Detect and Isolate Jamming attack in MANET using AODV protocol

Jaspreet Kaur
M.Tech Research Scholar
preet.jass91@gmail.com
+91-9878960142
Gurukul Vidyapeeth Banur, Punjab, India

Dr. Saurav Bansal
Assistant Professor
adap@gurukul.cc
Gurukul Vidyapeeth Banur,, Punjab, India

Abstract—The broad exploitation of smart phones has started to make them practical employment environments for actual-world at-scale MANETs (i.e., to give peer-to-peer based non-cellular services). Services like this, will surely subject to cyber-attacks, simplest of which one is radio frequency (RF) jamming. The accomplishment of these MANETs will require both: i) fast as well as exact ways of identifying the presence of jammers and ii ways of justifying jammer impacts. While observing through standard MANET operational measures such as: packet delivery ratio, delay, routing overhead, and hops travelled , this task finds out the effects of jamming strategies over the MANET. Hence, the delectability of active jammers heavily depends both on which compute is employed and the exact environment of the jamming approach employed. Besides, even if fundamental approaches such as constant jamming are detectable without any troubles, it is revealed that little work is requisite to construct for less detectable jamming strategies. In this paper we have proposed to design a new technique to detect and isolate the jamming attack in MANET(mobile adhoc network) using AODV protocol. Our aim is to understand the existing techniques of detection and isolation of jamming attack by the malicious node and develop a new algorithm to detect and isolate the same in more efficient way on the basis of the throughput of the network.

Keywords:- Jamming attack, wireless networking, jamming, MANET jamming attack, MANET, Isolate jamming node, adhoc network issues, AODV in jamming

I. INTRODUCTION

A network can be defined as the combination of different devices e.g. computers to establish a communication with each other. In a network there is a successful movement of information from one system to another in the network. We can also define it as a grouping of different connecting devices in a particular manner. When number of computer systems are connected to distribute the information over different devices they composite the network. In networking there is a sharing of the sources over a network. These shareable resources can be hardware based or software based. The netwok is organized in different measures of traffic, size and structure of the network with the help of networking protocols.

A network can be of two types:- wired network and wireless network. A network in which we employ wires to maintain a link across different devices are called wired networks and in which we use radio signals are called wireless networks [5]. In wireless networks there is no need of any kind of connecting wires for communication instead of which we use radio waves for communication purpose. It is also known as Wi-Fi or WLAN. The information can be shared easily with such networks through radio frequency. 802.11 is the IEEE standard for the same. The two modes of Wireless Operating are:1. Infrastructure Mode 2. Adhoc Mode or Infrastructure less Mode. Adhoc modes are meant to be used in emergency conditions. So these set a different standard for wirelss communication. This mode is for mobile nodes. There is no fixed infrastructure is required in ad hoc network like base stations. Nodes within each other radio range communicate wireless links directly [12]. There different types of Adhoc network available. These are as following: 1. MANET 2. Wireless Sensor Networks (WSN) 3. Wireless Mesh Networks (WMN). MANET stands for Mobile Ad hoc Network. It is a robust an adhoc network. In this network nodes are connected randomly forming any type of topology with the help of mobile nodes or both mobile and fixed nodes. At times they can be routers and hosts. Primary objective of routing protocol is to discover the route. In the routing protocol for MANET undertakes to setup and maintain routes between nodes. For example, AODV (Adhoc on Demand Distance vector) routing protocol.

A jammer is an entity whose main aim is to inhibit the acceptance of wireless communications by trying to enter the way of the physical transmission A jammer constantly produce RF signals to fill a wireless path so that legal traffic will be completely blocked. The common characteristics for all the jamming attacks are that their interactions are not amenable with MAC protocols[2]. The ratio of packets that are effectively sent out by a justifiable traffic cause as compared to the number of packets it suppose to send out at the MAC layer. In this attack number of source are formed instead of single source which sends rough packets to the transmission channels and jammed the channel. Due to this jamming, packet loss starts. This decrease the efficiency and reliability of the system. Due to this attack many problems are arise like channel becomes busy, delay in transmission, new packet drops begin due to buffer space full etc. Physical or Radio jamming in a wireless network is a trouble-free but disturbing form of DoS(denial of service) attack. A major advantage of MAC layer jamming is that the challenger node needs less power in targeting these attacks as compared to the physical or radio jamming. In this, we concentrate on DoS attacks at the MAC layer resulting in clash of RTS/CTS control frames or the DATA frames.

2. LITERATURE REVIEW

Ali Hamieh, Jalel Ben-Othman,2009 they have wished-for a new model based on the measure of relationship amongst the error and the correct reception times in order to detect the presence of jamming attack in ad hoc networks. Main purpose is to detect specific type of jamming, in which the when any official radio activity is signaled from its radio hardware only the jammer transmits the signal, that shows the major cause of such attacks. Our goal in the future is to use our method to find other DoS attacks, and to search an efficient reaction process to deal with jamming.

Loukas Lazos,2009 they proposed that in node compromise there is a trouble of control-channel jamming in multi-channel ad hoc networks. We proposed a randomized distributed channel establishment scheme which pemits nodes to select a new control channel using frequency hopping. Our method differs from classical frequency hopping in that the communicating nodes are not matching to the hoping sequence in the same manner. Or else, each node follows a unique hopping sequence. They showed that their scheme can uniquely identify compromised nodes with the help of their exclusive sequence and depart them from the network. We calculated the concert of our scheme based on the recently projected metrics of avoidance entropy, avoidance delay, and avoidance ratio. The proposed scheme can by utilize as a provisional way out for the control channel re- establishment until the jammer and the compromised nodes are removed from the network.

Priyanka Goyal,2011 they talk about the Mobile ad-hoc network which shows that this is a field which shows great potential for explore and progress of wireless network. As the activeness of mobile device and wireless network appreciably increased over the precedent years, wireless ad-hoc networks has now become one of the most electrifying and dynamic field of communication and networks. Due to cruel challenges, the distinct attributes of MANET get this technology immense opportunistic together. This paper explains the necessary problems of ad hoc network by including the idea, features, category, and exposers of MANET. This paper shows an summary and the lessons of the routing protocols. In addition, it includes different demanding issues, promising function and the future trends of MANET.

Caimu Tang, 2011 author discussed about future competent validation mechanisms for low-power devices. Here for mutual validation the mobile nodes need only one packet. For validation group pass code can be generated with the help of elliptic-curve-crypto system based trust delegation Mechanism. With the help of this validation process many active as well as passive attacks can be controlled including DoS attack. This is simple way of validating the mobile node with the main station as it requires few calculations and only one packet exchange rather than other validation schemes.

Pradeep kyasanur, 2005 author proposed, an addition to 802.11 DCF protocol to find the self-centered nature of the nodes in both infrastructure and ad hoc network topologies. The nodes which make all other nodes keep on waiting for the network by taking contentional window(CW) time and this reduces the overall throughput of the network. This proposed scheme has three components:- 1) Receiver will check it out whether sender is following the protocol or not. 2) Sender has to send the data over the particular time period fixed by the receiver as contentional time.

Karim El Defraweny and Gene Tsudik,2011 in this paper the author describes that the mobile nodes can move freely in their own environment . there will not be any issue of attacks if the the environment is safe. But if the environment is not exactly safe there will alwys be a possibility of the inside as well as outside attacks over the nodes. To make the environment safe we need to make the surety of mutual validation. For establishing a connection with the other node the mobile node has to show its current location.

3. RESEARCH OBJECTIVES

Following are the various objectives of this research work

- To study the previously proposed plans suggested for analysis and counter measurement of jamming attack.
- The aim of the study to detect the jamming attack in MANET using AODV protocol.

- Analyzing the effects of jamming attack in the light of Packet loss, throughput and end-to-end delay in MANET.
- To find new way of detecting malicious nodes in the network which causes jamming attack in the network.

4. RESEARCH METHODOLOGY

All possible attacks(i.e. inside and outside attacks) in MANET deteriorate the performance of a network**.** An attack in which the network's own node become malicious node and attacked the network is called an inside attack. On the other hand, when the node of some other network acts as a malicious node on our network, that type of attack is termed as an outside attack[3]. A passive outsider eavesdrops on all communication and aims to compromise privacy. Selective packet drop attack is the most common active type of attack amongst all the attacks discussed earlier. Jamming attack triggered by the malicious node or multiple malicious nodes in the network which results in partial DoS(denial of service). Many techniques have been planned to isolate jamming attack in the network in the earlier times. Throughput of the network reduces and the delay increases as the jamming attack triggered over the network. In our task, we focus on to detect and isolate jamming attack in AODV Protocol [10].

First of all we'll arrange the mobile adhoc network with the infinite number of nodes. All these nodes will be mobile nodes and are arranged randomly in a particular area. For defining a route we have to select source and the destination first. To establish a route source node will spread the route request packets and the adjacent nodes. These adjacent nodes further transmits the route requests to their respective adjacent nodes. As these adjacent nodes are ending requests to the adjacent nodes at the end it reaches the destination node. From destination node reverse process will start by acknowledging the route reply packets to their adjacent node till it reaches the sender. Then all the possible routes will be clear and one appropriate route will be selected on the basis of hop count and sequence number. The route having appropriate hop count and sequence number is established between the source and destination. The malicious node exists in the route which is act as source or multiple sources. This is the only node that will be responsible for triggering the jamming attack. The proposed methodology will detect the malicious node and isolate, it from the network. The methodology is based on the throughput of the network. When the throughput of the network, will degrades to certain threshold value, nodes in the network will go to monitor mode and detect the malicious node. The proposed methodology will be implemented in network simulator version 2. Thus by detecting and isolating jamming we will discuss about the performance of the network with different measuring factors such as throughput of the network, energy loss, packet delay etc.
Below the flow chart gives the overview of the entire work that is to be done on the detection and isolation of jamming in MANETs using AODV protocol.

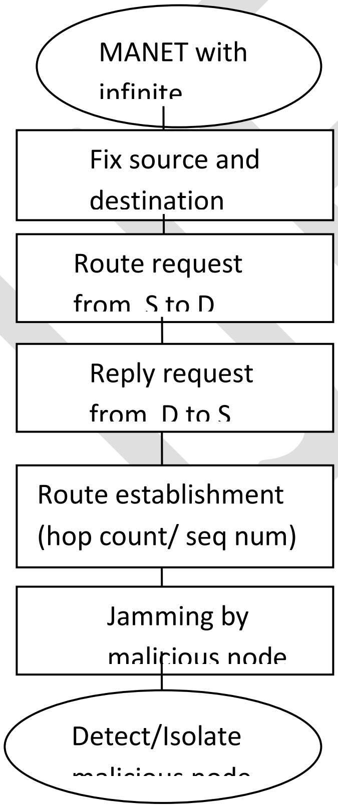
MANET with infinite
Fix source and destination
Route request from S to D
Reply request from D to S
Route establishment (hop count/ seq num)
Jamming by malicious node
Detect/Isolate malicious node

Figure 1 - Flow Diagram of the Proposed Approach

5. CONCLUSION

Jamming in the wireless networks is a great issue to be quite popular and necessary also. The new proposal will provide an efficient way to detect and isolate the jamming caused due to different nodes in the network. Jamming should be detected and isolate on different measures, such as throughput, energy loss, delay time other than the earlier measures.

REFERNCES:

[1] Ali Hamieh, Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", *IEEE, 2009*
[2] Loukas Lazos, Sisi Liu, and Marwan Krunz, "Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks" ACM, WiSec'09, March 16–18, 2009, Zurich, Switzerland, 2009
[3] Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks" , 10th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648, n.d.
[4] Pradeep kyasanur "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing, n.d .2005
[5] Priyanka Goyal, Vintra Parmar and Rahul Rishi ," MANET: Vulnerabilities, Challenges, Attacks, Application" , IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011.

[6] Tien-Ho Chen and Wei-Kuan, Shih , "A Robust Mutual Authentication Protocol forWireless Sensor Networks" *ETRI Journal*, Volume 32, Number 5, October 2010

[7] Caimu Tang ,Dapeng Oilver "An Efficient Mobile Authentication Scheme for Wireless Networks",*IEEE,* 2011
[8] Karim El Defrawy, and Gene Tsudik , "ALARM: Anonymous Location-Aided
Routing in Suspicious MANETs", IEEE TRANSACTIONS ON MOBILE COMPUTING, Vol. 10, No. 9, September 2011
[9] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada "On Alarm Protocol in Wireless Sensor Networks*",IEEE, 2010*
[10] S. Sharmila and G. Umamaheswari, " Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012

[11] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", IJSER*, 2005*

[12] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" ,Springer ,2006

[13] Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", IEEE, 2010