A NOVEL FRAMEWORK FOR ANALYSIS OF SECURE ROUTING IN MOBILE ADHOC NETWORK

[1]ANAGANI NAVYA SREE, [2]P.SATISH KUMAR
[1] Student of M.Tech, Dept. of CS & SE , [2]Research Scholar, Dept. of CS&SE
Andhra University College of Engineering (A)
Visakhapatnam, Andhra Pradesh, India

Abstract: Mobile Ad-hoc Networks (MANETs) is one of the fastest growing areas of research in communicating technology. The flexibility and mobility of Mobile Ad hoc Networks have made them increasingly popular in a wide range. Many problems and challenges exist in this field because of the frequent and unpredictable MANET topology changes. To protect these networks, security protocols have been developed to protect routing and application data. The use of communication security protocols originally developed for wired and Wi-Fi networks. They also place a heavy burden on the limited network resources of a MANET. To address these issues, a secure routing communication and a novel secure framework is proposed. The framework is designed to allow existing network and routing protocols to perform their functions while providing node authentication, access control, and communication security mechanisms. A secure protocol and a watch dog approach is been implemented for security mechanism in wireless networks.

***Index Terms* - mobile ad-hoc networks, authentication, access control, communication security, watch dog approach**

I. INTRODUCTION

Mobile ad hoc network (MANET) has become very famous due to their infrastructure-less quality and dynamic nature in communicating technology. They contain a large number of nodes which are connected and they communicate to each other in wireless nature. MANET is an ad hoc network for mobile or much simply called as mobile ad hoc network which is a continuous self-ordered, infrastructure-less network of mobile devices connected wirelessly. Every node also works as a router since they route packets from one to node to the other nodes. Due to its wireless nature and lack of any central authority in the background, Mobile ad hoc networks are always vulnerable to some security issues and performance issues. The security imposes a huge impact on the performance of any network.

Definition: A collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services.

There is a widespread of applications in mobile ad hoc network in the commercial, Military and private sectors. Mobile Adhoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. Wireless communication can be trivially intercepted by any node in range of the transmitter. This can leave MANETs open to a range of attacks.

II. EXISTING SYSTEM

Secure routing communication that provides node authentication, access control and communication security mechanism in mobile adhoc networks is implemented, where the strength of the connection changes with time. MANET's rely on intermediate nodes to route message between distant nodes. AODV and OLSR lack security mechanisms, allowing malicious nodes to interfere with the network in a variety of ways. Diffie Hellman key exchange algorithm is used. Generating keys for every node to connect to the other node causes overhead.

III. PROBLEM STATEMENT

MANETs rely on intermediate nodes to route messages between distant nodes. They lack infrastructure to administrate the manner in which packets are routed to their destinations. Reactive protocols, such as Ad hoc On-demand Distance Vector (AODV) plan routes when messages need to be sent from source node to the destination node by polling nearby nodes in an attempt to find the shortest route .The basic versions of AODV and OLSR lack security mechanisms, allowing malicious nodes to interfere with the network in a variety of ways. Generating keys for every node to connect to the other node causes overhead. The key contributing factor to this problem is an inability to distinguish legitimate nodes from malicious nodes.

IV. PROPOSED SYSTEM

Secure MANET routing protocol have been proposed. Secure Ad hoc On-demand Distance Vector (SAODV) is the secure implementation of AODV respectively. Verification of the source node's identity must be performed. Each node is assumed to have a digital signature. A watch dog tool is implemented to monitor and evaluate the transaction between the nodes using certain parameters like digital signature and transaction id. Secured Hashing algorithm (SHA2) is been used for generating digital signature. Malicious and authorized nodes are been identified.

4.1 Adhoc On demand Distance Vector (AODV) routing protocol

The AODV routing protocol is a reactive routing protocol. Routes are determined only when needed. In this protocol the routes are kept for packet transmission as long as they are needed by the source node. AODV enables dynamic, self-starting, multi-hop routing between mobile nodes wishing to establish and maintain an ad-hoc network. AODV allows for the construction of routes to specific destinations and does not require that nodes keep these routes when they are not in active communication. AODV avoids the ―counting to infinity problem by using destination sequence numbers. This makes AODV loop free.

AODV defines 3 message types:

- RREQ messages are used to initiate the route finding process.
- RREP messages are used to finalize the routes.
- RERR messages are used to notify the network of a link breakage in an active route.

The Path Discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in its table. Every node maintains two separate counters. A node sequence number and a broadcast id. The source node initiates path discovery by broadcasting a route request (RREQ) packet to its neighbors.

The pair uniquely identifies a RREQ broadcast id is incremented whenever the source issues a new RREQ. Each neighbor either satisfies the RREQ by sending a route reply (RREP) back to the source or rebroadcasts the RREQ to its own neighbors after increasing the hop count. Notice that a node may receive multiple copies of the same route broadcast packet from various neighbors. If it has already received a RREQ with the same broadcast id and source address it drops the redundant RREQ and does not rebroadcast it.

Nodes can keep track of connectivity to neighbors using available data link or network layer mechanisms. RERR message processing is initiated when

- Node detects a link break for the next hop of an active route, or
- Receives a data packet destined for a node for which it has no (active) route, or
- Receives a RERR message from a neighbour for at least one active route in its routing table.

Nodes must increment the destination sequence numbers of the routing entries contained in the RERR message before transmitting to nodes in precursor list. Nodes receiving RERR messages simply update their sequence numbers with those contained in the RERR message. Nodes must also mark these routing entries as invalid regardless of whether they are transmitting and/or receiving. This ensures that no predecessors may reply to a RREQ from a node on their successor path, thus providing loop freedom. RREQ messages are ultimately forwarded back to the originator who may initiate another RREQ message.

4.2 Flow Diagram

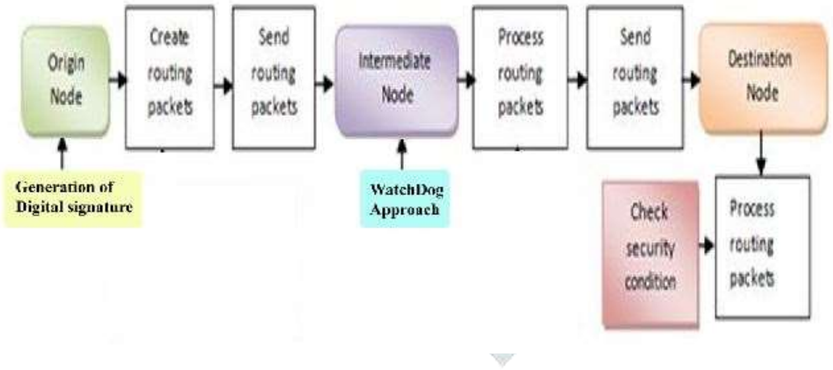


Fig. 1 Adding security features for the routing protocols

4.3 Digital signature

A type of asymmetric cryptography used to simulate the security properties of a signature in digital.

4.4 Watchdog Tool

- Monitors the transactions between the nodes and verification of digital signatures.
- Evaluating malicious activity and blocking them.

4.5 Algorithms

4.5.1 Malicious node detection

BEGIN

Step1: Static and dynamic Parameters initialization.

Step2: Put all identity on the first node.

```
        Step3:   Update the identity of the watch table
        Step4:   Select an edge to reach to the next node.
        Step5:   Compute the amount of energy consumed to transmit the data
        Step 6:  Update the edge of nodes and their identity
        Step7:   IF Have all have secure identity completed their solutions THEN GOTO
        Step 8:   ELSE GOTO Step 4.
        Step 9:  Find the route and transmit the data
        Step 10:  Perform routing with the intermediate id for packet transmission
END
```

4.5.2 Digital signature Generation

```
    Begin
        Step1:   Initialize hash chain.
        Step2:   Generate hash chain.
        Step3:   Max hop count.
        Step4:   Define hash function type.
        Step5:   Generate hash based on Source address.
        Step6:   Extract auto key
        Step7:   Generate signature.
    End
```

4.5.3 Checking and verifying signature integrity

```
    Begin
        Step1:   IF the signature is invalid THEN simply drop the packet.
                     ELSE
                        Signature verified.
    End
```

V. RESULTS

Python 2.7.5 version is installed in windows 10 and after installing python the program is executed. But few packages are to be installed before execution. SHA generated keys for nodes that want to transfer the data in form of packets by forming a network and stored in database.

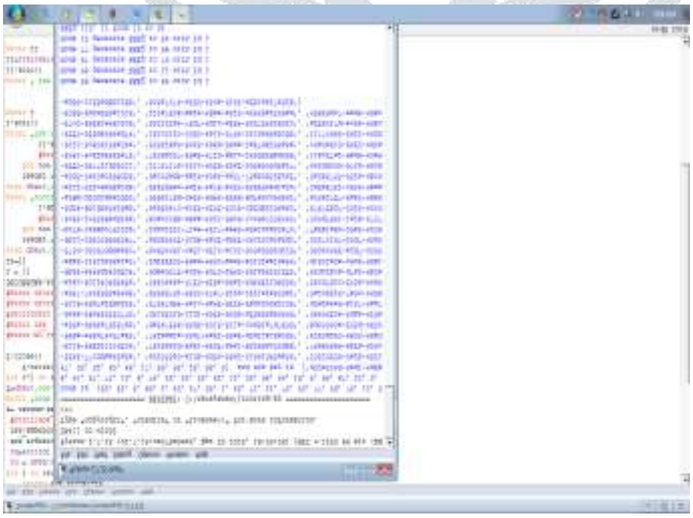


Fig. 2 Digital signatures generation

.

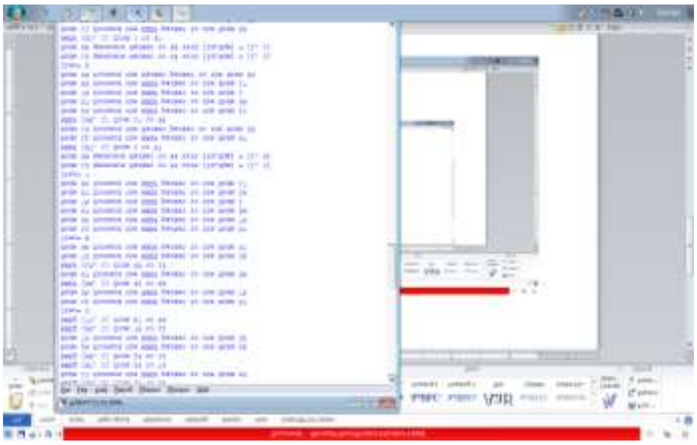
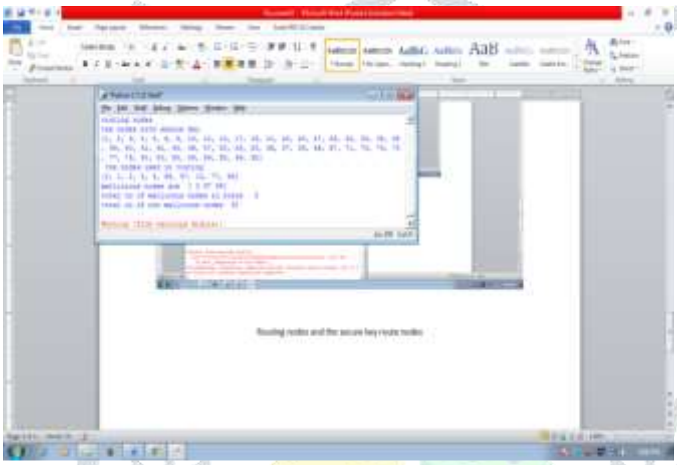


Fig. 3 RREQ generated for the packets between the routes

Routing nodes and malicious nodes are displayed which are used in routing.



Routing nodes and the secure key route nodes

Fig. 4 List of malicious nodes

The above graph is obtained after identifying the secure nodes and malicious nodes in routing the packets from source to the destination. The red points indicate malicious nodes, green points indicate authorized nodes.

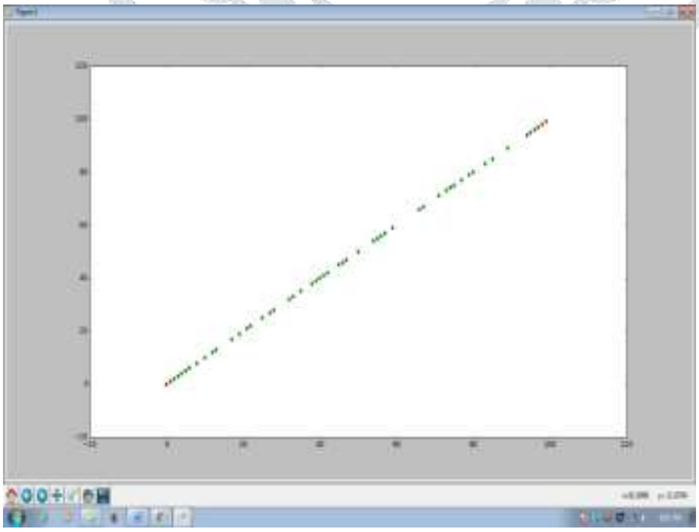


Fig. 5 Graph representation

VI. CONCLUSION

The use of infrastructure free network such as MANET's has increased tremendously. In such environment, the security is more important because the data should be safe and the identification of nodes should be done. Routing protocols and the process should also be secure. A novel frame work for analysis of secure routing in mobile adhoc network is been proposed. A secure routing protocol AODV is implemented for transmission of data packets. Digital signature is been generated for the nodes before the transmission. A watch dog approach is been implemented for security analysis in the routing process. The results have shown the transmission of data packets between nodes securely by identifying the authorized nodes and the malicious nodes. Many more routing protocols can be proposed. Comparison between different routing protocols with security and watch dog approach can be used.

REFERENCES

[1] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. "Efficient and Secure Source Authentication for Multicast". In Network and Distributed System Security Symposium, NDSS '01, pages 35–46, February 2001.
[2] C.E. Perkins, E. Royer, and S.R. Das. "Ad hoc on demand distance vector (AODV) routing", Internet Draft, March 2000.
[3] C.Siva Ram Murthy and B. S. Manoj. "Ad hoc wireless networks: Architecture and Protocols". Prentice Hall Publishers, May 2004, ISBN 013147023X.
[4] C.K. Toh**.** "Ad Hoc Mobile Wireless Networks: Protocols and Systems". Prentice Hall publishers, December 2001, ISBN 0130078174.
[5] Charles E.Perkins and Elizabeth M. Royer. "Ad hoc on demand Distance vector routing". Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.
[6] D. Hurley-Smith, J. Wetherall, and A. Adekunle, "Virtual closed networks: A secure approach to autonomous mobile adhoc networks," in Proc. 10th Int. Conf. Internet Technol. Secured Trans., 2015, pp. 391–398.
[7] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, "A cluster based approach to consensus based distributed task allocation," in Proc. 22nd Euromicro Int. Conf. Parallel, Distrib. Netw.-Based Process. 2014, pp. 428–431.
[8] D B. Johnson, D A. Maltz, and Y. Hu. "The dynamic source routing protocol for mobile ad hoc network, "Internet-Draft, April 2003.
[9] David B. Johnson David A. Maltz Josh Broch. **"**DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks'. In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.
[10] Frank Kargl, Alfred Geiß, Stefan Schlott, and Michael Weber.**"**Secure Dynamic Source Routing". Proceedings of the 38th Hawaii International Conference on System Sciences – 2005.
[11] G. Montenegro and C. Castelluccia. "Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses". Network and Distributed System Security Symposium (NDSS '02), Feb. 2002.
[12] Hongmei Deng, Wei Li, and Dharma P. Agrawal. "Routing Security in Wireless Ad Hoc Network,"IEEE Communications Magazine, vol. 40, no. 10, October 2002.
[13] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and JorjetaJetcheva. "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols". IEEE Journal on Selected Areas in Communication, 1999.
[14] KimayaSanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer. "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002, pp. 78-90.
[15] L. Zhou and Z. Haas."Securing Ad Hoc Networks". IEEE Network magazine, special issue on networking security, Vol. 13, No. 6, November/December 1999.