Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 88 (2015) 36561-36564

ISSN: 2229-712X

An approach to Handle Man in Middle Attack in Cluster based Architecture

Avinash Jethi[1] and Seema[2]

[1]Department of Computer Engineering, Bhai Gurdas Institute of Engg and Technology, Sangrur.

[2]Yadavindra College of Engineering, Guru Kashi Campus,Talwandi Sabo.

ARTICLE INFO

Article history:

Received: 05 July 2012;

Received in revised form:

18 November 2015;

Accepted: 23 November 2015;

Keywords

Adhoc networks,
Authentication,
Attacks,
Delay Time,
Security.

ABSTRACT

This paper presents wireless ad hoc network which communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. The principle behind ad hoc networking is multi-hop relaying, which means that the messages are transmitted by the other nodes if the target node is not directly reachable. For communications with the nodes which are not within the radio range of nodes to the route must be taken from the intermediate nodes to reach the destination. These intermediate nodes acts as router which receives the data coming from the source and forwards the data to destination This situation is of potential security concern as there can be attack possible by the intermediate node like Man in Middle Attack. Hence an authentication procedure is be used for authenticating the mobile nodes to each other and proper encryption decryption mechanisms is also employed. Also intermediate nodes can act as malicious nodes which must be removed or alternate route should be found which does not include nodes already used in previous route. Thus we have developed architecture will provide secure routing mechanism which will use two kinds of encryption techniques. Then the possible attacks are being analyzed and removed from the architecture.

© 2015 Elixir All rights reserved.

Introduction

A wireless ad hoc network 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. The principle behind ad hoc networking is multi-hop relaying, which means that the messages are transmitted by the other nodes if the target node is not directly reachable.

Due to these issues such as shared physical medium, lack of central management, limited resources, no fixed and highly dynamic topology, ad hoc networks are much more vulnerable to security attacks.

In an Ad Hoc network each mobile node discovers the neighbor nodes which are within communication range and establishes direct communications paths with the nodes in the range. For communications with the nodes which are not within the radio range of nodes to the route must be taken from the intermediate nodes to reach the destination. These intermediate nodes acts as router which receives the data coming from the source and forwards the data to destination This situation is of potential security concern as their can be attack possible by the intermediate node.. Here is where an authentication procedure must be used for authenticating the mobile nodes to each other. Also the secure routing procedures must be used and proper encryption decryption mechanisms must be employed.

Security Requirements:

The security requirements of MANETs are similar to that of other networks. They can be briefly summarized as follows:

- **Access control:** The need to restrict access of network resources to the authorized entities and the unauthorized entities must be restricted from the use of the network resources.
- **Authentication:** The authentication scheme must be such that it properly identifies the node and checks for the authenticity of the node and also checks that the node is actually the same to which it claims to be. The mechanism must also check that the data packets that are coming are from the source from which it are supposed to come from.
- **Integrity:** Integrity ensures the data to be in its original form as it starts from the source. It ensures that data is not being tampered on the way from source to destination.
- **Confidentiality:** It ensures that data from source to destination goes in such a way that no other node on the way can have access to the data and only the authorized entity for which the data has been intended to reach can have the access to the data. To ensure confidentiality proper encryption decryption mechanism must be employed.
- **Availability:** Network resource must be available to only the authorized entities without much delay.

Attack Categories on Ad Hoc Networks

The nodes in the Ad Hoc network are connected through the wireless range that every mobile nodes and due to this they form a topology. Also in Ad Hoc network nodes can move at any time resulting in the change of the neighbor and so because of this mobility the network topology changes.

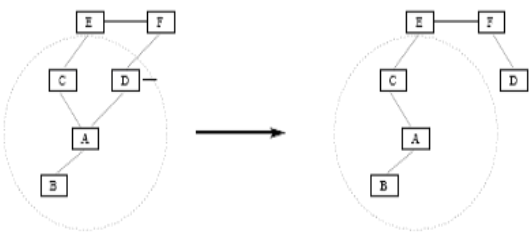

Figure shows the topology change by the movement of the nodes

Tele:

E-mail addresses: avinashjethi@ymail.com

© 2015 Elixir All rights reserved

Due to this continue mobility and change in the network topology there are various attack possible on the networks. These attacks are divided in two categories:

1. ACTIVE
2. PASSIVE

Active Attacks

Active attacks are those in which the attacker actually disrupts the traffic or send bogus packets to the destination node. Some of active attacks are explained below:

Modification Attacks: Attacks using modification are generally targeted against the wholeness of routing calculations and so by modifying routing information an attacker can cause network traffic to be dropped, redirected to a different destination, redirected to take a longer route to the destination increasing communication time and send back to such a node creating loopback in the communication .

- The black and grey hole attacks are launched by modifying the routing packets to point to a particular node, which in turn drops or forwards packets at its own judgment.
- Routing loop attacks takes place in by modify routing information in such a way that routing packets take such a path that the packets traverse a cycle, so the packets will keep on traversing in a circle and don't reach their intended destination.
- In increase in route length attack routing information is modified in such a way that routing packets take a longer path to the destination. This attacker in such cases are the compromised nodes that lies in the path from source to destination and compromised nodes send packets to a route longer that the shortest path possible.
- In Battery Exhaustion Attack routing packets are modified in such manner that the network traffic is concentrated towards a single target node. This node's battery will be consumed in receiving excess packets.

Fabrication Attack: Fabrication attacks are performed by generating false routing messages. These attacks are difficult to recognize as they are received as genuine routing packets. The rushing attack is a typical instance of malicious attacks using fabrication. This attack is targeted against on demand routing protocols that use duplicate containment at each node. An attacker quickly disseminates routing messages throughout the network, suppressing any later genuine routing messages when nodes drop them due to the duplicate suppression. Similarly an attacker can nullify a working route to a destination by fabricating routing error messages claiming that a neighbor can no longer be contacted.

Impersonation Attack: A malicious node can launch many attacks in a network by masquerading as another node (spoofing). Spoofing occurs when a malicious node misrepresents its identity by altering its MAC or IP address or ID in order to alter the change the look of the network topology to the other nodes. As an example, a spoofing attack allows the creation of loops in routing information collected by a node with the result of partitioning the network.

Passive Attacks: In passive attacks the attacker does not perturb the routing protocol. Instead, it only eavesdrops on the routing traffic and tries to extract valuable information like node hierarchy and network topology from it. For example, if a route to a particular node is requested more frequently than to other nodes, the attacker might expect that the node is significant for the operation of the network, and disabling it could bring down the entire network. Likewise, even when it might not be possible to isolate the exact position of a node, one may be able to find out information about the network topology by analyzing the contents of routing packets. This attack is virtually impossible to detect in the wireless environment and hence also extremely difficult to prevent.

Man in Middle Attack

The major attack on the mechanism is the main in the middle attack. The attack could be on the routing mechanism that is being followed for communication between the two nodes. A node can be compromised at any time in the network which can also be full member in the network. Suppose that when the two nodes are communicating to each other they had to follow the route which is of shortest length to the destination and in the route lies the malicious node. The attack by a malicious node is possible in two ways:

1. The transfer of keys take place when the communication is needed b/w two nodes. So while transferring of public keys to each other. The middle node can impersonate the nodes by transferring its own public key to the nodes and can disclose the contents of communication which are not meant for it.
2. Second possibility is that the malicious nodes in the middle can disrupts the whole communication either in the start of the communication or in the middle of communication. Firstly node has to initialize the communication by sending the initialization request to the receiver which can be interrupted by the malicious node. Secondly while the communication starts then the malicious node can drop the packets and sender has no way to know that whether the packets are received or not.

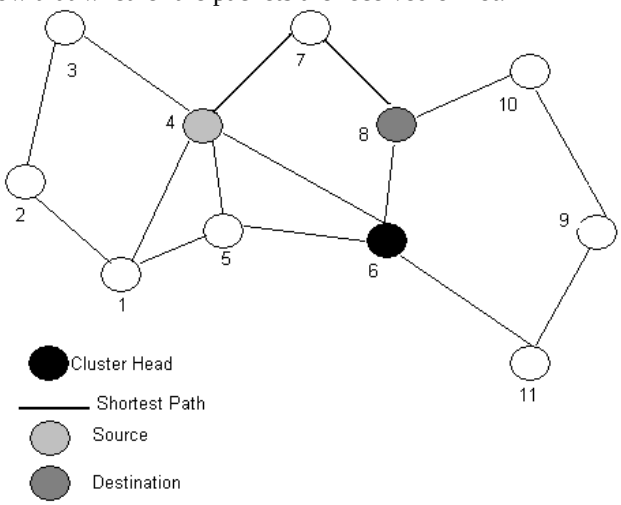

Figure shows the shortest path by dark lines from source to destination

Solution

In the routing mechanism used the route taken to receiving node is shortest path and malicious node resides in the route. The scheme is as that each node must find alternate path to the destination node which is not the shortest path.

The solution to the problem works in two phases:

1. Finding the shortest route to the destination
2. Finding the alternative path that does not involve any of the nodes that lies on the way to shortest path. After that getting the acknowledgement from that path about the ongoing communication.

Shortest Path Algorithm

1. Input to the algorithm is the N×N matrix that is the distance matrix generated at the start of the algorithm.
2. Define an array that will store the distance and a matrix that will store the whole route.

3. Generate the neighbor list for the source node and put in the matrix
4. Starting from the first neighbor generate the next neighbor.
5. Check if that neighbor already exist in the list if yes than it is a loopback and goto step5
6. Generate the route from all the neighbors for the destination and continue on that path.
7. Generate the route to destination from all neighbors where ever possible.
8. Compare the route length generated by all the possible routes. Compare all the routes in the distance matrix and choose the path to destination which has the lowest path length.
9. If there is no route possible to destination then print not found and exit else print the path which has lowest path length.

The shortest path algorithm is the basis for finding out the alternative path. The output path that is being generated after running the shortest path algorithm is being passed to the alternate path algorithm that generates the alternative path.

Algorithm to Find Alternate Path

1. Establish a network for any number of nodes.
2. Generate an N×N matrix and initialize all the elements of matrix with 0.
3. Calculate the distance from one node to all other nodes and store in an N×N matrix.
4. Give the range of the network node and set all other elements that are outside the range to 0.
5. for (i=0;i<n;i++)

```
{
   for (j=0;j<n;j++)
      {
         If j is neighbor of i
         Neighborarray[i][j]=1;
   }   }
```

Find the shortest path from source to destination.

6. Initialize the source node and put it in another array. Name the array as array [].
7. Search the neighbor list and pick a random node from the list and put that node in the array.
8. Compare the random node with all the elements of the shortest path array. If the array[top] element matches with any of the elements in the list then

```
Array[top]=0
Top=top-1
```

Make the entry corresponding to that node in neighbor array as 0 Goto step 5

10. Compare the neighbor list of the generated node with all element of array.

```
If all the neighbor matches
{
   Array[top]=0
   Top=top-1
   Make the entry corresponding to that node in neighbor array as 0
         Goto step 5
   }
   Else
      Pick a random node from the list and put it in the array
```

11. if array[top]=destination
then return route and exit
else Goto step 5

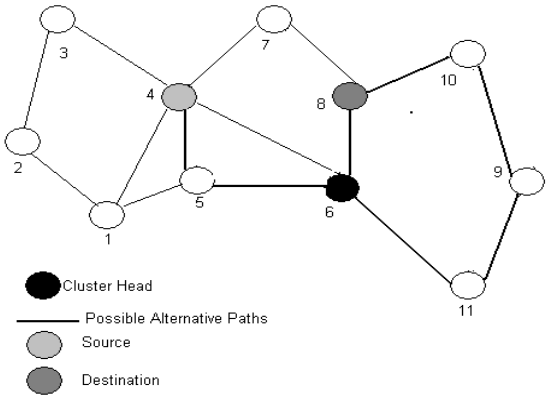

Figure shows the possible alternative paths that can be traversed to reach the destination.

Simulation And Results

Following table shows results of examples taken with their alternative route and delay time and also shortest path with their delay time.

No. of Nodes	No. of Edges	Shortest Distance(m)	Time Delay(sec)	Alt. Distance(m)	Alt. Time Delay(sec)
3	3	(1:3) 12	1.970	(1:2,2:3) 15	2.463
3	3	(1:2,2:3) 15	2.463	Does not exist	-
4	5	(1:3, 3:4) 15	2.463	Does not exist	-
4	6	(1:3,3:4) 15	2.463	(1:2,2:4) 16	2.627
5	7	(1:3,3:4,4:5) 11	1.806	(1:2,2:5) 13	2.134

References

[1] Lijun Qian and Ning Song(2006), " Secure Anonymous Routing in Clustered Multihop Wireless Ad Hoc Networks" , IEEE, pp.1629-1634.

[2] Marianne A. Azer, Sherif M. El-Kassas nad Magdy S. El-Soudani, "Security Schemes in AD HOC Networks a Survey and New Challenges" ,Ubiquitous Computing and Communication Journal, pp.1-8.

[3] Kalpana Sharma, M.K. Ghose, Deepak Kumar, Raja Peeyush Kumar Singh and Vikas Kumar Pandey(2010), "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", International Journal of Advanced Science and Technology, Vol. 17,pp.31-44.

[4] Ejaz Ahmed, Kashan Samad, Waqar Mahmood(2006), "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks", R&D Stream, pp.46-56.

[5] Rajani Poosarlat, Hongmei Dengt, Alok Ojhatt and Dhanna P. Agrawalt(2004), In Proceedings of IEEE, pp.171-175.

[6] Joydeep Chandra, Lisham Lekhendro Singh(2005), "A Cluster Based Security Model for Mobile Ad Hoc Networks", In Proceedings of IEEE, pp.413-416.

[7] Elisavet Konstantinou(2008), "Cluster-based Group Key Agreement forWireless Ad hoc Networks", in Proceedings of IEEE(The Third International Conference on Availability, Reliability and Security) , pp.550-557.

[8] M.-H. Guo, H.-T. Liaw , D.-J. Deng and H.-C. Chao(2010), "Cluster-based secure communication mechanism in wireless ad hoc networks", The Institution of Engineering and Technology, Vol. 4, pp. 352–360.

[9] Sharvani G S, Cauvery N K and Dr.Rangaswamy.T(2009), "Adaptive Routing Algorithm For MANET:TERMITE", International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, pp.38-43.

[10] Sumit Arora Hyunyoung Lee Ramakrishna Thurimella, "Algorithms for Finding Disjoint Paths in Mobile Networks", NSF,pp.1-10.
[11] V.G.Rani and Dr.M.Punithavelli(2010), "Optimizing On Demand Weight -Based Clustering Using Trust Model for Mobile Ad Hoc Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.4,pp.81-91.
[12] An Huiyao, Lu Xicheng, and Peng Wei, "A Cluster-Based Multipath Routing for MANET", In Proceedings of National momentous foundation research task and National natural science fund, pp.405-413.
[13] Mamoun Hussein Mamoun(2011), "A New Reliable Routing Algorithm for MANET", International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 2, No. 3,pp.638-642.
[14] Chunxue Wu, Fengna Zhang, Hongming Yang(2010), "A Novel QoS Multipath Path Routing in MANET", International Journal of Digital Content Technology and its Applications, Volume 4, Number 3.
[15] T. Senthil kumaran and V. Sankaranarayanan(2011), "Early Congestion Detection and Optimal Control Routing in Manet", European Journal of Scientific Research, Vol.63 No.1, pp. 15-31.
[16] Stephen Mueller, Rose P. Tsang and Dipak Ghosal, "Multipath Routing in Mobile Ad Hoc Networks:Issues and Challenges", In Proceedings of Sandia National Laboratorie(USA)