DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4432

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

REVIEW PAPER

Available Online at www.ijarcs.info

SECURITY ASPECTS OF VEHICULAR AD-HOC NETWORK (VANETS): A REVIEW

Manju
Scholar
Department of Computer science & Engineering
University Institute of Engineering & Technology
M.D. University, Rohtak, Haryana, India.

Dr. Sunita Dhingra
Assistant Professor
Department of Computer science & Engineering
University Institute of Engineering & Technology
M.D. University, Rohtak, Haryana, India.

Abstract: Recent advancement in communication technologies is enabling the design and implementation of a range of different types of networks. One such network that becomes a great attention from the research community is Vehicular ad-hoc Network (VANET). VANET provides road safety, traffic efficiency and congestion control to the users. Because of open source network more security attacks and threats occur during communication, so security becomes a major issue in VANET. Many of the researchers are working on these security problems, but these problems can be solved by implementing new type of routing protocols over existing routing protocols.
So, the present work focuses on working, Architecture and previously used routing protocols in VANET.

Keywords- VANET, Security, Simulation, Communication

1. INTRODUCTION

Vehicu1ar ad-hoc Network is a subclass of mobile ad-hoc network which allow communication between moving nodes by hoping message. Moving node can be any vehicle equipped with transceivers or Road Side Unit (RSU). The Vehic1e to Vehic1e (V2V) Communication and the vehic1e to road side base station communication is possib1e in VANET. It provides secure and safe transportation to the users. The security challenges faced in VANET is the weak 1ink between the nodes. Because most nodes in a VANET are continuously moving with very high speed in the same way as a vehicle moves on roads. The main purpose of research in VANETs is enhancement vehic1e safety by gathering information about traffic on road with the help of inductive loops, cameras, roadside sensors and surveys. Severa1 different app1ications are emerging in VANETs. These app1ications inc1ude safety applications to make driving much safer, mobile commerce and other information services that will inform drivers about any type of congestion, driving hazards, accidents, traffic jams. VANET have various different properties which distinguish it with other ad-hoc networks. In VANET nodes are moving with high ve1ocity due to which the topo1ogy changes rapid1y and connection lost easily. Besides providing safety, security and life-saving applications, VANET also proved an important source of communication tool for their users. These approaches make vehicular ad-hoc network most promising and important field of research.

Vehicular communication network (figure 1) is a network of vehicles and entities on roadside infrastructure that interconnect without any underlying infrastructures to send and receive informational alerts related to current road traffic situation.

Architecture of VANET mainly can be described as three layers: a sensor layer, a communication layer, and a data process layer [1]. In sensor layered vehicles are considered as a dynamic sensor node which uses the on board units (OBU) to sense the traffic data, node location and velocity. The On Board Unit (OBU) is an electronic device used in vehicle which is able to sense, communicate, and compute data over network. Another device Road Side Unit (RSU) is also used in VANET, which work as a router between the vehicle on road and other devices over network. RSU helps to forward the packet, facilitating reliable communication [1].

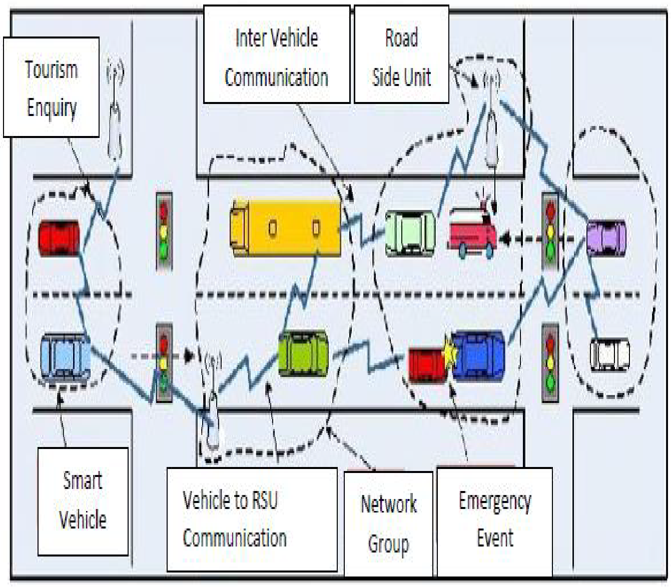

Figure1. Vehicular communication Network [7]

The architecture (Figure 2) of VANET shows that the communicating nodes in a VANET can be either vehic1es

(V2V) or base stations. Vehicles can be private (belonging to individuals or private companies) or public (public transportation e.g., buses, and public services such as police vans). The communication Base stations can be governmental or private service providers. As shown in figure the vehicles are interconnected with each other and communicating with Road Side Units (RSU) interchangeab1y.

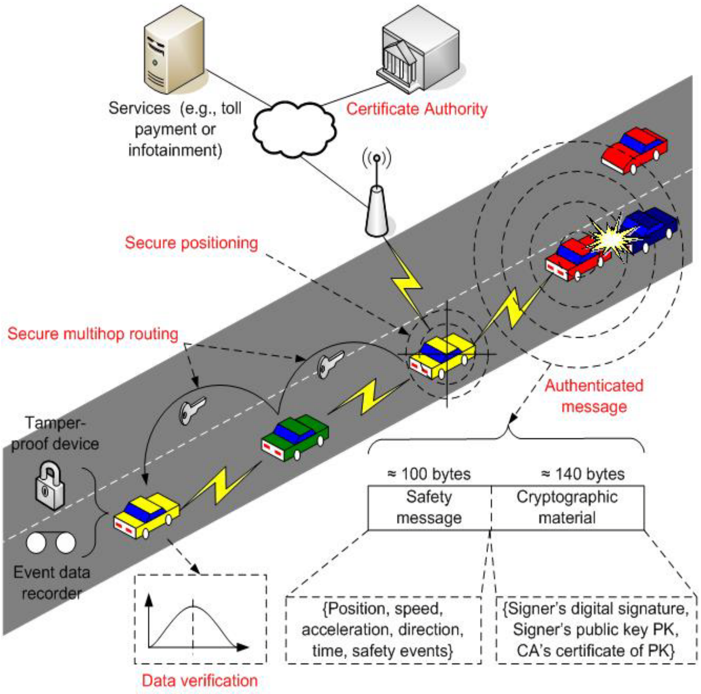

Figure.2 Architecture of VANET [8]

Vehicular ad hoc network integrates vehicles and Intelligent Transportation Systems (ITS). ITS is an application which uses information technologies for vehicles safety and security like sensors, cameras and other sensing devices. ITS system also helps in finding places, forecasting traffic congestion that makes interactive and cooperative vehicle movement on road. So VANET is advance application of ITS which uses facilities like Google maps, GPS for identifying the appropriate route and Wi-Fi devices and makes transportation service very effective.

2. LITERATUE REVIEW

Various advancements have been made towards different security enhancing techniques on Vehicular ad-hoc network that overspread the techniques of delivering safety favours & preserving driver isolation for Wireless Access in Vehicular Environments uses. Many researchers already have done the work on different ad-hoc networks techniques. They tackle many issues to establish communication network. Intercommunication in VANET is not so easy to establish and manage between dynamic nodes. VANETs network technology is recent burning topic for the research scholars as well as for IT companies. Therefore VANET is used to fulfil the latest needs of users that consists of mobile entities having dynamic topology which make it difficult to tackle various issues like less path redundancy, unpredictable node density, short lifetime of communication link. The work done by various researchers is briefly discussed hereby:-

Park and Soyoung [1] proposed a timestamp series technique to protect from Sybil attack in a vehicular ad-hoc network which was based on road side unit support. This mechanism was basically suitable for initial deployment of VANET where vehicles communicate over basic network infrastructure RSU. It was secure due to uses of digital certificates instead of public key infrastructure. Moreover, this timestamp series technique required a fixed infrastructure which did not uses internet accessibility but uses certificates. A Sybil attack could only be detected when vehicle having similar timestamp sent message for communication. This could only be handled if vehicle show its previous timestamp to RSU and verify it. This approach solve the problem of traffic congestion, complex roadways etc.

Lin et al [2] VANET is an important and essential field of research which assured the smart transportation to derivers and also introduced various protocols i.e. unicast protocol, multicast protocol, geocast protocol, mobicast protocol, and broadcast protocol. The drawbacks of VANET could be overcome to establish low network overhead routing protocols along with low frequency delay and low time complexity.

Martinez et al [3] proposed the advanced Street Broadcast Reduction (eSBR) scheme to reduce broadcast packets congestion problem and also increase the number of nodes for communication. This scheme overcomes the redundancy, contention, packet collisions problems and increase network throughput.

Taha et al [4] proposed a location privacy scheme which has used Network Mobility protocol (NEMO). The attacker's confusion was increased by hiding the location information of moving vehicles. The motive behind discussed approach was to confuse the attacker by enhancing the estimation errors of their RSSs measurements with using fake-points and cluster-based sub schemes.

Bhoi et al [5] proposed a new Position Based Secure Routing Protocol (PBSRP). Which is further classified into Most Forward within Radius (MFR) and Border Node based Most Forward within Radius (B-MFR) routing protocols? These protocols contained security modules which protects system from various attacks. The main idea behind the proposed approach was to provide secure vehicular communication to set an accident free journey for the users across the entire world.

V.Lakshmi Praba and A.Ranichitra [6] proposed modified version of existing Ad hoc On Demand Distance Vector (AODV) protocol to achieve road safety goals. The AODV protocol was a topology based protocol which was analyzed using the performance over metrics Packet Delivery Ratio, Throughput, Dropped Packets and network overhead. This mechanism has provided secure communication between the moving vehicles by using security routing protocols.

Raw et al [7] proposed VANET's technical and security aspects which could be implemented to resist the intrusions. Few major attacks was also discussed which effected network security. VANET provided various communication facilities and removed various security threats. VANET also assured smart transportation to drivers as well as passengers.

Sirola et al [8] proposed various routing attacks such as Sybil & Illusion attacks and also discussed security issues on network layer in VANET. Vehicular Ad-hoc Network (VANET) is the most interesting research area which provided Intelligent Transportation System (ITS) services to the users. Because of its high mobility and dynamic nodes, implementation of protocols in VANET is very imperative task. VANET used to provide effective driving environment and various related services to the users. Security played a major role in wireless network and also in VANET applications, where threats could affect the human lives.

Rabieh et al [9] presented privacy-preserving routing scheme which enabled VANET traffic management instead of warning vehicles during congestion. This mechanism worked on encrypted segment-based route information and provided secure route to road side units (RSUs) for communication. RSUs worked by computing the encryption for a number of vehicles in each segment of cell, without having the knowledge of exact routes of vehicles. Traffic Management Centre (TMC) contained the information of every route of vehicles where RSU could predicate route congestion or traffic. RSU could change his alternate route for security and privacy. Privacy-Preserving Routing Scheme for Traffic Management in VANET proposed public key cryptography based scheme which ensures the security protection, confidentiality and non-repudiation.

Manjunatha et al [10] VANET is sub form of mobile ad hoc network which provided secure communication between two mobile nodes, vehicle to vehicle or vehicle to infrastructure. It provided secure and smart transportation to the users with the help of security routing protocols. VANET provided challenging security aspects due to communication between high mobile nodes.

Kamani et al [11] considered Sybil attacks as a serious security threats to VANET and sensor networks. In this kind of attack original identity of the vehicle was stolen by a hacker to create multiple fake identities. The main focused task in this field was to detect and remove attackers from the network. It discussed various Sybil attack detection mechanisms on which the work already has been done by many of researchers in this area.

3. ATTACKS IN VANET

Due to wireless open network, possibilities of attacks and threats are very high. There exist number of attacks and threats over network. We discuss some generic and significant attacks that are commonly available in literature. Mainly attacks can be categorised in three groups: Availability, authenticity, Confidentiality [7].

a. Threats to availability Various availability threats vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) have been identified:

- *Denial of Service (DoS)* it is a very popular attack. Purpose of this attack is to disturb the whole communication channel. This attack makes system useless for short time of period or permanently. These attacks affect the network by flooding or jamming the network for authentic user. Flooding control the channel by sending high volume traffic. Jammers prevent the communication across the network by interfering signal.
- *Broadcast Tempering* In this attack *false* information is being injected into the network which can create serious problem over network.
- *Black Hole attack* A black hole attack is performed when established node is drop out and does not participate in communication.

b. **Threats to authenticity** Authentication is mandatory during communication over network. Unauthenticated user can create serious problem in user's lives. Some attacks are mentioned here:

- *Masquerading* In this attack attacker stole authentic user's ID and pretends to be as an authentic user after using it. For example, the attacker hides his own identity and act as an emergency vehicle to mislead other vehicles or leave place for it [17].
- *Spoofing* This kind of attacks happen when attacker knows all information about the driver or user. The attacker found the position of vehicle by using driver's address and can misuse his address.
- *Sybil Attack* Sybil attack generates when an attacker uses huge number of pseudonymous, instead of his real identification and misguide genuine users by using pseudonymous. It is named after subject of the book Sybil which is a case study of a woman diagnosed for dissociative disorder.

c. **Threats to confidentiality** In this attack the attacker collect information about the user through eavesdropping and misuse that information when user is unaware.

- *Sinkhole Attack*: In this type of attack, attacker keep full information of particular place or area and when node passes through this area attacker access credentials of user.

4. CHALLENGING ISSUES IN VANET

VANET is quite different from other network. Due to the highly sensitive nature of information being sent via VANET, managing security is a challenging task here. This section will discuss different security challenges in VANET:

- Mobility: VANET can be distinguished from the existing Mobile Ad hoc network (MANETs) by its various characteristics. One of them is uses of dynamic nodes with high speed. Due to high speed of moving vehicle connection established for a short time period, therefore quality of communication is being affected.

- Network Management: VANET is a huge network with covering more than 85 million vehicles over the entire world. The network management is a difficult task because coverage of wide area and uses of dynamic nodes in VANET. Hence topologies are also changing rapidly and affect the quality of connection.
- Efficient Routing: Generally, Establish an optimal route, to send data packets between communicating nodes is main motive of routing algorithm, but in VANET establishment of an optimal path via intermediate nodes is also a challenging task because of highly moving nodes.
- Environmental Impact: For communication VANET uses the electromagnetic waves. These waves can be affected by the environmental changes. Due to variation of climate over the world environmental impact also affected.
- Congestion and collision Control: Signals congestion and collision is a big problem due to unbounded network size in VANET. The traffic load fluctuates low and high in different areas due to which the network partitions occur frequently. In rush hours the traffic load becomes very high which creates congestion and collision of signals.

5. ROUTING PROTOCOLS

Various types of challenges in vehicular communications have been identified and addressed. A large number of routing protocols have been proposed for VANET. Routing Protocols are used to forward data

from source to destination. Routing protocol establishes route or path between two communication nodes and sends packets from source to destination or vice versa [2].

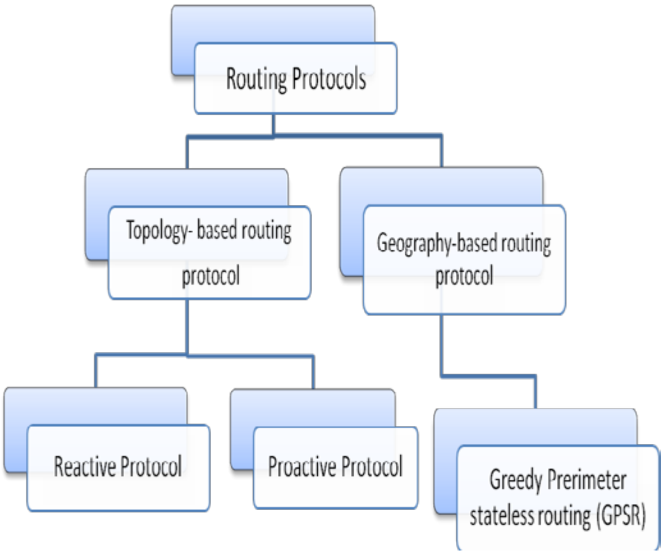
Routing Protocols
Topology- based routing protocol
Geography-based routing protocol
Reactive Protocol
Proactive Protocol
Greedy Preimeter stateless routing (GPSR)

Figure.3 Taxonomy of Routing Protocols

VANET routing protocols can be classified as **topology-based** and **geographic (position-based)**. Topology-based routing protocols can be further divided into proactive (table- driven) and reactive (on-demand) routing protocols. Proactive routing protocols maintain routing path information all time even if connection is not in use [2]. Whereas Reactive routing protocols maintains route information for only those connections which are currently in use or implement route on demand basis.

Position Based routing protocols do not maintain any route information itself. It Locate neighbor nodes obtaining by beaconing method and destination's position can be obtained by location discovery services such as GPS.

Enough research has already been done including the comparison of various routing protocols and their performance evaluation based on various existing protocols. It will be interesting to evaluate the performance of one of the routing protocol by varying the number of mobile nodes. For this purpose Greedy perimeter Stateless Routing (GPSR) protocol can be simulated because it has been observed that GPSR is a better approach as compared to Ad-hoc Distance Vector (AODV)[13] and other discussed routing protocols.

Greedy perimeter Stateless Routing (GPSR) protocol is a geographic-based reactive routing protocol, which works on position based pattern. GPSR maintains the established routing path in the given period and copes well with fast-changing network topologies and high relative vehicle speeds, density. The performance of the proposed protocol can be evaluated using simulation tools, mainly- Network Simulator (NS-2)[12] and MOVE (Mobility model generator for Vehicular networks) [9] over SUMO (Simulation of Urban Mobility) [13].

6. CONCLUSION

VANET is very effective mode of communication between moving vehicles which provides Safety, security, traffic management and congestion related information. But some open medium networks exposed the security threats that influence the reliability of discussed features. Therefore VANET provided security routing protocols for secure communication. VANET security routing protocols provides security and privacy against security attacks to the vehicular drivers as well as passengers. Protocols ensure data integrity, reliability and congestion control, also can handle various security threats.

The presented paper discussed the work already done by various researchers along with already available security protocols and concludes GPSR protocol as an efficient VANET protocol.

REFERENCES

[1] Park, Soyoung, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support." Military Communications Conference, IEEE, pp37-48, (2009).

[2] Lin, Yun-Wei, Yuh-Shyan Chen, and Sing-Ling Lee. "Routing Protocols in Vehicular Ad Hoc Networks: A Survey and Future Perspectives." Journal of Information science & engineering, Volume.26, Number.3, pp 913-932, (2010).

[3] Martinez, Francisco, "Evaluating the impact of a novel warning message dissemination scheme for VANETs using real city maps." International Conference on Research in Networking. Springer Berlin Heidelberg, pp 265-276, (2010).

[4] Taha, Sanaa, and Xuemin Shen. "A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs." IEEE Transactions on Intelligent

Transportation Systems, Volume.14, Number.4, pp 1665-1680, (2013).

[5] Bhoi, Sourav Kumar, and Pabitra Mohan Khilar. "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services." Communications and Signal Processing (ICCSP), International Conference on. IEEE, pp 1170-1174, (2013).

[6] V. Lakshmi Praba, “Isolating Malicious Vehicles and Avoiding Collision between Vehicles in VANET,” International conference on Communication and Signal Processing on IEEE, Volume.4, pp 127-132, (2013).

[7] Raw, Ram Shringar, Manish Kumar, and Nanhay Singh. "Security challenges, issues and their solutions for VANET." International Journal of Network Security & Its Applications Volume.5, Number.5, pp 95-105, (2013):

[8] Sirola, Priyanka, Amit Joshi, and Kamlesh C. Purohit. "An analytical study of routing attacks in vehicular ad-hoc networks (VANETs)." International Journal of Computer Science Engineering (IJCSE) Volume 3, Number 4, pp210-218, (2014).

[9] Rabieh, Khaled, Mohamed MEA Mahmoud, and Mohamed Younis. "Privacy-preserving route reporting scheme for traffic management in VANETs." Communications (ICC), International Conference on. IEEE, pp 1-11, (2015).

[10] Manjunath, P. S., and Narayana Reddy. "Assesment of vanet routing protocols in safety paradigm." Applied and Theoretical Computing and Communication Technology (iCATccT), International Conference on. IEEE, pp 70-82, (2015).

[11] Kamani, Jaydip, and Dhaval Parikh. "A Review on Sybil Attack Detection Techniques." Journal for Research| Volume 1. Number.01, pp 2395-2400, (2015).

[12] Saravanan D, Agalya V, Amudhavel J, Janakiraman S. “A brief survey on performance analysis and routing strategies on Vanets”. Indian Journal of Science and Technology. Volume.9, Number.11, pp 1–6, (2016)

[13] E. M. Royer and C.K. Toh, “A Review of Current Routing Protocols for Ad-Hoc Mobile Ad hoc Networks,” IEEE Personal Communications, Volume.15, Number.6, pp 30-39, (1999).

[14] Yan-tao Liu “Stationary of Random Direction models”, Second International conference on network security, wireless communications and trusted computing. pp1-7, (2010)

[15] Liu, Jianqi, & Wan, Jiafu & Wang, Qinruo & Deng, Pan & Zhou, Keliang & Qiao, Yupeng "A survey on position-based routing for vehicular ad hoc networks." Telecommunication Systems, Springer, Volume 62, No.1, pp 15-30 (2016).

[16] Kumar, Sushil, and Anil Kumar Verma. "Position based routing protocols in VANET: A survey." Wireless Personal Communications, Springer, Volume 83, No.4, pp 2747-2772 (2015).

[17] Zeadally, Sherali, Ray Hunt · Yuh-Shyan Chen Angela Irwin and Aamir Hassan"Vehicular ad hoc networks (VANETS): status, results, and challenges." Telecommunication Systems Volume 50, No.4, pp 217-241(2012).

[18] Gillani, Saira, Amir Qayyum, and Rashid Mehmood "A survey on security in vehicular ad hoc networks." International Workshop on Communication Technologies for Vehicles. Springer, pp 59-74, (2013).