Secured Back up Routing Protocol for Adhoc Networks

G. Lavanya, C.Kumar and A. Rex Macedo Arokiaraj

Abstract—**Adhoc mobile networks are very dynamic, self organizing, self healing distributed networks which support data networking without an infrastructure. The user can use the network services efficiently and securely while moving, by using our proposed protocol. This protocol is used to store secured backup routes from multiple routes available between source and destination, in order to provide the next possible route immediately when the link fails during the data transmission. Furthermore, it incorporates security attributes as parameters into Adhoc route discovery.**

Index Terms—**C Backup routes, on-demand routing, routing protocol, wireless networks.**

I. Introduction

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 anaccess 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, direct communication between nodes are possible by using wireless network 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 networks are secured routing \[11], service location issues \[4], routing and security \[8]. To overcome the problems faced in routing the data securely in the networks, we propose a new protocol for the same network which reconnects the nodes in case of link failure due to any disturbances.

Each move of the mobile nodes will change the topology of the network in the transmission route. Sometimes leads to the disconnection of link, because communication is through radio waves. When there is a poor environment and the distance between the nodes is large, disconnection may occur \[3]. Due to lack of trusted nodes, Mobile adhoc networks require specialized authentication protocol. To overcome the issues of malicious nodes which paralyze the network by inserting erroneous routing updates, replaying old routing information, changing routing updates or advertising incorrect routing information\[8], we propose an approach to routing that incorporates security levels of nodes in the path information.

Generally, routing protocols are categorized as table driven and on demand. Table driven routing protocol maintain consistent and up to date routing information among the nodes in a routing table. On demand routing protocols \[6] discover a new route, when a route is required from the source to the destination node. It serves the user¡¯s issue in adhoc mobile networks. Dynamic source routing protocol \[7] is one among many on-demand routing protocols. It includes two major phases, route discovery and route maintenance phase. In the route discovery phase, a source needs to find a new route to the destination by broadcasting a route request message with a unique request ID. When the destination node receives this request, it sends an acknowledgement message with path information to the source. In the route maintenance phase, each node along the route detects the transmissions of data packet by a passive acknowledgement. If a node does not receive the acknowledgement forwarding the packet along the route, a route error packet is generated by the node and sent to the original source node, informing the disconnection of link to the source \[7]. DSR has a long delay when a route is reconnected or rebuilt. To improve the quality of routing \[2] and protection \[14] in ad-hoc networks, we propose a secured on demand backup node setup routing protocol for these networks to reconnect the nodes immediately if any link failure happens during the communication using the backup.

The security issues are emerging in dynamic adhoc networks at the routing level with a battlefield communication scenario. Most of the time, the adhoc networks \[5] has more than two parties and information must pass over some intermediate stages, nothing but the other nodes in the network. Therefore, the information flow must be secured \[8] from the third party devices even if it is on the flow. Since adhoc network is generally on air communication it is open for eavesdropping or interference \[1]. So these networks should be prevented from such kinds of attacks. In our proposed protocol, the sender can make decisions about the quality of protection by embedding security attribute along with the route request message in the route discovery phase. As the secured route is discovered, the data packets are securely transmitted without being hacked by unauthorized nodes.

II. Trust Key Generation

A common trust key is given to all the group nodes. Any node that has the same trust key can participate in routing. Therefore, the key has to be generated by each node by installing a common proposed algorithm. The proposed algorithm works with respect to time. Initially, all the group

email :lavanya_joyce@yahoo.co.in, ckumarme81@gmail.com

nodes are synchronized.

Taking the system time as the input, the trust key generator converts into total seconds and the time is seconds¡¯ acts as a key for encrypting the route request packet. The trust key is added along with the route request for identifying the secured route. The route request packet size is increased in the proposed routing protocol. The trust key in all the nodes vary for every short time period ¡®Td¡¯ ,it should not be too small, so that the route request packet trust key should match with the intermediate node and destination node¡¯s trust key. Td should not be too large, because the hackers might try to find the trust key to participate in routing. The trust key has to be moderate in order to provide secured routing process.

III. SBRP Protocol

Our SBRP protocol involves three phases

1. Secured route discovery across the nodes.
2. Back up node setup.
3. Route maintenance across the nodes.

It requires three kinds of cache, RD request cache, Backup route cache and Fresh route cache \[3]. 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 secured fresh routes after a data transmission process is finished.

A. *Secured Route Discovery across the nodes*

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¡± routes to D in Fresh route cache are found, S runs Route confirm process. Otherwise, S runs new secured route discovery process to find a secured new route to the destination node.

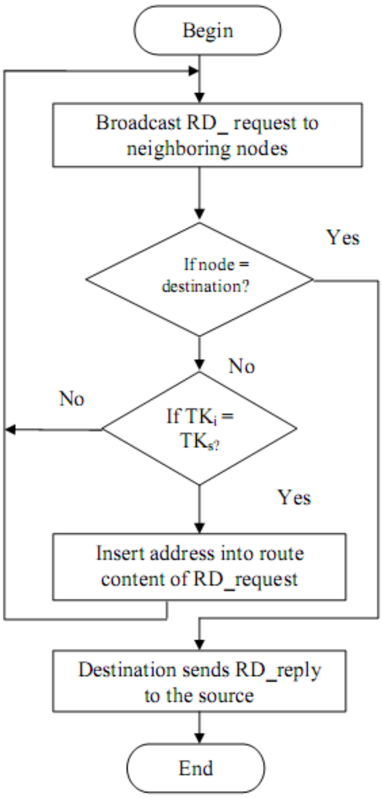
Begin
Broadcast RD_ request to neighboring nodes
If node = destination?
Yes
No
No
If TK$_i$ = TK$_s$?
Yes
Insert address into route content of RD_request
Destination sends RD_reply to the source
End

Fig.1 Secured route discovery process with trust key

1) *New secured route discovery process*

Source node S broadcasts RD request to nearby nodes; RD request includes a sequence number field to distinguish the route discovery process from others , a route content field for node address along the path from S to D and the trust level of the source. After the intermediate node receives RD request from an upstream node X (See Fig. 1), it inserts its address into the route content field of the RD request only if it is in the same trust level of the source by confirming the trust key 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 from source to the destination in the Fresh_route cache, the source node S adds the secured 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 checks 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 through this original route.

B. *Backup node setup phase*

When RD_request or RC_confirm reaches the destination D, it may gather many secured routes with in a period ‘TC’. 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 secured 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 secured routing process, the address of a back up node 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 \[3].

C. *Route maintenance across the nodes*

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 secured backup 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 secured backup route from 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 secured route. If backup_route cache includes no other secured 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-enters the route discovery phase to establish a secured 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 secured backup routes are established and stored in backup nodes. If the current route is still alive, the situation that any node along the secured backup route moves will not influence the communication of the current route. If the secured 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 secured backup routes from backup_route cache in Fresh_route cache.

IV. Simulation and Results

The performance analysis of SBRP is carried out by simulating the model of mobile Ad hoc networks in Network Simulator (NS 2). Simulations could be carried out with more complex scenarios using higher traffic rates. However, the simulations take much longer time to complete and the trace file generated by each run ends up to few MB of user space. After each simulation, trace files recording the traffic and node movements are generated. These files are parsed in order to extract the information needed to measure the throughput. Each node is placed at the random position in the simulated area mentioned in table 1. After sending a packet to the next node, the packet is dropped if the sender does not receive an acknowledgement from the next node. The timer of SBRP is assigned a period of 20 ms.

Mobile Nodes	50
Transport Protocol	UDP
Application	CBR
CBR packet size	512 Kb
CBR interval	0.05 sec
Routing Protocol	ABRP
Node Velocity	20 m/s
Interface queue type	Drop Tail
Mac Type	802.11
Max packet in ifq	50
Topography	1600m X 1600m

Table.1 List of Simulation Parameters

The total number of packets received by the destination using SBRP routing protocol is higher than the ad hoc backup routing protocol.

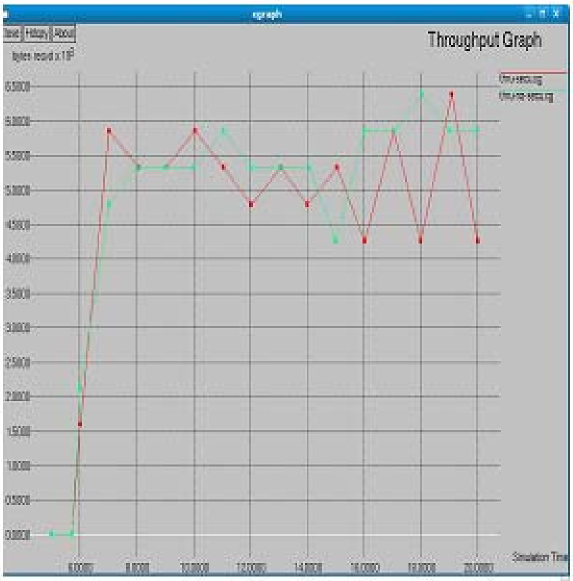

Fig.4 Throughput comparative graph of SBRP and ABRP

Simulation of Backup routing protocol is carried out with security and no security. (Analysis is carried out between ABRP and SBRP). The throughput measured at every instant of time is shown in fig.4 the average through put graph is shown in the fig.5.

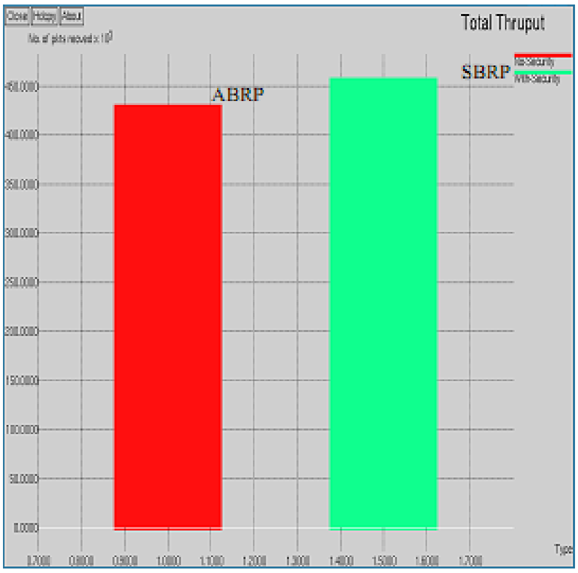

Fig.5 Average Through put for ABRP and SBRP

V. Conclusion

The SBRP is an on-demand routing protocol in a mobile ad hoc wireless network. It discovers a secured route for communicating packet from source to destination through a trust key included in the route request packet. It addresses how to reconnect quickly when the transmission route fails and to retransmit the packets to the destination. According to the proposed SBRP, many secured routes can be found to reach a destination in a given period. Those routes, almost always more than one, from the source node to the destination node can be analyzed to obtain some good secured backup routes to support reconnection and retransmission in a secured manner in case of link failure. Issues such as Qos and multicast will be addressed to enhance the capability of the SBRP .Moreover, supporting hierarchy and heterogeneous interfaces in ad hoc wireless networks can also be considered in order to enhance the scale of application for SBRP.

REFERENCES

[1] Murat Cihan, Cetin Kaya Koc, "Setting Initial Secret Keys in Mobile Adhoc networks", Oregoen State University, Oregon 97331, USA.

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

[3] Ying-Hong Wang and Chih-Chieh Chuang,"Adhoc On-Demand Backup Node Setup Routing Protocol", Journal of Information Science and Engineering, 20, pp 821-843, 2004.

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