysis and Defence Mechanisms in VANET", International Journal of Advanced Research in Computer Science and Software Engineering,ISSN: 2277 128X, Volume 3, Issue 1, January 2013

[5] Y.Bevish Jinila K. Komathy,"An Efficient Authentication Scheme for Vanet Using Cha Cheon's ID Based Signatures", Research papers computer science,Volume : 4,Issue : 6, June 2014 ,ISSN - 2249-555X

[6] Ali Akbar Pouyan, Mahdiyeh Alimohammadi, "Sybil Attack Detection in Vehicular Networks", Computer Science and Information Technology, 2014, http://www.hrpub.org, DOI: 10.13189/csit.2014.020403

[7] Rohini Avinash Nere, Prof. Uma Nagaraj , "Intersection RSU in VANET", International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 3, Issue 3, March 2015

[8] Soyoung Park, Baber Aslam, Damla Turgut, Cliff C. Zou, "Defense Against Sybil Attack In Vehicular Ad Hoc Network Based On Roadside Unit Support" ,Paper ID# 900042

[9] José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks", Handbook of Research on Mobility and Computing, www.igi-global.com

[10] Ankita Agrawal et. al, "Security on Vehicular Ad Hoc Networks (VANET)", International Journal of Emerging Technology and Advanced Engineering ,ISSN 2250-2459,, Volume 3, Issue 1, January 2013

© 2016, IJCSMC All Rights Reserved