ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Trusty Message transmission using routing protocols and cryptography techniques for effective mobile adhoc networks

A.Nagajyothi[1]
Computer Science and Engineering
Dept. of Management Studies
Sasi Institute of Technology and Engineering
Tadepalligudem – India

M.V.S.S.Nagendranath[2]
Computer Science and Engineering
Dept. of Management Studies
Sasi Institute of Technology and Engineering
Tadepalligudem – India

Abstract: ***A mobile adhoc network is self established infrastructure-less network formed without using any wires. Because of framework-less feature the nodes of the network will freely move from one location to another location easily. Therefore the devices will change its link to other device periodically. The routing path in between these nodes is established by using different routing protocols. After establishing a path in between these nodes we can transfer messages from source node to destination node through this path. There are number of ways we can use to transfer the data from one node to another. In this, source node will transfer packets to the neighboring node; if the neighbor node is destination then it stops the packet transmission. If the neighbor node is not a destination then the received node again transfers received packet to its neighbor node and this process continuous until the packet transmitted to destination. In this paper we focus on different routing protocols and cryptography techniques used to transfer message securely to the destination node.***

Keywords: Adhoc Network; Routing Protocols; Secure message transmission; Trust based routing; Packet dropping attack; encryption.

I. INTRODUCTION

Mobile Adhoc Networks are self established, infrastructure fewer networks designed without using any wires. Due to its impetuous feature the link in between nodes is established whenever required. And this route is established by using number of routing protocols. When the routing path is formed one can transfer message from one node to another. This message transmission can be done in trusty by using different secure routing protocols, they are proactive routing protocols, on demand routing protocols and Hybrid routing protocol. Whenever a route is established between the nodes then there a chance to occur an attack[1]. Different attacks includes the following

- Inclusive Packet Dropping attack:

In this, the selfish node simply drops all received packets by generating positive acknowledgements to their neighbor node.

- Selective Packet Dropping attack:

In selective packet dropping attack the selfish node drops the packets only it receives from the selected sources.

- Random Packet Dropping attack:

In this, selfish nodes drop limited part of received packets once per resending time completes.

The Remaining portion of this paper is discussed as follows: Section 2 discusses with Proactive routing protocols, Section3 discuss with reactive routing protocols, Section 4 discuss with secure message transmission technique. Section 5 discuss with proposed work. Finally Section 6 concludes the paper.

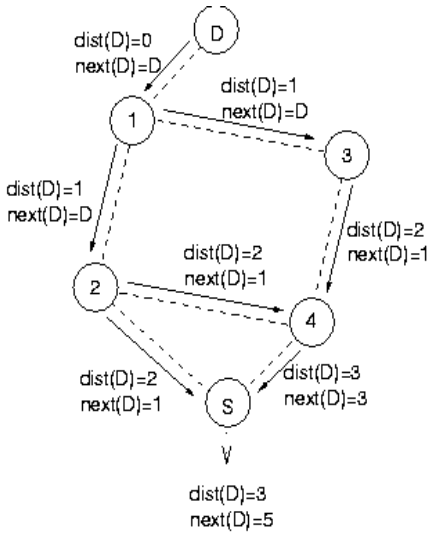
II. PROACTIVE ROUTING PROTOCOL

Proactive routing protocols are used to provide routing in between the nodes. In this case the node manages full routing details of the network. If there are any changes occur in the network then each node sends a broadcast message to the network. Different proactive routing protocols includes the following

- Distance Vector Routing
- Link State Routing Protocol
- Cluster Head Gateway Routing Protocol

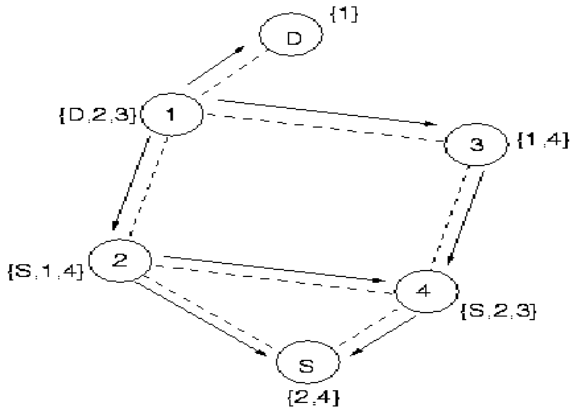
Distance Vector Routing:

Distance Vector Routing[2] is an example for proactive routing protocol. Through this we can establish a route between the nodes. This route is used to transfer messages to destination node safely. This protocol uses routing algorithm, through that nodes continuously transmit routing updates to all their neighbors. Following Fig shows the representation of Distance Vector Routing protocol



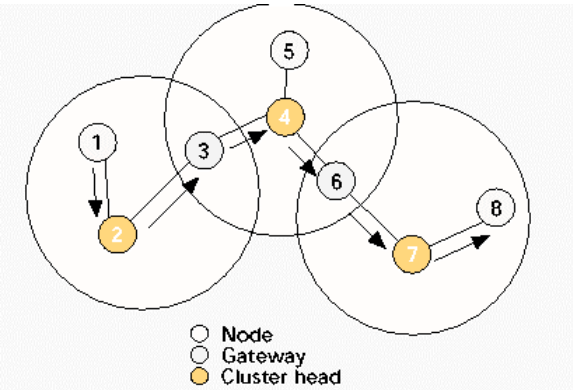
Link State Routing Protocol:

Link State routing protocol[3] is used to build a route for message transmission. In link state protocol each router build an association with each of its neighbor node. In this each router sends data packet to their neighbors. The data packets outlines each of the link and recognizes status, metric cost and any neighbors that must be connected to the link. This process continues with all the neighboring nodes and this process is shown below



Cluster Head Gateway Routing Protocol:

Cluster Head Gateway routing protocol[4] is used to form a route between the nodes to transfer data. Following is the procedure to establish a route: In this, to determine node as a cluster head node it uses distributed cluster head algorithm. When the source wants to send a packet then first it has to be transferred to cluster head. From that cluster head the packet will be transferred to a gateway and then to another cluster. This process continuous until the cluster head of the destination node is reached. Below diagram shows how the routing is established by using cluster head gateway routing protocol.



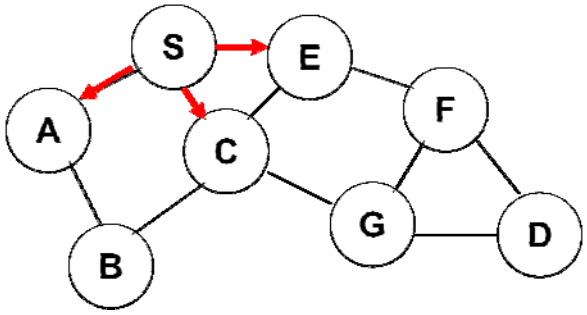
III. On Demand Routing Protocol

On demand routing protocols are used to form a route between the nodes whenever necessary. That means when the source want to transfer data to destination then only the path will be established between the sender and receiver. So the transmission burden will be reduced. Following are the examples for reactive routing protocols.

- Ad hoc On-demand Distance Vector Routing (AODV).
- Dynamic Source Routing (DSR)

Ad hoc On-demand Distance Vector Routing (AODV):

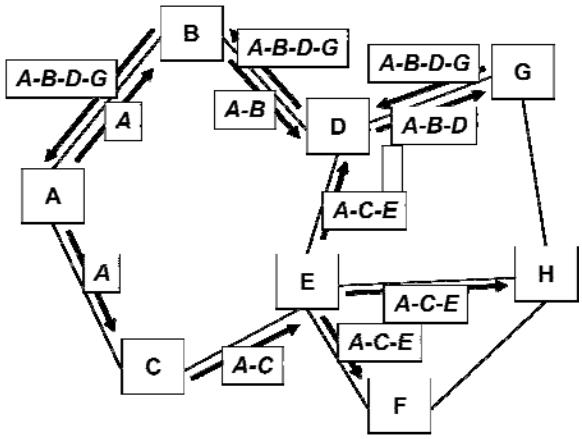
AODV[5] protocol is used to establish a path whenever necessary. For this it maintains three messages. Those are route request, route reply and route error messages. In addition to this the nodes maintains sequence number. First the source sends route request message to all the neighboring nodes until receiver node receives. Then the neighboring node sends route reply message to the source node. If any node does not transfer route reply message then the source deletes that node from path and sends route error message to the remaining nodes of the path. Like that the path is established by using AODV and after the path is established we transfer the message securely from source node to destination. Following is the diagram which represents AODV.



Dynamic Source Routing (DSR) :

DSR[6] is an example for reactive routing protocol. In this case also routing is established whenever the source node wants to transfer data to destination. This protocol has to perform two operations to transfer the data. First is route discovery and

second one is route maintenance. Route discovery is used to form the route and route maintenance is used to maintain the route until the data is transmitted. Following Fig shows the diagram for Dynamic Source routing protocol.

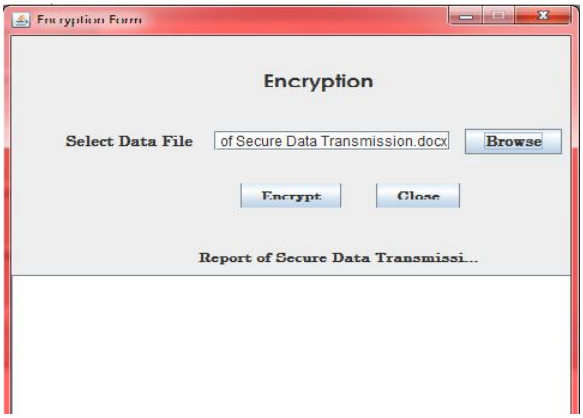


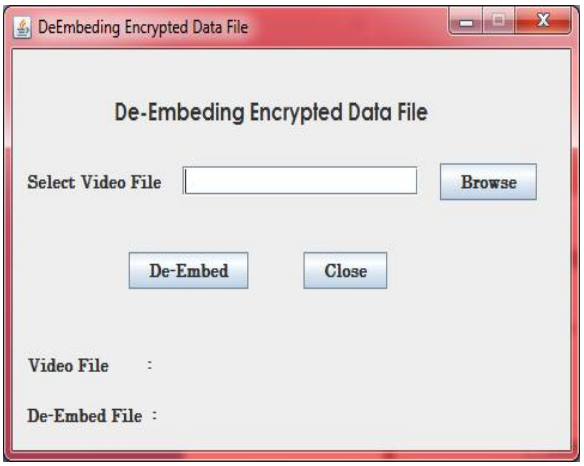
IV. SECURE MESSAGE TRANSMISSION

After a route is established a message can be transmitted securely[7] by using encryption algorithms. If we use these encryption algorithms then the data can be transferred securely from source to destination node. So that the source node and destination node can only know the actual transmitted data. No other nodes will identify the message transmitted by the source. Because whenever a data is transmitted then the source sends private key in addition to packets. The source encrypt the code by using either Huffman code or arithmetic code.

V. PROPOSED WORK

This project is used to transfer message securely from source node to destination. In this for transferring data from one location to another location first path has established by using routing protocols and after that data will be transmitted by using encryption with RSA algorithm. In this RSA algorithm each user generates private or public key by selecting two large prime numbers at random, compute their system module and then randomly select the encryption key. If the source want to transfer any message to destination then it has to send private key to the destination in advance. So that the source transmitted message can be viewed by only destination and no other node can view the message. So that no modifications will be performed for the message by the intermediate nodes. Therefore message transmitted by the source will be send securely to destination by using this encryption process. Following are the results obtained after implementing this project





VI. CONCLUSION

This project gives security to the transmitted message by using encryption techniques. The solution is provided in two ways one is by using routing protocols and second one is by using encryption techniques. So that the source can transfer data securely to the destination.

References

1. Baruch Awerbuch, Reza Curtmola, David Holmer,Cristina Nita-Rotaru, Herbert Rubens “Mitigating Byzantine Attacks in Ad Hoc Wireless Networks”, ACM MobiCom, Aug-2000.
2. Y.-C. Hu, D.B. Johnson, A. Perrig, Secure efficient distance vector routing in mobile wireless ad hoc networks,in: Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSAÕ02), June 2002, pp. 3–13..
3. S. Cheung, An efficient message authentication scheme for link state routing, in: 13th Annual Computer Security Applications Conference, 1997.
4. Q. Liang, “Clusterhead election for mobile adhoc wireless network,” in Proc.14th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC) , Sept. 2003, pp. 1623 1628
5. Charles E.Perkins and Elizabeth M. Royer, “Ad hoc on demand distance vector (AODV) routing (Internet-Draft)”, Aug-1998.
6. David B. Johnson. Routing in Ad Hoc Networks of Mobile Hosts. In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, pages 158–163. IEEE Computer Society, December 1994
7. V.Anitha, Dr J.Akilandeswari “Secured Message Transmission in Mobile AD HOC Networks through Identification and Removal of Byzantine Failures” in IJRICSN,August 2010