RESEARCH ARTICLE OPEN ACCESS

Designing a Distributed Framework to Detect a Selfish Node in MANET by using a Collaborative Approach

Jagmeet Kaur, Prabhjit Singh
Department of Computer Science and Engineering
Global Institute of Management & Emerging Technologies
Amritsar, Punjab
India

ABSTRACT
A mobile ad-hoc network (MANET) is a compilation of wireless mobile nodes that dynamically self-organize to shape up random and momentary network. The mobile nodes can communicate with each other without any permanent infrastructure. MANET can be set up rapidly to make possible communication in a antagonistic environment such as battlefield or emergency situation. Wireless ad-hoc network is wide area of research work from precedent few years. Due to its openness and lively topology network is vulnerable from attackers. Mobile Ad-Hoc Networks has the ability to organize a network where a traditional network infrastructure environment cannot possibly be deployed. The various severe security threats are increasing on the MANET. One of these security threats is the availability of selfish node in the network which drops all received data packets intended for forwarding. In the past, many people have worked on this selfish node problem and proposed numerous methods to detect these selfish nodes. This research provides information about various methods that can make network free from the impact of selfish node(s). Selfish node is destructive to the network and it is responsible for the loss of data, decline in throughput, degrading performance etc. Mechanism should be available and must be followed for the detection and elimination of malicious node from the network. In the approach, it is analyzed there are huge number of threats associated with network. Although, numerous solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works fine in the presence of single malicious node, it cannot be appropriate in case of multiple malicious nodes. After referring multiple approaches, and applying Conniver broadcasting node technique mode after the detection of selfish node would surely decrease the rate of loss in data packet.

Keywords:- MANET, WLANs

I. INTRODUCTION

Wireless networks are gaining popularity to its peak today, as the user wants wireless connectivity irrespective of their geographic position. Wireless network is a network set up by using radio signal frequency to communicate among computers and other network devices. Wireless networks have emerged as a subsidiary of wired networks [1]. Devices in a wireless network are set up to either communicate indirectly through a central place an access point or directly, one to the other. Wireless communication is the level at which the transfer of user data over a distance without the use of "wired" or electrical conductor. The term "wireless" referred to telecommunication. Communication between two or more device can be within the short range or may be thousands of kilometres range. Wireless Networks term is refers to a kind of networking that does not require cables to connect with devices during communication. Radio waves are used for transmission at physical level [2]. It is widely known as Wi-Fi or WLAN. With the help of this network, devices can be joined easily with the help of radio frequency without wires to sharing information.

II. MOBILE WIRELESS NETWORKS

There are currently two variations of mobile wireless networks

- Infrastructures networks.
- Infrastructure less networks.

The infrastructure networks, also known as Cellular network, have fixed and wired gateways. They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is

able to continue communication seamlessly throughout the network. Example of this type includes office wireless local area networks (WLANs).

The other type of network, Infrastructure less network, is known as Mobile Ad Network (MANET). These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.

The chief difference between ad hoc networks is the apparent lack of a centralized entity within an ad hoc network. There are no base stations or mobile switching centers in an ad hoc network. The interest in wireless ad hoc networks stems from of their well-known advantages for certain types of applications. Since, there is no fixed infrastructure, a wireless ad hoc network can be deployed quickly. Thus, such networks can be used in situations where either there is no other wireless communication infrastructure present or where such infrastructure cannot be used because of security, cost, or safety reasons.

III. CLASSIFICATION OF ROUTING PROTOCOLS [25]

Routing protocols define a set of rules which governs the journey of message packets from source to destination in a network. In MANET, there are different types of routing protocols each of them is applied according to the network circumstances. Figure 1 shows the basic classification of the routing protocols in MANETs.

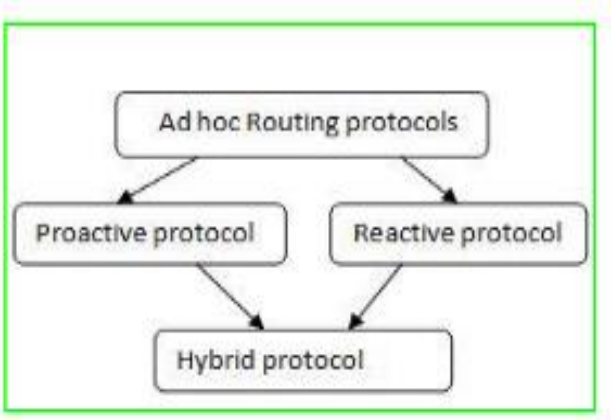

Fig 1- Classification of the routing protocols in MANET[25]

IV. ATTACKS IN AD-HOC NETWORKS

There are a variety of attacks possible in Ad-hoc networks. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols. A passive attack does not disrupt the normal operation of the network. The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring [7]. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. It may cause unavailability and congestion by sending false information for the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks [7].The ultimate goals of the security solutions for Ad-hoc networks is to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users. The various possible attacks are:-

A. Black hole attack

According to this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. When the attacker receives a request for a route to the destination node, it creates a reply message which advertises itself as a valid path to destination. The attacker consumes the intercepted packets without any forwarding [5].

B. Gray hole Attack

The gray hole attack is also termed as misbehaving attack. In this attack, the attacker selectively drops the packet with certain probability. Also, in this attack the intruder node behaves

maliciously for the time it selectively drops the packets and then switches to its normal behavior.

C. Wormhole attack

In this attack, an attacker records the packets at one location in the network and tunnels them to another location. The routing can be disrupted when routing control messages are tunneled.

D. Byzantine attack

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services.

V. ISSUES AND CHALLENGES FOR MANET SECURITY [23]

A. Shared broadcast radio channel

Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc wireless networks is broadcast in nature and is shared by all nodes in the network. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

B. Insecure operational environment

The operating environments where ad hoc wireless networks are used may not always be secure. One important application of such networks is in battlefields. In such applications, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

C. Lack of central authority

In wired networks and infrastructure-based wireless important central points (such as routers, base stations, and access points) and implement security mechanisms at such points. Since ad hoc wireless networks do not have any such central points, these mechanisms cannot be applied in ad hoc wireless networks.

D. Lack of association

Since these networks are dynamic in nature, a node can join or leave the network at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join into the network quite easily and carry out his/her attacks. Limited resource availability: Resources such as bandwidth, battery power, and computational power (to a certain extent) are scarce in ad hoc wireless networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

E. Physical vulnerability

Nodes in these networks are usually compact and handheld in nature. They could get damaged easily and are also vulnerable to theft. [2]

VI. TECHNIQUES FOR DETECTION OF SELFISH/ MALICIOUS NODE (S)

A. End-to-end Acknowledgements [10, 11]

This mechanism consists of monitoring the reliability of routes by acknowledging packets in an end-to-end manner, to render the routing protocol reliable. In this, the destination node gives acknowledgement of receipt of packets by sending a feedback to the source.

B. Watchdog [12, 14]

It aims to detect misbehaving nodes that don't forward packets, by monitoring neighbors in the promiscuous mode. The solution also includes component that selects route based on the link reliability knowledge. The advantage of this scheme is it is able to detect misbehaving nodes in many cases, and requires no overhead when no node misbehaves. But it fails to detect misbehavior in cases of collisions, partial collusion and power control employment. It fails when two successive nodes collude to conceal the misbehavior of each other. It doesn't control detected misbehaving nodes.

C. Pathrater [13]

To check reliability of each path in the network, each node is preloaded with path rater. It gives the rate to path by averaging the reputation of each node of that path. If there are multiple paths to reach destination in network, the path which has highest rate is selected for transmission of packet.

D. Probing

It is a combination of route and node monitoring. This approach consists of simply incorporating into data packets commands to acknowledge their receipt. These commands are called probes and intended for selected nodes. Probes are launched when a route that contains a misbehaving node is detected.

E. Ex-Watchdog

It is implemented with encryption mechanism and maintaining a table that stores entry of source, destination, and sum and path. Its main feature is ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving. This method is used to overcome the drawback of Watchdog method but this method fails when malicious node is on all paths from specific source and destination.

F. ACK Scheme

This technique concentrates on the issue of distinguishing getting out of hand connections as opposed to making trouble hubs The 2ACK plan recognizes misconduct through the utilization of another sort of affirmation parcel, termed 2ACK. A 2ACK bundle is doled out a settled course of two jumps (three hubs) the other way of the information movement course.

VII. PROBLEM FORMULATION

Selfish node attack is a kind of Denial of Service (DoS) attacks in MANET. In this attack, a malicious node advertises that it has the best path to the destination node during the route discovery process. Whenever it receives the RREQ message, it immediately sends out a fake RREP to the source node. The source node first receives the RREP from the malicious node ahead of other RREPs. However, when the source node starts sending the data packet to the destination by using this route, the selfish node drops all packets instead of forwarding.

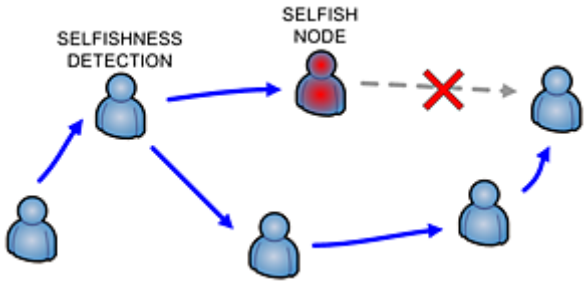

Figure 2- Effect of Selfish node [10]

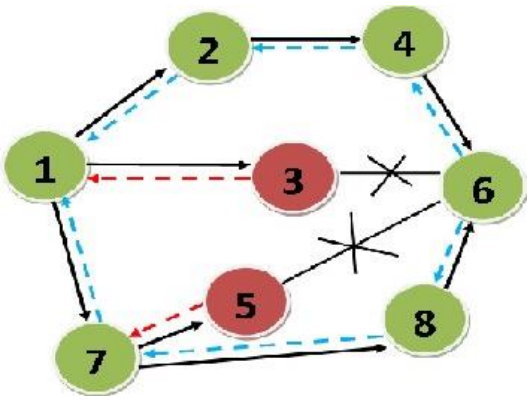

Figure 3- Scenario of packet drop [11]

The selfish nodes do not participate in the routing and data transmission process, which intentionally drop the packets. These misbehaviors of the selfish nodes will impact availability, efficiency, reliability, and fairness. The selfish node utilizes the resources for its own purpose, and it neglects to share the resources to other nodes. So, it is important to detect the selfish nodes in MANET.

VIII. METHODOLOGY FOLLOWED

The Proposed Protocol Dynamic Source Routing (DSR) protocol presented in is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broadcasting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the mobile has not yet seen the request and if the mobile's address does not already appear in the route record. A route reply is generated when the route request reaches either the destination itself, or an intermediate node, which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the

destination or such an intermediate node, it contains a route record yielding the sequence of hops taken. If the node generating the route reply is the destination, it places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply. To return the route reply, the responding node must have a route to the initiator. If it has a route to the initiator in its route cache, it may use that route. Otherwise, if symmetric links are supported, the node may reverse the route in the route record..

Proposed Algorithm: Planner Broadcasting Algorithm

Step 1: Generate entire network scenario using NS-2.

Step 2: Start with some initial basics like 'transmission range', 'neighbor node', 'source node and Destination node.

Step 3: Initialize the transmission with n no. of nodes.

Step 4: Implement planner broadcasting node Technique.

Step 5: Start Data Transmission with planner broadcasting node Technique system.

Step 6: In planner broadcasting node Technique system, a node act as planner and it will find Malicious node in the network.

Step 7: Planner node will broadcast the location of a Malicious Node in the network by broadcasting the routing table. It continuously keeps on broadcasting the routing table with the location of malicious node in network till each node get updated.

Step 8: Then finally data will be transferred from Source to Destination with planner broadcasting node Technique. Planner broadcasting node keeps on updating network with malicious node location so that source and destination will not accept the request of malicious node.

Step 9: Safe path free from attackers for efficient data transmission is established for the entire duration.

IX. SIMULATION AND RESULTS

Figure 4 shows the basic setup of simulation. Here, 21 nodes are used to represent the scenario. Nodes are labeled as node 0, node 1, node 2 upto node 20. Node 0 is shown in red color, this means that it is assumed as a malicious node and it will not act as a part of communication. Node 1 is an initiator, it will start communication. There is only one node except malicious node at the left side of node 1 i.e. node 20. So the transmission will takes place to the right side of node 1 i.e node 2. In figure 5 it is shown that the node 1 starts the transmission towards node 2.

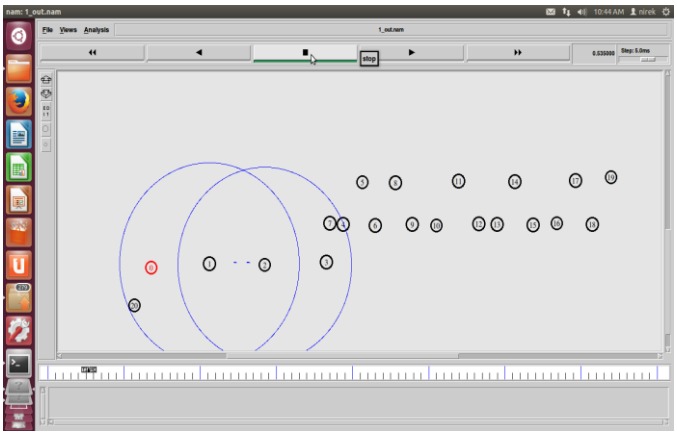

Fig 4- Basic Setup

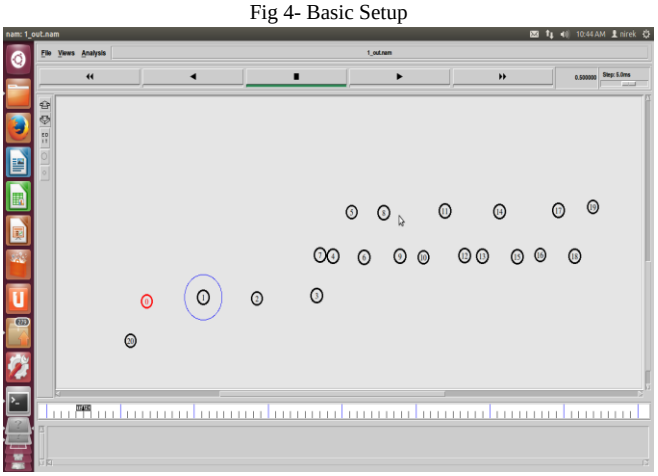

Fig 5- Transmission initiated

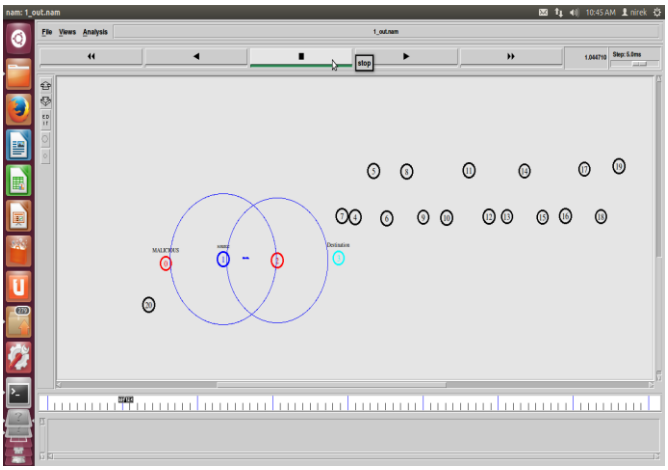

Fig 6- Source and destination

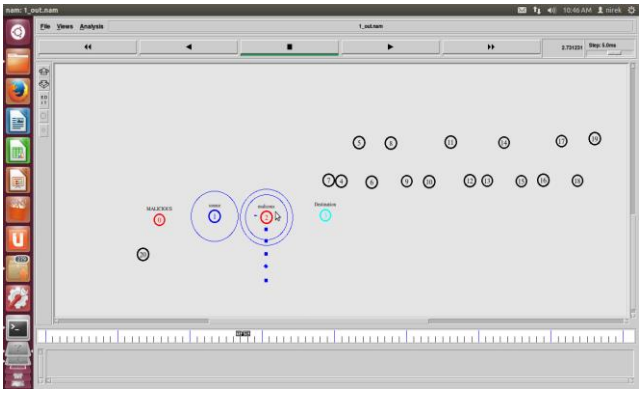

Fig 7- Packet Loss

Figure 6 depict that the node 1 is transmitting data to node 2. Node 0 in the scenario is acting as malicious node and node 3 in pink color is acting as a destination. Node 1 starts flooding of packets to the nearby nodes. Figure 7 shows the loss of packets. Packets transfers from node 1 to node 2 but the destination is node 3. Node 2 fails to forward packets to node 3. It means node 2 is a selfish node and responsible for the packet loss. Node 2 accepts the packets from node 1 but never forward it to node 3. So, all the data loss is due to the selfish activity of node 2.

Figure 8 depicts that when source node confirmed that packets are not reaching to the destination. Then it changes its position and byepass the node 2 as it is also a selfish node in the scenario. As source node knows about node 0 and node 2 that both these are behaving strangely. In figure 9 Source node initiated alarms as it knows that there are selfish nodes available in the network. Packets didn't reached to the destination node 3. On the way all the packets are lost.

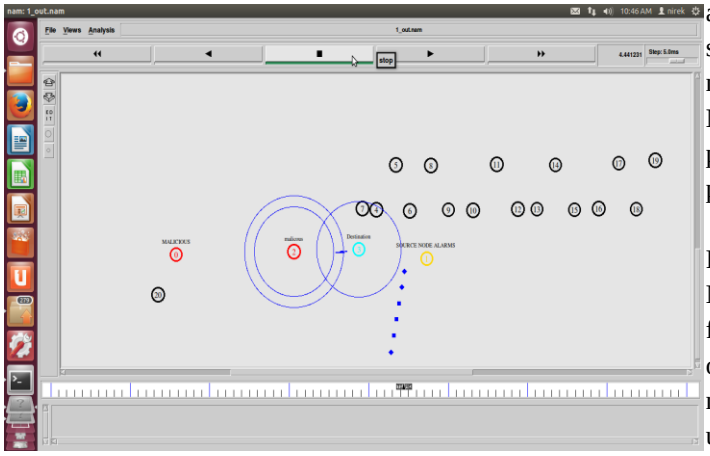

Fig 8- Source changes its position

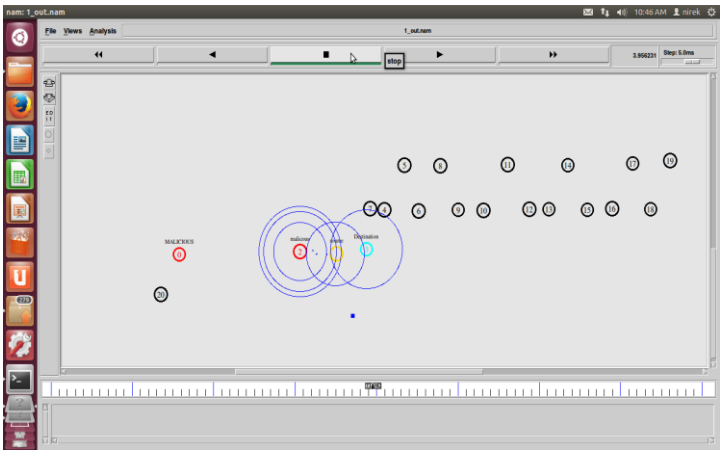

Fig 9- Alarm initiated

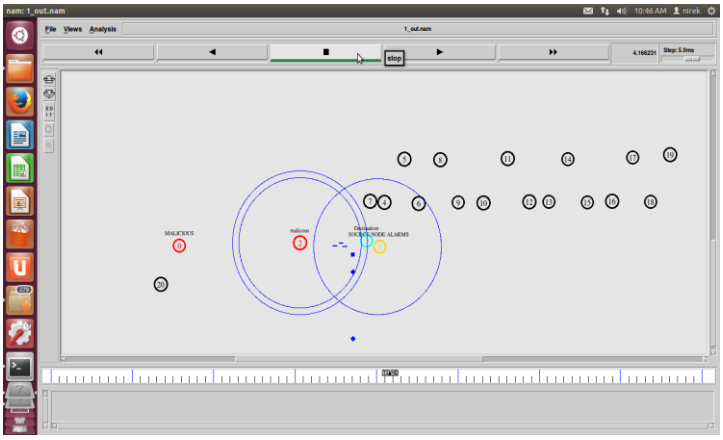

Fig 10- Source node alarm

In figure 10, source node changes its position and traveling around other nodes by highlighting the alarm and informing all the other nodes in the network about the status of node 0 and node 2. Both these nodes are selfish nodes and reflecting strange behavior. All the packets that are transferred to the node 2 are lost on the way and failed to reach at destination. Node 1 as a source node informing other nodes about the performance of node 0 and node 2. In the meanwhile all the packets are lost as it is shown in the figure 10

Flooding is performed in the figure 11, all the packets are lost. No productive work is performed in the mean time. So, in the figure 11 it is reflected that during upstream and downstream of data, it is detected that the malicious node is present in the network which will harm the network by performing unexpected activities which will result in the loss of data. Figure 12 also shows the flooding, this will update the actual status of nodes. The status information is travelling at higher rates.

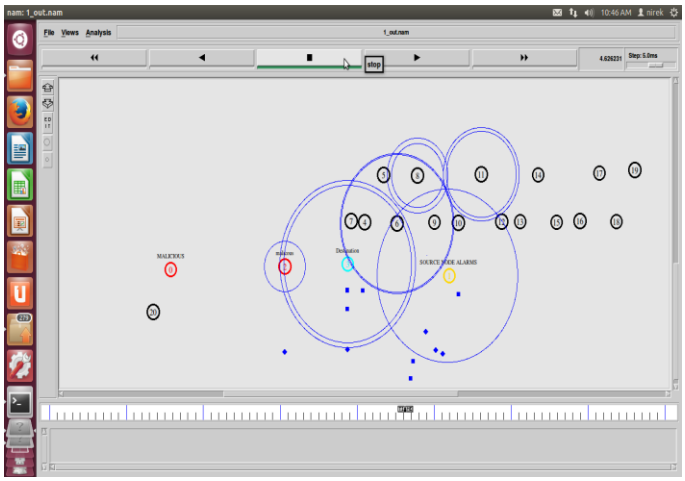

Fig 11- Notifying all other nodes

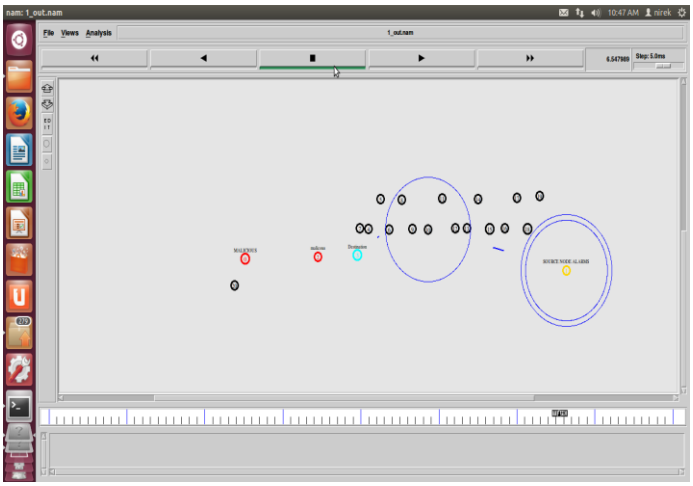

Fig 13- New path followed

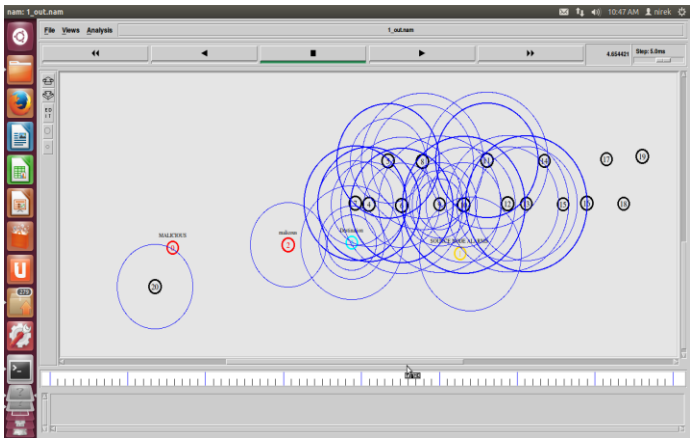

Fig 12- Flooding

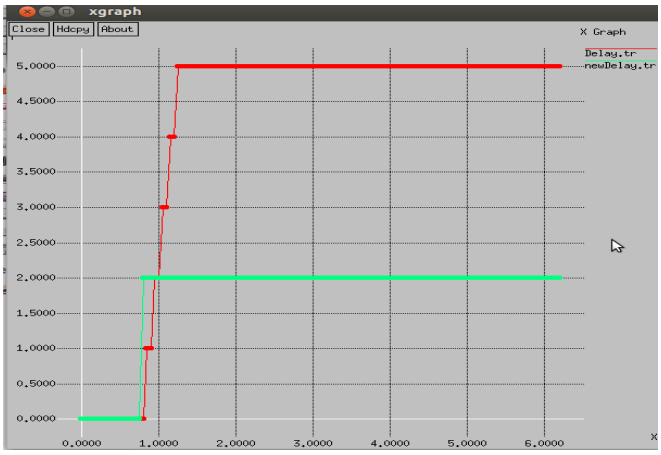

Fig 14- Delay graph

In figure 13, it is shown that due to selfish nodes in the network, source node changes its position and along with that change in position it also changes its path. Now, the packets are transferred from node 1 to node 3 through nodes 9, node 6 and node 4. Selfish nodes are no longer a part of an actual network.

Figure 14 shows the graph of delay in which a delay of packet transmission is shown. This fig. depicts the both cases of the scenario and evaluates the delay of packet during transmission through selfish node and without selfish node. Figure 15 reflects the packet loss graph in which the effect of packet loss is shown. When the packet loss is more, that it is confirmed that the throughput of the network will be highly affected.

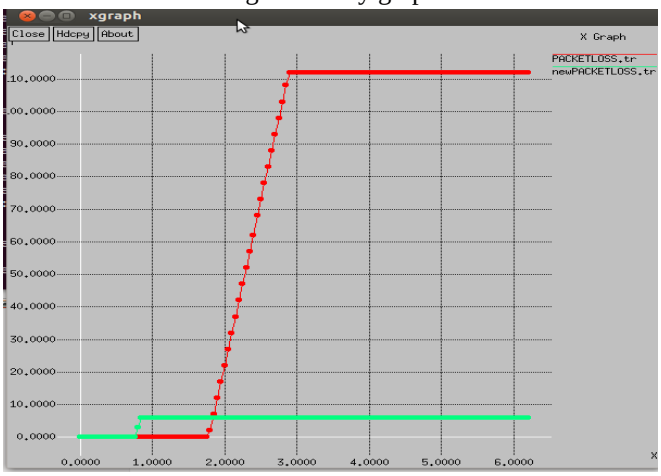

Figure 15- Packet loss

In Figure 16 throughput of network is shown. This throughput graph shows throughput of the network when transmission is done through selfish node and when it is done without making a selfish node a part of network.

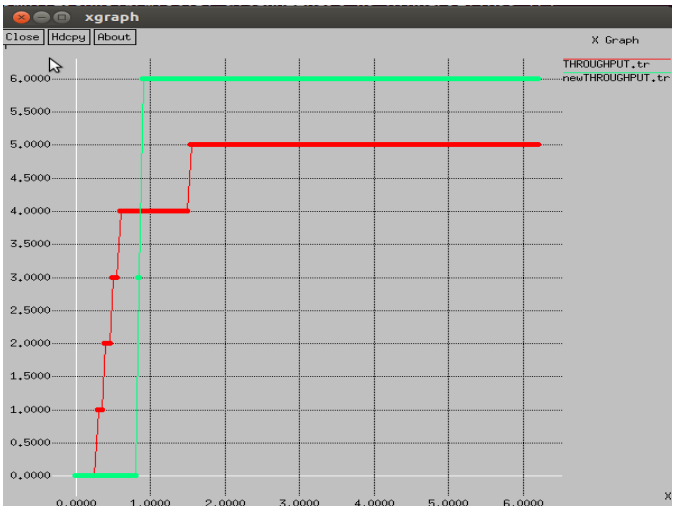

Fig 16- Throughput graph

X. CONCLUSION

Wireless ad-hoc network have been enormous area of research work from precedent few years because its extensively used application in battlefield and business purpose. Due to openness and lively topology network is vulnerable from attackers. Mobile Ad-Hoc Networks has the ability to organize a network where a traditional network infrastructure environment cannot possibly be deployed. Selfish node is destructive to the network and it is responsible for the loss of data, decline in throughput, degrading performance etc. Mechanism should be available and must be followed for the detection and elimination of malicious node from the network. In the approach, it is analyzed there are huge number of threats associated with network. Although, numerous solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works fine in the presence of single malicious node, it cannot be appropriate in case of multiple malicious nodes. After referring multiple approaches, and applying Conniver broadcasting node technique mode after the detection of selfish node would surely decrease the rate of loss in data packet. More ever, the Conniver broadcasting node Technique mode is applied only for nodes that were attacked rather for applying for all the nodes. Hence loss of energy is surely avoided.

REFERENCES

[1] Salmin Sultana et al., "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacksin Wireless Sensor Networks", IEEE transactions on dependable and secure computing, 2015.

[2] K.Sangeetha et.al, "Secure Data Transmission in MANETS Using AODV", International journal of Computer and communication engineering research, 2014.

[3] Josh Kumar etal.," A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT", Communications and Networking, Springer, 2015.

[4] Snehal R.Sawale, Dr.V.S.Gulhane, "Result Paper on Secure Channel Condition Estimation to Protect Wireless Networks from False Channel Condition", International Journal of Advanced Research in Computer Science and Software Engineering, 2015.

[5] R. Gayathri, J.Maria Sofi Anusuya, "Preventing Malicious Node and Provide Secure Routing In Manet", IOSR Journal of Electronics and Communication Engineering, 2015.

[6] T.Manikandan, S.Shitharth, C.Senthilkumar, "Removal of Selective Black Hole Attack In by AODV Protocol", International Journal of Innovative Research in Science, Engineering and Technology, 2014.

[7] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE, Volume 40, Number 10, 2002, pp 70-75.

[8] Ei Ei Khin, Thandar Phyu , "Impact of Black hole Attack on AODV Routing Protocol ", International Journal of Information Technology, Modeling and Computing , 2014.

[9] Anusha Bhide M, Mr. Annappa Swamy D.R and Syed Arshad, "Channel Aware Detection based Network Layer Security in Wireless Mesh Networks", International Journal of Advanced Engineering and Global Technology 2014.

[10] http://onlinelibrary.wiley.com/store/10.1002/ett.2545/asset /image_n/ett2545-toc-0001.png?v =1 &s=7 a32a21c0039eb6c3d158f57886f32a242f45008.

[11] http://www.ijser.org/paper/A-Robust-Technique-for-Secure-Routing -Against-Blackhole-Atta ck - in-AODV-Protocol-for-MANETs.html

[12] Salmin Sultana et al., "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacksin Wireless Sensor Networks", IEEE transactions on dependable and secure computing, 2015.

[13] K.Sangeetha et.al, "Secure Data Transmission in MANETS Using AODV", International journal of Computer and communication engineering research, 2014.

[14] N.Madhuri1 et al., "Secured Routing through Multi Stage Authentication in MANETs, International Journal of Computer Science and Network Security, 2014.

[15] A.Janani et.al, "Survey of packet dropping attack in manet", Indian Journal of Computer Science and Engineering, 2014.

[16] Sagar Patolia, Harmandeep Singh, "Review of Isolate and Prevent Selective Packet Drop Attack In MANET", International Journal of Innovative Research in Science, Engineering and Technology, 2014.

[17] Anubha Goyal, "Selective Packet Drop Attack in MANET- A Review", A Monthly Journal of Computer Science and Information Technology, 2014.

[18] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE, Volume 40, Number 10, 2002, pp 70-75.

[19] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.

[20] LathaTamilselvan and V Sankarnarayana, "Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp. 13-20.

[21] N.Bhalaji and Dr.A.Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", Journal of Software, Vol. 4, Number 6, August 2009, pp. 536-543.

[22] http://virtual.cpcc.edu/content/web/110/ntf/chapterlessons/NTF_lesson1_files/image049.jpg

[23] Bhavik Panchal, "Survey Paper For Detection Of Malicious Nodes In Routing Of Mobile Ad-Hoc Network", International Journal of Engineering Research and General Science, 2015.

[24] Gajiyani Rizwana, Ghada Wasim, "Enhanced Intrusion Detection & Prevention Mechanism for Selfishness in MANET", International Journal of Innovative Research in Computer and Communication Engineering, 2015.

[25] Dr. S.S.Dhenakaran, A.Parvathavarthini, "An Overview of Routing Protocols in Mobile Ad-Hoc Network", nternational Journal of Advanced Research in Computer Science and Software Engineering , 2013.

[26] Santosh Kumar & Suveg Moudgil, "Detection of selfish node in DSR based MANET using reputation based scheme", International Journal of Research in Engineering & Technology, 2014.

[27] Bhavik Panchal, "Survey Paper For Detection Of Malicious Nodes In Routing Of Mobile Ad-Hoc Network", International Journal of Engineering Research and General Science, 2015.

[28] Sheethal Sunny, Dr.C.D.Suriyakala, "Performance Analysis of Selfish Nodes in Mobile Ad-hoc Networks", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2014.

[29] Santhosh Kumari D, Thirunadana Sikamani K, " Revival of selfish nodes in clustered Manet", International Journal of Advances in Engineering & Technology, 2015.

[30] V.Pavani1, T.Rama Mohan2, A.Vijay Kumar, "Managing selfish nodes through node cooperative incentives in MANETS", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2013.

[31] Gayathry S S, R N Gaur, "Handling Selfishness in MANETs – A Survey", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2014.

[32] Gajiyani Rizwana, Ghada Wasim, "Enhanced Intrusion Detection & Prevention Mechanism for Selfishness in MANET", International Journal of Innovative Research in Computer and Communication Engineering, 2015.

[33] Vaibhav V. Bhujade, Deepak Chaudhary, Suraj V. Raut, "A Review Paper on Behavior of Node in MANET", International Journal on Recent and Innovation Trends in Computing and Communication, 2015.

[34] N.Sridivya, I.Sibiya, D.Suvitha, A.Ashokraj, " Intrusion Detection of Selfish and Malicious Nodes in Manets", National Conference on Research Advances in Communication, Computation, Electrical Science and Structures, 2015.

[35] Gaurav, Naresh Sharma, Himanshu Tyagi, " An Approach: False Node Detection Algorithm in Cluster Based MANET", International Journal of Advanced Research in Computer Science and Software Engineering, 2014.

[36] Mangesh M. Ghonge, Dr. P. M. Jawandhiya, "Survey on Selfish Node Detection System in MANETs", International Journal of Research in Advent Technology, 2015.

[37] Virali Girdhar, Gaurav Banga " A Incentive Based Scheme to Detect Selfish Nodes in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, 2015.

[38] Karuturi Satish, K. Ramesh et al., "Intrusion Determent using Dempster-Shafer Theory in MANET Routing", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 1, pp. 37-41, 2015.