International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, September 2015
www.ijates.com
ijates
ISSN 2348 - 7550

DETECTION OF BLACK HOLE ATTACK IN VANET

Ms Annu[1], Ms Sarul[2]

[1-2]M.Tech Scholar Department of Computer ScienceEngineering, RIEM Rohtak (India)

[3]Assistant Professor, [1]Department of Computer scienceEngineering, RIEM Rohtak (India)

ABSTRACT

In the black hole attack, the attacker node that wants to interrupt node packets utilizes the routing protocol to establish the false fact that it has shortest path to the node. This is termed as black hole attack. When the malicious nodes are present between the communicating nodes, it performs any sort of action with those packets that crosses them.Users require safety on road in vehicular network and it could be possible by implementing VANET applications. Vehicular applications must be secured; if attackers change the content ofsafety applications then users are directly affected. Attackers change their attacking behavior and they launch different attacks at different time. In this thesis, we can identify attacks and understand attackers by using the classes of attack. We will develop such system to identifyattacks in network with respect to some specific class of attack. If we control attackers and theirattacks then it would help in saving human life. Also, an effective solution is proposed for DOSbased attack (Black hole attack) which use the redundancy elimination mechanism consists of rate decreasing algorithm and state transition mechanism as its components.

Keywords: Black Hole Attack, VANET

I. INTRODUCTION

Attackers can be classified according to scope, nature, and behavior of attacks [15,16]. Some typesof attackers are discussed:

i. Some attackers eavesdrop only on the wireless channel to collect traffic information which maybe passed onto other attackers. As these attackers do not participate in the communicationprocess of the network, they are called passive attackers. On the other hand, some attackers either generate packets containing wrong information or do not forward the received packets.These are called active attackers.

ii. Attacker may be an authentic member of a VANET having authentic public keys and access toother members of the network. Such attackers are called insider. Outside attackers (outsider) areintruders and they can launch attacks of less diversity .

iii. Some attackers are not personally benefited from the attack. Their aim is to harm othermembers of the network or disrupt the functionality of a VANET. These attackers are malicious.On the other hand, rational attacker seeks personal benefit and is more predictable in termsoftype and target of the attack.

iv. Local attacker launches an attack with a limited scope, that is, an attack is restricted to aparticular area. An attack can be extended, where an attacker can control several entitiesdistributed across the network.

VANET is a special type of MANET, in which vehicles act as nodes. Unlike MANET, vehicles move on predefined roads, vehicles velocity depends on the speed signs and in addition these vehicles also have to follow

traffic signs and traffic signals [5]. There are many challenges in VANET that are needed to be solved in order to provide reliable services. Stable & reliable routing in VANET is one of the major issues. Hence more research is needed to be conducted in order to make VANET more applicable. As vehicles have dynamic behavior, high speed and mobility that make routing even more challenging.

II. CLASSES OF ATTACK

i. Class A

Even if there are advances in VANET but still it has many challenges to be overcome. This challenge is attacks on VANET. Raya et al. [34] classifies attacker as having three dimensions: "insider versus outsider", "malicious versus rational", and "active versus passive". Before designing any security solution for VANETs [35, 36], we should firstly know different types of security threats or attacks. There are different classes of attacks:

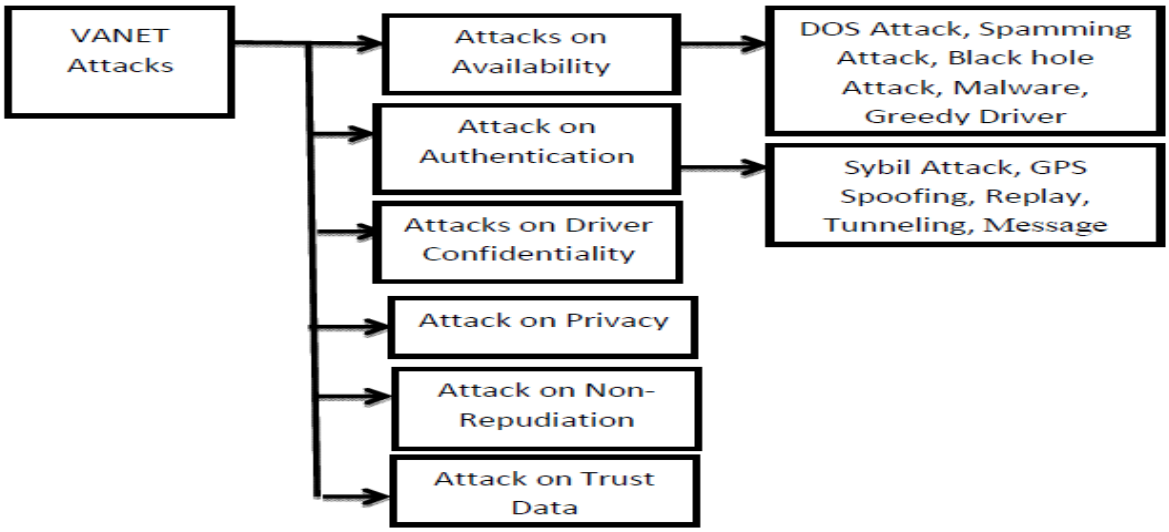


Figure 1: Type of attack

i. Class A : Attack on Availability

1. In basic level the attacker overwhelm the node resource so that it cannot perform other necessary tasks which results in be-coming the node continuously busy and not able to do anything else.
2. In extended level the attacker jam the channel by generating the high frequency in thechannel so no vehicle is able to communicate to other vehicle in the network.
3. Drop the packets.

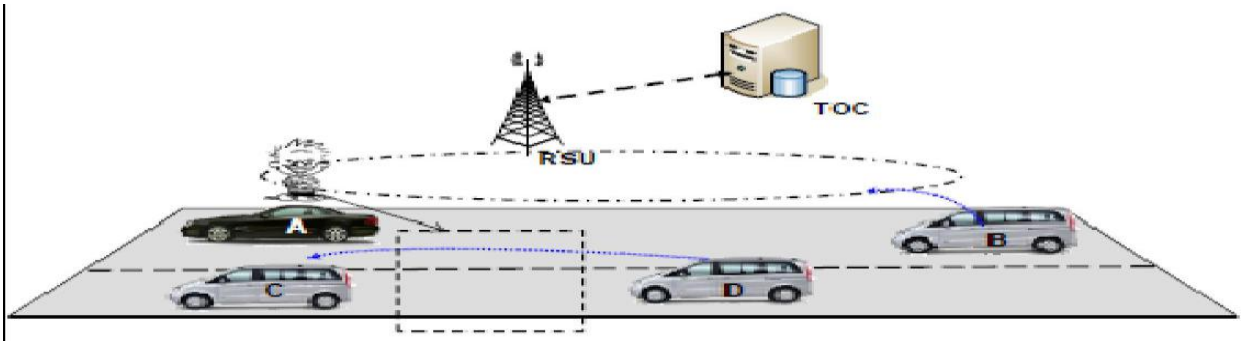


Figure 2

ii. Class B: Attacks on Authentication

- It is a critical attack. In this attack an attacker pretends to have multiple identities [41]. An attackertransmits multiple messages with different ids to the other vehicles. In this way other vehicles feelsthat these messages are coming from different vehicles, so there is a jam further and they areenforced to take alternate route [42]. In other words we can say that the main task of the attacker isto provide an illusion of multiple vehicles to other vehicles and to enforce them to choose alternateroute and leave the rode for the benefits of the attacker. This task is done by sending multiplemessages with different ids.

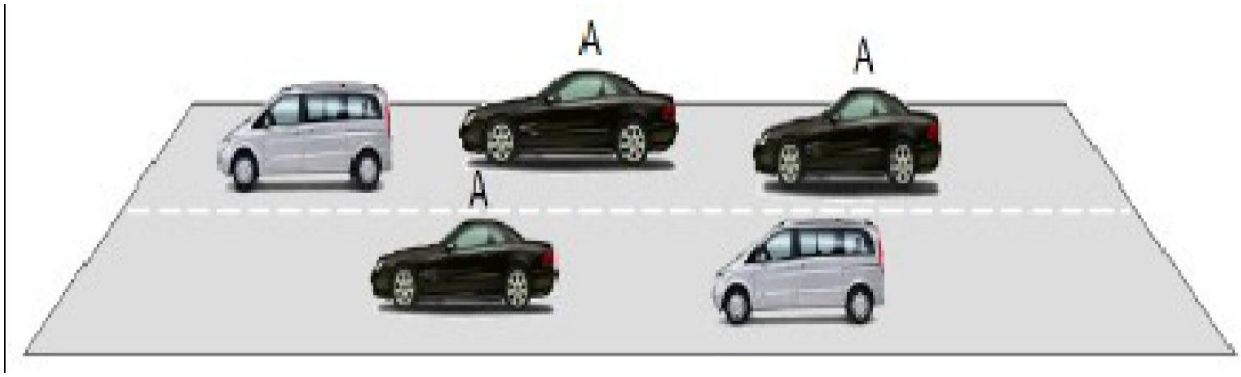


Figure 3

iii. Class C: Attacks on Driver Confidentiality

Confidentiality of messages exchanged between the users of a typical VANET is vulnerable withmalicious techniques such as eavesdropping and also collecting location information availablethrough the broadcast messages. In the case of eavesdropping, attacker can collect informationabout exist users without their permission and use the information at a time. Location privacy andanonymity are important issues for vehicle users. Location privacy involves protecting users byobscuring the user's exact location in space and time [47]. By concealing a user's request so that itis indistinguishable from other users' requests, a degree of anonymity can be achieved.

iv. Class D: Attack on Privacy

This type of attack is related with unauthorized accessing important information about vehicles.There is direct relation between driver and vehicle. If the attackers illegally access some data this directly affect the driver's privacy [44]. Usually a vehicle owner is also its driver, so if an attacker is getting the owner's identity then indirectly vehicle could put its privacy at risk; this type of privacy attack is called as identity revealing. Location tracking is also one of the well known privacy attacks. In this attack the location of vehicle or the path followed by that vehicle at particular period of time is considered as a personal data.

v. Class E: Attack on Non-Repudiation

When two or more user shares the same key then non-repudiation [48] is occurred. Due to this, twousers are not distinguished from each other and hence their actions can be repudiated. An identical key in different vehicle should be avoided using a reliable storage.

vi. Class F: Attack on Data Trust

Data trust can be compromised by simply inaccurate data calculation and sending affected message,this can be done by manipulating sensors in vehicle, or by changing the sent information [44]. This affects the whole

system reliability. And hence some mechanisms must be developed to protect against such attacks in practice in vehicular network.

III. DESCRIPTION OF BLACK HOLE ATTACK

Security is the major issue in VANET. Majority of the attacks were against Physical, MAC and fewmore layers which deals with routing mechanism of Vehicular ad hoc network. Primarily the attacks were classified based on the purpose (i.e) not forwarding the packets through routing mechanism, which affects sequence number and hop count. In the Black Hole attack malicious vehicle waits for the neighbors' to initiate a RREQ packet. Since the receivable RREQ Packet reaches the vehicle, it will immediately send a false RREP packet with a modified higher sequence number. A malicious vehicle where there is a possibility of Black hole attack which submerge all data packets of all objects and the packet will not be distributed further. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each vehicle of the network has to shares their routing tables among each other. Black Hole attack involves some modification of the data stream or the creation of a false stream

[6]. Figure 1 below show a simple scenario of this attack with one malicious vehicle.

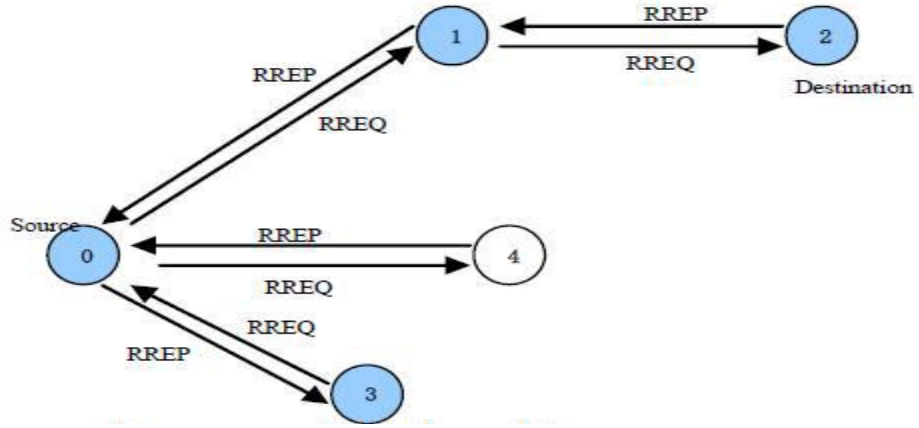


Figure 4

The AODV protocol is vulnerable to the well-known black hole attack. AODV uses sequencenumbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a vehicle selects the route with the highest sequence number. If multiple routes have the same sequence number, then the vehicle chooses the route with the shortest hop count. A malicious vehicle sends Route Reply (RREP) messages without checking its routing table for a fresh route to a destination. As shown in Figure 1 above, source vehicle 0 broadcasts a Route Request (RREQ) message to discover a route for sending packets to destination vehicle 2. A RREQ broadcast from vehicle 0 is received by neighboring vehicles 1, 3 and 4. However, malicious vehicle 4 sends a RREP message immediately without even having a route to destination vehicle 2. A RREP message from a malicious vehicle is the first to arrive at a source vehicle. Hence, a source vehicle updates its routing table for the new route to the particular destination vehicle and discards any RREP message from other neighboring vehicles even from an actual destination vehicle. Once a source vehicle saves a route, it starts sending buffered data packets to a malicious vehicle hoping they will be forwarded to a destination vehicle. Nevertheless, a malicious vehicle (performing a black hole attack) drops all data packets rather than forwarding them on.

IV. NS2 INTRODUCTION

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation toolthat has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done usingNS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field. Among these are the University of California and Cornell University who developed the REAL network simulator the foundation which NS is based on. Since 1995 the Defense Advanced Research Projects Agency (DARPA) supported development of NS through the Virtual Inter Network Test bed (VINT) project [49]. Currently the National Science Foundation (NSF) has joined the ride in development. Last but not the least, the group of researchers and developers in the community are constantly working to keep NS2 strong and versatile.NS2 provides users with executable command ns which takes on input argument, the name of a Tclsimulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTclsets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a front end). The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object,

variables in the OTcl domains are sometimes referred to as handles. Conceptually, a handle (e.g., n as a Node handle) is just a string (e.g.,_o10) in the OTcl domain, and does not contain any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped C++object (e.g., of class Connector). In the OTcl domain, a handle acts as a frontend which interacts with users and other OTcl objects? It may define its own procedures and variables to facilitate the interaction. Note that the member procedures and variables in the OTcl domain are called instance procedures and instance variables (instvars), respectively. Before proceeding further, the readers are encouraged to learn C++ and OTcl languages.

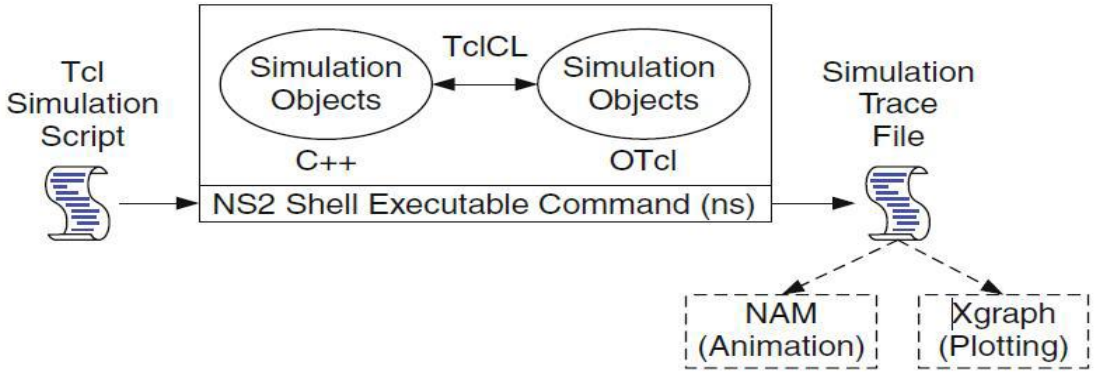


Figure 5

V. RESULT AND FUTURE SCOPE

Vehicular Ad hoc Networks is a special kind of mobile ad hoc network to provide communication among nearby vehicles and between vehicles and nearby fixed equipments. VANETs are mainly used for improving efficiency and safety of (future) transportation. There are chances of a number of possible attacks in VANET due to open nature of wireless medium. VANET generally consist of On Board Unit (OBU) and Roadside Units (RSUs). OBUs enable

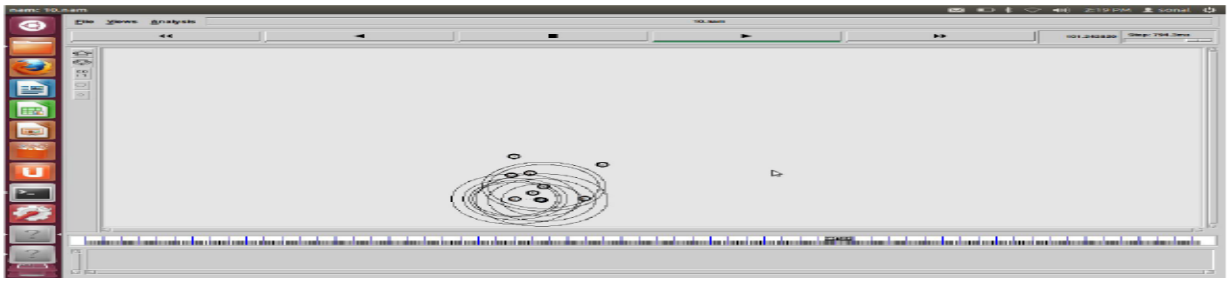


Figure 6: Running nam file of 10 nodes.

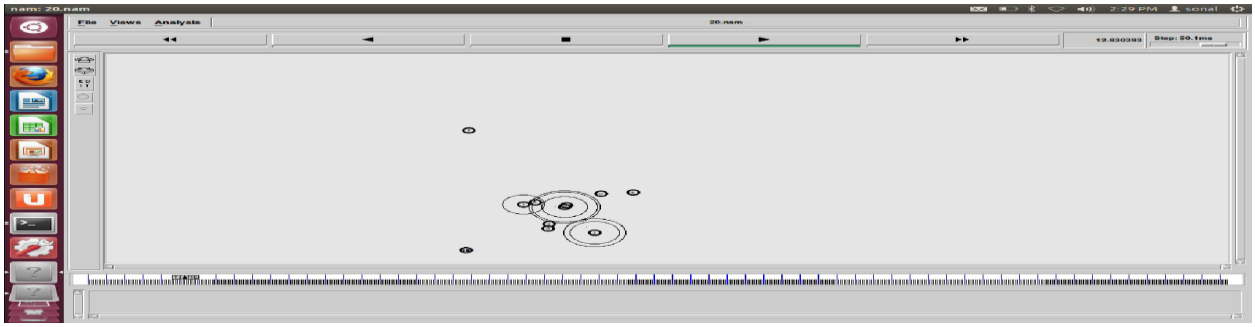


Figure 7: Running nam file of 20 nodes.

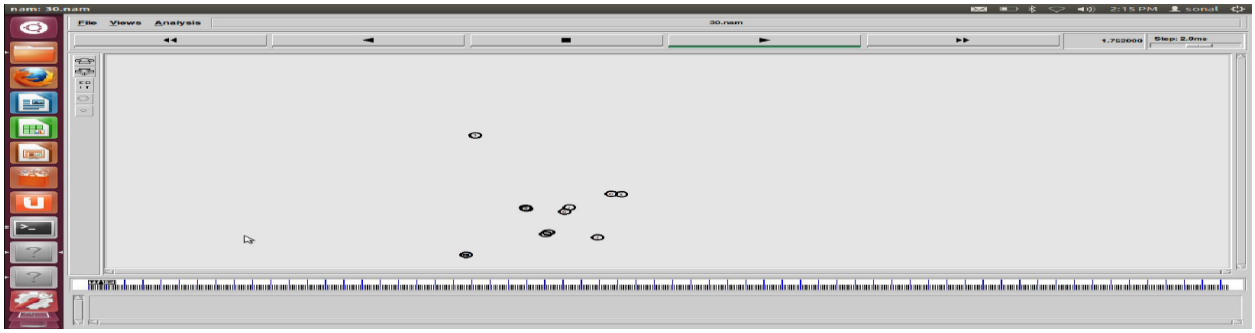


Figure 8: Running nam file of 30 nodes.

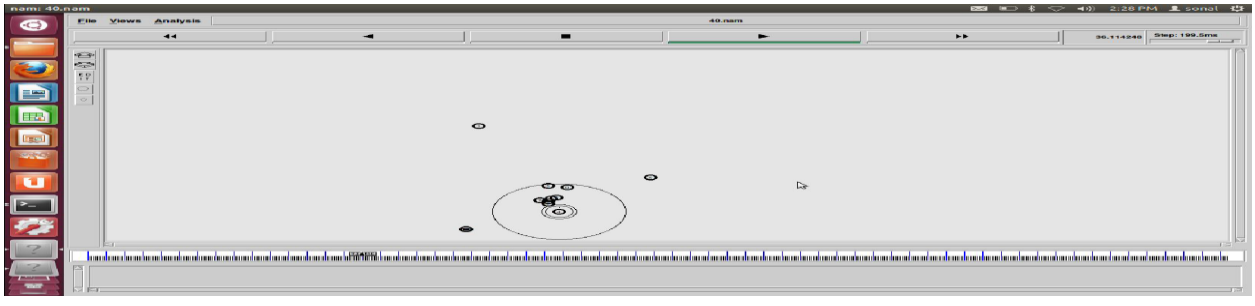


Figure 9: Running nam file of 40 nodes.

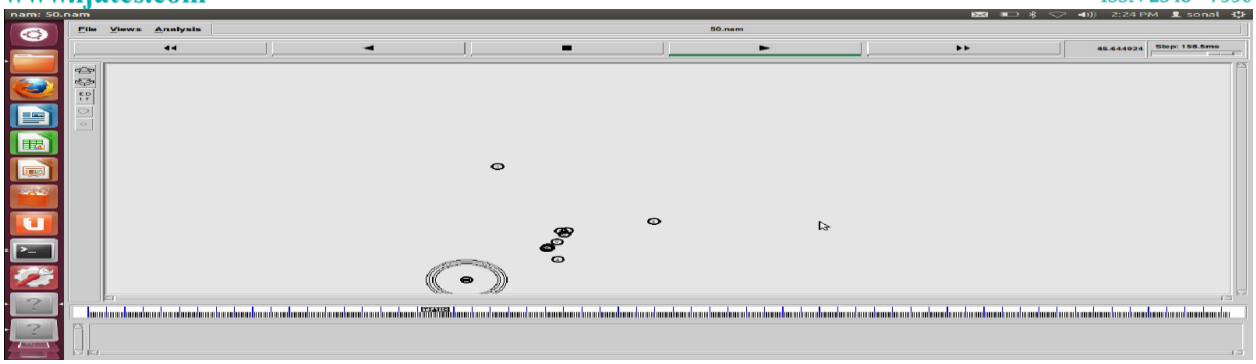
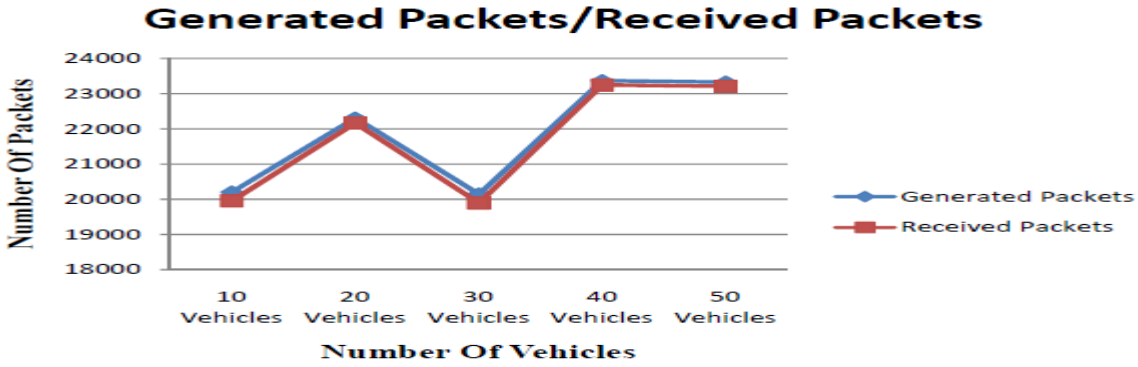
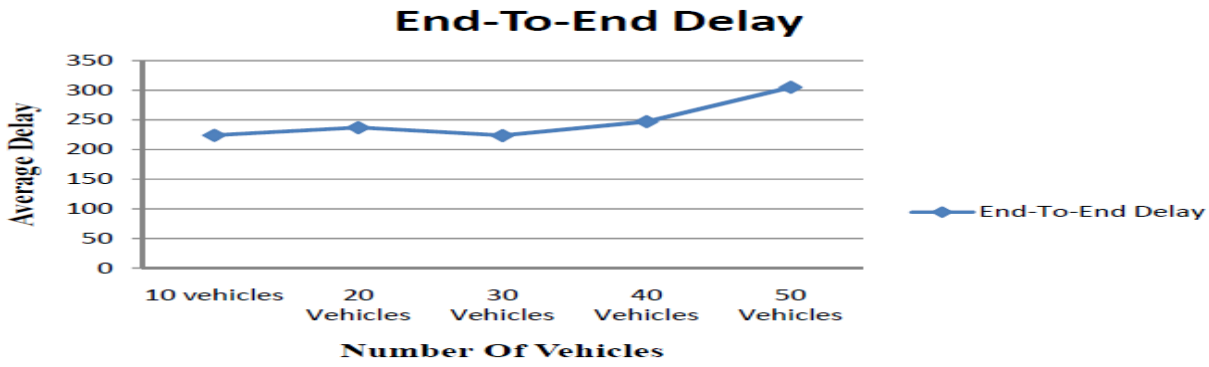
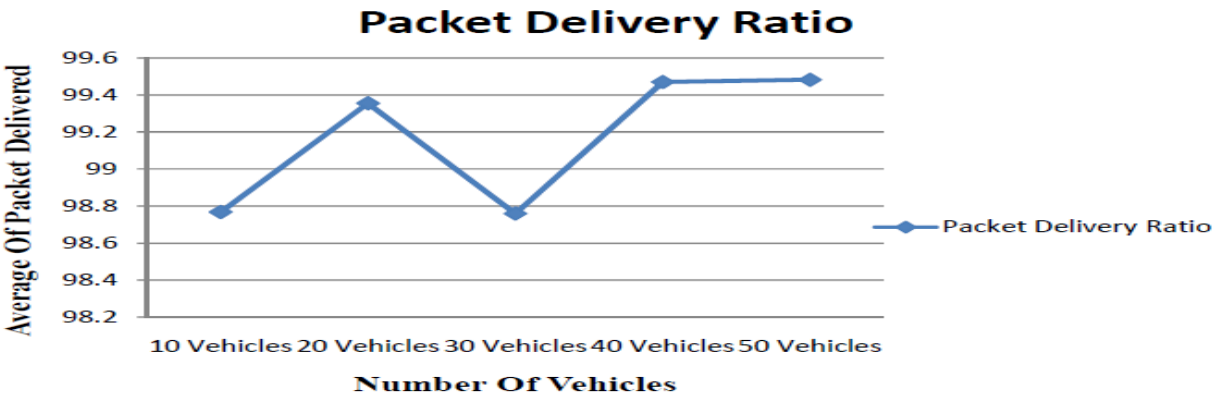


Figure 10: Running nam file of 50 nodes.







Vehicular Ad hoc Networks is a special kind of mobile ad hoc network to provide communicationamong nearby vehicles and between vehicles and nearby fixed equipments. VANETs are mainlyused for improving efficiency and safety of (future) transportation. There are chances of a numberof possible attacks in VANET due to open nature of wireless medium. VANET generally consist ofOn Board Unit (OBU) and Roadside Units (RSUs). OBUs enables short-range wireless ad hocnetwork to be formed between vehicles.Each vehicle comprises of

hardware unit for determining correct location information using GPS.Roadside Units (RSUs) are placed across the road for infrastructure communication. The number ofRSU to be used depends upon the communication protocol.

VANET provide assistance to vehicle drivers for communication and coordination amongthemselves in order to avoid any critical situation through Vehicle to Vehicle communication e.g.road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseenobstacles etc. Besides safety applications VANET also provide comfort applications to the roadusers. Due to the dynamic nature of nodes in VANET the routing of data packets is much complex.Several factors like the type of the road, daytime, weather, traffic density and even the driverhimself affect the movements of vehicles on a road. Hence, the network topology changefrequently, and the routing protocol used has to adapt itself to these instantaneous changescontinuously.

There is safety and non-safety messages are forwarded between the Vehicle to Vehicle (V2V) andVehicle to Infrastructure (V2I) on this communication medium. Cooperation between the vehiclesis essential to communicate with each other because of the short range of wireless communicationmedium. The attacker generates problems in the network by getting full access of communicationmedium due to open nature of the medium. Attacker may be authentic user/users (insiders) of the NETWORK that possess detail knowledge of network which they will be use for understanding the design and configuration of network. Therefore, it is easy for them to launch attacks and create more problem as compare to outsider attacker which is a kind of intruder which aims to misuse the protocols of the network. In the black hole attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other. A malicious node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In this work Black hole attack is efficiently removed by the extended AODV technique. By using this technique black hole attack is easy to detect, manage and recover. Here packet delivery ratio is increased and end-to-end delay gets decreased.

ACKNOWLEDGMENT

This research was supported by the RIEMRohtak under their strategic award program. I am thankful to Ms. Sarulfor their support and proper giddiness.

REFERENCES

[1]. Farzad Sabahi (2011) Third International Conference on Computational Intelligence, Communication Systems and Networks

[2]. Manvi, S.S., Kakkasageri, M.S., Mahapurush, C.V., “Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols In Vehicular Ad hoc Network Environment” In International conference on future Computer and Communication., pp. 21-25, April. 2009.

[3]. Bernsen, J. Manivannan, D., “Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service” In the fourth international conference on Wireless and Mobile Communications., pp.1-6, Aug. 2008.

[4]. Wex, P. Breuer, J. Held, A. Leinmuller, T. Delgrossi, L., “Trust Issues for Vehicular Ad Hoc Networks” IEEE,VTC Spring 2008., pp. 2800-2804, May.2008.

[5]. T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto, "A stable routing protocol to support its services in vanet networks" IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3337–3347, November 2007.

[6]. SheraliZeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan (2012) Telecommunication System, Vol. 51, Issue 2&3. P. Papadimitratos, V. Gligor, J-P.Hubaux, "Securing Vehicular Communications – Assumptions, Requirements, and Principles", Proceedings of the Workshop on Embeded Security on Cars (ESCAR) 2006, November 2006.

[7]. Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, October 2006.

[8]. Tim Leinmuller, Elmar Schoch, and Frank Kargl, "Position Verification Approaches for Vehicular Ah Hoc Networks", IEEE Wireless Communications, October 2006.

[9]. P. Papadimitratos, L. Buttyan, J-P.Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for Secure and Priviate Vehicular Communications", Proceedings of the 7th International Conference on ITS Telecommunications, June 2007.

[10]. P. Papadimitratos, L. Buttyan, J-P.Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture forSecure and Priviate Vehicular Communications", Proceedings of the 7th International Conferenceon ITS Telecommunications, June 2007.

[11]. [Maxim Raya, and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of

[12]. ComputerSecurity, Vol.15, No.1, pp.39-68, 2007.

[13]. Tim Leinmuller, ElmarSchoch, and Christian Maihofer, • gSecurity Requirements and SolutionConcepts in Vehicular Ad Hoc Networks • h, Proceedings of Forth Annual Conference on Wirelesson Demand Network Systems and Services, 2007.

[14]. T. Leinmuller, E. Schoch, and C. Maihofer, (2007) • gSecurity requirements and solutions concepts in vehicular ad hoc networks • h. In Proceeding of Fourth Annual Conference on Wireless on Demand Network Systems and Services.

[15]. P. Papadimitratos, V. Gligor, and J.-P.Hubaux,(2006) • gSecuring vehicular communications. assumptions, requirements, and principles • h. In Proceedings of the Workshop on EmbeddedSecurity on Cars (ESCAR).

[16]. M. Raya and J.-P.Hubaux,(2007) • h Securing vehicular ad hoc networks • h. Journal of Computer Security, 15(1), 39.68.

A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M.Gerlach, R. Kroh, andT. Leinmuller,(2006) gAttacks on inter-vehicle communication systems.an analysis • h. In Proceedings of the 3rd:international Workshop on Intelligent Transportation (WIT).

[17]. Zheng. Challenges in vehicular networks.

[18]. Nai-Wei Lo, Hsiao-Chien Tsai, • \Illusion Attack On VANET Applications . A Message Plausibility Problem., Global Workshops, IEEE 2007

[19]. NavidNikaein, SoumyaKantiDatta, IrshadMarecar, Christian Bonnet, • gApplication Distribution Model and Related Security Attacks in VANET • h, 2001.

[20]. Maxim Raya and Jean-Pierre Hubaux, • gSecuring vehicular ad hoc networks, • h Journal ofComputer Security 15 (2007) pp. 39.68.

[21]. Philippe Golle, Dan Greene, Jessica Staddon , • gDetecting and Correcting Malicious Data in VANETs • h,2004.

[22]. Gongjun Yan, Stephan Olariu, Michele C. Weigle, • gProviding VANET Security Through Active Position Detection • h, 2007. Yi Qian, Nader Moayeri • gDesign Secure And Application-Oriented Vanet • h ,2007

[23]. Robert K. Schmidt, TimLeinmuller, ElmarSchoch, Albert Held "Vehicle Behavior Analysis to Enhance Security in VANETs",2009.

[24]. Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, And Bertrand Ducourthial, "Sybil Nodes Detection Based On Received Signal Strength Variations Within Vanet", International Journal of Network Security, Vol.9, No.1, PP.22{33, July 2009.

[25]. SurabhiMahajan ,Alka Jindal 2010 proposed "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks", International Journal of Computer Applications (0975 – 8887) Volume 1– No.20, 2010.

[26]. J.T. Isaac, S. Zeadally, J.S. Ca´mara, "Security attacks and solutions for vehicular ad hoc networks", IET Commun., 2010, Vol. 4, Iss. 7, pp. 894–903 & The Institution of Engineering and Technology 2010 doi: 10.1049/iet-com.2009.0191.

[27]. Irshad Ahmed Sumra,Iftikhar Ahmad, HalabiHasbullah , Jamalul-lail bin AbManan ,"Classes of Attacks in VANET ",2011.

[28]. Mina Rahbari1 and Mohammad Ali JabreilJamali, "EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[29]. Bo Qin, Qianhong Wu, Josep Domingo-Ferrer ,Lei ,Zhang Preserving Security and Privacy in Large-Scale VANETs,2011.

[30]. Chavhan K.L. and Patil P.A, "VANET SECURITIES AGAINST ATTACKS",BIOINFO Security Informatics ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 1, 2012, pp.-28-32.

[31]. AnupDhamgaye, 2Nekita Chavhan, "Survey on security challenges in VANET" IJCSN International Journal of Computer Science and Network, Vol 2, Issue 1, 2013.

[32]. Maria Elsa Mathew AndArun Raj Kumar P "Threat Analysis And Defence Mechanisms In Vanet" International Journal Of Advanced Research In Computer Science And Softwar Engineering, Volume 3, Issue 1, January 2013.

[33]. Raya, M., &Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.

[34]. T. Leinmuller, E. Schoch, and C. Maihofer, (2007) "Security requirements and solutions concepts in vehicular ad hoc networks". In Proceeding of Fourth Annual Conference on Wireless onDemand Network Systems and Services.

[35]. P. Papadimitratos, V. Gligor, and J.-P.Hubaux,(2006) "Securing vehicular communications—assumptions, requirements, and principles". In Proceedings of the Workshop on Embedded Security on Cars(ESCAR).

[36]. Ahmed Soomro, Hasbullah H.B., J.lb. AbManan (2010) WASET issue 65, ISSN 2070-3724.

[37]. Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jam-alul-lail bin AbManan (2011) ICUMT: 1-8.

[38]. Sharma, Sheenu, Roopam Gupta, M. Tech Student Reader, RGPV SOIT, and RGPV UIT. "Simulation Study Of Blackhole Attack in the Mobile Ad hoc Networks." Executive Developmen 21 (2008): 22.

[39]. Farzad Sabahi(2011) Third International Conference on Computational Intelligence, Communication Systems and Networks.

[40]. Sumra, Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, and J-L. binAbManan. "Classes of Attacks in VANET", In Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, pp. 1-5. IEEE, 2011.

[41]. Douceur J. (2002) First international workshop on peer to peer (P2P) system, pp:251-260.

[42]. FarzadSabahi (2011) Third International Conference on Computational Intelligence, Communication Systems and Net-works.

[43]. Samara et al (2010) 4th International Conference on New Trends in Information Science and Service Science.

[44]. Panigrahi, Sunil Kumar, Soubhik Chakraborty, and Jibitesh Mishra. "A Statistical Analysis of Bubble Sort in terms of Serial and Parallel Computation." (2012).

[45]. AKK. Aboobaker, "Performance analysis of authentication protocols in vehicular ad hoc networks (VANET)," 2010.

Ms Annu is presently pursuing M. Tech. final year in CSE Department (from RIEM Rohtak, India.

Mr. Sarul is working as an Assistant Professor in CSE Engineering Department (from RIEM Rohtak, India).