IJCSC International Journal of Computer Science & Communication Vol. 1, No. 1, January-June 2010, pp. 125-127

Secure Routing in Mobile Ad hoc Network

Tirthraj Rai[1] **& Ashish Jain**[2]

[1]Department of Computer Science & Engineering, Thapar University, Patiala, India
[2]Department of Computer Science & Engineering, U.P. Tech. University, Lucknow, India
[1]tirthraj.rai@gmail.com, [2]ishash100@yahoo.com

ABSTRACT

Mobile ad hoc networks (MANETs) are a collection of large number of mobile nodes that form temporary network without aid of any existing network infrastructure or central access point. Each node participating in the network acts both as host and a router and must therefore is willing to forward to packets for other nodes. The characteristics of MANETs such as: dynamic topology, node mobility, provides large number of degree of freedom and self-organizing capability of that make it completely different from other network. Due to the nature of MANETs, it more prone to attacks. So to design and development of secure routing is challenging task for researcher in an open and distributed communication environments. In this work we proposed a secure routing protocol named ASRP (Authenticate Secure Routing Protocol) for MANETs.

Keywords: MANETs, NS2, Security.

1. INTRODUCTION

In mobile ad hoc network each nodes are mobile, connected via wireless link and free to roam about while communication with other. The path between each pair of users may have multiple links, this allows an association with various link to be a part of same network [1, 2, 3]. The network topology may change with time as the nodes move or adjust their transmission and reception parameters. Therefore MANET has several salient characteristics [2] i.e. dynamic topology, resource constraints, limited physical security and no infrastructure. It has extensive application, e.g. disaster recovery, tactical battlefield etc. There are large numbers of routing protocol have been proposed by researcher but no one can secure in all security aspects and also there is no security mechanism to detect malicious and selfish node collectively. The secure routing protocols are mainly divided into two categories: proactive protocols that maintain routes to all destinations whether it is needed or not, such as DSDV [3] and reactive protocol that discover routes to its destination when it required, such as AODV [4] and DSR [7]. ASRP follows the reactive approach to sending the data or information to other nodes within the network. Also we implement a mechanism, Extended Public key Cryptography (EPKCH) that able to detect the malicious nodes and selfish nodes collectively in order to achieving security goals such as; Authentication, Integrity, Confidentiality and Non-Repudiation.

2. RELATED WORK

We classify related work into the following three categories:

- Providing basic security infrastructure: MANET is a network without any basic infrastructure; hence there is no trust infrastructure like PKI [5, 6] for all the participating nodes in MANETs. The first step to establish a security system is to setup the basic security infrastructure and establish security associations between communicating nodes.
- Secure routing [5, 8]: In MANETs, every node participates in the routing activities in MANETs. There are two concepts in secure routing here: one is exchanging routing information to keep the network connected and the other involves secure data packet forwarding.
- Misbehavior node detection and response [6, 8]: The wireless and mobility nature of ad hoc networks makes it vulnerable to malicious and selfish node.

2.1. ASRP and its Description

Now in this work we proposed a secure routing protocol named, ASRP, which is based on reactive approach, means when a node want to send data to particular node first it broadcast RDP to all its neighbor to finding the route, RDP contain address of destination, its own identity, timestamp *t*, nonce *n*, and it bind using its own private key to bind it (Source=Add$_{\text{Destination}}$ *t*, *n*, Cert), Source) K_{A-}. Each intermediate node receives it and checks if it is destination then generate REP (Replay) message otherwise it sign on it and broadcast it all its neighbor nodes. After receiving route information to particular destination, the source node sends data to particular destination through same route. Each intermediate node receives and verifies its key and signature if there is any alteration then generate message for malicious node otherwise forward it to destination. The authentication of each node is provided by issuing certificate and time stamp of each node. The node before entering to the network first it contact to TTP (Trusted third party for issuing certificate and key, then after receiving Cert. it join the network.

2.2. Assumption

Our proposed secure protocols aim to protect the network from attackers. Our proposed schemes work under several assumptions as follows:

- The network link is bidirectional. That is, if node A is able to transmit to node B, then B is also able to transmit to A.
- At a time the node can either malicious or selfish.
- The wireless interface supports promiscuous mode operations. That is, each node can receive a copy of the messages being transmitted by other nodes within its receiving range.
- A public key infrastructure exists in the MANET under consideration [8]. Each mobile node stores the public key of all other nodes.
- The trust relation could be instantiated. For example: by knowing public key of other nodes.
- There is a security association between source node and destination node.
- The existence of security association is justified because, host chose to employ a secure communication schemes and consequently, should be able to authenticate each other [8, 9].

3. RESULT PERFORMANCE EVALUATION AND ANALYSIS

This section we explain various simulation results and analysis being done by comparison.

3. 1. Simulation

We use NS2 simulator to evaluate the performance of the proposed ASRP routing protocol with and without the malicious node. We simulate a mobile ad hoc network consisting of 20 nodes randomly deployed in a field of 50m × 50m square area. Nodes have same transmission range in one experiment. The simplest and usually the first thing to setup a network is creating a node. A network is build up from its layers components such as Link layer, MAC layer and PHY layer. The components have to be defined before a node can be configured.

Table 3.1
Shows the Parameter and Keys used for Simulation

Parameter Name	*Parameter Value*
Channel Type	Wireless
Cryptography	EPKCH
Key Length	64 bit
Radio model	Two Ray Ground
netif	Physical/WirelessPhy/802_15_4
Mac protocol	Mac/802_15_4
Number of node	25
Number of Malicious/ Selfish node	1
Simulation Time	Different

In the simulation of simple ASRP, experiment is carried over 25 nodes. In the ns2- allinone package NAM is a build-in program. NAM helps us to see the flow of route request (RREQ) and route reply (RREP). It also shows the packets are dropping or reaching to the destination properly. When the TCL file is written, NAM is invoked inside that file. Figure 4.1 and figure 4.2 are animation capture of MANET with25 nodes. The source (node 10) is broadcasting RREQ message to all its neighbors and Node 1which is the destination node, is sending RREP (route reply) back to the source. The nodes with the same frequency will receive the message and forward it to its neighbor, while the nodes with different frequency will drop the packet. In figure 4.2, a packet of blue color is on transmission from the source (node 10) to the destination (node 1).

Since there is peer-to-peer communication between source node (10) and destination node (1), so no packet will be dropped. In figure 4.3 tracegraph proves that dropped packets are zero. This high throughput is expected because all the nodes are using the same frequency.

Secure outing in MANETs.

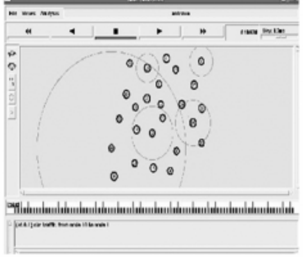


Fig 4.1: Source Nodes Broad RREQ Packet to its Neighbor

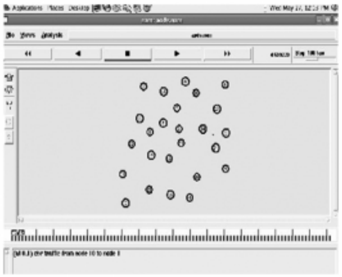
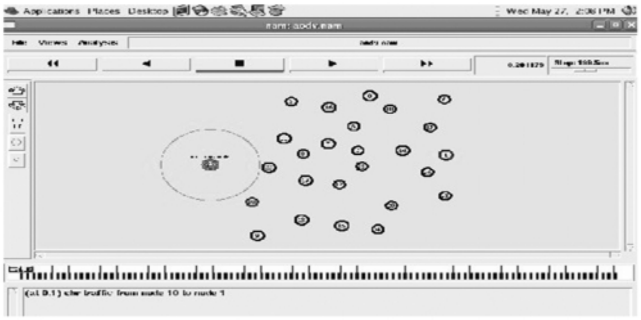


Fig 4.2 Transmission of Data Packets from Source Node to Destination Node

3.2. ASRP with Malicious Node



(at 0.1) cbr traffic from node 10 to node 1

Fig 4.3: Malicious Node Broadcast RREQ

3.3. ASRP with Malicious Node and Frequency Hopping

When frequency hopping is applied to the network (with malicious node), the network performance increases as the simulation time increases. Table 4.1 explains how the throughput increase as the simulation time increases. A data packet is received by the destination only when source and destination are using the same frequency. The throughput varies as two frequencies are hopped with different period of simulation time. The throughput is increased when period of simulation becomes longer. The throughput has been analyzed with awk script and trace graph.

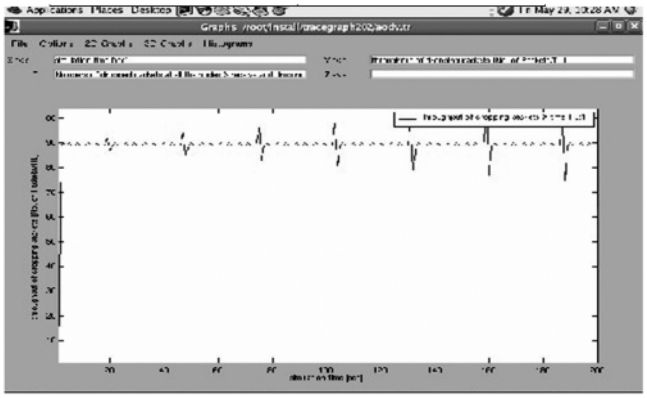

Applications Places Desktop
Graphs /root/install/tracegraph202/aodv.tr
File Colors 2D Graphs 3D Graphs Histograms
100
90
80
70
60
50
40
30
20
10
20
40
60
80
100
120
140
160
180
200
simulation time [sec]

Fig 4.4: Throughput of Dropping Packet with Malicious Node

4. CONCLUSION AND FUTURE WORK

Security is a significant issue in Mobile Ad hoc Networks. Intrusion of malicious nodes may cause serious impairment to the security. In the presented work, we have discussed all the modes of ASRP (simple mode and frequency hopping) along with their working. We sincerely hope that our work will contribute in providing further research directions in the area of security based on frequency hopping. In this thesis work, ASRP over MANETs is simulated with different operation modes.

Table 4.1
Percentage of Received Packets at the Destination Node

Simulation Time(secs)	*Throughput in %*
50	58.8
100	79.4
200	89.7
300	93.1
400	94.8
500	95.8
1000	98
1500	98.6
2000	99

An important contribution of this work is the comparison of the performance of routing protocol with and without malicious node using the frequency hopping technique. With the results of AWK programming and tracegraph, we can conclude that there is no packet drop and throughput is 100%. But when two frequencies are hopped in the network with different simulation times, throughput is less than 100% but increases continuously with respect to simulation time. After a simulation time of 2000 seconds (~33 minutes) almost 98 percent packets reach the destination safely.

REFERENCES

[1] C.Perkins, Ad Hoc Networks, Addison-Wesley, 2001

[2] M. Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.

[3] C.E. Perkins, P. Bhagwat, "Highly Dynamic Destination Sequenced Distance-vector Routing (DSDV) or Mobile Computers", *Computer Communications Review*, pp. 234-244, October, 1994.

[4] C. E. Perkin and E. M. Royer, " The Ad hoc On-Demand Distance Vector Routing Protocol," in C. E. Perkin (ed.), Ad hoc Networking, pp 173-219, Addison-2000

[5] B. Dahill, B. Levine, E. Royer, and C. Shields. A Secure Routing Protocol for Ad Hoc Networks. Technical Report UMCS- 2001-037, CS Dept., Umass 2001.

[6] H. Yang, X. Meng and S. Lu: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks, ACM, 2002.

[7] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall Englewood Cliff, NJ 07632, 2002

[8] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Network," in Proc. CNDS 2002.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, " Ariadne: A Secure On Demand Routing Protocol for Ad hoc Network," in Proceeding of 8th ACM Int'l, Conf. on Mobile Comp, Georgia, September 2003.

[10] M. G. Zapata and N. Asokan, " Secure Ad hoc Routing Protocols," in Proceeding of the ACM Workshop on Wireless Security, Atlanta, GA September, 2002.