FUTURE TECHNOLOGY HORIZONS
SCIENCE TECHNOLOGY & INNOVATION JOURNAL
Journal homepage: http://www.Techhorizon.futureu.edu.sd

FUTURE UNIVERSITY- SUDAN
ISSN: 1858-6368

RESEARCH PAPER

AN ALGORITHM TO ENHANCE ROUTING AND SECURITY FOR WIRELESS MESH NETWORKS.

[a]Halima Muhammad Dalhat , [b]Ashraf Gasim Elsid
[(a)]*Postgraduate student at the department of telecommunication and space engineering, Future University – Sudan.*

Accepted 10 May 2016

ABSTRACT

Wireless mesh networks are vulnerable to malicious attacks due to the nature of wireless communication and the lack of centralized network infrastructure. Therefore, wireless mesh networks pose new challenges and call for more effective and applicable solutions. In this paper we proposed an algorithm for identifying intruder nodes when they attempt to intrude into the network by attacking routing protocol. In addition the research also proposed a procedure to find the node with the shortest distance.

KEYWORD: wireless mesh network, ad hoc network, security, intruder, shortest distance, routing protocol.

1. INTRODUCTION

Wireless Mesh Network (WMN) has emerged as a new technology to cope with the challenges of next-generation wireless networks, such as providing flexible, adaptive, and reconfigurable network architecture while offering inexpensive solutions to wireless Internet service providers (ISPs). ISPs are choosing WMNs to provide Internet connectivity to costumers as it allows a fast, easy, and cost-efficient network deployment.

WMNs are typically self-organized, self-configured, and self-healed networks [1] [2][3][4][5]whereas the mesh nodes automatically establish a multi-hop ad hoc network and maintain the connectivity among the participating nodes. The mesh nodes transmit traffic from others nodes to reach a destination which they could not reach by themselves. This multi-hop routing strategy widens the wireless service area and enables the network self-managing and self-healing properties, e.g., if a mesh node can no longer operate or has a temporary loss of connection, its neighbors simply find an alternative route through one or more intermediate nodes and the network continues operating.

2. RELATED WORK

Securing Wireless Mesh Network Routing Protocols, If we agree with the idea reflected in the paper by Asherson and Hutchison [7], that the best approach is to use different routing protocols for the infrastructure part and for the ad hoc part (which would use a routing protocol for ad hoc networks), then the problem of securing WMN routing protocols becomes a much simpler one. The mesh network is composed by the infrastructure part and by the ad hoc networks that are connected to the infrastructure network through the access points.
The infrastructure part can use a routing protocol suitable for fixed networks, the ad hoc networks can use a secure routing protocol suitable for MANET networks, and the access points play as gateways of both the infrastructure and the ad hoc networks. Because the access points act as gateways between two networks that use different routing protocols, they will use “administrative distances” to prioritize the use of routes of the infrastructure part. In case there is a route to the same destination provided by two different routing protocols, the one with lowest “administrative distance” is used. Routing protocols for fixed networks are relatively easy to secure [8] [9]. Therefore, the real challenge is to secure the routing protocol of the ad hoc part of the mesh network.

3. THE PROPOSE ALGORITHM

the propose algorithm is to identify the intruder node in the ad hoc part of the wireless mesh networks, the node are distributed in the simulation area moving randomly including the intruder node.

The overall system flowchart

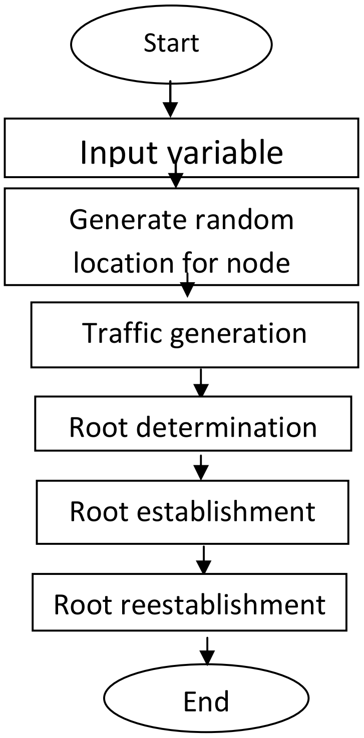

FIGURE 3.1: system flowchart

To identify the intruder node we analyze two algorithms:

3.1 Algorithm one: finding the nodes with the shortest distance

There are many criteria to decide whether a node has ability and capacity to become an intermediate node in a route. In such a dynamic topology like WMNs, it difficult to find a completely good routing protocol which can automatically reform and maintain connection. The criteria procedure is finding node with the shortest distance they guarantee for a stable and high-speed connection. When a node wants to communicate with another one, the following steps are processed:

```
initial
if route request = 1
for i =1…n
d1 (i) = $\sqrt{(x(s) - x(i))^2 + (y(s) - y(i))^2}$
end
if d1(i) < mrg
e1 = e1 + 1
Vr (e1) = i
end
end
if vr(i)==Dnode

  route request=0
else
  route request=1
end
if route request>0
for i = 1…e1
for j = 1… n
d2 (i, j) = $\sqrt{((x(vr(i)) - x(i))^2 + (y(vr(i) - (y(i)))^2}$
end
end
if d2 (i, j)< mrg
e2 = e2 + 1
vr2 (i, e2) = j
if vr2(i,e2)==Dnode

    reqst=0
end
root vector = [Snode vr vr2(i,e2) Dnode]
```

d represent the distance, **e** = represent the establish nodes and **i** represent the node with the shortest distance and Vr the vector of establish node.

d1 (**i**) ≤ max range where node **i** = node 1, node 2…. Node n **ei** = **ei** +1 and **Vr** (**e1**) = **i** , where **Vr** is the vector with the establish node. If **Vr** (**i**) = **D** the route request = 0 else if route request = 1 reestablish to check for another short route, d2 (**i, j**) < = max range where node **j** = node 1, node 2… node n, **e2** = **e2** + 1 and **Vr2** (**i, e2**) = **j** is the vector with establish node if **Vr2** (**i,e2**) = **D** node route request =0.Root vector = [S node vr vr2(i,e2) D node]

3.2 Algorithm two: identify the intruder node

```
if (Intruder node==Dnode)
if (Intruder node~=1)
Intruder node=Intruder node-1;
else
    Intruder node=Inode-2;
end
elseif (Intruder node==Snode)
if (Intruder node~=1)
  Intruder node=Intrudernode-1;
else
  Intruder node=Intruder node+1;
End
```

Figure3.2 present routing table where the intruder is attempting to modify the routing mechanism.

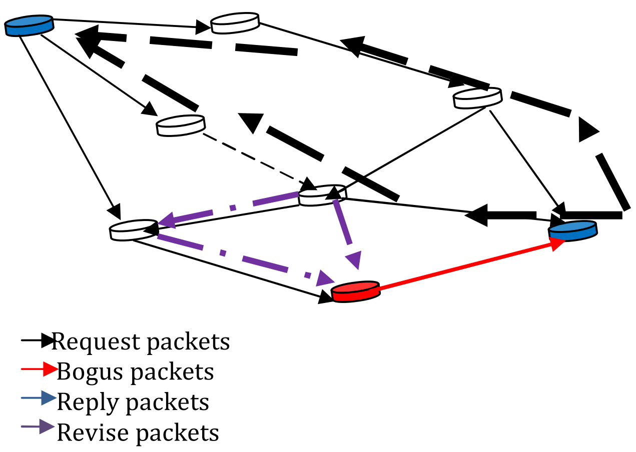

Figure3.2 Identify intruder Node

Assume X is attacker and it is trying to access to the route between A and D. Normally, RREQA =1, A floods its request to find the node with shortest distance D. In the Figure3.2, RREQB,H,F = 2 because they are neighbors of A, and RREQG,E = 3 and so on until the RREQ reaches D. If X is a legal node and it is in network topology, RREQX must be 3, but it modified this index, suppose RREQX = 2, and sends to D. D will "think" the route include X is optimal, and choose this route. But now D can send back RREP to other route different from the first route, like D,E,H,A and D,G,F,A . After that, B and E can themselves calculate the real RREQ index of X, and find it have to logical = 3. Also, if RREQX = 2, it means X have to a neighbor of A like B,E,F, but A can itself determine C is not a neighbor because A cannot directly communicate with X. In briefly, the algorithm above can definitely detect X is intruder.

4. SIMULATION AND RESULT

The MATLAB simulation first model a network of 30 wireless mobile nodes. The nodes are distributed over 1000*2000 area as shown in figure 4.1 the research set up a mobility environment. The nodes have the range of 300m. The aim is to verify whether the algorithms are capable of driving the application with efficient routing and identifying intruder node.

4.1 Simulation environment

TABLE 1. Simulation environment model

Simulation area	1000*2000
Average speed	20 Speed in meter per second
Inter arrival time between two connection	0.1[s]
Simulation time	3600 [s]
Average connection duration	180 [s]
Maximum distance for the Bluetooth	300[s]
Number of node including the intruder node	30

4.3 Simulation result

Step 1: The research simulates to find the connection from the transmitter node to receiver node, where N represents the set of node, S is the source node and D represent the destination node I the intruder node. The maximum range between the S nodes and D node is 300m, if the distance ≤ max range of 300m it will transmit, if the distance > max range it will not transmit the node because it exceed the range it proceed to fine another node.

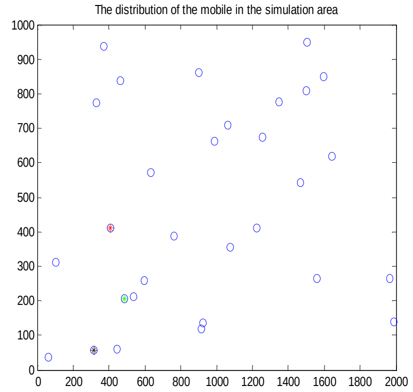

FIGURE 4.1 the simulation area with 30 nodes

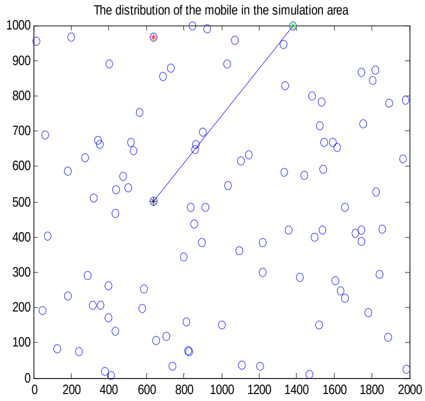

FIGURE 4.2 show the simulation area with 100 node, the distance between the source node and the receiver node exceed the range of 300m the algorithm cannot detect the intruder node.

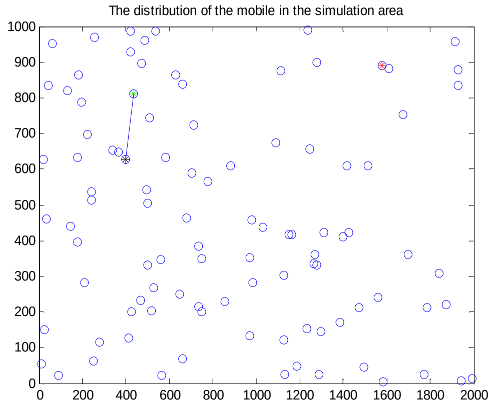

FIGURE 4.3 show the simulation area with 100, the source node and the receiver node are within the range of 300m the algorithm can detect the intruder node.

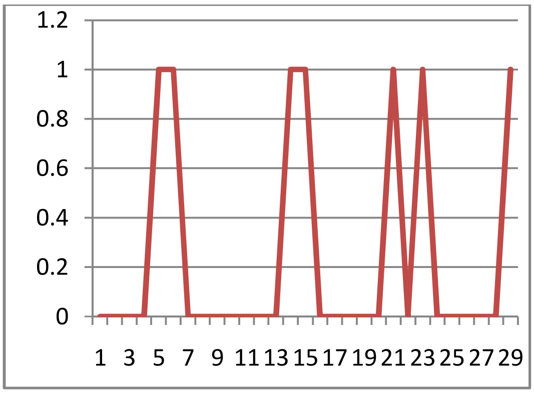

FIGURE 4.4 the result show that detection is delaying before it fined the node within the range of 300m.

Step 2: The research proposed to find the node with the shortest distance. From the simulation the vector **Vr** = [**113 18 19 20 23 26**] are the route with the established nodes, if the node with the shortest distance found in that means the best route is found. If not, we can also find the best route by reestablishment at the final step. The algorithm enhances the routing protocol and high speed connections.

5. CONCLUSION

The MATLAB simulation is useful software to simulate the network because it includes many of the random generators. The lack of security and routing enhancement makes wireless mesh networks more vulnerable. The proposed Algorithm is to enhance routing and security in ad hoc part of wireless mesh networks. It is expected that the algorithm would be both efficient and effective and give higher route establishment. The proposed algorithm can work with currently used protocols and completely solved routing problem for nodes in different wireless network.

6. RECOMMENDATION

Although the simulation is presented in Chapter 4, the proposed solution still has potential for further improvements, Evaluate the performance detection rate using some probability function is needed to strongly prove the result of this algorithm. Also, it is needed to continue applying this algorithm in experiments and find out the best fit for each specific system.

REFERENCES

[1] BWN lab wireless mesh networks research project, [Online]. Available: http://www.ece.gatech.edu/research/labs/bwn/mesh/.

[2] Seattle wireless, [Online]. Available: http://www.seattlewireless.net/.

[3] Microsoft Mesh Networks. [Online].Available:http://research.microsoft.com/mesh/.

[4] MIT Roof net homepage, [Online].Available:http://pdos.csail.mit.edu/roofnet/doku.php.

[5] *The IEEE 802.16 Working Group on BroadbandWirelessAccessStandar,[Online].Available:http://wirelessman.org/.*

[6] Hu, Y., Perrig, A., and Johnson, D. B. Ariadne: a secure ondemand routing protocol for ad hoc networks. Wireless Networking vol. 11 (2005), pp. 21–38.

[7] S. Asherson and A. Hutchison, (2006).Secure routing for Wireless Mesh Networks. In Proceedings of the Southern African Telecommunication NetworksandApplications Conference (SATNAC).

[8] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. (2003). Ad hoc on-demand distance vector (AODV) routing. Internet Request for Comments RFC 3561.

[9] C. E. Perkins and E. M. Royer, (1999).Ad hoc On-Demand Distance Vector Routing. In Proceedings of the 2nd IEEEWorkshop on Mobile Computing Systems and Applications, New Orleans, pp. 90–100.

[10] Yan Zhang, Jun Zheng, and Honglin Hu. Security in wireless mesh networks 2009, pp. 171