A Review of General Issues and Challenges for Vehicular Ad Hoc Network (VANET)

Vipin
Dept. of Computer Science and Application, Maharshi Dayanand University, Rohtak, Haryana, India.

Dr. Rajender Singh Chhillar
Professor & HOD, Dept. of Computer Science and Application, Maharshi Dayanand University, Rohtak, Haryana, India.

Abstract – Vehicular Ad Hoc Network (VANET) is an emerging technology and it taking very important role in human life. VANET is also provides dynamic communication which is most needed in present time. VANET have features of communication between different vehicles, these vehicles as nodes in a network. These vehicles work as wireless routers or nodes to connect with each other to form the network with wide range. When any vehicle is fall-out from the range of network, that vehicle is drop out from communication. Because this network is works as Ad Hoc Network. VANET have life saving features. Such as it need more reliability and security. Attacker is one who can intentionally moderate the infrastructure and behaviour of other vehicles by malicious attacks in the network. These malicious attacks are of different forms. Distributed Denial of Service (DDOS) attack in Vehicular Ad Hoc Network (VANET) is performed due to large node traffic and heavy network communication. DDOS attack is degrades the overall performance and reliability of network. For this reason DDOS attack are detected and prevented in Vehicular network. In this work a group controlled model is applied to the VANET. It observes the attack in the network and preventive path is generated. It works for reducing the communication delay and communication loss. It applies parameter driven analysis in the network and identifies the attacker node in the network. How to utilize the routing protocols in VANET. When the attacker node is identified then preventive path is generated. VANET have solution of security problems by utilization of routing protocols. These issues and challenges on vehicular network in many form of that impact on performance of communication in network.

Index Terms – VANET, Attacks, Security, DOS Attack, Routing Protocols, Issues and challenges, DDOS Attack.

INTRODUCTION

To design a mobile network for vehicles VANET technology is used, it provides formation of the network by implementing moving cars as nodes in the network. In Vehicular Ad-Hoc Network every car is act as wireless router. Dedicated sort range communication is used for small range network by connecting deferent vehicle in the range of network [1].

VANET is a new technology that integrates technologies like IRA, Bluetooth, Wi-Fi, ZIGBEE and mobile connecting protocols [2]. Due to heavy traffic growth and sharp growth of vehicles on roads network, there are requirement to increase of safety features and traffic efficiency for network communication [3]. VANET are different from MANET by its hybrid network architecture, new application features and node movement characteristics, these things make different the VANET.

Characteristics of VANET

In VANET [1] communication between different nodes are very fast and very fast data transfer, mobility requires much dynamic and fast manner in VANET. These are the characteristics:

High mobility and Dynamic topology

VANET is network formation in which vehicles travels very quick on roads. So vehicles are in communication range with other vehicles for very less time and the connection between them are formed by connecting links, connecting nodes and connecting network coverage [2]. The formulation of fresh routes for communication is implemented and previous route is avoided. Previous routing protocols in MANET are not suitable for VENAT.

Mobility Modelling and Predicting Network

In VANET communication established by connecting vehicular nodes on prebuilt and defined highways, roads and streets, it provides the speed of vehicle and next up-coming location or future position and destination of vehicles provided quickly on the map [3]. It provide prediction of traveling network of vehicle by predefine path and prediction of distance for destination.

Geographic Position of Vehicle

Geographic position of vehicles in the coverage network is provides better communication and reliable network [2]. It helps in accurate positioning systems by graphical formation like maps. GPS can be used more for traveling the specific location by vehicle users.

Hard Delay Constraints in VANET

VANET have application like pre-crash sensing and collision warning system. It requires dynamic information and data exchange over network [3]. It has hard delay constraints and fast exchange of data that required for collision avoidance.

No Power Constraints in VANET

In VANET nodes are vehicles or cars as compare to mobile computing devices such as power constraint are neglected by rechargeable batteries. VANET have no power constraints as compare to other network like MANET [3].

ROUTING PROTOCOLS IN VANET

The routing protocols in VANET are categorised into five categories based on application and area of working, like: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, Geo Cast routing protocols and Broadcast routing protocol [4],[5],[6].

(i) Topology Based Routing Protocol

These Routing protocol uses links information for packet forwarding in the network. Topology based routing protocols are further categorised into three types, like: Proactive Routing Protocols, Reactive Routing Protocols and Hybrid Routing Protocols [9].

(a) Proactive Routing Protocols:-

Proactive Routing Protocol develops a routing table. The routing table is store the routing information. Next hop address for forwarding node is stored in the routing table [9]. Proactive routing table advantages are no route discovery since the destination route stored in the routing table. Its demerit is providing latency in real time application [4].

Information regarding every node is stored and maintained in the routing table [5]. Information stored in the stored regarding next hop node for particular target. It also control data path for participating node in the network. Proactive routing protocols are: DSDV, AWDS, LSR, FSR,

(b) Reactive Routing Protocols:-

Reactive Routing Protocol will perform or come into play when active nodes communicate with other active node in the network [9]. It store only information of active routes and provide better performance for routing the information from one node to other node [6].

It also takes less space for routing table which provide better utilization of space and fast processing [4]. Reactive Routing Protocol are flooded the query packets in the network for path search and find the original path. Reactive routing protocols are PGB, DSR, AODV and TORA.

(c) Hybrid Routing Protocols:-

Hybrid routing protocols are the advance form of routing protocols which consist of positive features of both the routing protocols like: proactive routing protocols and reactive routing protocols [5]. It reduces the process overhead and improves the performance in providing route in the network. Like: ZRP, OORP, HSLS

(ii) Position Based Routing Protocols

Position based routing protocols (PBR) is used for sending packages with help nearest node to end node of network by algorithms [4][5]. It sends packets without any support of geographical output of neighbour hop [6]. PBR is route the packet with regarding to position of node to the destination node.

(iii) Cluster Based Routing Protocols

Cluster based routing protocols (CBRP) are works in clusters. It identifies the group of nodes as part of cluster and a node is formed as cluster head [5]. The cluster head will broadcast the packet to the whole cluster. It requires better scalability for larger network, because network delay and overhead are formed in network when highly dynamic vehicle network is processing [11]. It requires virtual network infrastructure for clustering of nodes for executing scalability. Cluster based routing protocols are: COIN, LORA.

(iv) Geo Cast Routing Protocols

Geo cast routing protocols are location based multicast routing protocols. It performs task of sending packet from initial node to the all other node in the particular geographical region [6]. The geographical areas which have vehicle are connected by network and packet is delivered to the other vehicles in the geographical region. Like: LAR, ZHLS, ZOR, ZOF.

(v) Broadcast Routing Protocols

Broadcast Routing Protocols are generally used in VANET. It perform task for sharing of data, traffic information sending, emergency situations alerts, conditions of road for vehicles and delivering advertisements and announcements [11]. Broadcast routing protocols are: BROADCOMM, UMB, DV-CAST and V-TRADE.

ISSUES AND CHALLENGES IN VEHICULAR AD-HOC NETWORK (VANET)

Security:

In VANET security issues are mostly effected the performance of network and reduces the reliability of the network [3]. Security issues are biggest challenge in front of network communication and reliable data transmission from node to node or vehicle to other vehicle [8]. VANET provides fast delivery of data and information but it also requires reliable

exchange of data. Security issues are explained by figre-1. Security requirements and impact on network are for reliable VANET. Attacks in VANET are like: Denial of Services (DOS), DDOS.

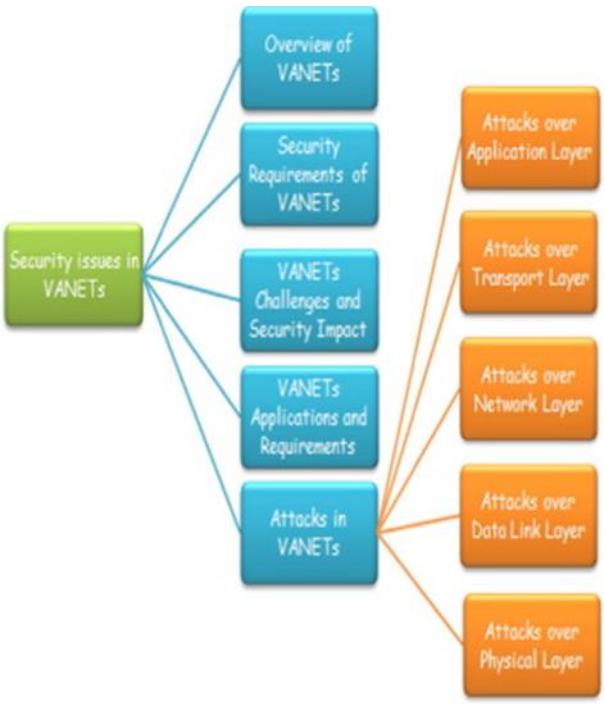

Figure 1:- Security Issues in VANET

Bandwidth Limitation:

In Vehicular Ad hoc wireless network the networking formation is more distributed [8]. It will be more complex when more number of vehicles connected in the network. In such formations of network there is mostly requirement of optimal utilization of the bandwidth [2]. Adaptive protocols are used for counter the problem of bandwidth limitation in vehicle ad hoc network.

Traffic Congestion:

Traffic congestion increased every year by a large amount. It increased day by day in present time and continues increasing with population increase. Traffic congestion also a big issue in VANET, because it reduces the performance of network directly and reduce the efficiency of network communication [3].

Scalability:

The main challenge is deployment of VANET in highly overload and sparse network. VANET operability will be tested in Inter-Vehicle Communication (IVC) and increasing number of nodes in the network. Scalability is also a challenge for VANET for information circulation in the network with coverage of all the regions of dense as well as sparse form of network [7]. Also the bandwidth management took place in the network for continuous delivery of message.

Network Congestion:

Network congestion took place in VANET by improper communication and data exchange in large number of nodes. Number of vehicles are more in VANET, it produce network congestion for communication between different vehicles [12]. Broadcasting of messages in the VANET also creates network congestion because large number of broadcasting message has more utilization of resources in the network.

Network Overhead:

In VANET, the network overhead is produced due to improper utilization of resources. When any node in network can perform communication with other node or vehicle it consume the network resources and get busy the communication part of network [10]. It assist that network work load become higher than network capacity, network communication performance degrade.

DOS Attack:

Denial of Services (DOS) Attack occurs in network when large amount of traffic processed in the VANET. It introduces congestion in the networks that degrade network efficiency and create vulnerability of channels and at nodes. In VANET due to dynamic nature of nodes or vehicles, it requires dynamically changing topology, which also increases the chances of attacks in the network [13]. It also have decentralised network control, which also increase the chances of attacks in network

DDOS Attack:

Distributed Denial of Services (DDOS) Attack is executed in the VANET due lack of infrastructure in network. DDOS Attack is occurs due to heavy traffic in the vehicle network. DDOS Attack is slow down the network communication. DDOS Attack is disrupts the access of services and resources in the network. DDOS Attack also made unavailability of services of services like situations in vehicular network [14]. A group controlled analysis method is used for detection and prevention of DDOS Attacks.

For early stage detection and prevention of DDOS Attack a group adaptive controller based model is used in vehicular network. Due heavy traffic flow at road side network causes loss of communication in the vehicular network [8][15]. Group formation is performed by taking consideration of direction, position and speed specification. The DDOS Attack is prevented by vehicle node taken by including mobility and position of nodes. It can be provide the solution of DDOS attack in VANET by group controlled method. DDOS attacks are identified at the earlier stages and prevent by group controlled analysis method.

CONCLUSION AND FUTURE SCOPE

This research paper represents an overview and class of different types of issues and challenges in the Vehicular Ad-hoc Network (VANET). In research paper various types of challenges in vehicular ad-hoc network have been identified and try to solve out the solution of these challenges. All the vulnerabilities in the vehicular ad-hoc network are handled with high mobility and hard delay with dense connected network. The DDOS attack in VANET are identified and prevented by group controlled analysis method and provide a better connecting network with reliable communication.

In the research paper problems that are faced in the real time situation are identified and prevention of those problems is provided by help of different research that are made in the field of VANET vulnerabilities. The Attacks on VANET identified in the early stages is also better for reliable communication and prevention of these attacks. All the issues and challenges in VANET are gives opportunity for finding solution of these vulnerabilities and made better, reliable and dynamic communicating network.

REFERENCES

[1] G. M. T. Abdalla, M. A. Abu Rgheff and S. M. Senouci " Current Trends in Vehicular Ad hoc Network", IEEE Global Information Infrastructure Symposium, Morocco July 2007.

[2] Al. Sultan S. , "A Comprehensive Survey on Vehicular Ad Hoc Network" , International Journal of Computer Network and Applications, Vol. 2, Issue 4, Dec 2014.

[3] S. Yousefi, M. S. Mousavi, M. Fathy "Vehicular Ad Hoc Network (VANET) Challenges and Perspectives", 6th IEEE International Conference on ITS Telecommunication, June 2006, p.p. 765-769.

[4] Shilpi Dhankar, Shilipy Agarwal, "VANETs A Survey on Routing Protocols and Issues" International Journal of Innovative Research in Science Engineering and Technology, Vol. 3, Issue 6, June 2014.

[5] Uma. Nagaraj, Dr. M. U. Kharat, Poonam Dhamal "Study of Various Routing Protocols in VANET" IJCST Vol. 2, Issue 4, Oct-Dec 2011.

[6] Kumar R. and Dave M., "A Comparative Study of Various Routing Protocols in VANET", International Journal of Computer Science Issues (IJCSI), Vol. 8, Issue 4, Nov 2011.

[7] Timo Kosch, Christian J. Adler, Stephan Eichler, Christoph Schroth and Markus Strassberger "The Scalability Problem of Vehicular Ad Hoc Network and How to Solve It", International Conference on Vehicular Communication, Singapore, Nov-2014, p.p. 345-357.

[8] Sivasakthi M, Suresh S. R, "Research On Vehicular Ad Hoc Network (VANET) An Overview", International Journal of Applied Sciences and Engineering Research, Vol. 2, No. 1, 2013.

[9] Hemlata Chaudhary "A Review of Topology Based Routing Protocols for Vehicular Ad Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 4, Issue 2, Feb 2014.

[10] A. R. Girard, J. B. de Sousa, J. A. Misener and J. K. Hedrick, "A Control Architecture for Integrated Cooperative Cruise Control and Collision Warning Systems", in IEEE Conference Decision Control, 2013, p.p. 267-275.

[11] Y. Kumar, P. Kumar and A. Kadian, "A Survey on Routing Mechanism and Techniques in Vehicle to Vehicle Communication in VANET", International Journal of computer science & engineering, Vol. 2, No. 1, Feb 2014.

[12] Md. Humayun Kabir " Research Issues on Vehicular Ad Hoc Network" International Journal of Engineering Trends and Technology (IJETT), Vol. 6, No. 4, Dec 2013.

[13] Kim Y, Kim I, Shim CY," A Taxonomy for DOS Attacks in VANET" , 14th International Conference on Communications and Information Technologies, Incheon, 2014, p.p. 37-45.

[14] Pathre A, Agarwal C, Jain A, " A novel defence scheme against DDOS Attack in VANET" , 10th International Conference on Wireless and Optical Communications Networks, India 2013, p.p. 112-123.

[15] Chen Chen, Jie Zhang, Robin Cohen and Pin-Han Ho. "A Trust Modeling Framework for Message Propagation and Evaluation in VANET", In Information Technology Convergence and Services, 2010, 2nd International Conference of IEEE 2010, p.p. 345-356.