A Review on VANET Security Attacks and Their Countermeasure

Deeksha
Electronics and Communication
Dept. Thapar University,Patiala, India.
deeksha.jindal24@gmail.com

Ajay Kumar
Electronics and Communication Dept.
Thapar University,Patiala, India.
er.ajay.thapar@gmail.com

Manu Bansal
Electronics and Communication Dept.
Thapar University, Patiala, India
mbansal@thapar.edu

***Abstract*- In the development of smart cities across the world VANET plays a vital role for optimized route between source and destination. The VANETs is based on infra-structure less network. It facilitates vehicles to give information about safety through vehicle to vehicle communication (V2V) or vehicle to infrastructure communication (V2I). In VANETs wireless communication between vehicles so attackers violate authenticity, confidentiality and privacy properties which further effect security. The VANET technology is encircled with security challenges these days. This paper presents overview on VANETs architecture, a related survey on VANET with major concern of the security issues. Further, prevention measures of those issues, and comparative analysis is done. From the survey, found out that encryption and authentication plays an important role in VANETS also some research direction defined for future work.**

Keywords- Authentication, Attacks, Cryptography, DSRC,ECDSA, MANETs, Privacy, Security ,VANETs, V2Vcommunication

I. INTRODUCTION

In modern era, traffic accidents are serious botheration across the world. Traffic crashes on Road rated as 9 th foremost cause of death. Approximately 1.3 million people got died during road mishaps as well as additional 20 -50 millions are hurt globally. Some survey shows that if the driver acquires intimation about the accident still before 1/2 a sec of mishap then 60% of accidents can be abstained. Vehicular Ad hoc Networks (VANETs) accomplish the reason via sharing information about road safety which associated to traffic investigation, normal statistics like files etc by means of continuous internet association [1]. VANETs are a subgroup of MANETs. In VANETs, vehicles as well as roadside infrastructures are communicating nodes and MANETs featuring wireless communication while moving. At present, there are many applications of VANETs which focus on different facets of transportation organizations like driving aid, security of public, collection of tolls collection, control of traffic on roads, rising security as well as freeway system's potency. Due to Large storage capacity, energy sufficiency, high processing power, Predictable movement of nodes, VANET considered being different as of additional ad-hoc wireless networks of the similar category.

Table 1 Comparative Analysis between MANETs and VANET Networks

Parameters	**MANETs**	**VANETs**
Cost	Inexpensive	Expensive
Mobility	Low	High
Range	equal to 100 m	equal to 600 M
Reliability	Medium	High
Change of network topology	Slow	Frequent
Bandwidth	Hundred kbps	Thousand Kbps
Density of nodes	Sparse	Dense
Moving pattern of Nodes	Random	Regular

1.1 Comparison between MANETs and VANETs

In this section a comparative analysis between MANET and VANET is shown in table 1. The table shows that VANET network require more bandwidth for fast communication between vehicles.

1.2 Overview of VANETs Architecture

In this the basic architecture of VANETs has been shown in Fig. 1. The architecture includes V2V, V2I communication, OBUs Application Units (AU), RSU and Access network.

- Ad-hoc environment: It dwells intelligent vehicles (nodes) that contain fundamentally 2 components:
- OBU (On Board Unit): GPS module, wireless communication module, Central control module (CCM), and human-machine interface module are the four modules of OBU unit. CCM encloses processing of serial port information, memory, judgment as well as decision making and data transceiver [3]. The OBU unit has communicational capabilities. The connection of vehicle with RSU via DSRC radios is done by this unit where DSRC is at present acknowledged as mainly assuring standard of wireless to join I2V and V2V.

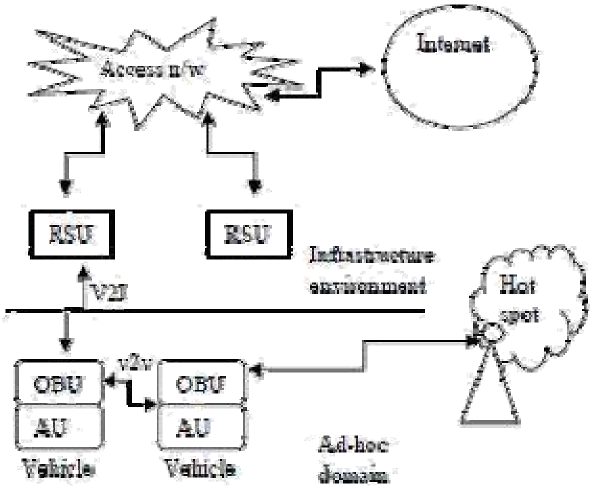

Figure 1 Architecture of VANET

- AU (Application Unit): This unit facilitates OBU to communicate by implementing program. The connection of AU to the OBU can be wired or wireless and AU could endure with the OBU in a particular physical component.
- Infrastructure environment: It includes RSU as well as access network.
- RSU (Road Side Units): It is a wave device usually permanent beside the road side or in devoted positions such as at the intersections or close to parking places. The work of RSU is to act as a router among the vehicles on the road as well as provide connections to further network devices. Main functions of RSU are:
  - Widening the range of communication of the ad-hoc network used to redistribute the data to further OBUs
  - Convey the data to other RSUs to further forward it to other OBUs.

1.3 Overview of VANETs Communication

The VANETs communication divided into two parts as explained below:

- **Vehicle-to-Vehicle Communication:** This is a wireless communication among vehicles. This communication pattern is useful where message is been sent to a group of vehicles or a specific vehicle i.e. in a multicast or uni-cast situation. For paradigm- To extend traffic safety, warning message ought to be sent to incoming vehicles after recognition of mishaps. Figure 3 represents diagram of V2V warning propagation.
- **V2I (Vehicle-to-Infrastructure) Communication:** In this communication, when a potential danger is detected, sending of messages is done either via infrastructure i.e. through RSUs or a vehicle. For the communication among vehicles as well as RSUs, high bandwidth connection is used.

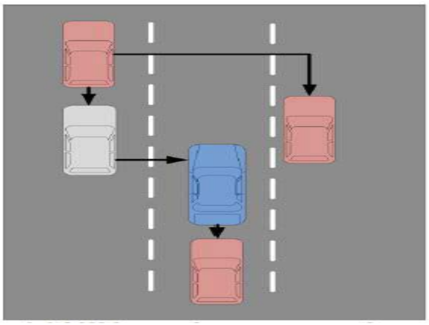

Fig.3 V2V Warning propagation [2]

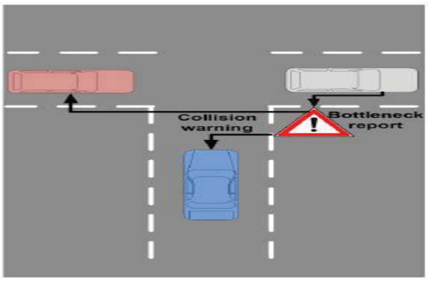

Fig.4 V2I Warning propagation [2]

Fig. 4 represents the diagram of V2I warning propagation. But there exist several attacks on VANETs that leads to insecure transmission of information. So, in next section we will give overview about attacks in VANETs.

1.4 VANET Security Requirements

In VANETs, security is required as VANET packets holds life critical information and it is essential that these packets must reach to the drivers without any modification or insertion of data; similarly the responsibility of drivers should also be recognized that they notify the traffic environment appropriately and within time. So, VANETs must satisfy following security requirements:

- **Authentication:** Authentication provides us a guarantee that data is engendered by an authentic client. It is crucial that the data which propagates in the organism must be accurate and engendered by an authentic client because in VANETs, nodes react acc. to the data established from the other end.
- **Integrity:** It ensures that the data at the sender and recipient side are same. Alteration of message is done by authorized users only. Recipient utilizes the same procedure as used at sender side to create a second digest from the message for comparing it with the original message. This procedure ensures the integrity in data. So, we should need to protect all messages against alteration attacks.
- **Non Repudiation (NR):** This avoids frauds from refusing their offenses because in this even if the attack occurs, NR will expedite the capability to recognize attackers.
- **Availability:** Vehicular networks will need real-time for many purposes so they must be accessible all the time. These applications require quicker reaction from sensor networks or Ad-hoc Network, annihilation of the result can occur or the massage

can become worthless if there is any holdup in seconds for various applications [4].

- **Confidentiality:** All driver's privacy ought to be confined**.** This security requirement is to guarantee that data will barely be read by approved users. Requirement of confidentiality is needed in in group communications, where barely group members are permitted to read such data [2].

1.5 Attacks in VANETs

Several types of attacks are possible on VANETs which are categorized as follows:-

- **DOS attack:** This attack forbids arrival of critical information by taking authority of resources of vehicles or by jamming the channel of utilized by the Vehicular Network.
- **Sybil attack:** In this attack, attacker convinces the vehicles to take alternate path by creating large number of pseudonymous, and tell other vehicles about jam by claiming more than a hundred vehicles ahead.
- **Replay Attack:** This attack confounds the authorities and prevents vehicles identification in hit and run accident by replaying transmission of previous data to seize benefit of the circumstances of the message at sending time.
- **Routing attack:** This attack either disturbs routing process of network or plunges the packets by exploiting the susceptibility of network layer routing protocols. Black hole attack, warm hole attack and gray hole attacks are the most common routing attacks in VANETs.
- **Timing attack:** Broadcasting of security message to the vehicle at right time is one of the imperative requirements of VANET. Timing attack includes several timeslots to the message which leads to receiving of message via a vehicle in accidental location rather than a safe location.
- **Eavesdropping:** This attack violates the confidentiality property and belongs to attack on network layer. Major target of this attack is to acquire access of private data.
- **Location Trailing:** This attack violates the privacy property. In this, attacker traces the vehicle and gets the confidential information about the driver by illegal trailing of the position or route followed by the car.
- **Fake Information:** In this, Attacker transmits fake data in the network for its own profit. For paradigm a nasty node can transmit fake data of intense traffic due to a mishap over road along with clearing his way.

The rest of the paper is organized as follows. Section II presents Literature Survey on VANET attacks and their countermeasure using cryptography algorithms. In Section III, discussed the comparative analysis of security issues on VANETs. In Section IV, defined the prevent measures and research directions. The last section shows the conclusion.

II. LITERATURE SURVEY

In this section, the survey on security issues on VANETs and the preventive measures of those issues are discussed. **Akhilesh Singh, *et al.*[1],** investigated that VANET, which is an infrastructure less network offers intensification in approaches which relates to safety as well as contentment while driving. Safety and traffic analysis information is shared by vehicles using VANET. Because of the contemporary advances in expertise and growth of smart cities worldwide, scope of VANETs application has increased. According to them, VANET offer a self aware scheme which has considerable impact in augmentation services of traffic as well as in abbreviating road mishaps. Data which is distributed in this scheme is sensitive to time along with desires for tough as well as rapid forming network links. VANET which is a wireless ad-hoc network delivers this function totally but is decumbent to attacks on security.

VANET networks enhances traffic management and safety because of envision of numerous new applications. In this paper, authors **Arturo Ribagorda, *et al.*[2]** proposed that traditional security methods are not acceptable all the time because of various exclusive characteristics of VANETs i.e. high mobility of nodes, geographic extension etc. They described and analyzed the most adumbrative VANET security developments in this paper.

Qiong Yang,*et al.*[3] presented a design along with implementation of the OBU in the VANET for highways, and apprehends V2V communication. OBU includes four parts i.e. GPS module, wireless communication module, Central control module (CCM), and human-machine interface module. In this, ARM11-based embedded development platform, DCMA-86P2 module, and a GPS module are hardware platforms. Embedded Linux operating system is the software platform. After testing, results showed that implemented OBU can send as well as receive data for safety assist driving, along with realization of all the required functions and can work firmly.

VANETs can increase security and traffic optimization**.** In this paper**, Indu Bhardwaj *et al.*[4]** stated that VANETs are eminent type of MANETs. In VANET, wireless gadget transmits data to vehicles in close proximity, as well as messages can be send from one to another vehicle. In addition to these advantages, there are some important and prominent issues in VANETS. Security issue is one of them. This paper proposed a analysis of necessities of security, attacks and confronts in security to execute security procedures in the VANETs.

Ahmed Shoeb Al Hasan, *et al.*[5] proposed a modern kind of MANET known as VANET that permits smart transport scheme to offer security of roads and diminish traffic jam via V2V communication or V2I communication. Nonetheless, major worry for researchers in VANETs is security issues. Dynamic topology and mixed structural design in VANETs make them diverse from other ad-hoc networks. Hence, conniving security methods to validate broadcasted messages and remove pernicious messages are pivotal in VANETs.

Lu Chen, *et al.*[6] surveyed a novel kind of Ad hoc i.e. VANET. It is generally employed in ITS, which contain several features as topological structure, fast moving nodes, easily divided networks and frequently changing. Hence, routing protocol design ought to be completely acknowledged these features by means of much node data so as to convey a great dispute to the security of VANET.

Ghassan Samara, *et al.*[7] presented that the awareness of these days research efforts is mainly towards security of VANET, while inclusive resolutions to shield the network from opponent and attacks still require to be enhanced, demanding to attain a satisfactory level, for the driver to attain protection of life and advertorial. They addressed many challenges that VANET are facing and also conferred a set of resolutions offered for these threats and troubles.

In this paper authors compared NS -2 and their own simulator. **Jason J., *et al.*[8]** represented that in simulation of VANETs, we use input traces of vehicle movements which are spawned by simulators of traffic that are based on models of traffic theory. They had expanded a novel VANET simulator that has the capability to handle a lot of additional vehicles than NS-2. They demonstrated outcomes of a cross-validation among NS-2 and their simulator and showed that both simulators generate statistically same outcomes. They proposed authentication method that depends on ECDSA signatures to analyze the proposed authentication and compared using TESLA to broadcast authentication. Each authentication scheme showed strength and weakness in terms of resulting reception rates and latency of broadcast packets.

GPS spoofing is a major threat to upcoming VANET technologies. **Asif Ali Wagan, *et al.* [9]** studied that till then, no one paid attention towards attacks on time synchronization . Thus, they did an study of the attack potential on VANET realizations in glance to spoofed time information. Thereby, they showed that this type of attack permits for brutal refusal of service attacks. Furthermore, via offering the feasibility to misuse authentication features, one can infringe the non-repudiation feature of the security scheme. Moreover, sybil attack can be realized and consistency of the fundamental data sets of time along with position within VANET messages is extremely doubtful by taking into account the outlined attacks.

Qingzi Liu, *et al.*[10] represented that nowadays scholars are paying more attention towards VANET security. In VANET, civil life along with property security is certainly shielded barely when both security and transportation are assured. They validated that architecture of security system act as a protective guard against overall hazards by starring the urgency and complicacy in resolving the worry of VANET by the system. The hierarchical framework of VANET Security System Architecture is considerably worried on, as the entire secure surroundings in VANET relies on bilateral synchronization of self-accomplishment in every hierarchy and mutual support for one another. Core technology applicable in every hierarchy for VANET is recognized and prospect breach for applicable research is exposed.

III. COMPARATIVE ANALYSIS OF VANET SECURITY ALGORITHMS

The comparative analysis is done on the basis of security algorithms used for VANET security as shown in table 2. The comparative analysis is done on the basis of technique used, which attacks covered and limitation of their techniques.

Table 2 Comparative Analysis of Security Algorithms for VANETS

Authors	Title	Techniques /technology Used	Attacks Covered/ Security dimensions	Limitations of used technology
Akhilesh Singh,et al.[1] (2016)	VANET security: Issues, challenges and solutions	Symmetric cryptography, digital signature, hash function, elliptical curve parameter and ID registration technique	Replay attack, DOS, Routing attack, , fake information attacks	-----
Arturo Ribagorda, et al.[2] (2010)	Overview of security issues in vehicular ad-hoc networks	Vehicular public key infrastructure, certificate validation, attribute- based encryption, plausibility check mechanisms	Eavesdropping, Identity revealing, Location tracking, DOS attack	These techniques hadn't addressed the issues on privacy problems due to radio frequency fingerprinting.
Shiang-Feng Tzeng, et al. [20] (2015)	Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET	System initialization, anonymous identity generation, message signing, and message verification.	Forgery attack	Effective solution for forgery attacks only. No solution for other attacks.

Lu Chen, et al.[6] (2013)	Analysis of VANET Security based on Routing protocol information	Elliptic curve algorithm, digital signature technology, Intrusion Detection	Integrity, reliability and confidentiality	
Asif Ali Wagan, et al.[9] (2015)	Emerging attacks on VANET security based on GPS Time Spoofing	Prevention of Time Stamp Jumps, short lived pseudonym certificates and retrospective attack detection via logging.	Denial of service attacks, sybil attack	No solution for other attacks.
Ahmed Shoeb Al Hasan, et al.[5] (2016)	Security threats in vehicular ad hoc networks	Public Key, Symmetric and Hybrid, Certificate Revocation , ID-based Cryptography	Privacy and security	Good privacy schemes with reduced overhead but no solution for attacks.
Ghassan Samara, et al.[11] (2010)	Security Analysis of Vehicular Ad-Hoc Network (VANETs)	Vehicular Public Key Infrastructure, group signature, Certificate Authority, ECC,	DOS attack, Fabrication attack, alteration attack, replay attack, message	
Ram Shringar Raw, et al.[12] (2013)	Security challenges, Issues and their solutions on VANETs	ARAN, SEAD, SMT (Secure Message Transmission), NDM (Non-Disclosure Method), ARIADNE	Replay Attack, Impersonation, False Warning, information disclosure, DOS, routing attack, resource consumption, location tracking effect	Efficient solution for privacy and authentication requirements but no solution for confidentiality.

Table 3 Prevention Measures for Existing Attacks

Property Violated	**Attacks**	**Preventive Measures**
Privacy	Location trailing	ID based system
Availability	Denial of Service (DOS)	IP Info. Handling
	Routing attacks	Cryptography Hashing etc.
Integrity and confidentiality	Eavesdropping	Creation of cipher
	Replay	Time-stamping
	Bogus info.	Hashing, Asymmetric cryptography
Authenticity	Sybil	Radio resource testing, Registration, Position verification, etc.
	Impersonation	Trust authority, PK1
	Timing attack	Encryption solution (TPM)
	Session hijacking	Encryption, Random SID generation

The survey and comparative analysis reflects that security is a big concern in VANET network. In table 3 the prevention measures are shown to resolve attacks.

IV. RESEARCH DIRECTIONS

In this section, some research direction defined on which further work can be done.

- Existing techniques for VANET focus mainly on security, delay and power. Memory is not of much concern in such techniques. Further research work is to develop new techniques which consume less memory such as use of lightweight algorithms in place of conventional algorithms.
- Till date, no mechanism which can alleviate the entire attacks or mainly eminent attacks with only one solution. So, our research work is to eminent most of the eminent attacks with single approach.

V. CONCLUSION

There are many applications of VANETs which focus on different facets of transport systems like driving aid, security of public, collection of tolls collection, control of traffic on roads, rising security as well as freeway system's potency are used. But, there exist several attacks on VANETs such as Sybil attack, timing attack, replay attack, routing attack, DOS attack etc. that leads to insecure transmission of information. So, VANET security plays an irreplaceable role in modern era. In this paper a survey on VANET architecture, attacks and their countermeasure using cryptography algorithm is done. Also, comparative analysis, prevention measure for attacks and research direction defined for VANET network.

ACKNOWLEDGMENT

The authors are grateful to DeitY for the financial support through 'Visvesvaraya Fellowship' and 'SMDP Chips to System Design' project. The authors also want to express their sincere gratitude towards the Director, Thapar University, Patiala for his persistent support and encouragement.

References

[1] R. Mishra, A. Singh and R. Kumar, "VANET security: Issues, challenges and solutions," *International Conference on Electrical, Electronics, and Optimization Techniques*, 2016.

[2] J. M. de Fuentes, A. I. Gonzalez-Tablas and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," *Handbook of Reseach on Mobility and Computing,* IGI Global, 2010.

[3] Yang, Qiong, Lin Wang, Weiwei Xia, Yi Wu, and Lianfeng Shen, "Development of on-board unit in vehicular ad -hoc network for highways," *International Conference on Connected Vehicles and Exp*, pp. 457-462, 2014.

[4] I. Bhardwaj and S. Khara, "An Analytic Study of Security Solutions for VANET," *International Journal of Computer Applications*, Vol. 132, No.10, Dec.2015.

[5] A.S. Al Hasan, Md. Shohrab Hossain, and Mohammed Atiquzzaman, "Security threats in vehicular ad hoc networks," *Conference on Advances in Computing, Communications and Informatic,* pp. 21-24, Sept.2016.

[6] Chen, L., Tang, H., & Wang, J., "Analysis of VANET security based on routing protocol information," *Fourth International Conference on Intelligent Control and Information Processing,* pp. 134-138, June 2013.

[7] Samara G., Al-Salihy, W. A. and Sures, R., "Security issues and challenges of vehicular ad hoc networks (VANET)," *4th International Conference on Trends in Information Science and Service Science,* pp. 393-398, May 2010.

[8] Haas, J. J., Hu, Y. C. and Laberteaux, K. P., "Real-world VANET security protocol performance,"*Conference on Global Telecommunications*, pp. 1-7, Nov. 2009.

[9] Bittl, S., Gonzalez, A. A., Myrtus, M., Beckmann, H., Sailer, S. and Eissfeller, B., "Emerging attacks on VANET security based on GPS Time Spoofing," *IEEE Conference on Communications and Network Security,* pp. 344-352, 2015.

[10] Liu, Q., Wu, Q. and Yong, L., "A hierarchical security architecture of VANET," *International Conference on Cyberspace Technology*, pp. 6-10, Nov.2013.

[11] Samara G., Al-Salihy, W. A., and Sures, R, "Security analysis of vehicular ad hoc networks (VANET)," *Second International Conference on Network Applications Protocols and Services*, pp. 55-60 , Sep. 2010.

[12] Raw, R. S., Kumar, M. and Singh, N., "Security challenges, issues and their solutions for VANET," *International Journal of Network Security & Its Applications*, 2013.

[13] Jin, H. and Papadimitratos P., "Scaling VANET security through cooperative message verification," *IEEE conference on Vehicular*, pp. 275-278 , Dec. 2015.

[14] Yan, G., Bista, B. B., Rawat, D. B. and Shaner E. F., "General active position detectors protect VANET security," *International Conference on Broadband and Wireless Computing, Communication and Applications*, pp. 11-17, Oct. 2011.

[15] Bariah L., Shehada D., Salahat E. and Yeun, C. Y, "Recent advances in VANET security: a survey," *82nd Conference on Vehicular Technology,* pp. 1-7 , Sep. 2015.

[16] Barskar R. and Chawla M., "Vehicular Ad hoc Networks and its Applications in Diversified Fields," *International Journal of Computer Applications,* Vol.123, Jan. 2015.

[17] Chetan, V. S., N. S. Benni, and C. Bhushan. "Security framework for VANET for privacy preservation," *Fourth International Conference on Computing, Communications and Networking Technologies*, pp. 1-6 , July 2013.

[18] Wagan, A. A., and Jung, L. T., "Security framework for low latency vanet application," *IEEE International Conference on Computer and Information Sciences*, pp. 1-6, June 2014.

[19] S. Biswas, R. Tatchikou and F. Dionl, "Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety," *IEEE Communication Magazine,* vol. 44, no 1, pp. 74-82, Jan. 2006.

[20] Horng, S., Tzeng, S.,Li, T.; Wang, X. and Huang, P.; Khan, M., "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET," *IEEE Transactions on Vehicular Technology,* 2015.