Secured Data Transmission In On Demand Routing Protocol Using Adhoc Networks

B.L. Rai
Department of Computer Science & Engineering, JNCT, Bhopal

Dr. Vivek Richhariya
Department of Computer Science & Engineering, LNCT, Bhopal

Abstract: ***Ad hoc networks are highly dynamic routing networks cooperated by a collection of wireless mobile hosts without any assistance of centralized access point, so that's why adhoc networks are very dynamic, self organizing, self healing distributed networks which supports data networking without an infrastructure. By this user can use the network services efficiently and securely while moving, by using our proposed scheme. Security mechanism in MANETs usually contains secure routing and secures data transmission. There are already some mechanisms to secure end-to-end transmission but there are limited number of strategies of securing the routing message or protocols. In this paper, we deliberate technique which is used to store backup routes from multiple routes available between source and destination.***
Keywords: Security mechanism in MANETs

I. INTRODUCTION

Mobile ad hoc network (MANET) is a relatively new innovation in the field of wireless technology. These types of networks operate in the absence of fixed infrastructure, which makes them easy to deploy at any place and at any time. The absence of any fixed infrastructure in mobile ad hoc networks makes it difficult to adopt the existing techniques for network services, and poses a number of various challenges in the area.

Wireless network enables communication between computers using standard network protocols, without network cabling. There are two kinds of wireless networks viz. Access point and Ad-hoc networks. In Access point, wireless network uses an access point or base station, which acts as hub providing connectivity between two different nodes, wired and wireless LAN, a node and wireless LAN, etc., In Ad-hoc networks [6], direct communication between nodes are possible by using wireless networking interface cards, without any access points. Because of its infrastructure less feature, ad-hoc wireless networks provide the facility for the user to use the network services while continually moving. The application scenario for the mobile adhoc networks is emerging in recent years. Three main parameters to be concentrated for the communication in mobile adhoc networks are routing, service location [8] and security issues [3]. To overcome the problems faced in routing the data in these networks, we propose a new protocol for the same networks, which reconnects the nodes in case of link failure due to any disturbances [4]. Each node in this network should be capable enough to connect high end Lap-tops to Low end PDA's and mobile phones [3]. So, a node should support multiple interfaces and become heterogeneous. Generally, routing protocols are categorized as table driven and on demand [5]. On demand routing protocols are preferred for quiet fast routing. It serves the user's issue in adhoc mobile networks [1]. In this paper, we propose an on demand backup node setup protocol for quick routing which supports heterogeneous interfaces at each node.

So we also concentrate on secure way of transmitting data using voice for generating encryption and decryption keys [7]. This paper proposes an on demand routing and secured data transmission for adhoc wireless networks supporting heterogeneous interfaces. The goal of this paper involves reconnecting the nodes with heterogeneous interfaces immediately, if any link failure happens during the secured communication using a back-up [4].

II. ADDRESSING IN ADHOC NETWORKS

We would like to say about the addressing of nodes in mobile adhoc network, before dealing with the design architecture of our protocol. Addressing can be done in two ways. a. Flat addressing b. Hierarchical addressing [3]. In flat addressing, a node address is independent of its location. The type provides flexibility reducing scalability. In hierarchical addressing, nodes are resisted to move within their branch of hierarchy. Each move of node requires the updation of hierarchy. Our approach uses flat addressing scheme. Each node selects and uses one IP address similar to the notion of a mobile IP home address. Each node is connected to different type of devices with the help of interfaces. Interfaces are identified by an interface index which is opaque identifiers. Each node chooses its interface indices independently. An example for addressing in our scheme is as follows

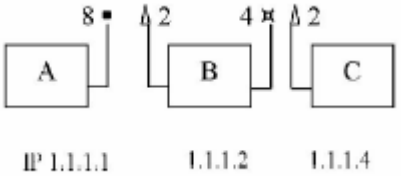

Fig. Addressing with Multiple Interface

Suppose if node A want to communicate with node C through interface indexed 8 in A and interface indexed 2 in C. The communication route is given as

A → B : B → C

1.1.1.1/ 8 → 1.1.1.2 /2 : 1.1.1.2/4 → 1.1.1.4/2

III. PROPOSED SCHEME

Our scheme involves four phases

1. Route discovery across the nodes with multiple interfaces.
2. Back up node setup.
3. Secured data transmission using voice
4. Route maintenance across the nodes supporting multiple interfaces.

Published By:
International Journal of Engineering Research in Current Trends

It requires three kinds of cache, RD request cache, Backup route cache and fresh route cache.

The RD request cache of a node is used to store temporary routing information in the route discovery phase. The Backup route cache is used to store back-up routes. The Fresh route cache is used to store the fresh routes after a data transmission process is finished [4].

A. Route discovery across the nodes with multiple interfaces

When source node S requires the route to destination D, S enters the route discovery phase and checks whether adequate "fresh" routes to D are already available in the Fresh route-cache. If some "fresh" route to D in Fresh route_ cache is found, S runs Route confirm process. Otherwise, S runs new route discovery process to find a new route to the destination node

1. New route -discovery process

Source node S broadcasts RD request to nearly nodes RD request includes a sequence number field to distinguish the route discovery process from others and a route content field for node address and interface indices along the path from S to D. After the intermediate node receives RD request from an upstream node X, it inserts its address and interface index into the route content field of the RD-request and then sends this modified RD-request to its neighboring nodes (excluding the upstream node X). The RD request cache of the intermediate node also records the information, including the sequence number of the RD-request and which neighboring nodes are sent only if the request is not duplicated. Otherwise, the duplicated request is discarded.

2. Route _ confirm process

If a "fresh" route is available to the destination in the Fresh_route_cache, the source node S adds the fresh route from S to D to the RC request and then transmits RC request along this route. When it receives the RC request, an intermediate node hecks its Fresh route cache to determine whether any other fresh route to D is included. If a "fresh" route is available, the node copies RC request and puts the route information in the route content field of the RC request before transmitting the RC request along this fresh route. If no "fresh" route is available, RC request is transmitted downstream according to its route content field. Eventually, after D receives the RC request, RD-reply is sent back to S, and S sends packets by this original Route

B. Backup node setup phase

When the RD request or RC-confirm reaches the destination D, it may gather many routes with in a period Tc [4]. The nodes of those routes which D received are compared pair wise from beginning to end to find whether any two paths have a section in common. The final node, excluding destination D, in such a section is the "backup node". A subset of backup nodes can be gathered from any two routes. Then, all the subsets of backup nodes are joined and the BS packet that includes each backup node and the partial path from the backup node to the destination node are generated. The destination node then uses BS_packet to separately setup the backup route cache of those backup nodes, where the BS-packet contains the sequence number of this routing process, the address of a back up node along with interface under the path from the backup node to the destination. The backup nodes store the partial paths from the backup node to the destination node in their backup_route_cache after they receive the BS-packet.

C. Secured data transmission using voice

After establishing the route, source S has to transmit the data. To avoid the data being hacked by unauthorized users in the route, data is secured by the following process. (See fig 2) The microphone setup gives the guidelines to place the headset in a correct position. In some situations, the microphone and headphone may not be in proper location. In such case the setup will give the proper procedure to connect the positions. The user has to atter his name or any keyword for voice authentication. To provide double protection, the user has to type the password.
The username that was spoken as well as the password typed by the user does the authentication.

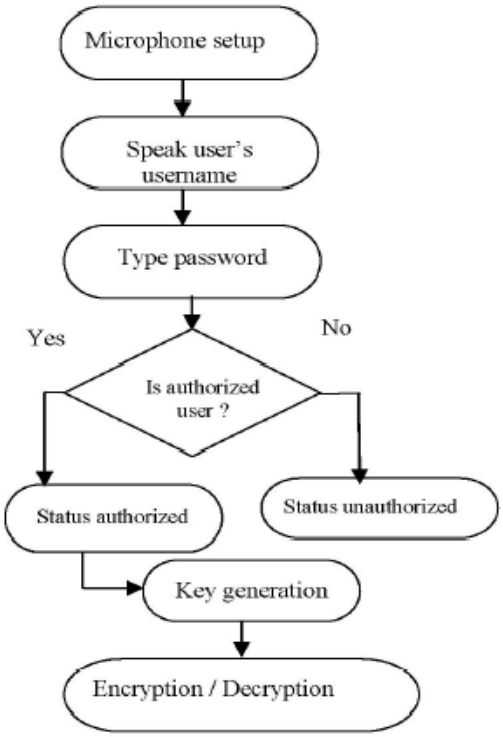

Fig. 2. Sender and Receiver Process

Using the voice authentication and text, the key is generated for each authenticated person uniquely which provides double security. The vocal patterns are unique to the user, so the voice authentication provides better security. Unfortunately, if any voice of 2 different users matches, then the second option that is the text authentication is used. Even if the attackers knows the username they are unable to read the message because the user's voice only acts as keying material to activate the stored key. If the user is a new person, then first the new user voice is trained and then the administrator has to generate the key for the new user and it will be maintained in the database. After the key generation, the data is encrypted using the key which is generated by the administrator using public key algorithm RSA. After the encryption the data packets are transmitted in the discovered route. When the destination receives the data packets, it has to generate the decryption key using the receiver's voice. By using this decryption key and RSA

algorithm the authorized receiver can retrieve the original message.

D. Route maintenance across the nodes with multiple interfaces

When a link fails, a node cannot continue to transmit. The node sends an error message, link_fail_message, to an upstream node along the reverse current route. This message is used to announce the back up node alone in the route to replace the ackup route. The alert message will not be passed by an upstream node until the message is returned to a backup node. When the backup node receives the message of link failure, the backup route of backup route-cache is fetched to replace the route behind the backup node, and the source node S is informed to change the route. Thus, the node S sends the packets along the new route. If backup route cache includes no other backup route, then the node has lost the identity of the backup node. Under such circumstances, no backup node exists. The source node will receive the link failure message and re-enter the route discovery phase to establish a new route to the destination. After the destination node replies with a path back to the source as the current route for sending data packets, some backup routes are established and stored in backup nodes. If the current route is still alive, the situation that any node along the backup routes moves will not influence the communication of the current route. If the current route is broken and replaced by a back up route, it can still work even though a section of this backup route has failed. That is because the link which failed will be detected and an alert message will be sent to find another back up node. When S does not have the route to D S will store the usable route into the fresh route cache and broadcast RE request to announce all backup nodes that this data transmission process is ending. The RE request packet contains the sequence number of this transmission process for distinguishing it from other process. When the backup node receives RE request, it will also save remnant backup routes from backup route cache in fresh_route_cache.

IV. CONCLUSION

Our proposed scheme is an on demand routing protocol with secured data transmission in a mobile adhoc wireless networks. It addresses how to reconnect quickly when the transmission fails, in case of nodes with heterogeneous interfaces. It provides backup node mechanism to reconnect quickly as required for adhoc wireless networks. It has a better performance than DSR in low mobility because it provides a mechanism of backup routes for shortening the delay of reconnection when a link fails. Furthermore, it also concentrate on secured way of transmitting data even it crosses through multiple intermediate nodes with heterogeneous interfaces.

REFERENCES

[1] D.B.Johnson and Maltz," Dynamic Source Routing in ad hoc Wireless networks", in T.Imielinski and H.Korth, mobile computing, Kluwer academic Publishers, Boston, 1996, pp- 153-181.

[2] Fabian Monrose, Michael Reiter.K, Qi Li, Susanne Wetzel, "Cryptographic key generation from voice", Bell Lucent Technologies, Murray Hill, New Jersey, USA,2001.

[3] J.Broch, D.A. Maltz, and D.B Johnson, "Supporting hierarchy and heterogeneous interfaces in multi-hop wireless ad hoc networks", in Proceedings of the 4th International Symposium on Parallel Architectures, Algorithms, and Networks, 1999, pp-370-375.

[4] Ying-hong Wang and Chih-Chieh Chuang," Adhoc On- Demand Backup Node Setup Routing Protocol", Journal of information science and Engineering, 20,821-843, 2004

[5] D.A. Maltz, J.Broch, J.Jetcheva, and D.B.Johnson, "The effects of on-demand behavior in routing protocols for multihop wireless ad-hoc networks",IEEE Journal on Selected Areas in Communications, Vol.17, 1999, pp.1439-1453.

[6] H.Li and D.Yu,"Comparison of ad hoc and Centralized multi hop routing", in Proceedings of 5th International Symposium on Wireless Personal Multimedia Communications, Vol.2, 2002, pp-791-795.

[7] Davida G. I, Frankel Y, and Matt B. J, "Onenabling secure applications through off-line biometric-identification". In Proceedings of the IEEE Symposium on Security and Privac, 1998.

[8] E.Guttman, C.Perkins et al,"Service Location Protocol version 2", Internet Engineering Task Force, RFC2608, June 1999.