A Review on Mobile Ad Hoc Networks Security Using Alternate Path Routing

Deepa Rathore
Assistant Professor
Department of Computer science and engineering
Sandip Institute of Technology and Research Centre (SITRC)
Corresponding Author's E-mail: *deepa841@gmail.com*

Abstract

Mobile ad hoc networks (MANETs) are made up of a collection of self-configuring wireless mobile nodes with no network infrastructure. The meaning of accountability is apparent: in a mobile ad hoc network, there is no clear assured border that can be combined or compared to a defined line in a traditional wired network. Invader attacks on these ad hoc networks are on the rise right now. Various algorithmic implementations are done to transport data over the network to avoid data breach to avoid the occurrence of these attacks. The design of MANETs raises a number of difficulties. We must provide maximal capability as well as security to these ad hoc networks in order to ensure secure communication. The shortest path algorithm is employed to provide these safeguards, however there are a number of other concerns that arise as a result of this algorithm's lack of security and efficiency, such as invader assault and concentrated load. We're looking for the Invader Safe path that's closer to the shortest than the shortest. These networks are very dynamic, mobile, and large-scale, yet they also provide static coercion, which is a source of power.

Keywords: *Security, Manet, Routing, MaxLen*

INTRODUCTION

There aren't a lot of access points in ad hoc networks that can provide any information to the members, therefore it behaves like a LAN. A LAN is a network that is created by randomly connecting various devices.

Page 50-54 © MANTECH PUBLIATIONS 2021. All Rights Reserved

Communication in MANETs is accomplished through the use of a wireless media. It can be claimed that MANETs have a dynamic topology since nodes are mobile and uncertain about their arrival or departure. Because they are located within the transmission range, the nodes that transfer data are referred to as neighbours. As a result, data can be transmitted straight from one device to another. When one node sends data to another node that isn't a neighbour, the shortest path succeeding with several hops is generated by the smallest number of nodes.

Existing Work

Communication between two nodes is always possible via the shortest path, according to the conventional method. The shortest path has a number of advantages, including Data transport between nodes is fast and reliable, and the implementation is simple. Here's an example of a typical algorithm for finding the shortest path:

Path(A,n)

/* A is the Weighted graph of n size to represent theAdhoc Network*/

{

Step 1: Generate the neighbour list for the source node and put it in the matrix.

Step 2: Generate the next neighbour by starting with the first.

Step 3: check if that neighbor already exists in the list if yes than it is a loopback and go to end;

Step 4: Generate the route from all the neighbors for the destination and continue on that path.

Step 5: Generate the route to destination from allneighbors where everpossible.

Step 6: 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.

}

This approach of data transfer is quite shared in the case of dynamic topology one of them is the sensor network. But the chances of Data hack are quite large as the hackers use the same approach. This diagram depicts the fact and reliable path which is most used by the client and that is the shortest path but it has some of the security issues which are listed below

Proposed Work

In this section, we'll go through the process for secure data transmission in an

Page 50-54 © MANTECH PUBLIATIONS 2021. All Rights Reserved

ad hoc network via an alternate path. With the help of new substitute routing paths, a new routing topology is generated at each round of the network. The following parameters must be met in order to locate an alternate path:

Maximum path length (MaxLen)

MaxLen denotes the length of a path that has been decided to be satisfactory, and is defined as the total of edge weights wi in the provided path. The path length represents a variety of physical properties, including distance, cost, delay, and the possibility of failure. It can be described in a variety of ways, including as an integer or a float value. The path length will be the number of hops from the source to the desired destination if the value of wi= 1 is true for all edges.

Maximum Number of Hops on the path (MaxHop)

The maximum number of hops on a path is represented by MaxHop. If there are k nodes on a path, the hop number is k-1. The value of MaxHopi is an integer.

Maximum Number of Shared Edges (MaxSE)

Edge sharing across three routes, also known as common edges, is divided into two types: double- and triple-shared edges, respectively. The corresponding maximum permissible number of double- and triple-shared edges is denoted by the integer numbers MaxSEdbl and MaxSEtrito. When numerous pathways are used between two routers and good network dependability is required, this limitation is critical.

PathAtoB (A,n.a.n)

/* A is the Adjacency matrix illustration of Given network, n is the no of nodes and a,b are two nodes between we have to transferdata*/

{

Step 1: Give the range of the network node and set all other elements that are outside the range to 0.

Step 2: Find the Neighbour of Each node of network starting from node a to nodeb.

Step 3: Find the shortest path from source to destination and store it in an array called array[].

Step 4: Search the neighbour list and pick a random node from the list and put that node in the array.

Step 5: Compare the random node with all the elements of the shortest path array. If

Page 50-54 © MANTECH PUBLIATIONS 2021. All Rights Reserved

the array[top] element matches with any of the elements in the list then Make the entry corresponding to that node in neighbour array.

Step 6: Compare the neighbour list of the generated node with all the elements of array otherwise Pick a random node from the list and put it in thearray
}

Finally, for the case of unicast, a list of given shortest paths is shown. This pass is extremely close to the shortest path but does not include any nodes from the shortest path list, resulting in secure transmission on the algorithm implementation occurrence of the Intruder.

CONCLUSION

The relevance of MANET is well documented, and we cannot dispute it as the world of computing continues to become more portable and compact. MANETs, unlike wired networks, present a number of security difficulties because to their unexpected dynamic topology, wireless shared media, heterogeneous resources, and tight resource constraints, among other factors. The security research field for many of the solutions is still open because they are created with a small scenario, threats, and weaknesses in mind. We are here to provide a solution to some of the issues by which we can protect ad hoc networks from active intruder attacks via algorithmic solutions. Because of intruder attacks in the same area, the path chosen for data transfer in an ad-hoc network is almost always the shortest path. As a result, we've created a path where no node from their shortest path is included. As a result, it will undoubtedly provide a secure and efficient solution to data transfer in unicast ad hoc networks.

REFERENCES

1. Akyildiz IF, Weilian Su, Sankarasubramaniam Y et al. A Survey on Sensor Networks", in Proc. of the IEEE Communications Magazine 2002; 40(8): 102-114.

2. Jiang Q, Manivannan D. Routing Protocols for Sensor Networks", in Proc. of the IEEE Conference 2004; 93-98.

3. Lewis FL. Wireless Sensor Networks Smart Environments: Technologies, Protocols, and Applications", New York: ed. D.J. Cook and S.K. Das, John Wiley, 2004; 1-18.

Page 50-54 © MANTECH PUBLIATIONS 2021. All Rights Reserved

4. Pham NN, Youn J, ChulhoWon. A Comparison of Wireless Sensor Network Routing Protocols on an Experimental Testbed. in Proc. Of the IEEE International Conference on Sensor Networks, 2006; 35-42

5. Rakotoarivelo T, Senac P, Seneviratne A et al.Enhancing QoS through Alternate Path: An End-to-End Framework. in Proc. of the IEEE INFOCOM, Conference on Computer Communications, 2000; 14-22.

6. Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. University of California at Berkeley, Tech. Rep. F33615-01-C-1895.

7. Perrig A, Szewczyk R, Wen V et al. SPINS: Security Protocols for sensor networks", International Conference on Mobile Computing and Networking (Mobicom 2001), 2001: 189-199.

8. Wood AD, Stankovic JA. Denial of service in sensor networks", IEEE Computer 2002; 35(10): 54-62.

9. Dijkstra E. A note on two problems in connection with graphs. Numerical Mathematics 1959; 1:269-271.

10. Korkmaz T, Krunz M, Tragoudas S. An efficient algorithm for finding a path subject to two additive constraints, in Proceedings of the ACM SIGMETRICS '00 Conference 2000; 1: 318-327.

11. Sami S, Al-Wakeel, Saad A et al. PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks. in Proc. of the IEEE Communications Society 2007; 4159-4163.

Page 50-54 © MANTECH PUBLIATIONS 2021. All Rights Reserved