INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
*ISSN-2455-099X,*
*Volume 2, Issue 5 May 2016.*

# A REVIEW PAPER ON A NOVEL CLUSTER BASED APPROACH FOR PREVENTING DOS ATTACK IN VANET

Gaurav Sharma [a,*], Maninder kaur [b]

[a] Gaurav.sharma098@gmail.com, [b] maninderecediet@gmail.com

[a,b]Department of ECE, Doaba institute of Engg and technology, Kharar (Pb)

**ABSTRACT**

This research is to classify Vehicular Ad hoc Network is like a fork to Mobile Ad hoc Network, where the nodes are mobile vehicles moving in constrained road topology. VANET networks are envisioned to be used in practical ITS systems around the world. A network standard has been developed as Wireless Access In Vehicular Environment (IEEE 802.11p) to be used in VANET which is an amendment to IEEE 802.11 standard. With every new technological applications especially computers and network applications, come new security challenges. Every network in modern day is susceptible to security attacks and VANET is no exception. The most infamous of those attacks is the Distributed Denial of Service Attack which is unavoidable because unlike other security attacks the data packets used in it are legitimate packets.

*Keywords:* VANET, vehicular communication, network, security, DDos

## I. INTRODUCTION

VANET stands for Vehicular ad hoc network which uses cars as nodes so as to create a vehicular network. A VANET turns every participating car into wireless router or a node and in turn create a network with a wide range. As the cars moves far from signal range and drop out of network others cars can join in connecting vehicles to one another. Vehicular Ad-Hoc Networks (VANETs) is self-organize and self-manage the information in a distributed manner. They contain vehicles and roadside units that assist within the management of the network. VANET is a sort of systems in which the vehicles can convey two or more vehicles with one another on the roadside. VANET application has been tolerant or liberal classified into security and non security applications. Security applications are most essential in nature as these are instantly associated with each others. Vehicular networking has gained a lot of popularity among the industry and academic research community and is seen to be the most valuable concept for improving efficiency and safety for future transportations. With the wireless technology becoming pervasive and cheap,

IJTC.ORG

several innovative vehicular applications are being discussed. These formal demand supply warmish related thoughts to drivers, for example, later advise on a street. VANET are one approach to actualize Intelligent Transportation System (ITS), a strategy for conferring data and correspondence innovation to transport foundation and vehicles. It is in view of IEEE 802.11p standard for Wireless Access for Vehicular Environment (WAVE). These systems have no altered framework, and they depend on themselves for actualizing any system usefulness. VANET is significant with safe for human life while these individuals are proceeding onward the streets. Non- security applications are excessively lovely the drivers and travelers, making it impossible to make the activity framework. Voyaging guide, open air auto stopping accessibility their points of interest are cases of this application. For the most part, protest be accomplished of both applications. Classifications are to give the right points of interest to clients or drivers on the streets. Consequently, secure condition is an intrusion, for example, not persistent can make issue to the clients. The motivation behind VANET is to allow wireless communication between vehicles out and about including the roadside remote sensors, empowering the exchange of data to guarantee driving safety and getting ready for element directing, permitting portable detecting and additionally giving in-auto stimulation. As VANETs have novel Characteristics which incorporate element topology, successive separation of the systems, and differing situations for correspondence, the directing conventions for customary MANET, for example, Ad hoc On-interest Distance Vector. This is particularly significant if the heavy-handed lives matter is being conveyed between a sender and a collector. Accessibility is one of the biggest securities required. Any of this hub needs to work with the other hub in the system or interchanges.

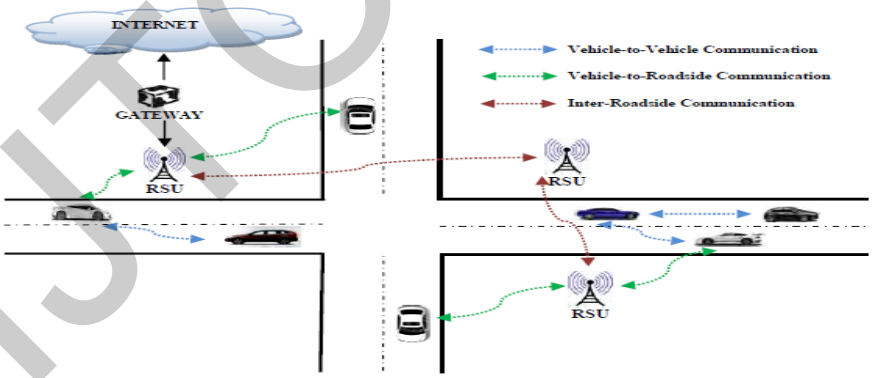


**Fig. 1.1: Vehicular Ad-hoc Networks (VANETs)**

## II. LITERATURE REVIEW

**Mina Rahbari et al. (2011)** works on "Efficient Detection of Sybil Attack Based on Cryptography in VANET" a node sends multiple messages to alternative nodes and every message contains a special fancied supply identity in such some way that the creator isn't proverbial. The fundamental goals of the assaulter are

IJTC.ORG

to produce associate illusion to alternative nodes by causation wrong messages and to enforce alternative nodes on the road to go away the road for the advantages of the assaulter [1].

**Karan Verma and Halabi Hasbullah et al.(2012)** Vehicular Ad hoc Networks (VANET) have emerged as a subset of the Mobile Ad hoc Network (MANET) application; it is thought to be a considerable way to deal with the Intelligent Transportation System (ITS). At the present time, vehicles are presented to numerous security dangers. One of them is the User Datagram Protocol (UDP)- based flooding which is a typical type of Denial of Service (DoS) assaults, in which a vindictive hub fashions countless characters, i.e.-, Internet Protocol (IP) mocking delivers so as to disturb the correct elements of the reasonable information exchange between two quick moving vehicles [2].

**S. Chang et al. (2012)** In urban vehicular networks, where privacy, particularly the area protection of mysterious vehicles is profoundly concerned, unknown confirmation of vehicles is vital. Therefore, an aggressor who succeeds in manufacturing various unfriendly recognizes can undoubtedly dispatch a Sybil assault, picking up a lopsidedly expansive impact. In this paper, we propose a novel Sybil assault identification component, Footprint, utilizing the directions of vehicles for recognizable proof while as yet protecting their area protection. All the more particularly, when a vehicle approaches a street side unit (RSU), it effectively requests an approved message from the RSU as the evidence of the appearance time at this RSU [3].

**Adil Mudasir et al. (2013)** works on "Security Attacks with an Effective Solution for DOS Attacks in VANET" handling any type of DOS attack. It also controls network traffic congestion, broadcast storm and delay while propagating emergency warning messages among vehicular nodes even in absence of DOS attacks. In short, it efficiently handles both DOS attacks and network transmissions [4].

**Vinh Hoa et al. (2013)** presented a survey on security attacks and solutions in vehicular ad hoc networks. Author discovers upto-date collection of attacks damaging VANETs and discussed the existing solutions to deal with that attack and characterized each attack to have a thorough look over it [5].

**Usha Devi Gandhi et al. (2014)** This paper presents VANET is used to make a versatile system that is in light of portable vehicles, for example, autos. It is a sub classification of MANET. It permits each taking an interest vehicle into a remote hub, allowing it give or take 100 to 300 meters of each other to partner and consequently, make a wide range framework. In this framework vehicles can join into one another so that a versatile web is made. It is used for ITS (Intelligence Traffic System) [6].

**Karan Verma et al.(2014)** The vehicular impromptu Network (VANET) has attracted expanding consideration late years because of its extensive variety of utilizations. At the present time, a vehicle's

IJTC.ORG

correspondence is presented to numerous security dangers, for example, Denial of Service (DoS) assaults, in which a noxious hub manufactures countless personalities [7].

**Ujwal Parmar et al(2015)** Vehicular Networks have gotten extraordinary consideration in most recent couple of decades. These systems are predominantly utilized for enhancing effectiveness and security of the transportation. As we realize that remote medium is utilized as a part of VANET for transmission of information or data from vehicle to vehicle so there are shots of different assaults in VANET [8].

## III. Characteristics of VANET

Vehicular ad hoc networks major concern is to give security. Each vehicle is furnished with locally available radar transduction and GPS that gives the area of the vehicle. Here are the major VANET highlights:

1. High elements of hubs bringing about quick topology changes. As the specialized gadgets are put in inside of vehicles, the system hubs are way more portable and that they move with a great deal of high velocity. Vehicles are confined to move misuse streets and to keep the movement rules, accordingly some quality examples will be found and a couple of measurable quality models for VANET are planned.

2. Data with respect to this position, development heading, current velocity, town delineate arranged development mechanical wonder of VANET hubs is offered, as a considerable measure of and a ton of vehicles are outfitted with GPS gadgets and route frameworks.

3. VANETs have absence of vitality imperatives, higher machine force and abundantly boundless memory capacity, contrasted with other impromptu systems (especially to sensing element networks).
4. VANET systems are once in a while of appallingly goliath size (instance of automobile overloads) however furthermore amid an exist in an exceedingly style of a few small, neighboring systems with a high risk of tearing and association.

## IV. Security Challenge in VANET

VANET poses a number of the foremost difficult issues on wireless ad hoc networks. Furthermore, the issues on VANET security turn out to be additionally difficult because of the particular choices of the system, similar to fast nature of system element or vehicle, and to a great degree extraordinary measure of system substances particularly, its fundamental to make beyond any doubt that "life-discriminating security " information can't be embedded or changed by an assailant; lethal to option clients. VANET security should fulfill the accompanying needs:-

IJTC.ORG

**Message Authentication and Integrity:** Message should be secured against any change and thusly the beneficiary of a message should validate the sender of the message. However respectability doesn't basically suggest identification of the sender of the message.

**Message Non-Repudiation:** The sender cannot deny of sent an information message.

**Entity Authentication:** The receiver isn't solely ensured that the sender generated a message, however additionally has evidence of the liveness of the sender**.**

**Access Control:** Access to specific services provided by the infrastructure nodes, or different nodes, is decided locally by police. As a part of access management, authorization establishes what every node is allowed to try and do in VANET**.**

**Message Confidentiality:** The information of a message is kept secret from unauthorized to access it.

**Availability**: The network and applications ought to stay operational even within the presence of faults or malicious conditions.

**Privacy and Anonymity**: Conditional privacy should be achieved within the sense that the user connected info, as well as the driver's name, the license plate, speed, position, and traveling routes at the side of their relationships, has got to be protected.

**Liability Identification:** Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes, or the transportation system. Several attacks are known which will be classified depending on the layer the attacker uses.

**Jamming**: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. In the VANET scenario, an attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power.

**Impersonation**: An attacker can masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. An adversary can also impersonate Road Side Units, spoofing service advertisements or safety messages. So an impersonator can be a threat.

## V. Conclusion

The vehicular ad hoc networks have very promising future as they provide with an insight to the safe road environment. If all the vehicles are providing with correct information to all the requesting vehicles then many applications such as road safety, traffic monitoring can be realized into real lives. We have studied the distributed denial of service attacks in our study and reduced the impact of flooding for the same. In my proposed solution to DDos I have assumed the sender node to have unique id throughout. But unlike computer networks where nodes are identified with their IP addresses which are then address resolved to respective MAC address. The nodes in VANET are dynamic and the connection is mostly extemporaneous in nature. Without a proper unique naming scheme the method described cannot be implemented.

IJTC.ORG

**ACKNOWLEDGMENT**

Working on this thesis **"A Novel cluster based approach for preventing DOS Attack in VANET"** provided a unique experience and analysis, I feel great pleasure and privilege in working over this research. I am deeply indebted to **"Doaba** institute of Engg and Technology,Kharar (PB) **"** for the invaluable guidance, support and motivation for the many other aids without which it would have been impossible to complete this project. I have no words to express my deep sense of gratitude for **Maninder kaur** (Mentor) mam for her enlightening guidance, directive encouragement, suggestions and constructive criticism for always listening to our problems and helping us out with their full cooperation. Last but not the least, Father suresh kumar Mother Naresh kumari that much strength to keep moving on forward every time, we are greatly thankful to them and have no words to express my gratitude to them.

**REFERENCES**

[1] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET", IJNSA, Vol.3, No.6, November 2011

[2] Karan Verma, Halabi Hasbullah "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VENET"IEEE 2012.

[3] S. Chang, , Y. Qi, H. Zhu, J. Zhao, X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, 1103-1114, 2012.

[4] G. Yan, S. Olariu, , M. C. Weigle, "Providing VANET security through active position detection,". Computer Communications, vol. 31, No. 12, 2883-2897, 2008.

[5] R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications," *IEEE Trans. Vehicular Technology*, vol. 59, no. 6, pp. 2772-2785, July 2010.

[6] S. RoselinMary, M. Maheshwari " Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)" IJSSAN, 2248-9738 Volume-1, Issue-4,

[7] Karan Verma, Halabi Hasbullah "IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET"IEEE 2014.

[8] Sinha, A. &Mishra, K,. (2014).Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DOS) Attack,2014.

[9] S.Roselin Mary, M.Maheshwari, M.Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked packet detection algorithm (APDA)", ICICES, pp.237-243, 20 13.

[10] Verma, K. & Hasbullah, H., (2014).IP_CHOCK (filter)-Based Detection Scheme for Denial of Service (DOS) attacks in VANET,.In Engineering and Computational Sciences, 2014. IEEE.

IJTC.ORG