STI Protocol Design to Improve the Security over Multi-hop Networks

Srinivasan J.
Research Scholar,
St.Peter's University,
Chennai.

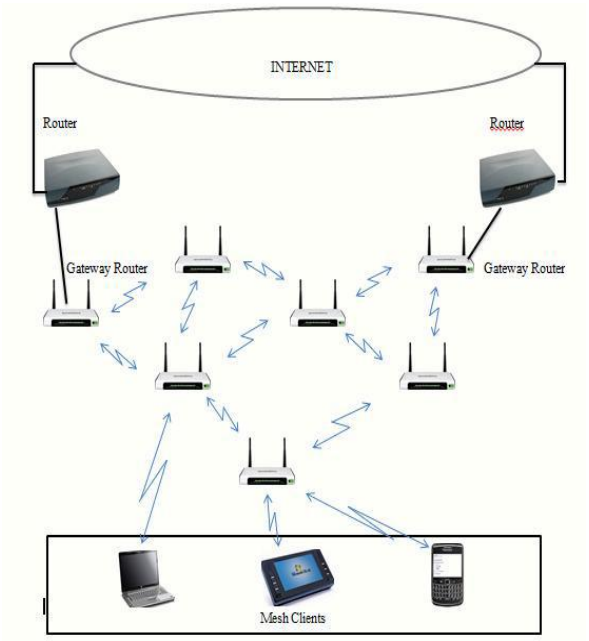
Audithan S.
Professor,
Prist University,
Kumbakonam

.

ABSTRACT
Wireless communication is very extensively used in the current world and we are rapidly moving to a hands-free swift world. Even with the arrival of advancements at such a rate in the wireless world, The Wireless Mesh Networks generally uses the AODV routing protocols to handle the traffic flow in the Mesh network. But our proposed routing protocol can securely discover the route between the pair of nodes in the Wireless Mesh Network. In this, we are utilizing Polynomial bi variate key pre distribution scheme to provide authentication and security. In this scenario each node is assigned with random key. In this paper, we present a simple and efficient method for secure traversal of information across the network through multiple intermediate hops in the network. The proposed scheme is evaluated by using the Network Simulator (NS2).

Keywords
Wireless Mesh Network, Routing metrics i.e. ETX, CAB, Routing protocol.

1. INTRODUCTION
Wireless Mesh Networks are many in number at diverse use in many fields. Routing is a fundamental networking function in every communication system, and mesh wireless networks are no exceptions. [1] Attacking the routing service, an adversary can easily paralyze the nature of the entire network.



Considering these facts, securing routing protocols is a primary task; however, designing such secure routing protocols is not a clear-cut procedure. Wireless Mesh Network (WMN) [2] consists of several radio nodes which are arranged in the mesh topology. The components of wireless mesh networks are mesh routers, mesh clients, gateways. Even though one node present the WMN could not operate for long time, the other nodes in the network can communicate directly or through some intermediate nodes. Wireless mesh network is an extraordinary kind of wireless ad-hoc network. WMN can offer dynamic connectivity in certain places. In WMN each and every node is act as router (i.e.,) the source node send the data too destination directly or through some intermediate nodes [3].

Generally, We use polynomial bi variate key pre distribution scheme with One way hash chain Algorithm to provide authentication. The authentication scheme uses randomly generated key and polynomial bi variate key which are used to provide the secure link between the nodes.

2. LITERATURE SURVEY
The research is going on to provide secure routing for wireless networks. There are several secure routing protocols especially for wireless networks like ad-hoc and sensor networks. The routing protocols that have been developed for an ad–hoc network can be applied to wireless mesh networks. But still we are not having the routing protocols provides hop by hop authentication in wireless mesh networks. The routing protocols for ad-hoc networks can be classified into three main categories. They are proactive and reactive routing protocol and hybrid routing protocol. The proactive routing protocol is otherwise called as table-driven routing protocol. This kind of routing protocol maintains a list of destinations and route to reach those destinations by periodically distributing routing table throughout the network. Proactive routing protocol periodically monitor the link exist between the nodes to provide readily available route. The main disadvantage of proactive routing protocol is delay will occur to reconstruct the route when there is link failure. The examples of proactive routing algorithms are Destination sequenced distance vector (DSDV) [2], Hierarchical source routing protocol (HSR) [3].

3. ROUTING IN WIRELESS MESH NETWORK
Wireless Mesh network is a collection of wireless access network which is connected by wireless Backbone. WMN It can be easily deployed than optical network and also the deployment requires low investment only. Wireless mesh network is a combination of mobile nodes and the access points. Figure .1 explains the general topology of wireless mesh network.

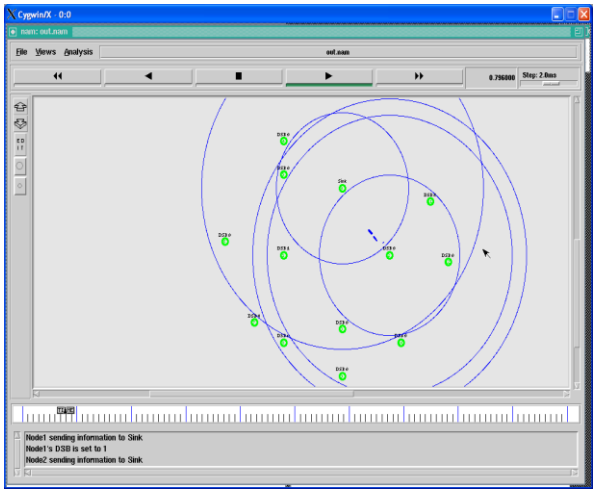


Figure 1: An Example Wireless Mesh Network

Wireless mesh network have distinctive characteristics that differentiate wireless mesh network from other wired and wireless networks[4]. Hence the already existing routing protocols should be reconstructed to provide the adaptation with WMN. The following are the some unique characteristics of WMN related to routing: Topology of the network, Pattern of the traffic flow, the interference occurs in the path exist between nodes, Quality of the link. The WMN have static topology and the traffic will occur between mobile node and the network gateway[5]. As the nodes of the WMN are mobile nodes the link quality may vary. There are several protocols available to discover the end to end route between the source and destination in WMN. Some of them are Mesh Networks Scalable routing (MSR), Hybrid wireless Mesh protocol (HWMP).

4. SECURE TRAVERSAL OF INFORMATION (STI ROUTING PROTOCOL)

Our proposed secure routing protocol for WMN is named as STI which is an on- demand

Routing protocol. This protocol persist the characteristics of AODV and also it has some extra feature such as authentication scheme[6]. The wireless mesh network is mainly used in the military application. So we need to route the confidential data packets very securely.

In our proposed scheme, the link between the nodes are established only when that two nodes are authenticated to each other. The authentication is provided by using polynomial bivariate key predistribution scheme.

The steps involved in STI to establish a route between two nodes is mentioned below:

- Initially, the randomly generated large prime number is act as a random key and
- polynomial keys are assigned to each node.
- The source node gets its neighbor list by analyzing the nodes which are all within itstransmission range.
- Verify that the intended destination is present in its neighbor list[7].
- If it is present, the source node has to establish a communication link between the nodes.

For that, it sends a sample message which contains its identification number. By usingthat, the node receiving that message verify that whether both are accessing thepolynomials from same pool.

- Both are accessing the key from same pool means the receiving node generate the communication key and send back to the source node. That communication key is usedto provide authentication between the source and destination.

4.1.Polynomial Bivariate Key Predistribution Scheme

In this section, we briefly explain the concept of polynomial bivariate key predistribution scheme. The bivariate polynomial is generated by using the following equation. The polynomials have the property of P(a,b)=P(b,a).

P(a,b)=P(b,a).
P (a, b) = i j0 ,( )*t*
$i\ j\ t\ c\ ij\ a\ b\ \sum < <$, c (ij) =c (ji)
Where,

c (ij) denotes communication cost

a ,b are denote the node ID

The identification number is added with each polynomial to differentiate the polynomials. For each node in the WMN, we preload the subset of n polynomials from polynomial pool. For each polynomial share preloaded in a node m is P(a,b), then we have to calculate P(m,b). If any two nodes m and n in the WMN want to communicate means,[7][8] first m should computes the key P(m,n) at each randomly preloaded polynomial key using the value of P(m,b) at the point n, and the node n computes its key P (n,b) at point a. If the two nodes establish a common key, the communication key is generated by the destination by using following equation.

C(K)=Hash(S,R(k))

Where C(K) denotes communication key and S is the public key which is known by all the

nodes in the WMN. R(k) denotes the randomly generated key assigned to each node. [9]The computed communication key is send back to the source node. For hop by hop communication, each and every intermediate node should know this communication key.

5. SIMULATION RESULTS

The proposed scheme is evaluated by using the NS-2 simulator. In our simulation, we are connecting the radio nodes in mesh topology. The initial energy set to each node is 20J[10]. The transmission power is 0.9J. The node consumes 0.8J for receiving the data. We have used two ray ground models for radio signal propagation. We have 21 nodes distributed in the area 1800×1000. The Results obtained by executing our proposed protocol is presented below.

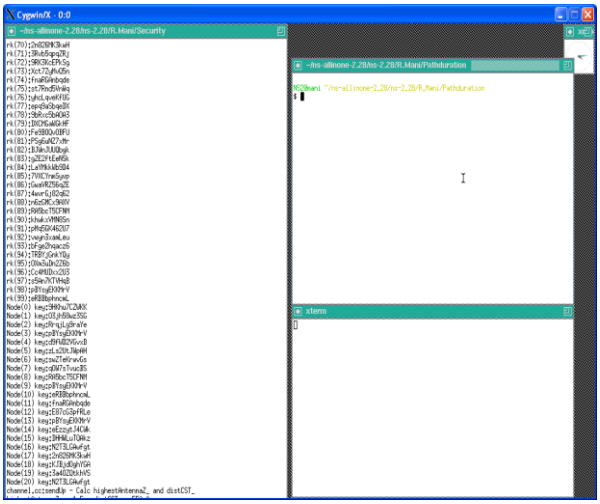


Figure 2: Keys assigned to each node in WMN

While executing the tcl file for this work, we are getting this output. Figure.2 shows the randomly generated keys which are assigned to each node[9]. The keys are initially generated and stored as a pool. The nodes are preloaded with keys by randomly pick up n number of keys. So, each node is assigned with randomly generated key and polynomial bivariate key.

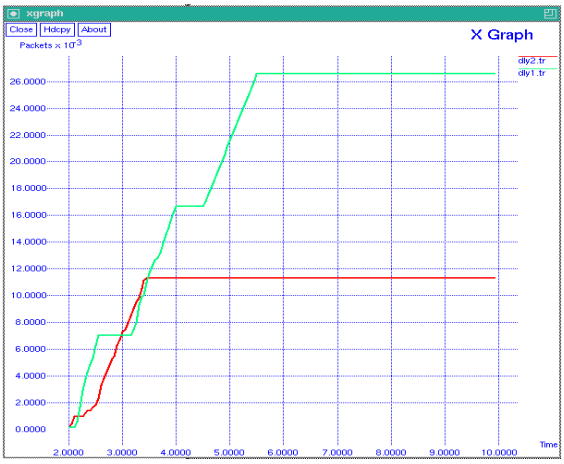


Fig 3.Stimulation Graph

The networks parameters are recorded in the trace file while the execution of simulation. The performance of the network is analyzed by using the graphs. The graphs are getting by executing the trace file in NS2 simulator. Figure.3 gives the throughput analysis of STI. The graph is plotted between the No. of packets received and the simulation time. From the graph we can extract the throughput of STI as 160 packets per unit time.

6. CONCLUSION

In this paper, we propose a secure routing protocol by combining the concept of authentication scheme with existing AODV protocol. In our work, the polynomial pool based key predistribution scheme is used for authentication. The RREQ message is also includes authentication key. After finding the route, the communication key is generated by destination node and sends back to the source. The communication key should known by all intermediate nodes to forward the data to the intended destination. So, the adversary cannot perform any attack while routing the packets.

7. REFERENCES

[1] F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," Computer Networks, vol. 47, no. 4, pp. 445-487, 2005.

[2] PERKINS, P. BHAGWAT "Highly Dynamic Destination-Sequenced Distance Vector (DSDV)for Mobile Computers" Proc. of the SIGCOMM 1994 Conference on CommunicationsArchitectures, Protocols and Applications, Aug 1994, pp 234–244.

[3] Guangyu Pei and Mario Gerla and Xiaoyan Hong AND Ching-Chuan Chiang, "A WirelessHierarchical Routing Protocol with Group Mobility" , IEEE WCNC'99, New Orleans, USA,September 1999.

[4] K. Sangiri and B. Dahil, "A secure routing protocol for ad hoc networks," Proceedings of 10thIEEE International Conference on Network Protocols, pp. 78-89, 2002.

[5] Y C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for adhoc networks," Proceedings of MobiCom, pp. 21-38, Atlanta, GA, Sep. 2002.

[6] M. Zapata and N. Asokan, "Securing ad-hoc routing protocols," Proceedings of ACMWorkshop on Wireless Security, pp. 1-10, Sep. 2002.

[7] Ghanbari, P, "HWMP path selection protocol based on learning automata for Wireless MeshNetworks" Application of Information and Communication Technologies (AICT), Oct. 2011.

[8] Sonia Waharte & Raouf Boutaba & Youssef Iraqi & Brent Ishibashi, "Routing protocols in wireless mesh networks: challenges and design considerations" Multimed Tools Appl (2006)29: 285–303.

[9] H. Hassanein and A. Zhou, "Routing with load balancing in wireless Ad hoc networks,"Proceedings of ACM MSWiM, pp. 89-96, 2001.

[10] Y C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Proceedings of MobiCom, pp. 21-38, Atlanta,GA, Sep. 2002.