International Journal of Advanced Trends in Engineering and Technology (IJATET)
Impact Factor: 5.665, ISSN (Online): 2456 - 4664
(www.dvpublication.com) Volume 2, Issue 1, 2017

DESIGN AND ANALYSIS OF SECURE VANET FRAMEWORK PREVENTING SINK HOLE AND GRAY HOLE ATTACK

K. T. Gowdhami* & D. Nithya**
Assistant Professor, Department of Information Technology, M.P.N.M.J Engineering College, Chennimalai, Erode, Tamilnadu

Cite This Article: K. T. Gowdhami & D. Nithya, "Design and Analysis of Secure VANET Framework Preventing Sink Hole and Gray Hole Attack", International Journal of Advanced Trends in Engineering and Technology, Page Number 55-59, Volume 2, Issue 1, 2017.

Abstract:
Vehicular Networks are considered as novel class of wireless networks, also called as VANET (Vehicular ad-hoc Networks). It is a key component of Intelligent Transport System (ITS). VANET technology is identified for improving road safety and transport efficiency. However, due to recent arise in security issues in VANET, VANETs must have a secure way for communication which is quite challenging and vital issue. This paper scrutinized the effects of packet loss in the network due to Sink Hole attack and Grey Hole Attack and also propositions a detection technique that competently detects both attacks in the network. In this research paper simulation is completed by using NS-2 simulator. In this research work the attack is performed and detected on AODV routing protocol. Furthermore, to determine the effects on attacks on network performance simulation is performed on different network scenarios.

Key Words: VANET, Sink Hole, Gray Hole & Routing Protocol

Introduction:

Rapid advances in wireless technologies offer opportunities to utilize the technologies in support of advanced vehicle safety applications. Specifically, the new Dedicated Short vary Communication (DSRC) offers the potential to effectively support vehicle-to- roadside and vehicle-to-vehicle safety communications that has become called Vehicle Safety Communication (VSC) technologies. Intelligent Transportation Systems (ITS) square measure the long run of transportation. As a result of merging standards, such as 5.9 GHz DSRC, VANET is introduced. It is a technology which allows vehicles to establish a connection when they require communication. VANET uses Wi-Fi IEEE 802.11 and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility due to these vehicles will soon be able to talk to one another as well as their environment. Therefore it is crucial that all the activities that are performed on VANET must be protected from malicious attacks. A number of novel problems are associated with a VANET is due to it's unique characteristics of the network. To begin, the main differences between a VANET and a MANET are a MANET typically has no infrastructure available. In the case of a VANET, it is achievable to tactically place access points along the side of the road, and consecutively consent to vehicles admittance to the services available from the infrastructure. Also, one of the greatest challenges is the vehicles in the network is mobility, speed of nodes is greater than the nodes in MANETs, leading to a network that can frequently become disjointed. Furthermore, security and privacy are essential apprehension for a VANET. Sink Hole Attack the attacker node behave normally first by compromising node tries to attract network traffic by advertise its fake routing update. One of the impacts of sinkhole attack is that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information. and when it become clear the node trust the attacker node it started dropping the packet while forwarding them in the network. Whereas in sink hole attack, malicious node through its routing protocol shows in the network that it has shortest route available for communication. This node advertises its availability of fresh routes irrespective of checking its routing table. Therefore, the purpose and the contribution of this paper is to make a first step towards secure VANETs by introducing a comprehensive security framework which implement these both attacks simultaneously in the network and also a detection technique to detect these attacks in the network. Furthermore, to determine the effects on attacks on network performance simulation is performed on different network scenarios. The rest of this paper is planned as follows. Section II, discusses the overview on the related work. Section III discusses the implementation of attacks and detection method used in this paper. In Section IV, result and analysis of the simulation is discussed. Conclusion and future work is discussed in the final section.

Related Work:

In this section we will discuss the previous work done on the different approach used to infiltrate the network and mechanisms used to ensure safety over VANET network, because VANET provides open access to the nodes to communicate in the network. So, attacker can use different approaches to infiltrate the network. In the associated research, Rauki Yadav et al. have described the various attacks, weaknesses and detection approach which can be possible on VANETs. In this author described the attack such as Sybil attack, Black Hole attack, flooding attack, selfish attack against VANETs, and the detection approaches considered till present against these attacks. In the associated research, Jorge Hartelano et al., has described the Watchdog

technique, which is useful to detect attack over the network. In their scheme they propose a tolerance threshold over network and used the Watchdog technique to detect the attack on the network. Gurpreet et al. has described the use of can protocol over the network to determine the malicious data over VANET. In their approach they use seven steps to detect malicious data over VANET. First step is to develop a VANET environment which has nodes and multiple no. of sensors. Next step involve collecting event data in which include behaviour of VANET in a given time slot. Next step involve they prepared pseudo logic to detect the system. Next step involve preparation of an attack simulation model which defines the way in which a fake message can pass by an attacker. Next step involve checking of system before and after attack to check the working of system that how it will work in the normal circumstances. In final step they detect the system after attacking it with malicious data and try to find the working of the system. Naresh Kumar et al., has described their efforts on the performance analysis of VANET. In this paper they designed congestion notice mechanism to detect areas of high traffic density and low speeds. Authors offered vehicle-to-vehicle communication approach to manage traffic obstruction, which will help in determining the change in the network. VANET provides the ability to watch out the traffic. For this the sensors are required to be aware of the neighbour node sensor. For that purpose positioning devices like GPS is used by authors in their model. The algorithm used for obstruction control in this paper has three stages: neighbour discovery, cluster-head selection, and maintenance stage. Vaishali Mittal has described her approach to detect Gray Hole Attack. In this paper author proposed routing protocol approach and then discovered the secure pathway in the network by avoiding Gray Hole attacks. Measurements and calculation are done to decide if network is under attack of Gray Hole and then by routing protocol approach author revealed a sheltered pathway in the network.

Proposed Methodology: AODV is an on-demand routing protocol which means that it discovers the path at run-time. It is a reactive routing protocol.

A. Attack Methodology: VANET has many advantages as well as it also possess threats in its network. Black Hole attack is one of the attacks that possess threat to VANET. In Black Hole Attack malicious node through its routing protocol shows in the network that it has shortest route available for communication.

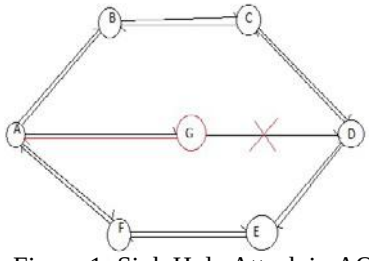

Figure 1: Sink Hole Attack in AODV

Figure 1 shows how Black hole Attack is achieved in the network. Suppose that node "A" Wants to transfer message to node "D" then the route should be A-B-C- D or A-F-E-D. But, when node "A" request for the route an attacker node, node "G" intercept the request message and before the other nodes send response the attacker node shows that it has the new route which is shortest to the destination. Now, node "A" will consider this path and reject other response of the nodes. Node "G" can transfer the packet to unknown path or can drop the packet. Gray Hole attack is another attack which causes disruption in the processing of VANET network. This attack is difficult to track until it started to disrupt the process of network. In Sink Hole Attack the attacker node behave normally first and project itself as authenticated node and when it become clear the node trust the attacker node it started dropping the packet while forwarding them in the network and sometimes it does for some specific nodes, that's why it is difficult to detect.

B. Detection Method for Sink Hole and Grey hole Attack: Detection method in VANET is not easy due to mobile nature of nodes. Nodes are constantly on move in VANET so when they want communication they connect and as soon as the requirement is finished nodes move on. So it's quite difficult because it took time to detect the disruptions in the network and if the connection is terminated before the detection then it is difficult to detect the disruptions in the network.

Pseudo code for the detection of Sink Hole attack: This section presents the algorithm used for the detection of Sink Hole attack.

SN: Source Node
DN: Destination Node
Flag: flag
IN: Intermediate Node

1. SN broadcasts RREQ to all Nodes
2. IN receives RREQ and forwards until reach DN
3. DN receives RREQ from SN or IN
4. DN gets Seq from RREQ and verifies with Seq in its routing table
5. If Seq of RREQ is greater than Seq of its routing table

6. DN selects Seq of RREQ and plus one
7. Source and destination will be decided.
8. Randomly Generate a Number in between 0 to maximum number of nodes. Initiate a source by making transmitter node same selected.
9. Generate the Route from selected transmitting node to any destination node with specified average route length.
10. Send packet to destination.
10. Sink Hole Detection
{
11. Check the nodes for the flag
12. flag==NRTE
13. Node is Sink Hole Attacker.
}
14. Gray Hole Detection
{
15. Check the nodes for the flag
16. flag==DROP
17. Node is Gray Hole Attacker.
}
18. Repeat process.

Simulation Result and Analysis: This section will study the result obtained by various scenario in detail. Simulation is performed on Sink Hole and Gray Hole attack together and determines the effect of attack on the metrics such as packet delivery ratio (PDF), dropped packets by varying number of nodes, speed of nodes. Simulation parameters used to build scenarios are shown in table I. Simulation is performed under three different scenarios. Simulation is completed using NS-2.

Table 1: Simulation Parameters

Parameter	Value
Simulator	NS-2
Number of Nodes	20,22,25
Simulation Time	100ms
Traffic Type	CBR(Constant Bit Rate)
Simulation Area	1000x1000
Packet Size	1000
Network Structure	VANET
Routing Protocol	AODV Routing
Speed, Pause Time	5m/s,2sec

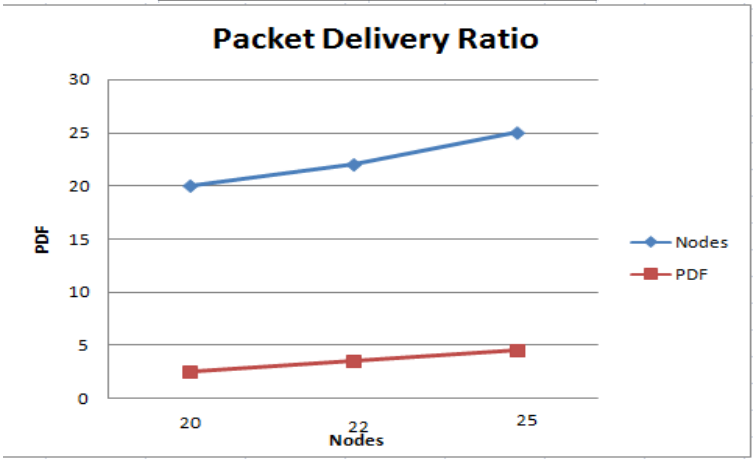

Figure 2: Number of Nodes v/s. Packet Delivery Ratio

In this paper network is fashioned by the parameters shown in table I. Number of nodes is increased in three different scenarios. In first scenario number of nodes is twenty, in second it is twenty two and in third it is twenty five to analyse the effect of both attacks on the network. When numbers of nodes are increase the packet delivery ratio increases as shown in fig 2. It is an understandable behaviour because as nodes increase packet delivery ratio also increases simultaneously.

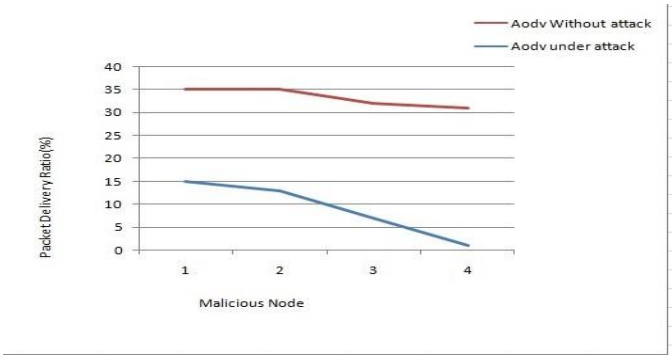

Figure 3: Number of Malicious Nodes v/s. Packet delivery Ratio

Figure 3 shows the behaviour of AODV routing protocol under attack and without attack. It is clear that when there was no malicious node the value of packet delivery ratio is higher in AODV. As soon as malicious nodes are introduces in the network the packet delivery ratio decreases. It is clear that when the number of malicious node is increase in the network packet delivery ratio decreases as shown in the figure

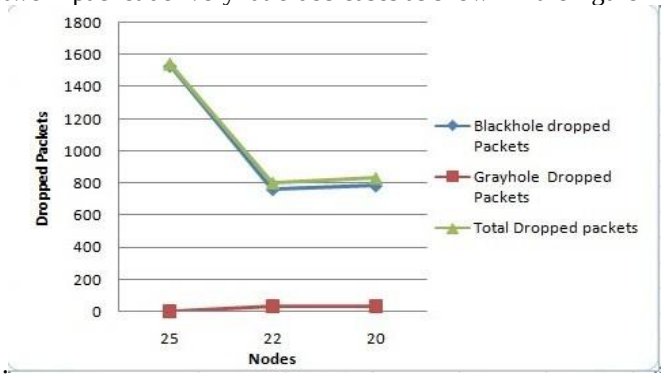

Figure 4: Number of Nodes v/s. Dropped Packets

Figure 4 shows the number of dropped packets in the network. It shows the behaviour of dropped packets in three different scenarios when Black hole and Gray Hole attack induces in the network together. It shows that when number of nodes is twenty five, number of packet dropped due to Gray hole is less but because of Sink Hole is more which affect the total dropped packets in the network, when number of nodes is twenty five total dropped packets are more in this scenario. When the number of nodes is twenty two, packet drop due to Gray Hole is more compare to twenty five nodes, but packet drop due Sink Hole is less in this case which affect the total dropped packet, in this scenario total packet drop is less than previous scenario. When number of nodes is twenty, packet drop due to Gray hole is more compare to both previous case but packet drop due to Sink Hole is less compare to both previous case which affect the total dropped packets also, in this case total dropped packets is less in comparison with both previous case.

Conclusion and Future Work: From the above shown graphs it is clear that the performance of network is decreased when there is malicious node in the network. The need to secure VANET is very high since it has many advantages in network and also research surrounding VANET is very precise to secure the VANET from the attacks due to its characteristics since this technology is seen as the future of network. In this work a framework is designed and analyzed against Sink hole and Gray hole Attack. In this work the effects of both attacks are premeditated and scrutinized over the network. In the analysis it is found that with different scenario the result obtained is different. In this work it is found that if nodes are increased than Sink hole attack will also increase and Gray Hole attack is decreased and vice versa. In this work it is concluded that both attacks can be implemented and detected over the network by their behavior over the network apart from of the fact that both attacks are catalogued differently. In this work they are successfully implemented and detected over network. VANET is very much researched topic after its evolvement in the network. It has vast opportunities in it to work and research. The future work of this work is to avoid these attacks by using cryptographic methods over the network to secure the network from these attacks.

References:

1. Rajendra Aaseri, Nirmal Roberts, Pankaj Choudhary, “Trust value algorithm: a secure approach against packet drop attack in wireless ad-hoc networks” in International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, May 2013.
2. Avinash P. Jadhao, Dr. D. N. Chaudhari, “Security Aware Adhoc on Demand Distance Vector Routing Protocol in Vehicular Adhoc Network” in International journal for Engineering applications and Technology, Vol. 2, Issue 12, December 2015.

3. Charles Harsch, Andreas Festag, Panos Papadimitratos, "Secure Position-Based Routing for VANETs" in IEEE, Vol.2, Issue 12, November 2007.
4. K. R. Viswa Jhananie, Dr. C. Chandrasekar, "Detection and Removal of Blackhole Attack Using Handshake Mechanism in MANET and VANET" in IOSR Journal of Mobile Computing & Application (IOSR-JMCA), Volume 2, Issue 1. (Mar - Apr 2015).
5. Jorge Hortelano, Juan Carlos Ruiz, Pietro Manzoni, "Evaluating the uselfusness of watchdogs for intrusion detection in VANETs", in IEEE Xplore , Volume 11, November 2010.
6. Rauki Yadav, Naveen Hemrajani, Dinesh Goyal, Savita Shivani, "Vulnerabilities, Attacks and their Detection Techniques in Ad hoc Network" in International Journal of Computer Applications, Volume 2, Issue 11, December 2011.
7. Gurpreet Singh, Seema, "Malicious Data Detection in VANET" in International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 7, September 2012.
8. Ankita Agrawal, Aditi Garg, Niharika Chaudhiri, Shivanshu Gupta, Devesh P, Tumpa Roy, "Security on Vehicular Ad Hoc Networks (VANET): A Review Paper" in International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 1, January 2013.
9. Osama Abumansoor and Azzedine Boukerche, "Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services" in IEEE Xplore, Volume 5, Issue 9, December 2011.
10. Jitendra Bhatia and Bhumit Shah, "Review on various security threats & solutions and network coding based security approach for VANET" in International Journal of Advances in Engineering & Technology, Volume 2, Issue 11, March 2013.
11. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges" in Springer, Volume 50, Issue 4, August 2012.
12. Sajid, A.H.S Bukhari, A.W. Shaikh ,"Privacy issues in VANETs Intelligent Applications" in Sindh University Research Journal (Science Series), Volume 43, Issue 35, December 2011
13. Trupti Gajbhiye, Akhilesh A. Waoo2, P.S Pathija "Traffic Management through Inter-Communication between Cars using VANET System", in International Journal on Advanced Computer Engineering and Communication Technology Volume1 Issue:1, December 2007.
14. Naresh kumar, R.Mustary, R.P. Chander and Moghal Nisar Ahmed Baig, "A performance evaluation of VANET for intelligent transportation system" in World Journal of Science and Technology, Volume 2 Issue 10, January 2013.
15. Maria Elsa Mathew and Arun Raj Kumar P, "Threat Analysis and Defence Mechanisms in VANET" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013.
16. Subir Biswas, Jelena Misic, Vojislav Misic. "DDoS Attack on WAVEenabled VANET Through Synchronization", in IEEE Global Communications Conference (GLOBECOM '12), 2012.Ikecukwu K. Azogu, Michael T. Ferreira, Hong Liu, "A security metric for VANET content delivery " in IEEE Xplore, Volume 3, Issue 7, December 2012.
17. Nitesh Kr. Prajapati, Jyoti Grover, M. S Gaur, "Implementation of Temporal Attacks in Vehicular Ad Hoc Networks" in International Journal of Computer Applications, Volume 12, Issue 5, December 2011.
18. Ana Isabel Gonzalez-Tablas, Arturo Ribagorda, Jose Maria de Fuentes, "Overview of Security Issues in Vehicular Ad-hoc Networks" in Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, Volume 12, Issue 10, January 2011.
19. Anup Prakash Singh, Jaydeeep P. Kateshiya, "Review To Detect and Isolate Malicious Vehicle in VANET" in International Journal of Innovative Research in Science, Engineering and Technology, Volume 4, Issue 2, February 2015.
20. Ana Cavalli, Vinh Hoa LA, "Security attacks and solutions in Vehicular Ad-hoc Networks: A Survey" in International Journal on Ad-Hoc Networking Systems (IJANS) Volume 4, Issue 2, April 2014.
21. Neelam Joshi, Kumud Dixit, Krishna Kumar Joshi, "A Novel Approach Of Trust Based Routing To Select Trusted Location In AODV Based VANET: A Survey", International Journal of Hybrid Information Technology Volume 8, Issue 7, April 2015.
22. Bartsoz Lipiński, Wojciech Mazurczyk, Krzysztof Szczypiorski, and Piotr Śmietanka, "Towards Effective Security Framework for Vehicular Ad- Hoc Networks" in Journal of Advances in Computer Networks, Volume 3, Issue 2, November 2015.
23. Vaishali Mittal, "Prevention of Gray Hole Attack in Mobile Ad-Hoc Networks by Enhanced Multipath Approach" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 4, Issue 5, May2015.