2017 2nd International Electrical Engineering Conference (IEEC 2017)
May 19 th -20 th, 2017 at IEP Centre, Karachi, Pakistan

Security in Vehicular Adhoc Networks

Yasir Iqbal[1*], Yusra Kaleem[2]

[1] Department of Telecommunication Engineering, Sir Syed University of Engineering and Technology,
Karachi, 75300, Pakistan (yasiriqbal.engr@gmail.com) * Corresponding author
[2] Department of Telecommunication Engineering, Sir Syed University of Engineering and Technology,
Karachi, 75300, Pakistan (yusra.kaleem13@gmail.com)

Abstract: Vehicular Ad hoc Networks (VANETs) are the hopeful method for drivers and travelers to give insurance. It is used to provide communication between vehicle to vehicle (onboard unit) or vehicle to infrastructure (roadside units). Wireless communication, security, and privacy are very important parameters to avoid threat in a network. It assumes an imperative part in clever transport framework which provide a self-aware mechanism that has major effect in enhancement of traffic services and in decreasing ratio of road accidents. But as the other networks, VANET has also challenges about security especially authentication, privacy and attacks against resources. This paper presents a survey that categorizes security issues, solutions, challenges and attack types according to different VANET applications.

Keywords: Vehicular Ad hoc Network, VANET, Attacks, Security threats.

I. INTRODUCTION

These days, the incidents related to road are common. The death rate has contacted 1.2 million individuals for every year on street mishaps [13]. Aside from road movement, the driver should be dynamic on road. We can make some assistance to driver by giving climate conditions or any risk on street. In this way, new kind of system is being introduced called VANET (Vehicular Ad-hoc Network). VANET is a segment of MANETs (Mobile Ad-hoc Networks) in which vehicle turned into a node. This is a huge system with more noteworthy number of nodes accessible on system and spread in different roads. The vehicles on system can connect to impart each other like V2V (Vehicle-to-Vehicle) correspondence. Be that as it may, each system needs administrations to keep up a system. Safety accomplished by trading of information through VANET that decreases the quantity of mischances on road. Every vehicle can give an alert call that could be produced when mishap happen, on that time the vehicle will work like a caution for another vehicle. Every vehicle is well-informed with such messages that could conserve life and will make essential strides. So, data must be solid and genuine. In this circumstance, the security prerequisites are critical. In the meantime, the security of every driver or vehicle is exceptionally vital from unapproved individual.

II. VANET FEATURES AND ISSUES

The interconnection of vehicles in a system on street is called Vehicular Ad hoc Network. As cell phone acts as hubs in mobile ad hoc network (MANET). When we supplant mobile with autos it's called VANET. In any case, the progressions of topology in VANET got to be distinctly extraordinary stage than MANET. The pattern of mobility of VANET, differs it, in such a way that it has particular paths so VANET nodes can be predicted by MANET [3]. The transceiver, road side unit (RSU) makes a network in VANET by connecting vehicles [4]. RSUs can be applied in particular section of road like stop signs, traffic lights and other intersections which is commonly called On-Board Units (OBUs) [6][7]. Figure 1 shows background structure of VANET.

Vehicles must be mounted with hardware system to allow information related to position like Global Positioning System (GPS) [2]. The DSRC (Dedicated Short Range Communication) is a moderate range protocol for wireless communication particularly assigned for automotive purpose. As DSRC enables high data rate between communication on vehicle-to-vehicle (V2V) or for communication between vehicle-to-roadside (V2R). IEEE 802.11p and IEEE 1609.x doled out of DSRC measures and stack of communication standards for Wireless Access in Vehicular Environments (WAVE). DSRC used 802.11p for groundwork and IEEE 1609 used as high layer of standard [4]. Intelligent Transportation System (ITS) is more secure and solid, furthermore make accommodating applications for public during travelling [7]. At of 5.9 GHz in which 75 MHz has been allotted to DSRC by U.S Federal Communications Commission (FCC) to be used unrestricted for communication of V2V and V2R [7].

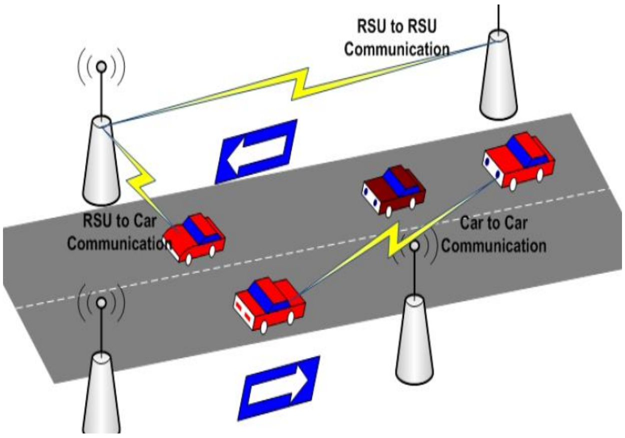

Fig. 1 VANET Background Structure.

A. Characteristics of VANET

- High Mobility of vehicle e.g. in highways makes difficult for algorithms to measure the position of vehicle and to make certain privacy for the vehicle [9] [13].
- Rapidly changing network topology**,** as the vehicle moves at high speed, requires fast processing and rapid change of topology continuously. A delay can cause problem for safety related information.
- Providing safe driving and enhancing traffic efficiency by communication among vehicle moving on road. So, it requires applications and communication link between nodes on network. The applications help drivers with warning messages if any accident occurs in the same direction of road. Nonetheless, more applications could be executed on network to facilitate traveler that could give climate update, traffic stream and other data like service station, shopping centers and fast food [18].
- Network size is unbounded, can be used for particular area, city or for countries [13].
- Exchange of information frequently.
- Wireless Communication.
- Time Critical: the time is extremely vital, message could be conveyed inside time restrain so a driver can settle on choice as needed.
- No power constraints: Power in MANET is critical but not in VANET. Because vehicles can provide continuous power to OBU through battery.

B. Types of attackers in network

a. Insider vs. Outsider

The insider attacker is one who is present with in a network and can communicate with each member of network and can give false information which is more critical than outsider attacks. The outsider attacker is one who is outside of network and can feed imprecise data and cause interrupt in network. [9]

b. Malicious vs. Rational

A malicious attacker is one who only harms the performance of network. A rational attacker is one who is keen to get private advantage but when he attacks on target, he could be predictable.

c. Active vs. Passive

An active attacker is one who can make message or signals which can bolster to network. An active attacker can make the traffic stop and change the destination or can create delays for communication. A passive attacker is one who involve as wiretapping, eavesdropping and monitoring of data traffic without harming the network.

III. SECURITY THREATS AND SOLUTIONS

A. Authentication

Authentication refers that every vehicle must be genuine in the network. Every message in network must be real. Because vehicles in network take decision upon the information received so authentication must be granted. The verification of message could be done by sending message along with private key and certification; the receiver will verify the message with key and certificate [10] [12]. The threat called impersonation, in which attacker grabs the identity of authentic node. This type of attacker may harm the network by spoofing services, impersonates RSUs, and may employ network layer and application layer [7] [13]. Another threat on authentication is Sybil attack, expresses as increase in number of nodes by using different identicalness. The attackers act as a hundred of vehicle at a place and try to show the congestion on road and convince other vehicle to go from another way [10], see fig 2. The solution to overcome such problem on authentication is ARIADNE, a safe on-request routing protocol for Ad-hoc system proposed in [17], in which two keys use as KSR and KRS for sender to collector and collector to sender individually by utilizing MAC. The verification builds up when sender sends any message with particular information, for example, timestamp then computes the MAC and sends using KSR. The authentication of routing is done by using MAC, Digital Signature and TESLA.

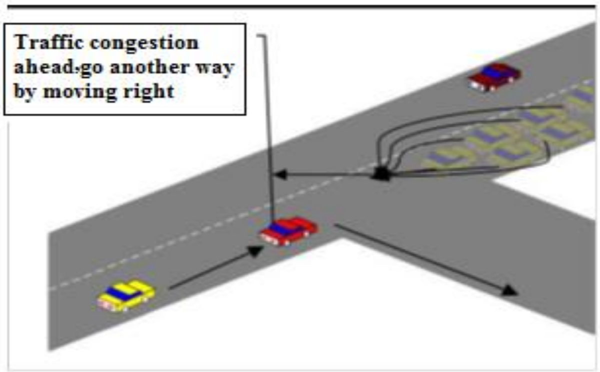

Fig. 2 Sybil Attack

B. Availability

The availability is most crucial requirement, as it refers that every vehicle should be able to transmit information at the time of need. Because availability means requirement of active network all time and delay in response from network may cause in result of ruinous. So, the unavailability of network makes the network unguarded to DoS attack. As the DoS threat occurs when attacker, can fetch out all required information and can jam transmission among vehicles. For this circumstance, the driver would be at danger and can achieve street incident and movement over-burden [10] [11]. This threat can be protected by SEAD (Secure and Efficient Ad hoc Distance Vector) which is based on DSDV (Destination Sequence Distance Vector) routing. The DoS attacker tries to utilize surplus network bandwidth. SEAD does not use asymmetric cryptography function but it works on one way hash chain function. It also prevents from the replay attack as the freshness of packet is provided by the destination sequence number [13] [15] [8].

C. Non-Repudiation

Non-repudiation is simply that no entity can deny after sending or receiving messages. All the data or any type of violation will be saved in any authorize server which can be easily fetch out at the time of need. So, if any node sends false information, there will be proof of that node. But, the attacker can dodge non-repudiation if same credentials are shared by two or more entities. The criminal could not be identified as they conspire to have same credential. The attacks in authentication process can be prevented by ARAN. The cryptography in ARAN use open key and require certificate server. As the public key is available to all nodes in network. The sender node sends the Route Discovery Packet (RDP) to the majority of its accessible nodes, as the nodes have record of source. The purpose of RDP is to locate the routing. When message receives, all the receivers attach sign and their own certificate and again forward to all available nodes. After getting response from destination, it replies to the primary node from which it got the message. Beside destination node, no any node can answer the RDP regardless of the possibility that it has path of destination. The destinations reverse from destination to source and will unicast the reply (REP). The sender of REP signs all the REP, which is likewise checked by the following hop. The source starts when it encodes the message Shortest Path Confirmation (SPC) and sends it to close-by node, encoded message is marked by the node and joins its certificate. As the destination node reverse back from destination to source, so it answers with the Recorded Shortest Path (RSP). One routing table require in ARAN for every node in network. The error message (ERR) is generated in two cases, when inactive route receives the message and when node is cut off due to node movement [14] [19].

D. Confidentiality

Confidentiality of communication is very important, that is, to make sure that only authorized entities will entertain the communication messages. Eavesdropping is a most renowned attack that link with network layer and passive attack by nature. The attacker can be placed in any vehicle of network and can gain all data that must be confidential. Before sending messages, it should be encrypted to save outsiders from driver credentials.

E. Integrity

Integrity must be achieved by saving information from attackers, because an attacker can change or modify the information that is being communicated among all nodes. Information must be received without any alteration [9]. Alteration attack targets on integrity. The primary purpose of attacker is to modify the message and sent to desired nodes. It could lead to many problems such as delay in transmission, traffic jam, traffic hazards and other problems regarding safety of human.

F. Privacy

The unauthorized entity must be unaware from driver's information. The information such as identification of drivers, location of node and their route history etc. Delay attack can be prevented from this privacy [13]. The NDM (Non-Disclosure Method) technique solved this problem which is founded on asymmetric cryptography and uses maximum Security Agents which uses public and private keys. The sender does not disclose any location during communication through SAs. The phenomena of sending message is that the sender first sends message to SA_1 then SA_1 further transmit it to SA_2 and so on. Every SA_i be informed the location of SA_{i-1} and SA_{i+1}. Each SA encloses the received message along its public key [13] [16].

IV. COMPARISON AND DISCUSSION

In this section, a comparison between different threats and their solutions are presented. VANET could be safer by implementing ARAN, SEAD, NDM and ARIADNE techniques as shown in table 1.

The discussion in table 1 gives the comparison of all results.

	Security Requirements	Technology Used	Attacks	Solutions
(i)	Authentication Integrity Non-Repudiation	Cryptography Certificate	Impersonation Alteration Replay	ARAN
(ii)	Availability Authentication	One way hash Function	DoS	SEAD
(iii)	Privacy	Asymmetric Cryptography	Location Tracking	NDM
(iv)	Authentication	Symmetric Cryptography MAC	Routing Attack Replay Attack	ARIADNE

V. CONCLUSION

Security in VANET has been a challenging job to execute because this could lead to a danger for human being. Therefore, in this paper, we have discussed some core security requirements of VANET such as authentication, privacy, integrity and availability, the ways how these security needs could be harmed by attacker with different types of attacks. We have also summarized the best solutions by which all the attacks can be prevented by implementing with specific techniques, discussed in comparison table 1.

VANET is a rising examination territory with promising future and extraordinary difficulties particularly in its security. It has been found that different techniques and solution have been proposed to beat these difficulties but at the same time different escape clauses are staying, which are yet to be found.

REFERENCES

[1] L.Ertaul, S.Mullapudi, “The Security Problems of Vehicular Ad Hoc Networks (VANETs) and Proposed Solutions in Securing their Operations”, *ICWN 209.*

[2] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges”, *Telecommunication Systems August 2012, Volume* 50, Issue 4, pp. 217-241.

[3] Saira Gillani, Imran Khan, Shahid Qureshi, Amir Qayyum. 2008, “Vehicular Ad Hoc Network (VANET): Enabling Secure and Efficient Transportation System”.

[4] H.Noori, B.Badihi Olyaei. “A Novel Study on Beaconing for VANET-based Vehicle to Vehicle Communication”, Smart Communications in Network Technologies (SaCoNet), 2013.

[5] Ján Janech, Štefan Toth. “Communication in Distributed Database System in the VANET Environment”. *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems* pp. 795–799.

[6] Luca Caviglione, Giuseppe Ciaccio, and Vittoria Gianuzzi. “Architecture of a Communication Middleware for VANET Applications*”. The 10th IFIP Annual Mediterranean Ad Hoc Networking Workshop 2011.*

[7] Yi Qian, and Nader Moayeri. “Design of secure and application-oriented VANETs” *Conference, VTC Spring. IEEE,* 2008.

[8] Xiaonan Liu, Zhiyi Fang, Lijun Shi. “Securing Vehicular Ad Hoc Networks”. Pervasive Computing and Applications. *ICPCA* 2007.

[9] P. Caballero-Gil, “Security Issues in Vehicular Ad Hoc Networks”. University of La Laguna 2011.

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

[11] José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda,” Overview of security issues in Vehicular Ad-hoc Networks”, 2010 - orff.uc3m.es.

[12] Sur abhi Mahajan, Prof. Alka Jindal, “Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks” *International Journal of Computer Applications* (0975 – 8887) Volume 1– No.20, February 2010.

[13] Ram Shringar Raw, Manish Kumar, Nanhay Singh, “Security challenges, issues and their Solutions for VANET”, *International Journal of Network Security & Its Applications (IJNSA),* Vol.5, No.5, September 2013.

[14] Kimaya Sanzgiri, Daniel LaFlammey, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, “Authenticated Routing for Ad hoc Networks”, Selected Areas in Communications, *IEEE Journal* on (Volume: 23, Issue: 3) 2005.

[15] Yih-Chun Hu, David B. Johnson, Adrian Perrig, “SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks.” Ad Hoc Networks 1 pp. 175–192, 2003.

[16] Andreas Fasbender, Dogan Kesdogan, Olaf Kubitz, “Variable and Scalable Security: Protection of Location Information in Mobile IP*”, IEEE VTS, 46th Vehicular Technology Conference,* 1996, Atlanta, USA.

[17] YihChun Hu, Adrian Perrig, David B. Johnson, “Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks”, *Journal Wireless Networks* Volume 11, 2005.

[18] Saif Al-Sultan, Moath M. Al-Doori, Ali H. Al-Bayatti, Hussien Zedan. “A comprehensive survey on vehicular Ad Hoc network”. *Journal of Network and computer application,* volume 37, January 2014.

[19] Dahill, B. N. Levine, E. Royer and Clay Shields, "A Secure Routing Protocol for Ad Hoc Networks", *Proceeding of IEEE ICNP*, pp 78-87, Nov 2002.