INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 2, Issue 4 April 2016.

Prevention of ICMP Based Attack Using Leader Election Based Algorithm with MAC Authentication

Nitin Kumar Gohal [a], Ranbir Singh [b]

[a]M.Tech Student, SUSCET Tangori, Nitin_taurous@yahoo.com
[b]Assistant professor, SUSCET Tangori

ABSTRACT

A mobile ad hoc network (MANET) is a wireless network that uses multi-hop peer-to-peer routing instead of static network infrastructure to provide network connectivity. There are no fixed routers- instead each node acts as router and forwards traffic from other nodes. We classified the number of attacks in the subsections and draw selfish node attack only. The selfish node interprets the packet data unit (PDU) and extracts the useful information, other unused information dropped in the wireless link. This attack degrades the performances of the network with increase of network load and delay. We here propose the system of MAC authentication by the Leader node of the network to prevent the Selfish Node entering the Network. The performance of the proposed algorithm herein is studied by simulating the Ad-Hoc based networks. The Simulation programs are using the OPNET, and the simulation scenarios present metrics of Network delay, Throughput and Network load

Keyword: MANETs, AODV, Leader Node, Selfish Node, Security

.

1. INTRODUCTION

The Internet Engineering Task Force has defined a Mobile Ad hoc Network (MANET) as: “An autonomous system of mobile routers (and associated hosts) connected by wireless links--the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet”.

The Mobile Ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration.. Under these circumstances, routing is much more complex than in conventional (static) networks. Many of the possible solutions are determined by the characteristics of the media, the behavior of nodes and the data flow. For a successful deployment, this is an important problem, since a wrong choice may have a severe impact on the performance, and consequently on the acceptance of the new technology. Also, providing just any protocol is not feasible, due to the different requirements on hardware and lower network layers.

1.1 Mobile Ad hoc network

A mobile ad hoc network is a collection of wireless mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. There are some unique characteristics of mobile ad hoc networks first, the connections between network nodes are wireless, and the communication medium is broadcast. The wireless connection provides the nodes with freedom to move, so the mobile nodes may come together as needed and form a network, not necessarily with any assistance from the cable connections. Second, unlike traditional wireless networks, mobile ad hoc networks do not have any fixed infrastructure. It is only a collection of self-organized mobile nodes, which are connected through high-variable quality links. Thus, the network topology is always changing; the execution context is extremely dynamic. In Latin, ad hoc literally means "for this purpose only," and usually means temporary. The interconnections between mobile ad hoc network nodes are not permanent; they are capable of changing on a continual basis to adapt this dynamically and arbitrarily pattern. Third, the membership is always changing. The mobile nodes are free to move anywhere, leave at any time and new nodes can enter unexpected. There is no mechanism to administrate or manage the membership. Fourth, the execution environment is insecure and unfriendly. Due to the lack of fixed infrastructure and administration, there are increased chances malicious nodes can mount attacks. Also, nodes may behave selfishly and result a degradation of the performance or even disable the functionality. Finally, the nodes in a mobile ad hoc network are usually portable mobile devices with constrained resources, such as power, computation ability and storage capacity.

1.2 Classification of mobile ad hoc network

Current researches classify mobile ad hoc networks into two categories. The first one is called a managed environment, where a common, trusted authority exists to provide certain services, such as a certificate authority. Another is called open environment, where a common authority that regulates the network does not exist. It is also referred as full self-organization environment, namely the network has the ability to work without any external management and configuration. Extensive work has been done recently in both areas

1.3 Security goals and threats

In mobile ad hoc networks, all networking functions, such as routing and packet forwarding, are performed by the nodes themselves in a self-organizing manner. For this reason, such networks have increased vulnerability and securing a mobile ad hoc network is very challenging. The following attributes are important issues related to mobile ad hoc networks, especially for those security-sensitive applications:

- Availability ensures the survivability of network services despite denial of service attack.
- Confidentiality ensures that certain information is never disclosed to unauthorized entities.
- Integrity guarantees that a message being transferred is never corrupted.
- Authentication enables a node to ensure the identity of the peer node it is communicating with.
- Non-repudiation ensures that the origin of a message cannot deny having sent the message.

Because of the nature of ad hoc, it is extremely difficult to achieve the above security goals in mobile ad hoc networks. Threats that mobile ad hoc networks have to face can be classified into two levels: attacks on the basic mechanism and attacks on the security mechanism. The vulnerability of the basic mechanism includes:

- Nodes risk being captured and compromised.
- Algorithms are assumed to be cooperative, but some nodes may not respect the rules.
- Routing mechanisms are more vulnerable.

Vulnerability of the security mechanism includes:

- Public key can be maliciously replaced.
- Some keys can be compromised.
- The trusted server can fall under the control of a malicious party.

Though physical layer or link layer are also vulnerable to malicious attacks, the attacks can be limited by lower-layer mechanisms such as the spread-spectrum technology or the WEP protocol. In this survey, we will focus on security issues of network layer in mobile ad hoc networks, especially on secure routing and node cooperation.

2. AODV PROTOCOL

Charles E. Perkins et al. proposed the Ad hoc On-demand Distance Vector routing protocol (AODV). AODV builds routes using a route request/route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network.

As the RREQ travels from a source, a reverse path is set up automatically since each node records the address of the neighbor from which it received the first copy of the RREQ. The Route reply (RREP) create forward path so that each node establish and maintained the connection as long as both side synchronized terminate the connection.

AODV implements path maintenance to recover broken paths when nodes move. If the source node moves and the route is still needed, route discovery is re-initiated with a new route request message. If the destination node or an intermediate node along an active route moves, the node upstream of the link break deletes the routing table entry for this destination and broadcasts a route error message, which is a special RREP, to all active upstream neighbors.

3. LEADER NODE ELECTION

Leader election is a fundamental problem in distributed systems and is a useful building, especially in ad hoc networks where failures are considered the norm and not the exception. Leader election is required in many applications, for example, when a mutual exclusion application is blocked because of the failure of a token holding node. It is also required in a group communication service, key distribution and management and routing coordination. The classical property of the leader election problem in distributed systems with a fixed number of nodes states that eventually there is a unique leader. When a network partitioning occurs, the network component will be without a leader until a partitioning is detected and the leader election process terminates. In the same way, when two network components merge, there will temporarily be two leaders in the resulting network component. Thus, the leader election problem definition should slightly be modified to be the following: every connected component will eventually have a unique leader. It uses three types of messages, viz. Election, ACK and Leader. The algorithm works as follows:

Election: If a leader node doesn't exist in the network, an initiator node transmits Election message to the immediate neighbor nodes. The neighbor nodes propagate the messages to their neighbors. This process is continued until all leaf nodes get the Election messages. This phase is referred as the growing phase of the spanning tree.

ACK: When any node receives an Election message from a neighbor (not parent), it immediately responds with an ACK message. Instead of sending ACK message to its parent, a node waits until it receives ACK from all its children. On receipt of the Election message, every leaf node sends an ACK message along with its own ID, to its parent. The parent node compares its own ID with these incoming IDs from all its children. Then it selects the highest one and sends it through the ACK message to its parent. This process is continued until the initiator node gets all ACK frames from all children. This phase is referred as the shrinking phase of the spanning tree.

Leader: When the initiator node gets ACK messages from all its children, it selects the highest ID as the leader node. It then broadcasts this ID in the Leader message to all nodes of the network. Figure 1 shows an example of such leader election. In figure 1(a), node 3 is the initiator that sends Election (E) message to its neighbor. In figure 1(b), nodes 2 and 5 set their pointers to point to parent node 3. They get Election messages from each other and immediately acknowledged. Immediate acknowledgements are not shown in the figure. In figure 1(c), a complete spanning tree is created. In figure 1(d), nodes 7 and 9 send their ACK messages (A) to their parents with their own IDs. In figure 1(e), nodes 2 and 5 compare their own IDs with the incoming ones and send the higher IDs in ACK to node 3. In figure 1(f), node 3 selects 9 as the leader ID and broadcasts it via the Leader message (L).

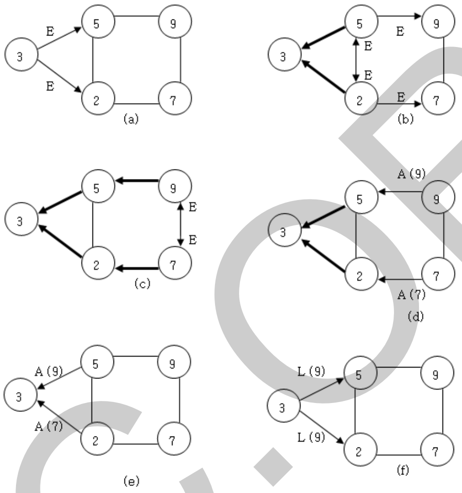

Fig. 1 an execution of leader election algorithm based on Dijkstra-Scholten termination detection algorithm

If the leader node crashes or goes out of the network, a new leader election is necessary for that network. The leader node of a connected network periodically (after each 20 seconds) sends heart-beat-messages to other nodes. The absence of heart-beat-messages from its leader for a predefined timeout period (6 times) triggers a fresh leader election process at a node.

4. EXPERIMENTAL TEST-BED

The OPNET provides better support on mobile Ad-Hoc networks and it has capability to support both IP version 4 and Version 6 addresses. Here, in the proposed Mobile Ad-Hoc network scenario we assign the Internet protocol version 4 addresses to different clients and base station. The model depict in the figure 2 prevent ICMP attack which already shown in previous work [5]. The Leader election algorithm given in the above said section in this paper has been implemented in this scenario for improving the performance of the network and preventing ICMP attack. The constant bit rate traffic (CBR) is used in this scenario

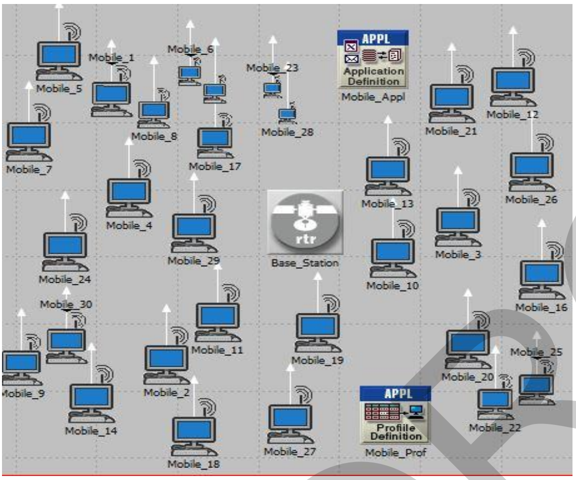

Fig.2: Attack Prevention Model

This simulation models prevent ICMP Attack with studied features were same as discussed in previous research paper [5]; but the nodes extend to 29.

5. RESULTS AND DISCUSSIONS

The experimental results discussed in the section 5.1, 5.2 and 5.3.

5.1 Network delay: We analyzed the load distribution in the network in order to get more information about the working behavior and preventing ICMP Attack and thus to identify Network delay shown in figure 3. The network delay less than 0.00035 seconds with overall running the OPNET simulation is 1000 seconds. The network delay as very less when leader election algorithm has been used.

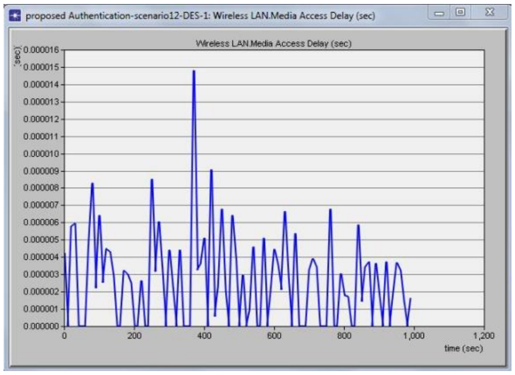

Fig.3: Network Delay

5.2Throughput: The wired and wireless scenario depends on media and resources. All the traffic passes through the media, so that clients are accessing for transporting data. If the current media is not available for transporting data then all the traffic suffers and resultant throughput decreases. The congestion on the network was less in the current scenario and achievable throughput is 600,000 bits/second.

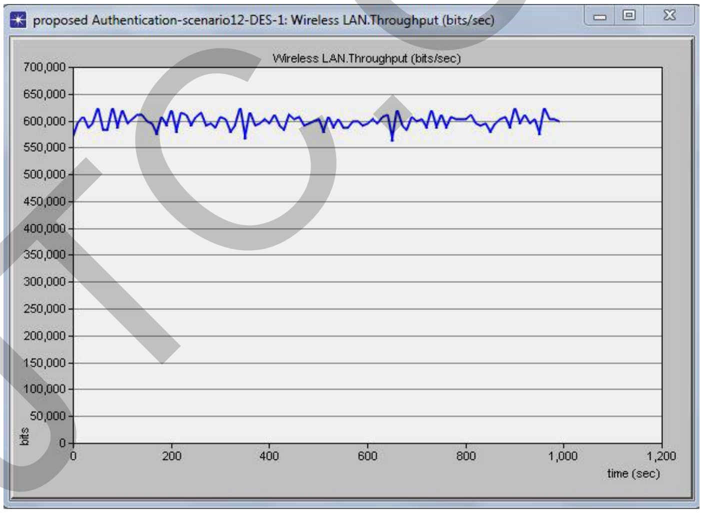

Fig.4: Throughput of MANET

5.3Network Load: In figure 5 depicted that 1200 s simulation pattern increases the network load utilization up to 20 percent.

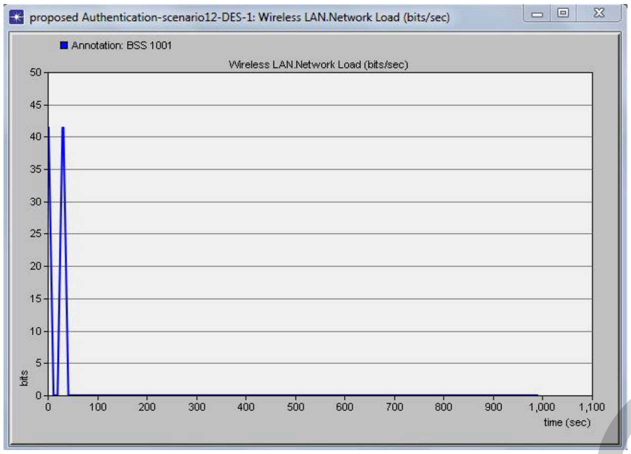

Fig.5: Network Load

This means it increases the performances of the network and the network delay inversely proportional to the network load. As the load increases in the network scenario the delay increases per routing payload. The number of unnecessary routing requests increases towards base station and overall performance of the network exponentially down but in this case the delay doesn’t affect the performance of the network.

6. CONCLUSION

The performance of the proposed algorithm herein is studied by simulating the Ad-Hoc based networks. The Simulation programs are using the OPNET, and the simulation scenarios present metrics of Network delay, Throughput and Network load. This approach requires much spare capacity of bandwidth to protect ICMP networks. After evaluation of ten times in the current scenario improve the performances of the previous paper [5].The other contribution for the proposed algorithm is to create new path to authenticate the clients on the same scenario by confirmation of MAC based address. Additionally, one link fails, and prior to this link being repaired, another link fails. If multiple links fail in the MANETs, they are repaired independently. The simulation results reveal that the proposed mechanism has greater performance and may involve cooperating network management.

REFERENCES

[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, “EAACK—A Secure Intrusion-Detection System for MANETs” IEEE transactions on industrial electronics, 2013,pp 1089-1098.

[2] SudarshanVasudevan, Jim Kurose, Don Towsley, “Design and Analysis of a Leader ElectionAlgorithm for Mobile Ad Hoc Networks", IEEE International Conference on Network Protocols, 2011, pp.34-39.

[3]Naveen Kumar Gupta, Ashish Kumar Sharma, Abhishek Gupta,“Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS) IJRREST, 2012,pp 31-34.

[4] Shailender Gupta, C. K. Nagpal, CharuSingla," Impact Of Selfish Node ConcentrationIn Manets",IJWMN,2011,pp.29-37.

[5] Nitin Kumar Gohal,Ranbir Singh “Simulation Modelling of Selfish Node Attack Using ICMP Protocol (IJARCET) Volume 3 Issue 12, December 2014

[6] MeeraGandhi,S.K.Srivatsa, "Detecting and preventing attacks using network intrusion detection systems",IJCSS,pp.49-60.

[7] Chun-Ta Li,Chou-Chen Yang,"A secure routing protocol with node selfishness resistance in MANETs", International journal of Mobile Communications,2012,pp.103-118.

[8] DjamelDjenouri, Nadjib Badache, “MANET: Selfish Behavior on Packet Forwarding” Encyclopedia of Wireless and Mobile Communications,2008,pp.576-587.

[9] Abdelouahid Derhab and Nadjib Badache“ A Self-Stabilizing Leader Election Algorithm in Highly Dynamic Ad Hoc Mobile Networks” IEEE Transactions on Parallel and Distributed Systems, VOL. 19, NO. 7, JULY 2008