IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol.7, No 1, Jan-Feb 2017

ROUTING PROTOCOLS AND SECURITY ISSUES IN VANETS

Taskeen Zaidi

CSE,Shri Ramswaroop Memorial University,

Lucknow,India

KavitaSrivastava,

CSE,Shri Ramswaroop Memorial University,

Lucknow, India

***Abstract:*VANET is a type of wireless network based on communication between vehicles, as V2V or V2I .It is one of the assuring components of Intelligent Transport System. Lots of research regarding routing mechanism, routing protocols, Quality of service and security issues in VANET has been conducted. In the current work a review of research works related to routing protocols with benefits and faults as well as security attacks, issues and challenges are studied.We have defined VANET research challenges that are needed to address for successful deployment and adoption of secure VANET.**

Keywords: *- VANET,MANET,TDMA,RSU,DOS,DDOS*

1. Introduction

In recent technological scenario a number of prospective application area has emerged, Vehicular Adhoc Network (VANET) is one of the most exciting emerging field of wireless technology.Before few years, vehicles were mechanical concern but with the sinking cost of electronic apparatus, competing rivalry among the vehicle manufactures along with differentiating product and safety services has rise the name vehicular adhoc network, an intelligent transport system with safe and secure provision to the drivers.Vehicular Adhoc Network is a wireless network that is created among the vehicles as per the requirement. In VANET environment participating nodes must be furnished with wireless transceivers and automated control component.

Wenbinet al [1] has proposed the ES strategy under synthetically considering data item size, bandwidth andcycle. Split strategies and backpacks theories are used in data broadcasting scheduling to remove inconsistency in data item size. A heterogeneous technology routing(HTR) focused on heterogeneity of devices and network technology in MANET was proposed [3].

A dynamic ID based scheme for protecting privacy of vehicles has been proposed[4] and simulation result depicts that Identity Privacy

Based Reliable Routing Method(IPRR) increases the delivery ratio as well as reduced E-E delay in the wireless network.

A survey was conducted by Sicarietal [5] to present research challenges and solutions in area of IoT security and suggestions were also given to conduct research in future.

Secure routing inwireless network against attacks has been proposed in [6].

Concept of clustering[7] in sensor networks introduced by authors and Low Energy Adaptive Clustering Hierarchy(LEACH) ,Distance and Residual Energy for Wireless Sensor Networks(DESA) for scheduling distance and energy as well as Energy Efficient Clustering Algorithm(EECA) for data aggregation are presented. A topology transparent broadcast protocol is proposed by Farzadetal[8] and mathematical analysis was done for estimation of probability of success and average delay.

2. Background:-

2.1 VANET Communication Infrastructures

In present scenario with the development of technology and telecommunication services the internet and the wireless communication networks has significantly associate with our daily life. Now such wireless communication development has given a prominent Wi-Fi environment like a Wi-Fi city with Wi-Fi road conditions with a rapid emergence. The VANET communication has been classified into two types well explained in [2], [4] as:

Vehicle to Vehicle Communication

In V2V type of communication, a vehicle communicates with other vehicles in the network to transmit, receive or exchange valuable traffic related information like roadway conditions, accidents on the road, traffic congestions, etc.

Vehicle to Roadside Infrastructure communication

In case of V2I type of communication, a vehicle establishes connection with fixed equipment referred to as the Road Side Unit (RSU) or Road Side Infrastructure in order to connect and communicate with outside networks like the Internet.

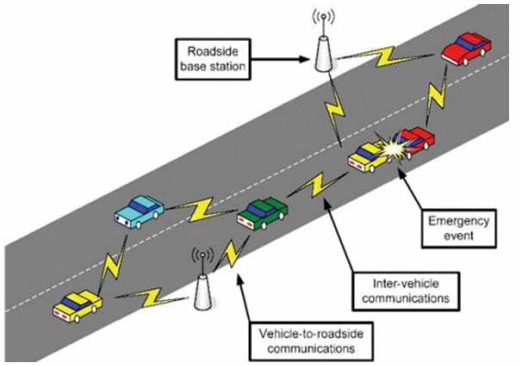

Figure 1: Figure of a Vehicular Network Architecture [4]

2.2 VANET Routing Protocol

In VANET, the routing protocols are classified into five categories: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, Geo cast routing protocol and Broadcast routing protocol.

2.2. 1. Topology based routing protocols

topology based routing protocols are based on topology of routing protocols in various ways

like proactive, reactive and hybrid protocol. It forwards the packets from source to destination using link information.

2.2.1.1. Reactive/Ad hoc based routing

An on-demand routing protocol doesn't kept routing information at network nodes and packets are flooded by route discovery. Examples are AODV and DSR.

2.2.1.2. Proactive routing protocols

Pro-active or Table-Driven routing protocols require each node to maintain up-to-date routing information to every other node (or nodes located within a specific region) in the network

2.2.1.3. Hybrid Protocols

Hybrid protocol is combination of proactive and reactive protocols.It is used to increase performance when nodes increased in network.Example of hybrid protocols are Zone Routing Protocol(ZRP) and Zone based Hierarchical Link State(ZHLS).

2.2.2. Cluster Based Routing Protocols

Cluster based routing protocols are used in MANETs in which nodes are divided into overlapping and disjoints clusters in distributed way and cluster head is selected which keeps information about members of a particular cluster. Examples are Cluster Routing Protocol with Handoff (TIBCRPH), Cluster-Based Directional Routing Protocol **(**CBDRP**).**

2.2.3. Position Based Routing Protocols

Position based routing protocol used location based service to find exact position of source node, neighboring node and destination node. It doesn't update or maintain routing information in routing table and forwarding is done by Greedy forwarding, restricted directional flooding and hierarchical approach.

2.2.4. **Geo Cast Routing Protocols**

It is a multicasting routing protocol that delivers packet from source to other nodes in a geographical region and Geo cast routing protocols are: Robust Vehicular Routing (ROVER), Dynamic Time-Stable Geo cast Routing (DTSG).

2.2.5. Broadcast Based Routing ProtocolsBRP is used for sharing of information related to weather,traffic ,roads among different vehicles and it also delivers any announcements or advertisements in network.The various Broadcast routing protocols areDistributed vehicular broadcast protocol (DV-CAST),Density-aware reliable broadcasting protocol(DECA), Position-aware reliable broadcasting protocol (POCA).

2.3 VANET Security issues

Secure in VANET is based on the secure delivery of packet from the vehicle to vehicle. So the safe and secure in VANET must be:

- **Authentication:**The commutation in VANET must be genuinetransfer of the messages. So it is the chief concern to authenticate the sender of the messages within the system.
- **Verification of data consistency:** There should be a proper checking of duration over which a vehicle can send a message and other vehicle receives the message must not exceed the pre decided duration.

- **Availability:** Though the VANET communication channel are extended to work with robustness but there may be the possibility of some attacks that may reduce or block the channel for the communication so there should be an alternative option to facilitate the requirement of the vehicles in to say in the system.
- **Non-repudiation:** If there are any accidents or such events occur then sender should not be able to reject such messages.
- **Real-time constraints:** due to high mobility the exchanging of the message should not be delayed.
- **Data integrity:** Data integrity refers that message or information's should not be changed by attackers. If such this will occur then vehicle users within the will be affected in the lack of such urgent information requirement. For example, if a vehicle X sends a message "road clear" to a malicious vehicle Y and this vehicle changes the send message as "jam ahead" and forward to the neighbour vehicle Z now his vehicle(Z) will change its route and may come into trouble.

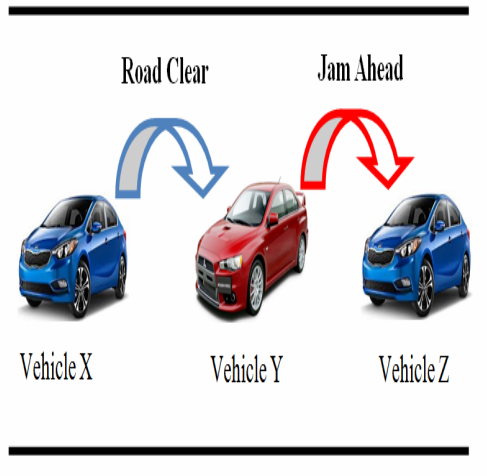

Figure 2: Data Integrity [2]

There are numerous attacks that can disturb the security of the VANET and the privacy of its nodes (vehicles). Attack causeseffects to security services in the system. Most common devastating forms of attacks that a VANET can suffer are well explained [2], [4], [5]:

Bogus Information: Attackers passes misguided information in the network to effect the driver, it may wrong information of an accident or non existent traffic jam.

Alteration Attack: Attacker amends the existing data or delaying the transmission of an information or amending the actual transmitted data entry.

Sybil Attack: Attacker uses fake identities at a time to affect a network.Due to fault identity confusion is created that there are other vehicles in network .

Denial of Service (DOS): Attacker bring down the network by forwarding unnecessary messages on the communication channel.

The Distributed DoS (DDoS) is more rigorous as compare to DOS because a number of malicious car attack over a car in distributed style with different location and time. for example numberof malicious car attack on vehicle X from different location and time so that the vehicle X cannot further establish communication with other
nodes.

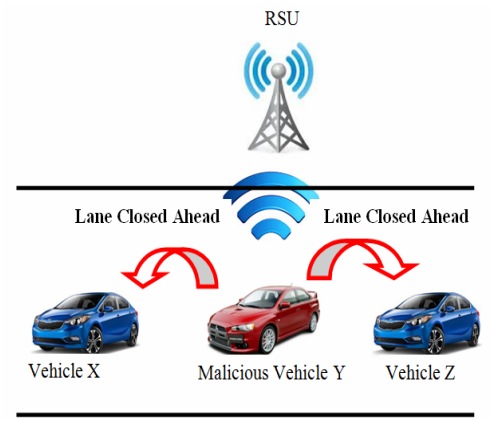

Figure 3: Denial of service [2], [4]

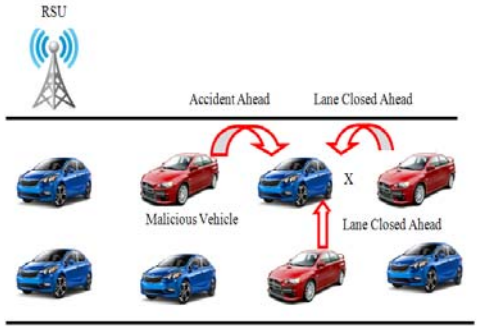

Figure 4: Distributed Denial of service [2]

- **Identity Revealing:**Attacker targets the vehicle owners identity to steal authenticated information and privacy put at risk.
- **Black Hole:**Attacker node refuses to be part of network and drops out from established network.All the nodes in VANET redirected to the specific node which really walkout of network results in lost of data.

3. Acknowledgement: In all humility and with much fervor, the authors are very thankful to Computer Science and Engineering Department, ShriRamswaroop Memorial University, Lucknow to carry out the above research work.

4. Conclusion: In this paperrouting protocols forVANET are surveyed and it is concluded that Security of VANET is most challenging as VANET suffers from numerous attacks and in the future we will focused to deploy a solution for securing VANET and to increase the performance of VANET by reducing E-E delay,packet transmission delay and average delay in network.

5. References:-

[1] Wenbin Hu, Chang Xia, Bo Du & Min Wu, “An on-demanded data broadcasting scheduling considering the data item size,” Wireless Network Springer (2015).

[2] Djamel F. HadjSadok ,Thiago Gomes Rodrigues, Rodrigo Diego MeloAmorim& Judith Kelner, “On the performance of heterogeneous MANETs,” Wireless Network Springer (2015).

[3] Di Wu, Xiaojing Wang, Limin Sun ,Yan Ling &Dongxia Zhang, “Identity privacy-based reliable routing method in VANETs,” Peer-to-Peer Netw.Appl.Springer (2014).

[4] Nai-Wei Lo & Hsiao-Chien Tsai, “A Reputation System for Traffic Safety

Event on Vehicular Ad Hoc Networks," Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking Volume (2009).

[5] S. Sicari, A. Rizzardi, L.A. Grieco& A. Coen-Porisini, "Security, Privacy and trust in Internet of things: The Road ahead :A survey."Elsevier computer network (2015).

[6] Chris Karlof& David Wagner, "Secure routing in wireless sensor networks: attacks and counter measures," Elsevier Ad Hoc Networks 1 (2003).

[7] R.Vignesh Kumar &J.GodwinPonsam "Securing Wireless Sensor Network Using GSTEB Protocol," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February (2015).

[8] Farzad Farnoud (Hassanzadeh) &ShahrokhValaee, "Reliable Broadcast of Safety Messages in VehicularAd Hoc Networks," IEEE INFOCOM(2009) proceedings.