Research Paper
Impact Factor - ***2.262***
Peer Reviewed Journal

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

A COMPREHENSIVE STUDY OF NITTY-GRITTY TO SECURITY CONCERN IN VEHICULAR AD HOC NETWORK

Mrs.K.Kiruthika*   Dr.C.L.Brindhadevi**
**Research Scholar, Bharathiar University, Coimbatore.*
***Assistant Professor, Dept. of Computer Science, Queen Mary's College, Chennai.*

Abstract

The number of automobiles has been increased on the road in the past few years. Due to high density of vehicles, the potential threats and road accident is increasing. Wireless technology is aiming to equip technology in vehicles to reduce these factors by sending messages to each other. Vehicular ad hoc network (VANET) is recognized as an important component of Intelligent Transportation Systems and it is a subclass of Mobile ad hoc networks which provides a distinguish approach for Intelligent Transport System (ITS). The main benefit of VANET Communication is seen in active safety systems, which target to increase safety of passengers by exchanging warning messages between vehicles. This paper emphasis the comprehensive study from the basic components, essential protocols to security threats in VANET.

Keywords: Architecture of VANET, Components of VANET, Application of VANET, Security Issues in VANET.

1. INTRODUCTION

Vehicular Ad-hoc Network (VANET) is an emerging technology that makes the human life more comfortable while travelling. This Network enrols the moving car as node and forms an advanced ad-hoc network to make vehicles to communicate. These vehicles can communicate with each other when they are approximately 100 to 300 metres apart. VANET is a special kind of Mobile Ad-hoc Network (MANET). Number of vehicles is increasing day-by-day resulting in heavy traffic in the roads around the world.

Innovations in safety, comfort and convenience like VANET have made the promise to change the face of vehicular travel. Technology such as VANET provides the ability for vehicles to instantly and wirelessly network with other vehicles nearby for providing travellers with new features and applications. To say in crisp, VANET is a wireless network that is formed between vehicles on an "as-needed basis".

Vehicles in order to participate in the network must equip with wireless transceivers and control modules. Moving Vehicles act as a node in this network. Each node can communicate with each other within few metres and when it is needed to transmit information to the remote node. The intermediate nodes forms a multi-hop network. Though moving vehicles forms a network, in the non-traffic area where movement of vehicles is not possible, permanent roadside unit is fixed to serve in the network. These roadside units open up a wide variety of services for vehicular networks, such as acting as a drop point for messages on sparsely populated roads, serving up geographically-relevant data, or serving as a gateway to the Internet.

Thus VANET achieve an intelligent inter-vehicle communications that provides seamless internet connectivity in improving road safety, essential alerts and accessing comforts and entertainments.

2. CHARACTERISTICS OF VANET

Some characteristics of VANETs remind the characteristics of MANETs [7] [8]. Though they resemble each other, some differentiating VANETs features are as follows

1. Highly dynamic topology
2. Frequently disconnected network
3. Communication Environment
4. Interaction with onboard sensors
5. High Mobility
6. Unbounded network size
7. Frequent exchange of information
8. Unlimited Battery Power and Storage

3. ARCHITECTURE OF VANET: Architecture of VANET [3] portrays three categories,

3.1 Pure Cellular / *WLAN:* In this type, both fixed cellular gateways and WLAN access points together form the network.

3.2 Pure Ad hoc: Vehicles and all the road-side wireless devices form Pure Ad hoc network architecture to achieve certain goals.

3.3 Hybrid: Combination of ad-hoc and infrastructure network is hybrid architecture.

4. COMPONENTS OF VANET

In VANET, Communication occurs either among vehicles or between fixed network and moving vehicles. This Communication is achieved through the wireless medium named WAVE (Wireless Access in Vehicular Environment).[1] The Core components are Application Unit (AU), On-Board Unit (OBU) and Road-Side Unit (RSU). To send and receive messages, each vehicle is equipped with Sensors and OBU.

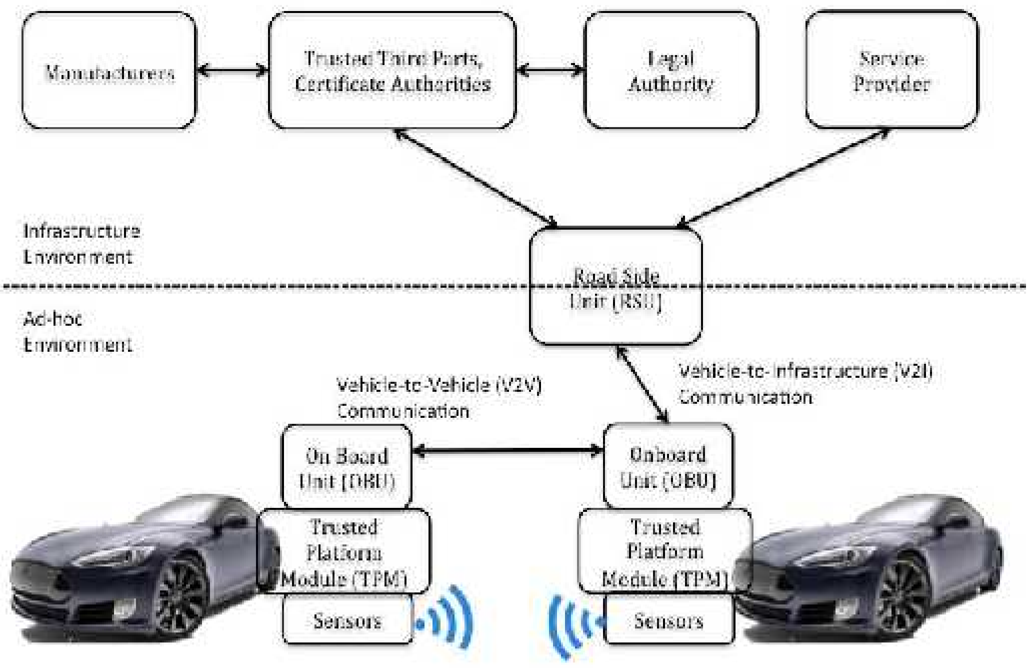
Manufacturers
Trusted Third Parts, Certificate Authorities
Legal Authority
Service Provider
Infrastructure Environment
Road Side Unit (RSU)
Ad-hoc Environment
Vehicle-to-Vehicle (V2V) Communication
Vehicle-to-Infrastructure (V2I) Communication
On Board Unit (OBU)
Onboard Unit (OBU)
Trusted Platform Module (TPM)
Trusted Platform Module (TPM)
Sensors
Sensors

Fig.1 Components of VANET [10]

4.1 Application Unit (AU)

The Application Unit is the device in the vehicle to use the providers application. This AU might be either an exclusive device for safety applications or a normal device like PDA that runs the Internet. AU and OBU are connected either through the Wired or Wireless medium.

4.2 On-Board Unit (OBU)

On-Board is also a device attached in the vehicle for information exchange. Usually OBU communicates with RSU or other OBUs. OBU is comprised of Resource Command Processor, Resources (R/W memory, User Interface, Specialized Interface) and Network Device. Additionally, another network device can also be attached for safety applications. OBU are connected to the RSU or to next OBU through a wireless link.

4.3 Road-Side Unit (RSU)

This is the device fixed along the road side to serve the moving vehicles. The RSU includes two network devices. One device is for dedicated short range communication and other is for infrastructural network. RSU hosts an application to provide services whereas OBU uses the service provided. In addition, RSU also connect to the Internet or another server.

5. APPLICATIONS OF VANET

Communications among the vehicles and the vehicles to road-side unit provide a wide range of information to drivers and travelers [2]. Network Interface, GPS receivers and Sensors attached to the Vehicle supports them to enhance the road safety and comfort travel [1]. Major Applications of VANET include,

1. Providing road safety information (Collision Avoidance)
2. Traffic Management (Traffic Optimization)
3. Toll Services (Payment Services)

4. Location based Services
5. Infotainment
6. Co operative Driving

6. Challenging Issues in VANET

Two main Challenging issues in VANET are,

- Technical Challenges
- Social and Economic Challenges

6.1 Technical Challenges

Technical Obstacles to be resolved before the deployment of VANET are considered to be Technical Challenges. Some of them are,

1. Network Management
2. Environmental Impact
3. Security
4. Congestion Control
5. Collision Control
6. MAC Design

6.2 Social and Economic Challenges

It is little bit tough to manufacture a system that conveys the traffic signal violation because consumer will not be convinced in monitoring. Building such a system to track the consumer while travelling even will leads to sensitive issues.

7. Routing Protocols in VANET

A routing protocol is a standard that controls how nodes decide route to transfer packets. A basic of communication is that, a node may intimate its presence to other nodes and also should listen the announcements of its neighbors. Routing Protocols are the basic building blocks for an efficient Communication in any network. To execute this, an efficient protocol is essential. Protocols applicable for MANET and VANET are more or less common. Architecture, Characteristics and Challenges are to be kept into consideration for choosing a routing protocols in VANET [4] [5] [6]. Routing Protocols in VANET are broadly classified into 5 main categories,

- Topology Based
- Position Based
- Cluster Based
- Broadcast
- Geocast

7.1. Topology Based

This routing, link information existing in the network and it is further divided two types Proactive (table-driven) and Reactive Routing (on-demand).

- Proactive Protocols - FSR, OLSR, DSDV, CGSR, WRP, TBRPF
- Reactive Protocols - AODV, TORA, DSR, PGB, JARR

7.2. Position Based This routing works with the knowledge of self and neighbor nodes geographic position through GPS.

Protocols - Position based greedy V2V protocols and Delay Tolerant Protocols.

7.3. Cluster Based

Group or Clusters of Vehicles is formed virtually, where each cluster possess a cluster head that is responsible for intra and inter cluster communication via direct links.

Protocols - COIN, LORA-CBF, TIBCRPH, and CBDRP

7.4. Broadcast

Flooding mechanism is used in this routing. Each node rebroadcasts the messages to all its neighbors except the sender.

Protocols - BROADCOMM, UMB, V-TRADE, and DV-CAST

7.5. Geocast

This is the location-based multicast routing. Here the packets are delivered from a source node to all other nodes within a specified geographical area.

Protocols - IVG, DG-CASTOR and DRG

8. SECURITY ISSUES IN VANET

Security in VANET paves more attention today to bring the safety in Traveling. The packets that are transferred through the VANET must be more secure.

8.1 Security requirements in VANET

VANET's Security system should satisfy certain requirements before deployment.

1. Authentication – ensures that the message is generated by the genuine user.
2. Availability – availability of information to all the genuine users.
3. Non-repudiation - Any node should not deny for message transmission.
4. Privacy – guarantee against the unauthorized nodes.
5. Data Verification – frequent data verification eliminates the false messaging.

8.2 Attackers in VANET

Stepping stone in Securing the VANET is discovering the attacker and their characteristics. Based on these , they may fall under three types,

8.2.1 Active Vs Passive

Active – Personalities those who generate signals and packets in the network
Passive - Persons those only sense the signals

8.2.2 Insider Vs Outsider

Insiders – Authenticated Persons in the network
Outsiders - Intruders

8.2.3 Malicious Vs Rational

Malicious - Members who do not possess Personal Profit over the attack
Rational – Those are personally profitable persons through the attack

8.3 ATTACKS ON SECURITY REQUIREMENTS IN VANET [9]

8.3.1 Denial of Service

In this attack, the attacker prevents the genuine user to access the information from the node in a way such as Distributed DoS attack, Jamming and SYN Flooding.

8.3.2 Eavesdropping

This attack breaks the confidentiality and aims in accessing the confident data.

8.3.3 Identity revealing

Usually the driver is the owner of the vehicle , getting his identity may sometimes out them in risk.

8.3.4 Impersonate

It aims in attacking the identity and privilege of an authenticated node to make use of the network resources.

8.3.5 Location Tracking

Present Location or the travelled path will helps to track the vehicle and drivers information easily.

8.3.6 Repudiation

In this attack, 2 or more two or more unit has common identity. Where this may leads to repudiation.

8.3.7 Routing attack

In this attack, the attacker totally disturbs the network process. Common routing attacks that might be executed are Black Hole attack, Worm Hole attack and Gray Hole attack.

8.3.8 Session hijacking

In almost most of the cases, authentication will be done during commencement only. This provides an easy way to take over (hijack) the session after establishing the connection.

CONCLUSION

This Paper highlights a comprehensive aspects related to VANET. Several tools are there to ensure the working of VANET. Some of them are NS2, NS3, GlomoSim, MOVE, TraNs, VANET MobiSim, NCTUns .Long way is there to travel in VANET. This paper, it explores the initial information needed to carry out the research in VANET. Right from the fundamentals and working component of VANET to the security threats, this paper exploits all the essential commodities briefly. Security is the major issue in VANET. Since the dynamic topology of the network have high risk in appropriate delivery of data. This paper conveys the basics of security threats. In future, those Security issues will be implemented to have the solution to overcome those attacks.

REFERENCES

1. Saif Al-Sultan, Moath M. Al-Doori, Ali H. Al-Bayatti, Hussien Zedan, “A comprehensive survey onvehicular Ad Hoc network”, 2012.
2. Rizwanul Karim Sakib , “SECURITY ISSUES IN VANET” .
3. Sun, Jinyuan, Chi Zhang, and Yuguang Fang. "An idbased framework achieving privacy and non-repudiation in vehicular ad hoc networks." In Military Communications Conference, 2007. MILCOM 2007. IEEE, pp. 1-7. IEEE, 2007.
4. Watfa, Mohamed. Advances in Vehicular Ad-Hoc Networks: Developments and Challenges,Information Science Reference, 2010.
5. Paul, Bijan, Md Ibrahim, Md Bikas, and Abu Naser. "VANET Routing Protocols: Pros and Cons." arXiv preprint arXiv:1204.1201 (2012) .
6. Kumar, Rakesh, and Mayank Dave. "A Comparative Study of Various Routing Protocols in VANET." arXiv preprint arXiv:1108.2094 (2011).
7. K. C. Lee, U. Lee and M. Gerla, “Survey of Routing Protocols in Vehicular Ad Hoc Networks,” in Advances in Vehicular Ad-Hoc Networks: Developments and Challenges,IGI Global, Oct, 2009.
8. V. Kumar, “Priority Based Data Scheduling in VANETs,” M. Tech Thesis, NIT Hamirpur, 2010.
9. Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, 2010.
10. Moh an Li, “Security in VANETs”, 2014.