IJARST

International Journal of Advanced Research in Science and Technology

journal homepage: www.ijarst.com

ISSN 2319 – 1783 (Print)
ISSN 2320 – 1126 (Online)

To Detect and Isolate the Selective Packet Drop Attack in MANET

Anumati Thakur*, Max Bhatia and Bikramjit kaur

Department of CSE, Lovely Professional University, Phagwara, Punjab, India.

****Corresponding Author's Email: salariaanu88@gmail.com***

A R T I C L E I N F O

Article history:

Received	15	May	2014
Accepted	06	July	2015
Available online	13	July	2015

Keywords:
AODV,
MANET,
Malicious node,
Wireless networks,
route request message,
route request errors,
route request response.

A B S T R A C T

The wireless ad hoc network is the self-configuring network; mobile nodes can leave or join the network when they want. These types of networks are much vulnerable to security attacks. Such type of active and passive attacks is possible in Ad hoc network. Among all the possible active attacks, Selective Packet Drop attack is the most common and harmful attack. The attack is triggered by the malicious node which is present in the network. In this research work, novel technique is proposed to detect and isolate malicious nodes from the network which are responsible for triggering the attack. In selective forward attack during transmission some packets gets dropped by the malicious node and that node will be acts as genuine node within the network. So incomplete data will be reach up to the destination. Therefore to detect and isolate malicious node from the network is difficult work to do. In previous work DSR Protocol was used to detect It by calculating the Energy Factor but not able to remove it completely. So, in this research work AODV protocol has been used. The new technique which is used in it is based on the Monitor Mode Approach. Through monitor mode technique messages would be flood across the channel in AODV mode and if any malicious node would be present, then instant acknowledgement would be given to source for retracing the path. This technique enhances the throughput level up to desired extent i.e. approx. 77% and other parameters like delay and packet loss also get reduced.

PAPER-QR CODE

Citation: *A. Thakur et. al., To Detect and Isolate the Selective Packet Drop Attack in MANET, Int. J. Adv. Res. Sci. Technol. Volume 4, Issue 4, 2015, pp.464-468.*

Introduction:

A network is a collection of two or more computer systems which linked together. It is medium of passing of information to interact with each other. It is a connection of computer devices which are attached with the communication facilities. Networking is used for data communication. Sharing resources are software type or hardware types. When number of computer are linked together to share information they form networks and share resources. Networking is used for data communication. It is central administration system or supports these types of system Sharing resources are software type or hardware types. Wireless Networks is a type of networking which don't requires cables to attach with devices during contact. It is also known as Wi-Fi or WLAN. Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols and without the using of cables protocols and without the using of cables. With the help of this network, devices can be joined easily with the help of radio frequency without wires to sharing information.

There are two types of Wireless Operating modes [1]:

1. Infrastructure Networks: In it, contact takes place only between the wireless nodes and the access points. Here the access point wants to run the normal access and it acts as the connection to the wireless and wired networks

2. Adhoc mode or infrastructure-less mode: it is connecting wireless consumers directly without the help

of access point and wireless router [2]. It has no central controller.

1. Wireless Sensor Networks
2. MANET
3. Wireless Mesh Network.

MANET:

MANET [2] stands for Mobile Ad hoc Network [3]. It can be established with the help of mobile nodes or by both fixed and mobile nodes. It is a robust infrastructure less wireless network. Nodes have ability to self-configure which makes this technology proficient for provisioning statement. They can act as both routers and hosts. For example, disaster-hit areas where there is no dealings in environment or in emergency search and release operations where a network relationship is at once compulsory. In MANET routing protocols [4] for both static and dynamic topology are used. Therefore, we combine wireless ad hoc network with mobile nodes as a Mobile Adhoc Network. The absence of an infrastructure in it poses great challenges in the operationality of these networks. More frequent using protocols in it are as follows:

1. AODV (Adhoc on Demand Distance vector)
2. DSR (Dynamic Source Routing)
3. OLSR (Optimized Link State Router)
4. Wireless Routing Protocol (WRP)
5. Zone Routing Protocol (ZRP)

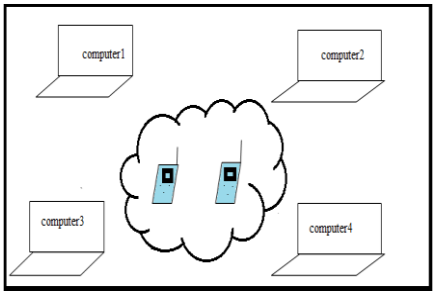

Fig: 1. Conceptual view of MANET

Types of Attacks in MANET:

1. Internal Attack:

These are as of compromised nodes that are component of the set of links. In an internal attack from the network the wicked node gains unofficial access and act as a real node. Congestion [4] can be checked between other nodes and may offer in the behavior of other networks.

2. External Attack:

It is approved by the nodes which do not fit in to network. It may cause unavailability and congestion by moving incorrect information in the network [5].

Selective Packet Drop Attack:

It is the type of denial of service attack [6]. Packet dropping attack is launched on the forward stage. They drop packets only to keep their resources not damages any other nodes. As the data will be send from sender to destination then there will be a malicious node present on the path, which will acts as genuine node and will drop some packets [7], and send incomplete data to next node. And acknowledgement will not be send to the source. As receiving node will receive incomplete data, which is destination then instant acknowledgement will be send to the source for data lost and will request for change the path for resending the data. Selective forwarding attack is compound attack to detect, since packet drops in antenna networks may be caused by unreliable.

Method:

In MANET inside and outside attacks are probable, which affects the presentation of the network. Selective packet Drop attack is the partial denial of service attacks which is triggered by the malicious nodes in the network. In the previous times, many techniques have been made to isolate Selective attacks from the network. When Selective packet attack [8] is triggered in the network, throughput of the network decreased and wait amplify as steady rate. In our work, we work on to detect and isolate Selective Packet Drop attack In AODV Protocol [9] with the help of Monitor Mode Approach

Firstly we arrange the mobile ad hoc network with endless number of mobile nodes. All the mobile nodes are indiscriminately deployed into the fixed area. For the route establishment cause node overflow the route request packet in the network and route reply packets are send back to the starting place by the neighboring nodes. The path is recognized between source and destination on the basis of hop counts and sequence numbers. The malicious node [10] will be responsible for triggering the selective packet drop attack. The used the methodology will notice the malicious node and separate, it from the network. In Delay sensitive selective packet drop attack [8] in which either packets drop or shift to other direction to reach to the goal by malicious node. In this proposed work we defeat the problem of dropped packet [12] by finding them and redirect to the source with the help of malicious node

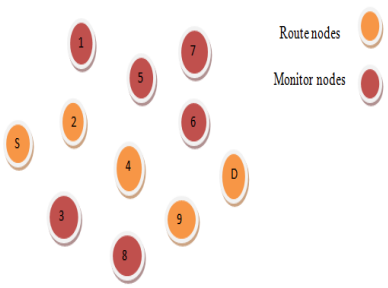

Fig: 2. Activation of monitor nodes

In fig: 2 The nodes which established the overflow messages goes to the monitor mode which is used to detect the mean node which readdress the pathway of the node. Other nodes are route nodes are measured in route nodes from basis to target after in receipt of false packets.

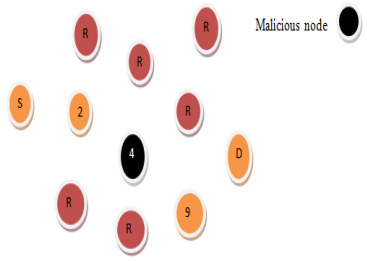

Fig: 3. Detection of Malicious node

In fig: 3, Monitoring node watches the deluge packets [11]. They acknowledged the malicious node which redirects the path from starting place to goal path to other path. When monitor nodes find the wicked node they all transmit reply message to the cause node to segregate the path.

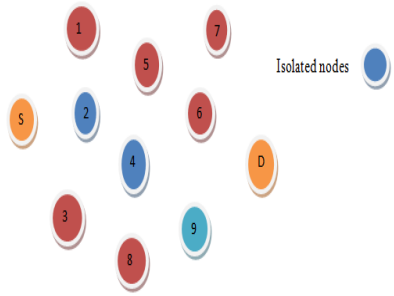

Fig: 4. Isolated Existing Path

In fig: 4, after getting reply message from the monitor node source node separates existing path and check out new path for interaction from source to the destination.

In this proposed work we have agreement with the throughput delay sensitive wormhole attack. Suppose we have a network in which huge number of nodes are present. There are two methods in which packets are migrated from source to destination. First of all, source sends false packets for the path establishment from cause to end. We can also manage that foundation sends fake messages. Secondly source overflows the packets in the network as data packets. The node which received data packets went to the monitor node. In this process starting place produce ICMP packets [12] that submerge in the network. The nodes which are get as a data packet goes to the promiscuous node. After getting monitoring packets other nodes than monitor nodes in the network, they begin checking midway nodes from source to destination. Monitor node sends packets on route. It does not transmit data packets but send accidental packets in the network. Now the nodes which will get the packets promote it to the end and regard as that way as a route. But the monitor nodes also verifying those nodes which affect the packet that is mean node dropped the packets or transmit it to the end by other paths. Monitoring nodes finds that node which additionally does not transmit it to the end point. So the nodes which check the malicious node acknowledge to a resource node wait for direction node so that basis segregate the pathway and stop forwarding extra packets.

Algorithm:

a. Deploy the wireless ad hoc network with fixed number of mobile nodes and in fixed area

b. Select the shortest path between the source and destination using AODV routing protocol

c. To verify the route

{

d. Source flood the monitor mode in the network

e. The nodes after receiving the monitor mode message start monitoring the route between source and destination

f. If (Malicious node ==exits)

{

g. The other nodes in the network send malicious node information to source

h. The source isolate the selected path

i. The source select the other best path

j. Else

{

k. The source keeps on communicating with destination

}

End

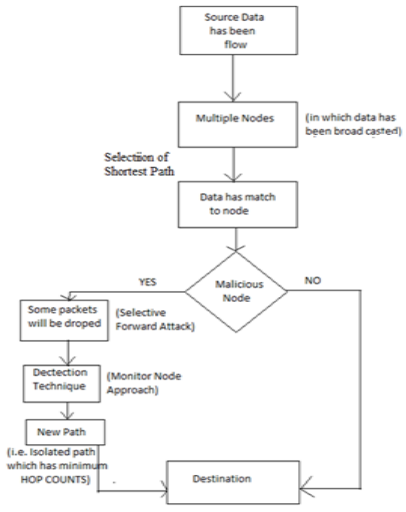

Fig: 5. Flow Chart of Research Work

Results:

NS2 tool has been used for creating the simulation and to get meaningful results, in short interval of time.

Depending on user's requirement the simulation are stored in trace files, which can be fed as input for analysis by different component.

1. A NAM trace file(.nam) is used for the ns animator to produce the simulated environment.
2. A trace file(.tr) is used to generate the graphical results with the help of a component with X graph.

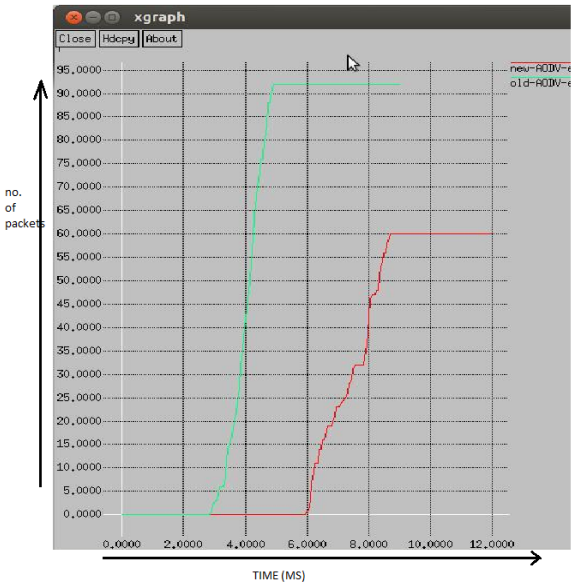

Fig: 6. Analysis of Delay

In the Fig: 6, it is shown that graph of network delay. The network delay is more in the previous scenarios. The network delay is reduced in the new scenario.

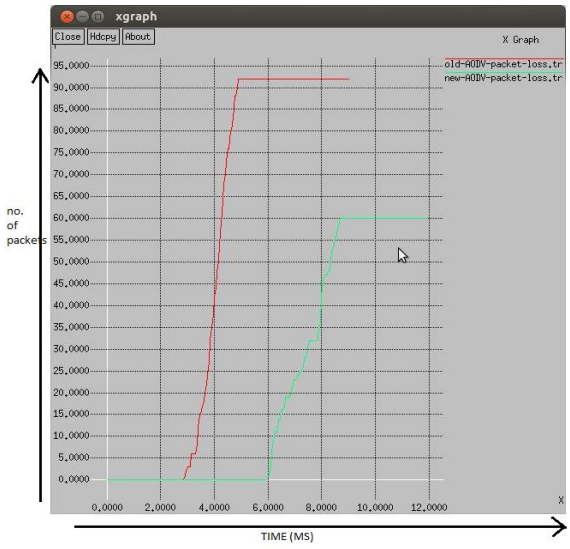

Fig: 7. Analysis of Packet loss

In the Fig: 7, it is shown that graph of packet loss. The packet loss is more in the previous scenarios. The packet loss is reduced in the new scenario

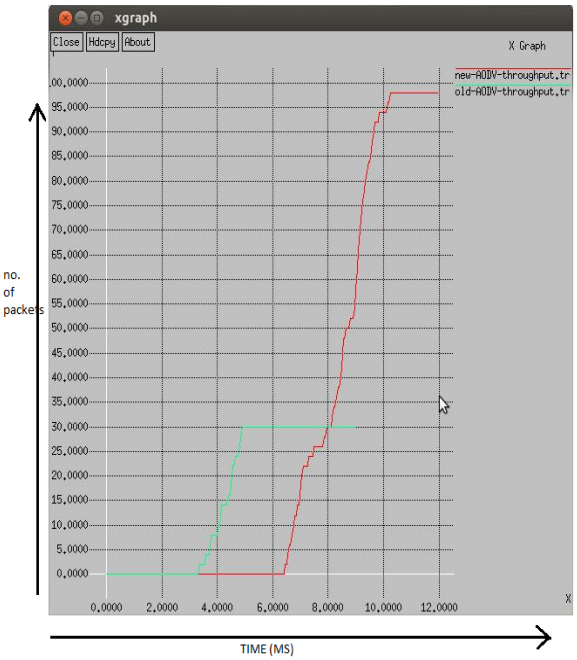

Fig: 8. Analysis of Throughput

In the figure 8, it is shown that graph of Throughput. The network throughput is more in the new scenario. In the old scenario it will reduced due to selective packet drop attack in the network which is triggered by the malicious node.

Conclusion:

A network is an interconnection of different nodes which will communicate with each other with or without wires. Wireless Networks term refers to a kind of networking that do not requires cables to connect with devices during communication. MANET stands for Mobile Ad hoc Network. It can be established with the help of mobile nodes or by both fixed and mobile nodes. They can act as both routers and hosts. They have capability to self-configure which makes this technology efficient for provisioning statement. We have used AODV protocol in our work to enhance the functioning of MANET i.e to detect the malicious node and to isolate it from the network and reduce the effect of selective forward attack. We have improved the functioning of AODV by applying monitor node approach in our work which will floods the monitor mode messages along with route request packets and will check that which node is dropping packets and will acknowledge back to source about that. As source will receive acknowledgement and came to know about packet loss and malicious node, it will retrace the path and send data to destination through another path. The energy consumption is less. Different assuming parameters like network throughput get improved up to 77%. Network delay and packet loss contents also get improved up to desired extent. Although by the help of monitor node approach, detection procedure is fast and accurate but still there is a need of 100% detection and enhanced throughput analysis.

References:

1. Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011
2. Abdul Haimid Bashir Mohamed, "Analysis And Simulation Of Wireless Ad Hoc Network Routing Protocols"2004
3. Giovanni VignaSumit GwalaniKavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool forAODV-based Ad hocWireless Networks", 2004
4. SevilŞen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", 2010.
5. RushaNandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)
6. Wenjia Li and AnupamJoshi , "Security Issues in Mobile Ad Hoc Networks- A Survey",2005
7. Gene Tsudik, "Anonymous Location-Aided Routing Protocols for Suspicious MANETs",
8. Karim El Defrawy, and Gene Tsudik , "ALARM: Anonymous Location-AidedRouting in Suspicious MANETs" , IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9, SEPTEMBER 2011.
9. Steven M. Bellovin and Michael Merritt "Limitations of the Kerberos Authentication",Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks" , 10th IEEE International Conference on Network Protocols (ICNP'02)1092-1648
10. Pradeep kyasanur "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing,2005.
11. CaimuTang ,DapengOilver "An Efficient Mobile Authentication Scheme for Wireless Networks",IEEE
12. Tien-Ho Chen and Wei-Kuan, Shih , "A Robust Mutual Authentication Protocol for Wireless Sensor Networks ETRI Journal, Volume 32, Number 5, October 2010.