A Review on Security in Vehicular Ad-hoc Networks

Ramandeep Kaur[1], Er. Rupinderpal Singh[2]

[1]M.Tech Scholar Computer Science & Engineering Department
[2]Asst. Prof. in Computer Science & Engineering Department
Global Institute of Management and Emerging Technologies, Amritsar

---

Abstract - There is a significant increase in the rate of car accidents in countries around the world and also the casualties concerned ever year. New technologies are explored relating to the vehicular ad hoc Network (VANET) due to the rise in vehicular traffic/congestion around us. Vehicular communication is very important as technology has evolved. The research of VANET and development of proposed systems and implementation would increase safety among road users and improve the comfort for the corresponding passengers, drivers and also other road users, and an excellent improvement in the traffic efficiency would be achieved. The paper investigates the current and existing security issues related to the VANET.

Key Words: VANET, V2V, V2I

1. INTRODUCTION

A Vehicular Ad-Hoc Network or VANET may be a sub variety of Mobile Ad-Hoc Network or MANET that has communication between vehicles and between vehicles and road-side base stations with an aim of providing economical and safe transportation. A vehicle in VANET is taken into account to be an intelligent mobile node capable of communicating with its neighbors and alternative vehicles within the network. VANET is especially aimed toward providing safety related info and traffic management [9]. The most elements of Vehicular Ad hoc network are vehicles, roadside unit, and on board unit (OBU). Vehicles are equipped with OBU and sensors to collect the data from roadside unit (infrastructure unit) or neighboring vehicles by disseminating alert messages [2].

2. ARCHITECTURE OF VANET

2.1 Vehicle to Vehicle Communication

This is vehicle to vehicle design wherever vehicles behave as both consumers and producers as vehicles collect data from different vehicles within the network and transmit that data to different vehicles within the network. So, both collection and dissemination of information are done inside the network for rapid distribution of messages [3].

2.2 Vehicle to infrastructure communication

Vehicle to infrastructure communication is that in which infrastructure is employed to gather data from vehicles and supply that data to different vehicles once necessary [3].

2.3 Hybrid

Hybrid is the combination of both Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) architectures [3].

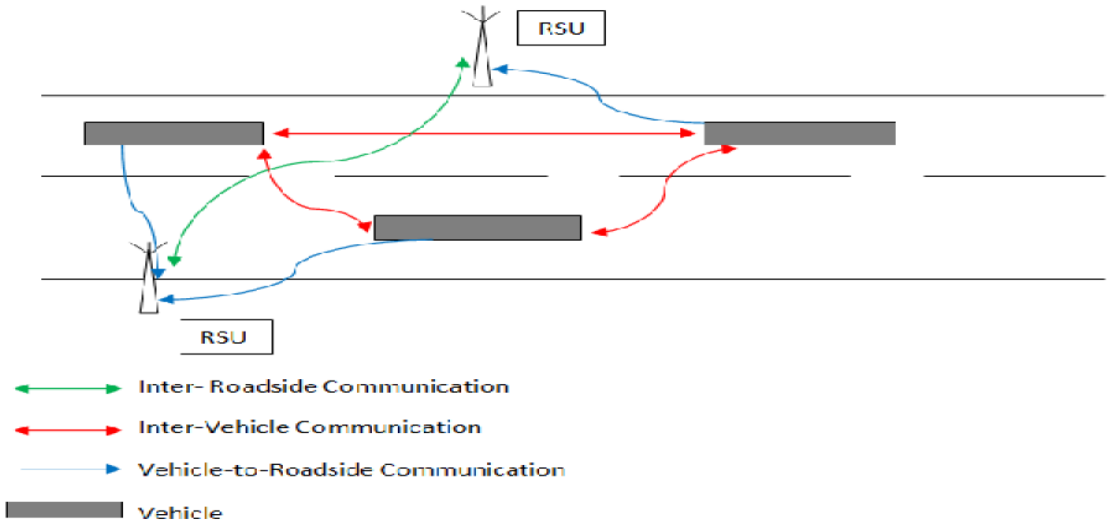

Fig -1: Architecture of VANET

3. APPLICATIONS OF VANET

3.1 Safety Applications

Safety applications are mainly focused on to minimize the possibilities of road accidents and the loss of lifetime of the occupants of vehicles. A vast amount of accidents that occur in all sections of the world are related to vehicle collisions. This category of applications primarily provides active road safety to avoid collisions by helping the drivers with timely data. Data is distributed among vehicles and road side units that are additionally employed to predict vehicle collisions [3].

3.2 Traffic Monitoring and Management Applications

This kind of applications mainly concentrated on enhancing the vehicular traffic flow, traffic coordination and traffic cooperation. It's liable for providing updated local info, maps and suitable messages finite in space and/or time [3].

3.3 Infotainment Applications

Infotainment applications offer ease and luxury to drivers and travellers. The objective of infotainment applications intend to supply all type of messages that provide entertainment and helpful messages to the driver and traveller. Finding the closest coffeehouse, movie theater, shopping mall, fuel station that offers the perfect cost in that region, or obtainable parking space are some examples of infotainment or documentary applications [3].

4. CHARACTERISTICS OF VANET

4.1 High Mobility

The nodes (vehicle) in Vehicular Ad-Hoc Network mostly are running at huge velocity. The node mobility is controlled by the road topology and design [6].

4.2 Quickly Changing Network Topology

Due to huge node movability, the network topology in Vehicular Ad-Hoc Network tends to vary regularly [6].

4.3 Unlimited Network Size

VANETs might involve the vehicles in one town, multiple cities, or may be a state. Therefore the VANETs network mustn't be reliant on the quantity of the nodes [6].

4.4 Anonymous Naming

Majority of the applications in VANETs need recognition of the vehicles in a definite area, rather than the particular vehicles. So, pseudo naming system must be followed to guard the secrecy of the driver [6].

5. ROUTING IN VANET

5.1 Topology Based Routing Protocols

For packet delivery in topology based routing protocol, connection info that available within the network is employed to perform packet delivery from source to destination. It's additionally partitioned into two categories as [12]:

5.1.1 Proactive Routing protocols

In this category of routing all the required data for routing is preserved in background regardless of communication requests. Packets are continually transmitting between nodes to keep up path & then routing table is maintained inside a node that specify upcoming hop regarding destination. [12].

5.1.2 Reactive Routing Protocols

Reactive routing protocols are also referred as on demand routing protocol. It solely opens the routes once it's required for a node to converse with one another. It solely keeps the routes that are presently required. Therefore it minimizes the network burden. It consists of route finding process in which the query packets are flooded into the network for route finding & once the routes establish then this part completes [12].

5.2 Position Based Routing Protocols

Position based routing is additionally known as geographic routing. In position based routing protocols every node should aware of its present location. Sender node transmits packet or message to destinations geographic location without the use of network address [8].

5.3 Cluster Based Routing Protocols

Cluster based routing relies on cluster. Cluster could be a collection of nodes. One among them is meant to cluster head to transmit the packets into cluster. It offers smart measurability for huge networks however it incurred the network delays and overhead once forming cluster [8].

5.4 Broadcast Routing Protocols

Broadcast routing is especially used for safety applications like for sharing weather, traffic, emergency, road conditions between vehicles & transmitting advertisements & announcements. Broadcasting is employed once message is to be delivered to the vehicles outside the transmission vary. In broadcasting similar message is distributed to all nodes in network. Bandwidth of the network is exhausted but it assures the transmission of packets [12].

5.5 Geo Cast Routing Protocols

It is mainly a location based multicast routing. Its major goal is to transfer the packets inside a particular geographical region (Zone of relevance ZOR). Vehicles that are beyond the ZOR are not warned or alerted. It simply describes a zone in which it transmits the message so as to minimize the overhead & congestion [12].

Protocols	Proactive Protocols	Reactive Protocols	Position Based Greedy Protocols	Cluster Based protocols	Broadcast Protocols	Geo cast Protocols
Prior Forwarding Method	Wire less Multi hop Forwarding	Wire less Multi hop Forwarding	Heuristic method	Wire less Multi hop Forwarding	Wire less Multi hop Forwarding	Wire less Multi hop Forwarding
Digital Map Requirement	No	No	No	Yes	No	No
Virtual Infrastructure Requirement	No	No	No	Yes	No	No
Realistic Traffic Flow	Yes	Yes	Yes	No	Yes	Yes
Recovery Strategy	Multi hop Forwarding	Carry & Forward	Carry & Forward	Carry & Forward	Carry & Forward	Flooding
Scenario	Urban	Urban	Urban	Urban	Highway	Highway

Fig - 2: Comparison of Various Protocols

6. SECURITY IN VANET

Security is a problem that requires to be cautiously addressed within the style of the vehicular communication system. Many threats probably exist, as well as bogus messages lead to interruption of traffic or may be danger, sharing driver's personal info, etc. Safety and traffic management need real time info and this sent info will have an effect on life or death choices. Because VANET movability is more than MANET, routing with the ability of guaranteeing security in VANET is additional challenging than Adhoc. Location secrecy and obscurity are main problems for vehicle users. A secure system, additionally the fundamental network nodes, can include a Vehicular Public Key infrastructure (PKI), a Secure Computing platform and numerous security mechanisms. Secure mechanisms include identity management using Electronic License Plates with certified public and personal keys connected to the owner, Authentication and Integrity with Digital Signatures, Privacy with Pseudonyms, Pseudonym managing and Certification Revocation mechanisms [10].

7. SECURITY CHALLENGES IN VANET

The security challenges should be thought of throughout the planning of VANET design, security protocols, cryptographic methods etc. The subsequent list presents various security challenges:

7.1 Real time Constraint

VANET is time crucial wherever security related message ought to be transmitted with 100ms transmission delay.
Therefore to attain real time constraint, quick cryptographic formula ought to be used. Message and entity authentication should be completed in time [11].

7.2 Data Consistency Liability

In VANET even a certify node will conduct malicious behavior that may cause accidents or disturb the network. Thus a technique ought to be planned to avoid this inconsistency [11].

7.3 Low tolerance for error

Some protocols are designed on the concept of possibility. VANET uses life crucial data on which activity is performed in extremely small time. A little error in probabilistic formula might cause damage [11].

7.4 Key Distribution

All the safety mechanisms execute in VANET must be reliant on keys. Every message is encrypted and required to decode at receiver end either with similar key or completely different key. Thus allocation of keys between vehicles is a big challenge in designing the security protocols [11].

8. SECURITY REQUIREMENTS IN VANET

8.1 Authentication

Authentication is a major necessity in VANET because it guarantees that the messages are delivered by the actual nodes and thus the attacks done by the greedy drivers or the opposite adversaries can be minimized to an enhanced level [4].

8.2 Message Integrity

Message integrity ensures that the message isn't altered in transmission that the messages the driver receive are not fake [9].

8.3 Message Non-Repudiation

In this safety based scheme a sender can be recognized simply. But solely particular authority is permitted for sender recognition. Vehicle could be recognized from the authenticated messages it delivers [9].

8.4 Access control

Vehicles should operate according to rules and they ought to simply execute those tasks that they're certified to do. Access management is ensured if nodes proceed according to given approval and create messages consequently [9].

8.5 Message confidentiality

It is a method that is required once sure nodes need to converse in secret. However anyone cannot do this. This could solely be fulfilled by the law enforcement authority vehicles to converse with one another to place across secret data. An example would be, to detect the position of a criminal or a terrorist [4].

8.6 Privacy

This method is employed to make sure that the data is not leaked to the unauthorized individuals. Third parties shouldn't be capable to track vehicle activities because it may be a violation of individual privacy. Location privacy is additionally required so that nobody ought to be capable to learn the past or future positions of vehicles [9].

8.7 Real time guarantees

It is necessary in VANET, as several security related applications rely on strict time guarantees. This feature is essentially needed in time sensitive road safety applications to keep away from collisions [9].

RELATED WORK

Kiho Lim et al. [2016] present a protocol for secure message delivery in VANET. The protocol must take into attention the restricted computation power of the OBUs. Since RSUs have a lot of computation power, authentication of messages and distribution of messages are done by the RSUs. If an RSU is not inside the communication range of vehicles sending messages, messages are delivered to the closely RSU through alternative vehicles by employing a routing protocol [1].
Samiksha et al. [2016] presents survey and comparison of various categories of VANET routing protocols. From the review it is clear that situation based, geo-cast and cluster based protocols are additional dependable for majority of the applications in VANET [5].
Harpreet Kaur et al. [2015] stated that in case of huge network, it impossible to employ the traditional safety schemes to protect the data communication over VANET and it's not possible to manage the keys at great scale for every vehicle. Thus there is required to establish a safe routing scheme for vehicles which might simply recognize the vehicles and may verify the information send by them. They explore the necessities of the authentication throughout the information transmission in VANET [7].
Navneet Kaur et al. [2016] stated Vehicular ad hoc networks (VANETS) is appeared as a latest area of information sharing. Vehicles in vehicular ad hoc networks are extremely unstable because of dynamic topology. Thus to offer well-organized information dissemination from source node to destination node, clustering is one in all the simplest panaceas (way out) for the above problem. They emphasize on the method of clustering how the cluster head is selected and re-scheduled and what are the issues in stable clustering that results in the betterment of clustering technique in VANETS [2].
Dr. Sandeep Singh Kang et al. [2016] stated that a Vehicular Ad-Hoc Network is a Sub type of Mobile Ad-Hoc Network that offers communication among vehicles and between vehicles and road-side base stations with the purpose of offering well-organized and secure transmission. They present VANET basics structure, its design, challenges, and applications. They additionally present information distribution varieties and its protocols comparison [3].
Harjit Kaur et al. [2016] stated that the Vehicular Ad-Hoc Network is a technology that employs movable cars as nodes in a network to form a mobile network. VANET turns each collaborating vehicle into a wireless router or node, permitting cars approximately hundred to three hundred meters of one another to join and, in turn, construct a network with a large range. They present several protocols employed in VANET and evaluating high performance using various parameters [4].

CONCLUSION

VANET is a region of research that holds promising future for vehicular users. VANET aims at reducing the accidents on our roads and increasing the flow of information among vehicle and the road users. The distinctive nature of VANET springs up problems like illegal pursuit and electronic countermeasures of the network. during this paper, we have a tendency to introduced VANET, its design, components, communication pattern and problems in its security, the routing protocols used in VANET that enabled road users to communicate and receive messages appropriately, which include: High quality, rapid changing, network topology, unbounded Network Size, Frequent Exchange of information, Wireless Communication, Time crucial, spare Energy and higher Physical Protection. VANET will cause a technological change and improvement for the road users. Useful data exchange will prevent future harm and accidents on our road.

REFERENCES

1. Kiho Lim and D.Manivannan, "An Efficient Protocol for Authenticated and Secure Message Delivery in Vehicular AdhocNetwork",http://dx.doi.org/10.1016/j.vehcom.2016.03.001,veh.commun 2016
2. Navneet Kaur, Er. Sandeep Kad, "Data Dissemination in VANET- A Review" International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869 (O) 2454-4698 (P), Volume-6, Issue-4, December 2016
3. Er. Gaganpreet Kaur, Dr. Sandeep Singh Kang, "Study of various Data Dissemination types and its Protocols- A Review" International Journal of Information Management and Technology, ISSN NO. 2356-2600, Volume 1, Issue 1, Aug 2016
4. Harjit Kaur, Kamal Jeet Kaint, Rakesh Kumar, "A Review on Different Approaches of Safety Message Transmission in VANET" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 6, Issue 6, June 2016
5. Samiksha, Anit Kaur, "Data Transmission in VANETS: A Review, Applications, Routing Protocols" International journal of Computer Applications (0975-8887) Volume 141-NO.7, May 2016
6. Sudha Dwivedi and Rajni Dubey, "Review in Trust and Vehicle scenario in VANET" International Journal of Future Generation Communication and Networking Vol. 9, No.5 (2016), pp. 305-314
7. Harpreet Kaur, "A Review of Secure Routing Over VANET" International Journal for Research in Applied Science and Engineering Technology & Engineering Technology (IJRASET), ISSN: 2321-9653, Volume 3, Issue V, May 2015
8. Omkar Shete1, Sachin Godse2, "VANET: A Survey on Secure Routing" International Journal of Science and Research (IJSR) ISSN (online):2319-7064, Volume 4 Issue 1, January 2015
9. Divya Chadha 1, Reena 2, "Vehicular Adhoc Network (VANETs): A Review" International Journal of Innovative Research in Computer and Communication Engineering, ISSN (online): 2320-9801, ISSN (print): 2320-9798, Vol. 3, Issue 3, March 2015
10. Senthil Ganesh N., Ranjani S., "Security Threats on Vehicular Adhoc Networks (VANET): A Review Paper" International Journal of Electronics Communication and Computer Engineering" ISSN 2249-071X, Volume 4, Issue (6) NCRTCST-2013
11. Ram Shringar Raw1, Manish Kumar1, Nanhay Singh1, "Security Challenges, Issues and their Solutions for Vanet" International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013
12. Santosh Kumari 1 and Dr Sushil Kumar 2, "Survey on routing protocols in VANET".