ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCED MINIMUM SECURED ROUTING PATH FOR MOBILE AD-HOC NETWORKS

[1] K.LAKSHMINARAYANAN, [2] Dr. S. PAVAIMADHESWARI

[1]Assistant Professor, Department of M.C.A, R.M.K Engineering College,Kavaraipettai,Chennai,India
[2] Professor, Department of CSE, R.M.K. Engineering College, Kavaraipettai, Chennai, India
E-mail: [1] klnarayanan_11@yahoo.co.in , [2] ac@rmkec.ac.in

ABSTRACT

The EMSR-path algorithm develops a new routing path from source to the destination based on the ascending order of the edge, the ascending order edge is get connected, in order to avoid congestion in routing path in Mobile Ad-Hoc networks. The routing is to reduce the congestion when it gets connected based on the priority and the path is secured by secured routing protocol. The discovery of route and secured transmission of routing path is EMSR-path algorithm.

Keywords: *Path, Networks, Protocol, Ad-Hoc,Congestion*

1. INTRODUCTION

Mobile ad hoc network (MANET) is an autonomous group of mobile users which communicate through relatively bandwidth constrained wireless links. Since the hosts are mobile, the network topology may change rapidly and unpredictably over time. one of the fundamental tasks that an ad hoc network should perform is routing path during routing congestion occurs the congestion is due to low bandwidth and weak link and flooding in order to reduce the congestion control we introduce a minimum routing and secured routing path in communicating from one node to neighborhood .once the node travels the priority of a path is based on the ascending order of the distance from one node to another These nodes are get connected from source node to the destination node .The data transfers from each node is secured by a EMSR-Algorithm. The efficiency of the algorithm is proved by the NS-2 simulator by creating a minimum spanning tree routing path and the performance is verifies by simulation technique.

2. RELATED WORK

In Mobile Ad-Hoc network the common problem is congestion control when it communicates from one network to another.The problem can be overcome by minimum spanning tree algorithm by minimize the length of the connecting network. To minimize the length of the connecting network it never pays to have any cycles it forms a acyclic path. The edges are added to the node in the increasing order of the weight. Minimum spanning tree is generated from relative neighbourhood graph (RNG). While connecting the nodes to form a acyclic graph G=(V,E).We propose a EMSR algorithm and the message transfer from source node to destination is encrypted and a ID is created and the ID is passed to receiver end .

3. PROPOSED ALGORITHM

Algorithm EMSR(Undirected graph, spanning tree)

```
Step 1 G=(V,E) be the undirected Graph
Step 2 |V| = n
Step 3  Start with graph T=(V,Ǿ) consisting of
        Vertices of G and no edges
Step 4 Arrange E in ascending order of the cost
Step 5  for i=1 to n-1
Step 6  select the smallest cost edge E
Step 7  connect the edge to form a path
Step 8  if the edge connects to a form a cycle
Step 9  discard the edge E
Step10  return T
```

I. ROUTING AND SECURE PATH

In an ad hoc wireless network, the routing and resource management are done in a distributed manner in which all nodes coordinate to enable communication among them as a group. This requires each node to be more intelligent so that it can function both as a network host for transmitting and receiving data and as a network router for routing packets from other nodes. As ad hoc networks significantly vary from each other in many aspects, an environment-specific and efficient key management system is needed. To protect nodes against eavesdropping, the nodes must have made a mutual agreement on a shared secret or exchanged public keys. For very rapidly changing ad hoc networks the exchange of encryption keys may have to be addressed on-demand, thus without assumption about a priori negotiated secrets. The main advantage of ad-hoc network is its economically less demanding deployment. In this work, a key exchange and encryption mechanism is presented where each node shares secret key only with authenticated neighbors in the ad hoc network thus avoiding global re-keying operations.The node is able to communicate with the neighbour node based on the priority.The data is encrypted by encryption technique and it creates an ID . The encrypted data is appended with the ID of the receiving nodes before forwarding it in the network. So, the authorized destination node initially checks the ID of the received packet. If it matches, it further decrypts based on the neighborhood key as well as the message specific key. This mechanism requires the nodes to be organized in a spanning tree fashion as spanning tree is constructed with minimum distance which can cover all the nodes without forming a cycle from a node to the neighbour node it travels .The formation of this spanning tree is Minimum secured path Algorithm.

A. *Encryption and ID KEY message transfer*

Active attacks involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data. External attacks are typically active attacks that are targeted to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls and encryption techniques. To secure group communication, nodes share a single symmetric key for encrypting and decrypting messages in existing systems. In the traditional group key exchange mechanism, if a new node joins or leaves, then the group key must be globally updated and distributed among the nodes in the group. This is referred to as group re-keying [1,6]. The disadvantage of this approach is that group re-keying needs access to a common server every time and can be complex and time consuming task. Access to a common server to generate a key every time a node joins or leaves in ad hoc environment is a time consuming process. Moreover it leads to consumption of resources in the ad hoc network. Group Key management is a subcategory of cryptography. Cryptography concerns itself with securing information so that unauthorized individuals cannot access and understand the messages sent. Key Management is essential for proper and secure distribution, creation and revocation of the keys used to secure messages

II. *MINIMUM SPANNING TREE FOR ROUTING*

Minimum Spanning tree is the possible way of construction with routes without forming a Cyclic path .our routing path is generated by Minimum routing path by spanning tree algorithm .The formation of minimum spanning tree is constructed by NS-2 Simulator. The distance between each and every node is computed as follows

$$\text{Distance (i, j)= } \sqrt{\mathbf{(xj\text{-}xi)^2} + \mathbf{(yj\text{- } yi)^2}}$$

Spanning tree is constructed with minimum distance which can cover all the nodes without forming a cycle as in figure 4. The minimum spanning tree of wireless nodes is constructed and the spanning tree path is indicated in the network animator. The purpose of constructing spanning tree is that it is simple, cheap and an efficient way to connect terminals. Spanning trees are very important in designing efficient routing algorithms. In the ad hoc environment, after a spanning tree is built to connect a group of mobile devices, a packet can be always flooded to all members along the tree structure without loop and duplicated transmission [1]. As spanning tree maintains security associations only with neighbors, the proposed security scheme makes use of this mechanism.

A. *Architecture of EMSR path*

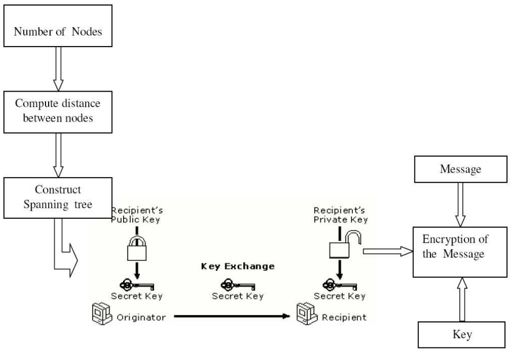


Fig 1 EMSR Routing Architecture

Spanning tree is constructed with minimum distance which can cover all the nodes without forming a cycle as in figure 4. The minimum spanning tree of wireless nodes is constructed and the spanning tree path is indicated in the network animator. The purpose of constructing spanning tree is that it is simple, cheap and an efficient way to connect terminals. Spanning trees are very important in designing efficient routing algorithms. In the ad hoc environment, after a spanning tree is built to connect a group of mobile devices, a packet can be always flooded to all members along the tree structure without loop and duplicated transmission [1]. As spanning tree maintains security associations only with neighbors, the proposed security scheme makes use of this mechanism. Node exchanges data only with its neighbors. Information about the neighbors is maintained in a neighbor table. A node also maintains an adjacency table which contains the list of all nodes with which it can exchange messages .

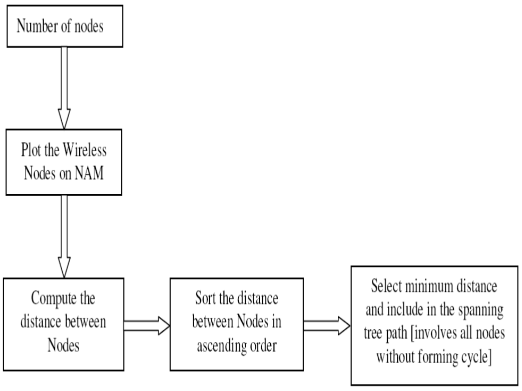
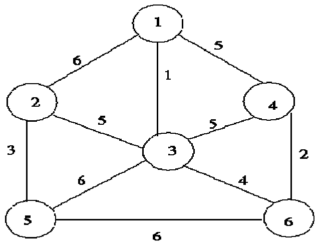

Number of nodes
Plot the Wireless Nodes on NAM
Compute the distance between Nodes
Sort the distance between Nodes in ascending order
Select minimum distance and include in the spanning tree path [involves all nodes without forming cycle]

Fig: 2 Generation Of Spanning Tree



1

Fig:3 Undirected Graph G=(V,E)

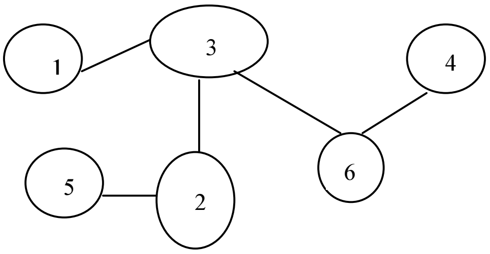


Fig :4 Generation Of Minimum Spanning Treee Routing Path

Let us consider the graph G for constructing Minimum spanning tree. The edges of the graph are arranged in the ascending order of their cost.select the minimum distance and include in constructing the path while constructing the path it should not form a cycle ,the routing of the message The proposed security scheme consists of RSA key exchange mechanism and a novel encryption mechanism to provide security. Each node in the network has its own symmetric key called the Neighborhood key. To perform encryption and decryption each node must have access to other nodes neighborhood key. At source, Neighborhood Key is encrypted with the public key of the receiver and transmitted to the destination node. At destination, neighborhood key is decrypted with the node's own private keyhould not form a cycle .A tree with n vertices has n-1 edges

4. AGREMENT OF TRANSFER OF KEY MECHANISM,

The proposed security scheme consists of RSA key exchange mechanism and a novel encryption mechanism to provide security. Each node in the network has its own symmetric key called the Neighborhood key. To perform encryption and decryption each node must have access to other nodes neighborhood key. At source, Neighborhood Key is encrypted with the public key of the receiver and transmitted to the destination node. At destination, neighborhood key is decrypted with the node's own private key Each node has its own symmetric key called neighborhood key which is encrypted. Then, the message is encrypted using the message specific key which is the MAC address. Further, the message specific key is encrypted with neighborhood key. Then, the sender appends the destination nodes ID and transmits this message to its authenticated neighbors. Source Node A creates a Message Specific Key[MKey(M)]. Message is encrypted with Message Specific Key [EMKey(M)(M)]. Further the Message Specific Key is encrypted with A's neighborhood key [ENKey(A) (MKey(M)]. Then, the Destination node's ID is appended to the Ciphertext [(ENKey(A)(MKey(M) EMKey(M)(M)) Node ID(B)].

5. DECRYPTION ALGORITHM

At receiving end, if the ID of the node matches, then it is the intended recipient and decryption is performed with neighborhood key of sending node and the plain text message is obtained. As a next step, further decryption is done with the message specific key and the original message is obtained. If the node is not the intended recipient, it again re-encrypts the message with the neighborhood key and transmits to its authenticated neighbor nodes. The procedure is repeated until destination node is found and the original message is decrypted at the destination node. Two different symmetric encryption algorithms are used to encrypt the message and the neighborhood key with the message-specific key. The advantage of implementing two different encryption procedures is to make it to improve the security of the message being forwarded in the ad hoc network which is susceptible to more vulnerable attacks.

6. NEIGHBORHOOD KEY EXCHANGE PROCEDURE

Key exchange with only neighborhood nodes aims at reducing crypto-functions processing overheads occurred in a pure reactive approach. This neighbor detection scheme is identity-free and is carried over through a handshake process between any pair of neighbors. Handshaking procedure is basically carried over for key exchanges between a given node and its new detected neighbors. After the handshake procedure, each pair of nodes shares a chain of secret keys. HELLO messages are periodically sent to the nodes in the group. To forward the information the RREQ and RREP messages are used by each intermediate node to establish the route between the source and the destination nodes in the network

7. SIMULATION RESULTS

The spanning tree is constructed using NS2 simulator. NS simulator is based on two languages: an object oriented simulator, written in C++, and OTcl (an object oriented extension of Tcl) interpreter, used to execute user's command scripts. A simulation script generally begins by creating an instance of this class and calling various methods to create nodes, topologies, and configure other aspects of the simulation, as the nodes are organized in spanning tree topology in this security scheme, the nodes exchange keys and data only with its authenticated neighbors. This avoids expensive global rekeying operations when the membership in the network changes or when the network is partitioned. Figure 3. is a simulation output of wireless nodes plotted on NAM in the form of a spanning tree and the packets transferred between the nodes involved in the spanning tree path is obtained. Figure 4. and Figure 5. Represents the simulation output of the throughput of the packets sent and the packets received.

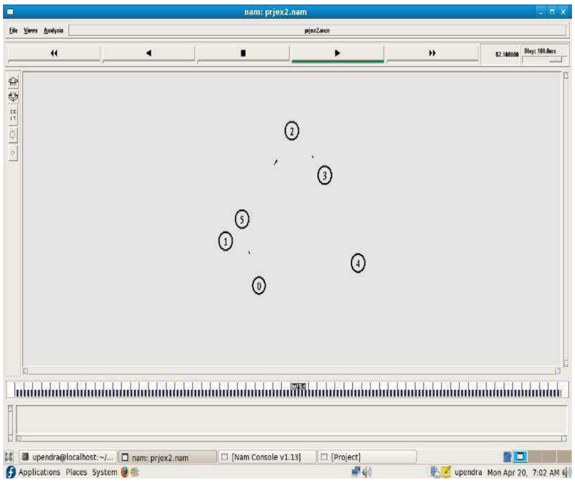
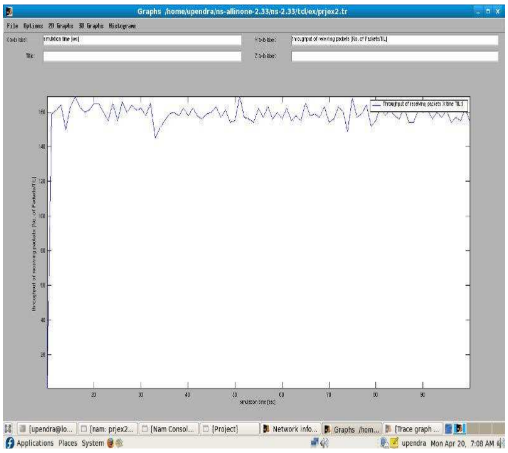
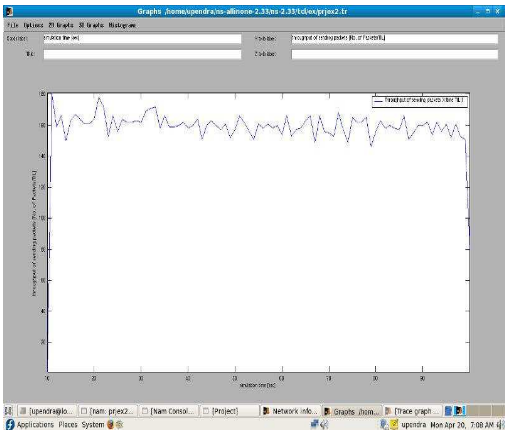


Fig:5 Packet Transfer Between Nodes In Spanning Tree


Graphs /home/upendra/ns-allinone-2.33/ns-2.33/tcl/ex/prjex2.tr

X axis label: simulation time [sec]
Y axis label: throughput of receiving packets [No. of Packets/TIL]
Title:
Z axis label:

Fig :6 Throughput Of Receiving Packets


Graphs /home/upendra/ns-allinone-2.33/ns-2.33/tcl/ex/prjex2.tr

X axis label: simulation time [sec]
Y axis label: throughput of sending packets [No. of Packets/TIL]
Title:
Z axis label:

Fig :7 Throughput Of Sending Packets

8. CONCLUSION AND FUTURE ENHANCEMENT

The advantage of EMSR routing path is to reduce congestion in routing due to less bandwidth and flooding and creation of minimum spanning tree reduces the distance and the efficiency of the routing path is more efficient and novel security scheme of encryption schemes, one with neighborhood key and other with message specific key, more security is imposed. It ensures backward secrecy (a new member of network cannot access data transmitted before the member joined and forward secrecy (a member cannot access the data that is transmitted after the member leaves the group). Whenever the topology changes withthe inclusion or exclusion of a member, new neighborhood key is computed and is distributed to all authenticated neighbors. Enhanced security scheme in ad hoc networks is presented which can address the security issues such as authentication, confidentiality and key management that would avoid global re-keying. The proposed EMSR aims at sender deniable encryption can be widely applicable for voting and auction protocols. This shall be applicable wherever group communications is to be established in a secured manner in an ad hoc environment. The future enhancement to the implementation of the proposed security scheme is to incorporate the key storage, message storage at the node level and compare the performance of spanning tree with and without the inclusion of features such as key storage and message storage.

REFERENCES

[1] Jorg Liebeherr, Guangyu Dong, "An overlay approach to data security in ad-hoc networks" Science Direct, Ad Hoc Networks, pp. 1055-1072, July 2010.

[2] Matthew J. Moyer, Josyula R. Rao, Pankaj Rohatgi, and Thomas.J, "A Survey of Security Issues in Multicast Communications", IEEE Network, November 2009.

[3] David Manz, Jim Alves-Foss and Shanyu Zheng, "Network Simulation of Group Key Management Protocols", Journal of Information Assurance and Security, pp. 67-79, January 2008.

[4] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE Network, November 2010.

[5] Vesa Kärpijoki, "Security in Ad Hoc Networks", Seminar on Network Security, 2000.

[6] X.B. Zhang, S.S. Lam, H. Liu, "Efficient group rekeying using application-layer multicast", in Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, (ICDCS 2005), June 2009.

[7] C. Gui, P. Mohapatra, "Efficient overlay multicast for mobile ad hoc networks", in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), March 2003.

[8] Y.C. Hu, A. Perrig, "A survey of secure wireless ad hoc routing", IEEE Security and Privacy 2 (3) (2004).

[9] Kevin Fall, Kannan Varadhan, " The ns manual", The VINT project, December 2008.

[10] Brent Welch, "Practical Programming in Tcl and Tk", Prentice Hall, May 2011.