Security In Multicast Mobile Ad-Hoc Networks

Mrs.N.Shanthi
National Engineering College,
Kovilpatti, TamilNadu, India.

Dr. L.Ganesan
Prof. and Head/CSE dept
Alagappa chettiar college of Engg. and Tech.,
Karaikudi, India

Summary

A Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes or terminals which communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Nodes in ad-hoc networks play both the roles of routers and terminals. Moreover, the routing path in ad-hoc networks is dynamic; it is not fixed as in wired networks. Therefore, some security mechanisms used in wired networks cannot simply be applied to protocols in ad-hoc networks. After analyzing various types of attacks against ad-hoc networks, a secure scheme for the famous routing protocol, MAODV (Multicast Ad-hoc On-Demand distance Vector routing protocol) is proposed. To guarantee the integrity in ad-hoc networks, Secure Hash Algorithm-1 (SHA-1) is used. Furthermore, NS2 (Network Simulator) software is used to simulate this scheme and performance analysis are made.

Key words: *MAODV, SHA-1, NS-2, Integrity, Authentication*

1. Introduction

In a multi-hop mobile ad-hoc network, mobile nodes cooperate to form a network without using any infrastructure such as access points and base stations. Instead, the mobile nodes forward packets for each others allowing communication among nodes outside wireless transmission range. Examples of applications for ad-hoc networks range from military operation and emergency disaster relief to community networking and interaction among meeting attendees or students during a lecture. In these ad-hoc networking applications, security is necessary to guard the network from various types of attacks.

In ad-hoc networks, adverse nodes can freely join the network, listen to and/or interfere with network traffic, and compromise network nodes leads to various network failures [1]. Since routing protocols are a fundamental tool of network-based computation, attacks on unsecured routing protocols can disrupt network performance and reliability.

2. Group Communication

Multicasting is a more efficient method of supporting group communication, as it allows transmission and routing of packets to multiple destinations with fewer network resources. Multicasting can improve the efficiency of the wireless links, when sending multiple copies of messages, by exploiting the inherent broadcast property of the wireless medium when multiple mobile nodes are located within the transmission range of a node. Providing efficient multicasting over MANET faces many challenges, including dynamic group membership and constant update of delivery path due to node movement [2]. The following section covers the routing protocol namely MAODV (Multicast Ad-hoc On-Demand distance Vector routing protocol).

3. Multicast AODV Protocol

3.1. Route Discovery

MAODV routing protocol follows directly from unicast AODV, and discovers multicast routes on demand using a broadcast route discovery mechanism employing the same route request (RREQ) and route reply (RREP) messages that exist in the unicast AODV protocol [3]. A mobile node originates an RREQ message when it wishes to join a multicast group, or has data to send to a multicast group but does not have a route to that group. Only a member of the desired multicast group may respond to a join RREQ. If the RREQ is not a join request, any node with a fresh enough route (based on group sequence number) to the multicast group may respond. If an intermediate node receives a join RREQ for a multicast group of which it is not a member, or it receives a RREQ and does not have a route to that group, it rebroadcasts the RREQ to its neighbors.

As the RREQ is broadcast across the network, nodes set up pointers to establish the reverse route in their route tables. A node receiving an RREQ first updates its route table to record the sequence number and the next hop information for the source node. This reverse route entry may later be used to relay a response back to the source. For join RREQs, an additional entry is added to the multicast route table and is not activated unless the route is selected to be part of the multicast tree. If a node receives a join RREQ for a multicast group, it may reply if it is a member of the multicast group’s tree and its recorded sequence number for the multicast group is at least as great as that contained in the RREQ. The responding node updates its route and multicast route tables by placing the requesting node’s next hop information in the tables, and

Manuscript received July 5, 2008
Manuscript revised July 20, 2008

then unicasts an RREP back to the source. As nodes along the path to the source receive the RREP, they add both a route table and a multicast route table entry for the node from which they received the RREP, by creating the forward path (Fig.1).

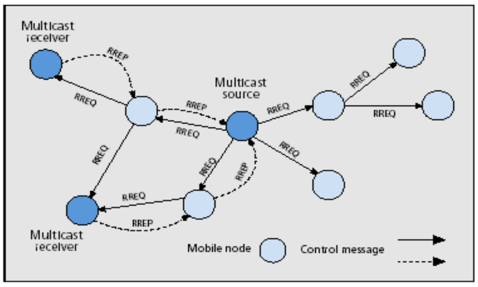


Fig.1 Route Discovery in MAODV

3.2. Multicast Route Maintenance

When a source node broadcasts an RREQ for a multicast group, it often receives more than one reply. The source node keeps the received route with the greatest sequence number and shortest hop count to the nearest member of the multicast tree for a specified period of time, and disregards other routes. At the end of this period, it enables the selected next hop in its multicast route table, and unicasts an activation message (MACT) to this selected next hop. The next hop, on receiving this message, enables the entry for the source node in its multicast routing table. If this node is a member of the multicast tree, it does not propagate the message any further. However, if this node is not a member of the multicast tree, it would have received one or more RREPs from its neighbors. It keeps the best next hop for its route to the multicast group, unicasts MACT to that next hop and enables the corresponding entry in its multicast route table. This process continues until the node that originated the chosen RREP (member of tree) is reached. The activation message ensures that the multicast tree does not have multiple paths to any tree node.

3.3. Group Leader in the Multicast Tree

The first member of the multicast group becomes the leader for that group, which also becomes responsible for maintaining the multicast group sequence number and broadcasting this number to the multicast group. This update is done through a Group Hello message. The Group Hello contains extensions that indicate the multicast group IP address and sequence numbers (incremented every Group Hello) of the multicast group

3.4. Link breakage in the network

Since ad hoc networks are highly dynamic by nature. The changes in the network topology may lead to two different situations*:* A link may be broken and the multicast tree may be partitioned. A node discovers a link breakage either actively or passively. Active discovery means that the MAC layer informs upper layers about reach ability problems. Passive discovery happens, if the node has not heard from it's neighbor for a while. In this case, it might try to ping the neighbor or ask a route towards it via RREQ.

Be it either case, when the node discovers connectivity loss with the multicast tree neighbor, if it is the downstream neighbor, it is responsible for correcting the situation. Now, the node sends a RREQ with a Multicast Group Leader Extension. This extension contains the old distance of the node to the group leader. Only multicast tree member nodes that have distance to the group leader equal or less than the one set in the extension may answer with RREP. This prevents the nodes on the same side of the break as the initiator of the RREQ from answering and thus creating possible loops. If the repair leads to a situation, where the node's new distance to the group leader is greater than the old one, and then it must inform its downstream nodes about this. This is done with MACT message where the update-flag is set. This MACT message is multicast to all of the tree members, also upstream. But upstream members see that this message comes from a downstream node and therefore discards the message.

3.5. Reconnecting the disconnected Link

When the node tries to reconnect the disconnected link and does not get an answer to the RREQ message number of retries times, then it must assume that the tree is partitioned. If this is the case and it is a member of the group, then it becomes a new group leader. It broadcasts group hello message with update-flag set indicating that there is a new group leader. However, if the node has multiple downstream nodes, then it selects any one of these and sends a MACT message with grpldr-flag set. This indicates that the receiving node should become group leader. If it is a group member, it becomes a leader, otherwise it continues seeking the leader with the previously described methods [4].When the group leader is finally found, it broadcasts group hello message with update-flag set to indicate that changes has occurred in the network. If the node trying to repair the break is not a multicast group member, then it must try to find a new group leader from the downstream nodes it has. If there is only one downstream node, then the node prunes itself from the tree.

4. Standard Security Services

The following are the standard security services [5].

Data Confidentiality: It is the property in which the information embedded in network traffic is prevented from unauthorized disclosure. Since one of the main reasons that an attacker can successfully attack network nodes and protocols is the leak of sensitive information such as passwords and configuration data, data confidentiality is a very important property of network security.

Data Integrity: It is the property in which the originality of the information transmitted over the network is ensured. It is often combined with data origin authentication since data integrity alone can not help receivers decide whether the received data are forged or have been tampered with.

Authentication: It is the property in which the identity of the connected entity (node) can be confirmed during connection phase (i.e., peer entity authentication), and the source of a message transmitted during the data transfer phase can be verified (i.e., data origin authentication).

5. Multicast Security in MANET

Integrity plays an important role in ad-hoc networks. To overcome man-in-the-middle attack in mobile-ad-hoc networks, SHA-1 algorithm is used. Normally, hop count field is mutable in nature. To protect this hop count value, hash values are found by using SHA-1 algorithm for those fields. Here, the packets are sent along with the hashed values of hop count field. Now, the malicious nodes, which forwards the false routing information, can be effectively defended [6].This algorithm takes input as source address, destination address and hop count with a maximum length of less than 2^{64} bits and produces output as a 160-bits message digest. The input is processed in 512-bits blocks. This algorithm includes the following steps [7].

Padding: The purpose of message padding is to make the total length of a padded message congruent to 448 modulo 512 (length = 448 mod 512). The number of padding bits should he between 1 and 512. Padding consists of a single 1-bit followed by the necessary number of 0-bits.

Appending Length: The 64-bit binary representation of the original length of the message is appended to the end of the message.

Initialize the SHA-1 buffer: The 160-bit buffer is represented by five four-word buffers (A, B, C, D, E) used to store the middle or finally results of the message digests for SHA-I functions and they are initialized to the following values in hexadecimal. Low-order bytes are put first:

Word A: 67 45 23 01
Word B: EF CD AB 89
Word C: 98 BA DC EF
Word D: 10 32 54 16
Wnrd E: C3 D2 El FO

Process message in 16-word blocks: The heart of the algorithm is a module that consists of four rounds of processing 20 steps each. The four rounds have a similar structure, but each uses a different primitive logical function. These logical functions are defined as follows:

```
Initialize hash value :
a := A
b := B
c := C
d := D
e := E
Main loop:
for i from 0 to 79
if 0 ≤ i ≤ 19 then
f := (b and c) or ((not b) and d)
k := 0x5A827999
else if 20 ≤ i ≤ 39
f := b xor c xor d
k := 0x6ED9EBA1
else if 40 ≤ i ≤ 59
f := (b and c) or (b and d) or (c and d)
k := 0x8F1BBCDC
else if 60 ≤ i ≤ 79
f := b xor c xor d
k := 0xCA62C1D6
```

The output of the fourth round is added to the input of the first round, and then the addition is modulo 2^{32} to produce the ABCDE value that calculate next 5l2-bits block.

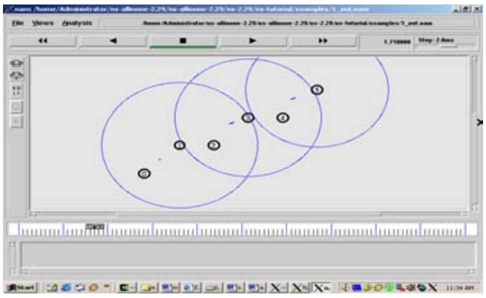
Output: After all 512-bits blocks have been processed, the output of the last block is the 160-bits message digest. These message digest values are sent along with the packets .So, the packets which are sent by malicious nodes are suppressed. Thus, the integrity is ensured.

6. Simulation Results

SHA-1 algorithm in MAODV protocol is simulated by using NS-2 (Network Simulator-2).

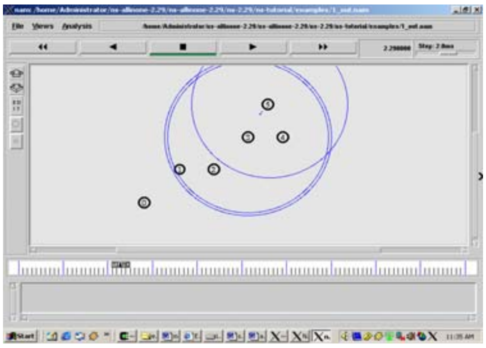
Scenario: 1

Scenario 1 depicts how unicast routing operation is performed in ad-hoc network from the source node 0 to the destination node 5.



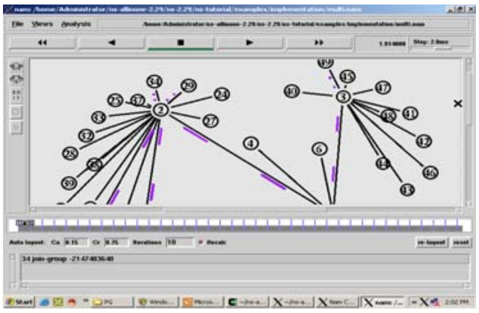
Scenario: 2

Scenario 2 depicts how the security is achieved by using SAODV protocol (Secure AODV) [8] during unicast operation.



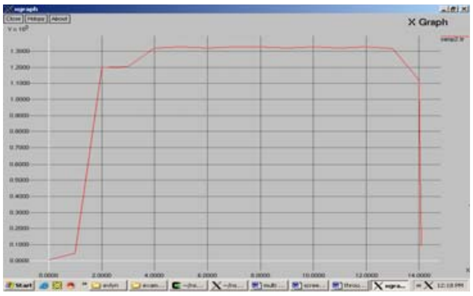
Scenario: 3

Scenario 3 depicts how the secured group communication takes place.



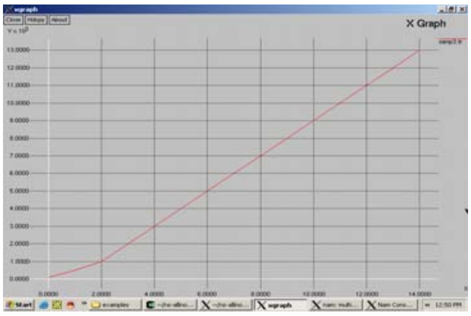
Scenario: 4

Scenario 4 denotes packet size vs end-to-end delay during group communication. Packet Size (bytes) values are given in x-axis and End-to-End Delay values are given in y-axis.



Scenario: 5

Scenario 5 depicts how the throughput is increased when the packets are transferred via the network during group communication. Packet Size (bytes) values are given in x-axis and average throughput of generating packets at node 0 is given in y-axis.



7. Conclusion and Future Work

The purpose of this paper is to find an efficient and secure communication in wireless ad-hoc networks. Here, SHA-1 algorithm is applied in MAODV protocol to achieve secure routing in MANET. There are still many problems such as tunneling attacks, selectively drop packets; etc are still persist in these ad-hoc networks. As future work, this project can be extended to solve those attacks.

References

[1] Carlos De Morais Cordeira, Hrishikesh Gossain and Dharma P. Agarwal, “Multicast Over Wireless Mobile Ad-Hoc Networks: Present and Future Directions” IEEE Network, 2003, pp 2-9.

[2] Charles E. Perkins, Elizabeth M.Royer, SamirR.Das and Mahesh K.Marina, “Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks”, IEEE Personal communications, 2001, pp 16-28.

[3] Perkins and E M Royer “Ad hoc On Demand Distance Vector Routing” Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp 1-10.

[4] Li Xiao Abhishek Patil, Yunhao Liu, Lionel M. Ni, Abdol - Hossein Esfahanian, “Prioritized Overlay Multicast in Mobile Ad Hoc Environments” IEEE Computer Society, 2004, pp 67-74.

[5] Lodong and Zygunt “Securing Ad Hoc Networks” IEEE Network, 1999, pp 24-30.

[6] Junaid Arshad and Mohammad Ajmal Azad, “Performance Evaluation of Secure on-DemandRouting Protocols for Mobile Ad-hoc Networks”, IEEE Network, 2006, pp 971-975.

[7] Dai Zibin and Zhou Ning, “FPGA Implementation of SHA-1 Algorithm”, IEEE 2003, pp 1321-1324 .

[8] Muhammad Asfand e-Yar and Muhammad Sher, “ Secure Route Path Formation in Ad-Hoc On-demand Distance Vector Routing”, Information Technology Journal on Asian Network for Scientific Information, vol. 3, pp 142-145

[9] Jiejun,Petros, Luo,Lu and Lixia “Providing Robust and Ubiquitous Security support for Ad-hoc networks”, IEEE 2001, pp 251-260.

[10] Panagiotis Papadimitratos and Zugmunt J. Haas, “ Secure Routing For Mobile Ad-Hoc Networks”, Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, (CNDS 2002), pp 1-13.