Modified Secure Associativity Based Routing

K. Muthumayil[1], M.Chitty Babu[2], P.Senthil Kumar[3]
Department of Information Technology, PSNA College of Engineering and Technology, Dindigul. Tamilnadu, India

kmuthumayil@gmail.com[1], chittyb.com[2], senthilkumarparmasivam@gmail.com

Abstract- **In large mobile ad hoc networks(MANET), associativity based long lived routing(ABR) protocol can offer significant performance improvement over other source-initiated on demand routing protocols by using associativity ticks to communicate with other mobile devices. In this paper we propose a Modified Secure Associativity Based long lived routing (MSABR)mechanism which provides source authentication and message integrity by using a shared secret key. In this paper, we have introduced SRP with different perspective to provide more security for ABR. By combining SRP with associativity based long-lived routing , we prepare a Modified secure associativity based long-lived routing, here any sender/receiver can verify each other.**

Keywords – MANET,ABR,Associativity ticks ,SRP, MSABR

I. Introduction

Mobile ad-hoc networks consist of nodes that are able to communicate through the use of wireless medium and form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network, all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not exist.

AODV[7] is perhaps the most well-known routing protocol for a MANET. It is a *reactive* protocol: nodes in the network exchange routing information only when a communication must take place and keep this information up-to-date only as long as the communication lasts. When a node wants to send a packet to another node, it starts a *route discovery* process in order to establish a route toward the destination node. Therefore, it sends its neighbors a route request message (RREQ). Neighboring nodes receive the request, increment the hop count, append their identifiers and forward the message to their neighbors, so that RREQs are actually broadcasted using a *flooding* approach. The goal of the RREQ message is to find the destination node, but it also has the side effect of making other nodes learn a route towards the source node (the *reverse route*): a node that has received a RREQ message, with source address S from its neighbor A, knows that it can reach S through A and records this information in its routing table along with the hop count (i.e., its distance from node S following that route).

The RREQ message will eventually reach the destination node, which will react with a route reply message (RREP). The RREP is sent as a unicast, using the path towards the source node established by the RREQ. Similarly to what happens with RREQs, the RREP message allows intermediate nodes to learn a route toward the destination node (i.e., the originator of the RREP). Therefore, at the end of the route discovery process, packets can be delivered from the source to the destination node and vice versa. A third kind of routing message, called route error (RERR), allows nodes to notify errors, for example, because a previous neighbor has moved and is no longer reachable. If the route is not active (i.e., there is no data traffic flowing through it), all routing information expires after a timeout and is removed from the routing table.

AODV routing was created without taking security into major concern, which it should be the most important factor to be looked at. The analysis

1

on the security threats that have been made to describe the requirements for AODV routing protocol to mitigate threats. A node is malicious if it is an attacker that cannot authenticate itself as a legitimate node due to the lack of valid cryptographic information. A node is *compromised* if it is an inside attacker who is behaving maliciously but can be authenticated by the network as a legitimate node and is being trusted by other nodes.

The security requirements [1] for AODV routing protocol include:

1) *Source authentication*: The receiver should be able to confirm that the identity of the source is indeed who or what it claims to be.
2) *Neighbor authentication*: The receiver should be able to confirm that the identity of the sender (i.e., one hop previous node) is indeed who or what it claims to be.
3) *Message integrity*: The receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit.
There are a number of secure protocols proposed especially for AODV to mitigate the attacks like S-AODV

II. Related Work

An extension of the *Ad Hoc On-demand Distance Vector* (*AODV*) [14][15][16][17]routing protocol has been proposed to protect the routing protocol messages. The *Secure-AODV*[6][7][14][15][16]scheme assumes that each node has certified public keys[1][2][3] of all network nodes, so that intermediate nodes can validate all in-transit routing packets. The basic idea is that the originator of a control message appends an *RSA signature* and the last element of a *hash chain*[8][9] (i.e., the result of *n* consecutive hash calculations on a random number). As the message traverses the network, intermediate nodes cryptographically validate the signature and the hash value, generate the *k-th* element of the hash chain, with *k* being the number of traversed hops, and place it in the packet. The route replies[5][15][17] are provided either by the destination or intermediate nodes having an active route to the sought destination, with the latter mode of operation enabled by a different type of control packets. The use of public-key cryptography imposes a high processing overhead on the intermediate nodes and can be considered unrealistic for a wide range of network instances. Furthermore, it is possible for intermediate nodes to corrupt the route discovery by pretending that the destination is their immediate neighbor[2], advertising arbitrarily high sequence numbers and altering (either decreasing by one or arbitrarily increasing) the actual route length. Additional vulnerabilities stem from the fact that the *IP* portion of the *S-AODV* traffic can be trivially compromised, since it is not (and cannot be, due to the *AODV* operation) protected, unless additional hop-by-hop cryptography and accumulation of signatures is used. Finally, the assumption that certificates are bound with *IP* addresses is unrealistic; roaming nodes joining *MANET* sub-domains will be assigned *IP* addresses dynamically (e.g., *DHCP*]) or even randomly

III. Modified ABR

Recent research has shown that associativity based routing (ABR)[6] can be a good alternative to Location Aided Routing (LAR) in large MANET's. By using associativity ticks of all the nodes, the path can be determined by the source, specifically associativity is measured by the nodes connectivity relationship with its neighbors changes as it is migrating and its transition period can be identified by associativity ticks or counts very often(for every 60secs).Associativity ticks are measured by sending the "HELLO" message to all the nodes. Then the nodes reply to the node from where the HELLO message has come. If the node will be available long time, it will send the positive reply, otherwise negative reply. So all the nodes are storing these positive valued nodes in their list.

Our proposed Modified ABR consists of three phases

1) Route discovery
2) Query propagation
3) Route reply

Initially when a source node wants a route, the "Secure Route Discovery" phase is invoked. After source sends the RREQs, "Secure Query Propagation" phase is invoked. Then the destination

receives the RREQs from all the paths and it invokes "Route Reply" phase.

A..Route Discovery Process.

When the source node wants to send a data packet to a destination node D and does not have a route to D. It initiates route discovery by broadcasting a route request RREQ (**broadcast** message) to its positive neighbors. Here a sequence number is used to uniquely identify each BQ packet.Once the query packet is broadcast by SRC, all intermediate nodes that received the query will check whether it is the destination or not. If it is not the destination the intermediate node appends its address and identifiers in the query packet and broadcasts to its neighbors. This process is repeated until the RREQ reaches the destination node.

After receiving all BQ packet through various paths, the destination will know all the possible routes and their qualities. It can then select the best route and send a reply packet RREP(**unicast** message) back to the source via the route selected.

B. Route Selection Rules.

Among a set of possible routes from source to destination if a route consists of mobile nodes having high associativity ticks then that route will be chosen by the destination despite of other shorter hop routes. However if the overall degree of association stability of two or more routes is same then the route with the least number of hopes will be chosen. If the multiple routes have the same minimum hop count, then one of the routes will be arbitrarily selected.

C. Secure Route Discovery Process.

The widely accepted technique for discovering the routes in MANET is broadcasting the query packets. The query packet are traversing the network, the relaying intermediate nodes append their identifier (IP address) in the query packet header. When one or more queries arrive at the destination, it replies to the querying node with all the possible routes. Then the source or querying node may use one or more of these routes_to forwarding the data.

This basic route query broadcasting mechanism yields a secure discovery called Secure Routing Protocol (SRP). Here SRP is combined with ABR with different perspective to provide secure route discovery process.

IV. Proposed Scheme

A. Basic Assumptions.

A security association (SA) between the source node 'S' and the destination node 'T' is assumed. In this bidirectional communication between any path of nodes, a shared socket key $\mathbf{K_{st}}$ that can be used for data traffic flow in both directions. This SA employs a secure communication scheme and should be able to authenticate each other. The identities of the traversed intermediate nodes are also stored in the route request packet. The source and destination and the unique query identifiers are the inputs for the calculation of Message Authentication Code (MAC). Associativity ticks are counted for each node by using their reply to the "HELLO" messages from various nodes.

B. Overview.

Our work provides a novel approach to the secure route discovery operation for MANET routing protocols. The proposed scheme guarantees the source route discovery process using Secure ABR and secure data forwarding by using SMT (Secure Message Transmission).

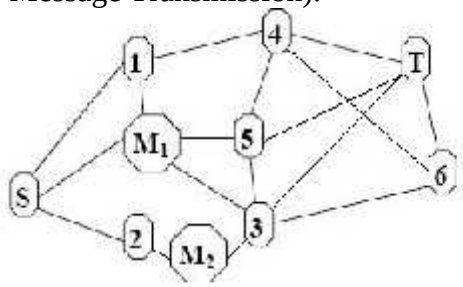

Figure 1: Source S communicates with Destination T through malicious nodes M1 and M2.

Secure ABR safeguards the route discovery and makes use of some cryptographic tools. In SRP only the end nodes have to be secured. It does not impose any cryptographic validation and verification of traffic at intermediate nodes for decentralized environment, SRP poses the overhead

3

on the end nodes, not at intermediate nodes. SRP provides one or more route replies, both from intermediate nodes and destination. So the destination node acquires correct network connectivity information of various paths and the ability to choose an optimal route based on the stability of the nodes or less number of hops or any route will be chosen arbitrarily. Finally, SRP produces the routing and control traffic overhead and protects end nodes against attacks. In this secure route discovery, any malicious node between source **S** and destination **T** cannot identify the original request because the MAC value is not known (since MAC is found using the shared secret key of source and destination) to attackers.

In general, SMT safeguards thedata forwarding operation. It determines a set of diverse paths connecting the source and destination nodes. It introduces limited transmission redundancy across the paths, by dispersing a message into N fragments. So the successful reception of any range of fragments allows the reconstruction of the original message at the destination. Each fragment equipped with a cryptographic header that provides integrity and secure exchange along with origin authentication and is transmitted over one of the paths. The destination generates an acknowledgement informing the source about the reception of fragments. Otherwise the source retransmits all the fragments after the negative acknowledgement. In this paper we have proposed SMT with different perspective, that is, it sends the whole data with cryptographic parameters along with ABR long lived routing protocol. At first, ABR will choose the high stability path among many paths available. If there are many paths with the same high stability, then the one which is having minimum hop-count will be chosen. If there are more than one paths having same hop-count, then one of the paths will be chosen arbitrarily. Finally with help of SMT, the ABR protocol will forward the data packets securely to the destination. Since the message is transmitted by encrypting it using the session key of source and destination, any malicious node between source and destination cannot decrypt the scrumbled message.

V. Operation

A. Route Request.

A source node 'S' maintains a Query Sequence number Q_{seq} for each destination it securely communicates with. This 32bit sequence number increases for each route request generated by S and allows T to detect outdated route request. For each outgoing Route Request, S generates a 32bit random Query Identifier (Q_{ID}), which is used by intermediate nodes as a means to identify the request.

Both Q_{ID} and Q_{SEQ} are input to the Message Authentication Code(MAC) one way hash function SHA-1 or MD5 along with the shared secret by **Kst.** The Route Request packet propagates towards the destination. So the accumulated address of the intermediate nodes are also included in the packet. The Message Authentication Code is calculated as

$$\mathbf{M=C(K_{st}\{RREQ,SA_{NUM},Q_{ID},Q_{SEQ},SA,DA\}),\ SA,DA}$$

This is the message, the SRP sends through intermediate nodes towards destination. This MAC value will be sent through intermediate nodes towards destination. The security of this proposed work lies in calculating MAC value. In figure 1, the intermediate nodes M1 and M2 cannot decrypt the MAC value because shared secret key of source and destination is only known to the source and destination but not to intermediate nodes. So SRP provides more security for the messages. So it avoids message tampering attack.

The source nodes S initiates the route discovery by constructing a route request packet identified by the following identifiers: a query sequence number, random query identifier.Also IP addresses of source and destination and security association number($\mathbf{SA_{NUM}}$).Then they are given as input for the calculation of the Message Authentication Code (MAC).

Intermediate nodes relay route request, so that one or more query packets arrive at the destination. The route requests reach the destination T, which constructs the route replies it calculates a MAC covering the route reply contents and returns the packet to S over the selected path.

4

B. Query Propogation.

After the source sends RREQ packet through intermediate routers, they will not verify the packet because they do not know the shared secret key of source and destination. Instead, intermediate nodes are adding their identifiers along with existing packet without any encryption, so the message after leaving from one of the intermediate routers looks like

$$M=C(K_{st}\{RREQ, SA_{NUM}, Q_{ID}, Q_{SEQ}, SA, DA\}), SA, DA, neigh\ ID_1$$

In this MAC value along with neighbor identifier are passed through many more intermediate routers until the destination is reached. Finally the packet reaching the destination will contain the MAC value, and the accumulation of ID's through which the message was traveled from source to destination. The destination can get different routes from different paths.

C. Associativity Count.

In general, every node sends a HELLO message to every other routers for every 60 seconds. The replies are stored at each node, that is called associativity count. This value will be sent to all the nodes in the particular network. Depending on the value of the node, the destination node will find the associativity stability of a path. If the destination receives the RREQs from various paths, it will select the high stability path. The high stability path will be calculated by "how long a node replies to the HELLO message of any other node. Each and every node will send the HELLO message for every 60 seconds. If any node replies to this HELLO message, it will be stored as a high stability node in sending node's table.

D. Route Reply.

After receiving the route requests from many paths, the destination will reply back to the source with the message that contains a session key(K_s) through the path based on the selection criteria. The session key will be used for encrypting/decrypting the original data .The session key is sent to the source by encrypting the session key along with security association number, query identifier, query sequence number, IP addresses of source and destination, route reply using the shared secret key of source and destination(Kst).Then all the values are subjected into a MAC algorithm like SHA-1 or MD5. The destination also finds the MAC value as,

$$M=C(K_{st}\{RREP,Ks,SA_{NUM},Q_{ID},Q_{SEQ},SA,DA\}),SA, DA, neighID_1,neighID_2\ldots\ldots neighID_n$$

By receiving this message from destination, the sender can decrypt and compute a new MAC value by using this message and then the sender compares the new MAC value with the one it received from receiver. If they are same the sender assures that there are no alteration in the transmission otherwise the message will be dropped. Here the destination will store all the query sequence number that it received. By using these query sequence numbers the destination will identify the message replaying and denial of source attacks.

E. Secure Data Transmission.

SMT safeguards the data transmission by using some cryptographic techniques. At first the ABR will choose the high stability path. If there is only one path with high stability, then the data is routed in that path. If there are more than one paths available with same high stability, then ABR will look for minimum hop-count path. If there is only one path with minimum hop-count, then the data will be routed in that path. If there are more than one paths available with same minimum hop-count, then one of the paths will be chosen arbitrarily. Then the data will be encrypted along with IP addresses, nonce value, timestamp and security association number in that path along with some cryptographic parameters like the secret key(Ks), security Association(SA),nonce value(N), timestamp(T) and so on. They are all given as inputs to the MAC function and then MAC value will be sent along with the intermediate node indentifiers. Finally the sent message will be looking like this,

$$X=C(K_s(Message,SA_{NUM},N_1,T_1,SA,DA)),SA,DA,N_1,T_1, neighID_1,neighID_2\ldots..neighIDn$$

5

By receiving this encrypted message the destination will find the new MAC value by decrypting message using the shared secret ket K_s. Then it will compare the new MAC value with the one that it had received. If they are same, the destination will ensure that there are no message alterations in transit.

VI. Conclusion

In this paper, we proposed an efficient secure routing protocol for mobile ad hoc networks that guarantees the discovery of correct connectivity information over an unknown network, in the presence of malicious nodes. The use of public-key cryptography imposes a high processing overhead on the intermediate nodes and can be considered unrealistic for a wide range of network instances. Furthermore, it is possible for intermediate nodes to corrupt the route discovery by pretending that the destination is their immediate neighbor[2], advertising arbitrarily high sequence numbers and altering (either decreasing by one or arbitrarily increasing) the actual route length.Here we use the symmetric key cryptography with no overhead at intermediate nodes.SRP is also represented in a different perspective with timestamps,nonce values and MAC value.Security Association number is also used between any pair of nodes.SMT provides an efficient data forwarding mechanism by using the cryptographic parameters along with ABR.

The resultant protocol is capable of operating without the existence of an on-line certification authority or the complete knowledge of keys of all network nodes. Its sole requirement is that any two nodes that wish to communicate securely can simply establish a priori a shared secret, to be used by their routing protocol modules. Moreover, the correctness of the protocol is retained irrespective of any permanent binding of nodes to IP addresses, a feature of increased importance for the open, dynamic, and cooperative MANET environment.

REFERENCES

[1]L. Zhou and Z.J.Hass, "Securing Ad Hoc Networks",IEEE Networks Magazine, vol.13, no.6, November/December 1999.

[2]F.Stajano and R.Anderson,"The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks,"Security Protocols,7th International Worshop, LNCS,Springer-verlag,1999.

[3]N.Asokan,P.Ginzboorg, "key Agreement in Ad Hoc Networks,"Computer Communications 23 (17):1627-1637 Nov.1 2000.

[4]Z.J.Hass, M.Perlmann,"The Performance of Query Control Schemes of the Zone Routing Protocol" IEEE/ACM Transactions on Networking, vol.9, no.4,427-438, Aug. 2001.

[5]C.K.Toh,"Associativity-Based Routing for Ad-Hoc Mobile Networks," Wireless personal Communications,vol.4,no.2,pp. 1-36,Mar.1997.

[6]C.E.Perkins, E.M.Royer,S.R.Das,"Ad Hoc On-Demand Distance Vector Routing,", draft-itef-manet-aodv-08.txt,IETF MANET Working Group, June 1st,2001.

[7]S.Yi, P.Naldurg, R.Kravets,"Security-Aware Ad-Hoc Routing for Wireless Networks," UIUCDCS-R-2001-2241 Technical Report, Aug. 2001.

[8]NIST.Fed. Inf.Proc, Standards, "Secure Hash Standard," Pub.180,May 1993.

[9]R.Rivest, "the MD5 Message Digest Algorithm," RFC 1321, April 1992.

[10] Narendra Singh Yadav, R.P.Yadav."The Effects of Speed on the Performance of Routing Protocols in Mobile Ad-hoc Networks" International Journal of Electronics, Circuits and Systems Volume 1 Number 2

[11] Y. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," in Proceedings of ACM MOBICOM 1998, October 1998, pp. 66-75.

[12] Narendra Singh Yadav, R.P.Yadav "Performance Comparison and Analysis of Table- Driven and On-Demand Routing Protocols for Mobile Ad-hoc Networks". International Journal of Information Technology Volume 4 Number 2

[13] Hao Yang, Xiaoqiao Meng, Songwu Lu "Self-Organized Network-Layer Security in Mobile Ad Hoc Networks" *WiSe'02*, September 28, 2002, Atlanta, Georgia, USA.

[14]Mohd Anuar Jaafar, Zuriati Ahmad Zukarnain "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment" European Journal of Scientific Research ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443

[15] Abdul Hadi Abd Rahman, Zuriati Ahmad Zukarnain "Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks" European Journal of Scientific Research ISSN 1450-216X Vol.31 No.4 (2009), pp.566-576

[16] Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam "Addressing Security Concerns of Data Exchange in AODV Protocol" World Academy of Science, Engineering and Technology 16 2006.

[17] I. D. Chakeres. AODV-UCSB Implementation from University of California Santa Barbara. http://moment.cs.ucsb.edu/AODV/aodv.html.

[18]I. D. Chakeres and E. M. Belding-Royer. The Utility of Hello Messages for Determining Link Connectivity. In *Proceedings of the* 5th *International Symposium on WirelessPersonal Multimedia Communications (WPMC)*, pages 504. 508, Honolulu, Hawaii, October 2002.

[19] Panagiotis Papadimitratos and Zygmunt J. Haas Wireless Networks Laboratory, School of Electrical and Computer Engineering, Cornell University, "Secure Routing for Mobile Ad hoc Networks" In Proceedings of the ***SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002),*** San Antonio, TX, January 27-31, 2002.