Hash Security for Ad hoc Routing

Ashwani Kush[1] and **C. Hwang**[2]

Submitted in June 2010; Accepted in November 2010

Abstract - ***A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Most of the protocols in this category are not incorporating proper security features. The ad hoc environment is accessible to both legitimate network users and malicious attackers. It has been observed that different protocols need different strategies for security. An attempt has been made to review some of the existing protocols. Finally a new scheme based on Hashing has been proposed to secure an existing protocol. One-way hash chain is used to protect hop-by-hop transmission. The scheme has been incorporated using AODV as base protocol and results have been explained using NS.***

Index Terms - Security, Ad hoc networks, Routing protocols, Key Management, AODV

1.0 INTRODUCTION

An Ad hoc wireless network is a collection of mobile devices equipped with interfaces and networking capability. It is adaptive in nature and is self organizing. A formed network can be de-formed and again formed on the fly and this can be done without the help of system administration. Each node may be capable of acting as a router. Applications include but are not limited to virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defense or attack, at airport terminals for workers to share files etc. Although security has long been an active research topic in wired networks, the unique characteristics of Ad Hoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. Consequently, the existing security solutions for wired networks do not directly apply to the Ad Hoc environment. The main goal of the security solutions for an Ad Hoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [1]. One distinguishing characteristic of this network from the security design perspective is the lack of a clear line of defence. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. Rest of the paper is designed as: Section 2 discusses Security Challenges, Survey of various protocols is given in Section 3, Section 4 describes new scheme and Conclusion has been made in Section 5.

[1]*Department of Computer Science, University College, Kurukshetra University, Haryana, INDIA*
[2]*Department of Computer Science and Engineering, Texas State University, San Marcos, Texas, USA*
E-Mail: [1]*akush20@gmail.com and* [2]*cjhwang@txstate.edu*

2.0 SECURITY CHALLENGES

All layers in network are prone to some security threats. Table 1 highlights a few of them

Layer Name	Attack
Physical Layer	Jamming, Interception Eavesdropping
Data Link Layer	Traffic analysis, monitoring, MAC disruption, WEP weakness
Network Layer	Routing attacks (DSR, AODV) like Wormhole, location disclosure, impersonation, blackhole, flooding, Cache overflow, route table overflow
Transport Layer	TCP ACK Storm Attack, Session takeover, SYN flooding
Application Layer	Malicious code like Virus, spyware, Trojan horse, lack of cooperation

Table 1: Layer attacks

In this paper, the prime concern is with the attacks targeting the routing protocols for Ad hoc Networks. These attacks [2,3,4,5] can be broadly classified into two main categories as: Passive attacks, Active attacks

2.1 Passive Attacks

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. An attacker just eavesdrops on the network traffic as to determine which nodes are trying to establish routes, or which nodes are pivotal to proper operation of the network and hence can be potential candidates for subversion and launching denial of service attacks. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring down the network. The nature of attacks varies greatly from one set of circumstances to another.

2.2 Active Attacks

These attacks involve some modification of the data stream or the creation of a false stream. It is quite difficult to prevent active attacks absolutely, as this would require physical

protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them. Figure 1 is a description of active and passive attacks.

There are various types of attacks that can be categorized on ad hoc network as:

2.2.1 Location Disclosure: This attack targets the privacy requirements of an ad hoc network.

2.2.2 Black Hole: In a black hole attack a malicious node gives false route replies to advertise itself as having the shortest path to a destination.

2.2.3 Replay: An attacker that performs a replay attack into the network routing traffic that has been captured previously.

2.2.4 Wormhole: The wormhole attack is one of the most powerful ones since it involves the cooperation between two malicious nodes that participate in the network.

2.2.5 Blackmail: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender.

2.2.6 Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network.

2.2.7 Rushing Attack: Rushing attack is that results in denial-of-service when used against *all* previous on-demand ad hoc network routing protocols.

2.2.8 Masquerading: During the neighbor acquisition process, an outside intruder joins illegally in the routing protocol do main by compromising authentication system.

2.2.9 Passive Listening and traffic analysis: The intruder could passively gather exposed routing information. Such a attack can not effect the operation of routing protocol, but it is a breach of user trust to routing the protocol.

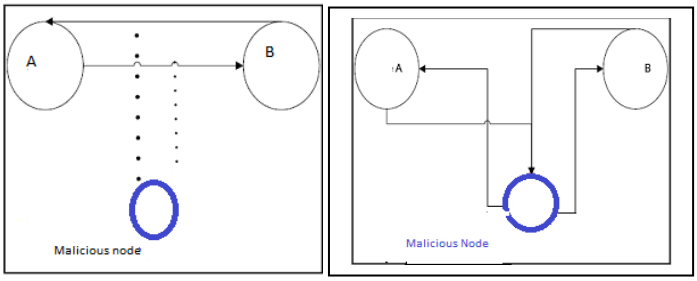


Figure 1: (a) Passive Attack (b) Active Attack

3.0 SECURE ROUTING PROTOCOLS

In this section some of the popular secured protocols have been analyzed. Efforts have been made to use same metrics for all and be bias less.

3.1 ARAN [6] : Dahill et al. proposed ARAN[6], It assumes managed-open environment, where there is a possibility for pre-deployment of infrastructure. It consists of two distinct stages. The first stage is the certification and end-to-end authentication stage. Here the source gets a certificate from the trusted certification server, and then using this certificate, signs the request packet. Each intermediate node in turn signs the request with its certificate. The destination then verifies each of the certificates, thus the source gets authenticated and so do the intermediate nodes. The destination node then sends the reply along the route reverse to the one in the request, reply signed using the certificate of the destination. The second stage is a non-mandatory stage used to discover the shortest path to the destination, but this stage is computationally expensive. It is prone to reply attacks using error messages unless the nodes have time synchronization. Authenticated Routing for Ad-hoc Networks (ARAN) detects and protects against malicious actions by third parties and peers in Ad-hoc environment. ARAN introduces authentication, message integrity and non-repudiation to an Ad-hoc environment [7].

Characteristics:

(i) ARAN is able to take care of Replay attacks
(ii) It is able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole and Worm hole
(v) It does not secure for Denial Of service
(vi) ARAN is loop free
(vii) It is based on Online trusted certification authority

3.2 SEAD [9]: This Secure Efficient Ad hoc Distance vector routing protocol (SEAD) is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, in spite of active attackers or compromised nodes in the network [9]. To support use of SEAD with nodes of limited CPU processing capability and to guard against DoS attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, it uses efficient one-way hash functions. It is based on DSDV. It has been designed to protect routing update packets.

Characteristics:

(i) SEAD is able to take care of Replay attacks
(ii) It is able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole and Worm hole
(v) It does secure for Denial Of service
(vi) SEAD is table driven
(vii) It is based on Clock synchronization
(viii) It is loop free and uses Distance as route metric

3.3 SRP [9] : Secure Routing Protocol [9] (Lightweight Security for DSR[16]), which one can use with DSR to design SRP as an extension header that is attached to ROUTE REQUEST and ROUTE REPLY packets. SRP doesn't attempt to secure ROUTE ERROR packets but instead delegates the route-maintenance function to the Secure Route Maintenance portion of the Secure Message Transmission protocol. SRP uses a sequence number in the REQUEST to ensure freshness, but this sequence number can only be checked at the target.

SRP requires a security association only between communicating nodes and uses this security association just to authenticate ROUTE REQUESTS and ROUTE REPLYS through the use of message authentication codes. At the target, SRP can detect modification of the ROUTE REQUEST, and at the source, SRP can detect modification of the ROUTE REPLY. It defends against attacks that disrupt the route discovery process. It is used with DSR, ZRP. It uses mechanism of secure certificate server.

Characteristics:

(i) SRP is able to take care of Replay attacks
(ii) It is not able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole, Worm hole and invisible node attacks
(v) It does secure for Denial Of service
(vi) SRP is loop free and uses Distance as route metric
(vii) It uses existence of security association between each Source and Destination

3.4 SECURE AODV [10] : The SAODV [10] implements two concepts secure binding between IPv6 addresses and the independent of any trusted security service, Signed evidence produced by the originator of the message and signature verification by the destination, without any form of delegation of trust. The AODV[15] protocol is comprised of two basic mechanisms, route discovery and maintenance of local connectivity. The SAODV protocol adds security features to the basic AODV mechanisms, but is otherwise identical. A source node that requests communication with another member of the MANET referred to as a destination D initiates the process by constructing and broadcasting a signed route request message RREQ.

Characteristics:

(i) SAODV is able to take care of Replay attacks
(ii) It is not able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole and Worm hole
(v) It does not secure for Denial Of service
(vi) SAODV uses Online key management scheme for acquisition and verification of keys
(vii) It is loop free and uses Distance as routing metric

3.5 SLSP [11]: The Secure Link State Protocol (SLSP) [11] for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within *R* hops, which is termed as their *zone*. Nevertheless, SLSP is a self-contained link state discovery protocol, even though it draws from, and naturally fits within, the concept of hybrid routing. To counter adversaries, SLSP protects link state update (*LSU*) packets from malicious alteration, as they propagate across the network.

Characteristics:

(i) SLSP is able to take care of Replay attacks
(ii) It is not able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole and Worm hole
(v) It does secure for Denial Of service
(vi) SLSP is table driven, Loop free
(vii) It assumes that Nodes must have their public keys certified by a Trust party
(viii) It uses Distance as Routing metric

3.6 ARIADNE [12]: A Secure On Demand Routing Protocol for Ad Hoc Networks (ARIADNE) using the TESLA[13] broadcast authentication protocol for authenticating routing messages, since TESLA is efficient and adds only a single message authentication code (MAC) to a message for broadcast authentication. Adding a MAC (computed with a shared key) to a message can provide secure authentication in point-to-point communication; for broadcast communication, however, multiple receivers need to know the MAC key for verification, which would also allow any receiver to forge packets and impersonate the sender. Secure broadcast authentication thus requires an asymmetric primitive, such that the sender can generate valid authentication information, but the receivers can only verify the authentication information. It is used with DSR. It is prone to selfish node attack. It prevents attackers from tampering uncompromised routes.

Characteristics:

(i) ARIADNE is able to take care of Replay attacks and immune to wormhole attack.
(ii) It is able to eliminate Rushing attacks
(iii) It does not effectively deals with location disclosure
(iv) It has no provision for Black Hole.
(v) It does secure for Denial Of service
(vi) It uses TESLA keys distributed to participating nodes
(vii) It is loop free and uses Distance as Routing metric.

3.7 SAR [14]: Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into adhoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols. We assume that the base protocol is an on demand protocol similar to AODV or DSR. In the original protocol, when a node wants to communicate with another node, it broadcasts a Route Request or RREQ packet to its neighbors. It is used with AODV. It uses sequence number and time stampings to stop replay attacks. In this route discovered may not be the shortest one.

Characteristics:

i) SAR is loop free
ii) It uses Security requirement as Routing metric
iii) SAR uses Key distribution or secret sharing mechanism
iv) SAR is not loop free, it depends upon selected security requirement
v) It is able to take care of Replay attacks

vi) It is not able to eliminate Rushing attacks
vii) It does not effectively deals with location disclosure
viii) It does secure for Denial Of service

4.0 PROPOSED PLAN

When a source node S needs to discover a route to a destination node D, it initiates a route request (RREQ) message, which includes the source (S) node and Destination (D) node, a request sequence number, and an initial hash value. The initial hash value is computed as H0 = Hash [n] , where n is a random number. The source node S appends the computed initial hash value H0 , and then broadcast the RREQ packet. The neighbor node, receiving this RREQ packet, would check the validity of source node. If any checking process fails, the node discards the packet, otherwise, rebroadcasts. Any intermediate node, say 1, receiving the packet checks whether it has already seen this packet by recognizing the combination of (source node, request sequence number) . If it has, discards the packet, as in regular AODV, otherwise it adds its address to the node list, replaces the hash value field with Hash(1, previous hash value) and rebroadcasts the packet.

S : H_0 = Hash [n]
S -> RREQ, S, D, Seq#,{ } ,H_0

H_1 = Hash [1, H_0]
1-> RREQ, S , D, Seq#,{1} , H_1

H_2 = Hash [2, H_1]
2-> RREQ, S , D, Seq#,{1,2} , H_2

D: [D, S , { 2,1 } , Seq#]

D->2 : RREP, D,S, {1,2} , Seq#
2-> 1 : RREP, D,S, {1,2} , Seq#
1->S : RREP, D,S, {1,2} , Seq#

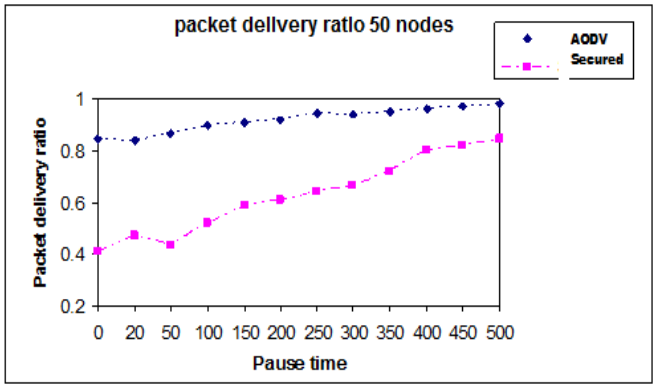
Figure1: Packets exchanged between nodes during RREQ phase.

When the destination node receives the RREQ, it performs a sequence of checking processes. It first unscrypts the received ciphertext and compare the result with the routing message received. If the comparison indicates a match, node D gets the initial hash value H_0. It would further verify the source node S. If the sequence number is greater than the last received sequence number from S, it checks the hash chain field is equal to

H [N_n, H[N_{n-1},H[.. H[N_1,H_0] ..]]]

If any step of the above checking process fails, the authentication fails, and the destination node discards the RREQ packet; otherwise, the destination node prepares the RREP packet. It first copies the accumulated node list from the RREQ packet, reverses it, and puts it to the source route.

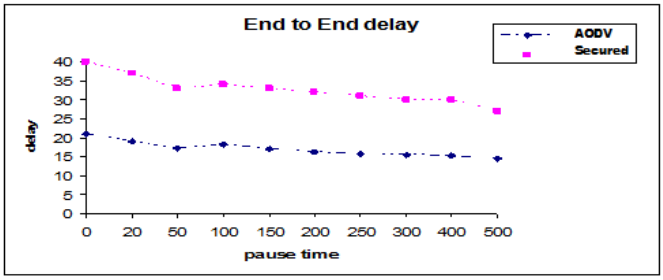
As is evident from proposed scheme, the format size will be increased with inclusion of Hash key generation. The routing load will increase due to incorporation of security. It is also clear that the scheme affects the packet delivery fraction and end-to-end delay. The packet delivery fraction will be marginally reduced. Also chances of packets drop may increase due to delay produced in route reply case. This could be improved by having higher timeouts for packets buffered for route discovery.



Graph 1: PDF using pause time

Simulation study has been carried out to study the performance study of proposed protocol. Simulation Environment used for this study is NS-2 [20]. Area selected is 1 × 1 KM and 50 nodes have been taken. Pause time is varied from 0 to 500 sec. Pause time 500 means minimum movement and 0 means maximum movement. TCP packets are used.

Graph 1 show the packet delivery ratio based on pause time. The packet delivery ratio is the fraction of successfully received packets, which survive while finding their destination. This performance measure determines the completeness and correctness of the routing protocol. Pause time of 0 means very fast moving nodes and 500 shows minimum movement.



Graph 2: End to end delay

As the graph indicates 'Secured' has less number of packets delivered, but this reduction in delivery is due to Hash keys calculations and evaluations. Graph 2 represents the end to end delay with respect to pause time. Average end-to-end delay is the delay experienced by the successfully delivered packets in reaching their destinations. More end to end delay is observed in this case for 'Secured'. The reason is again the more calculation part involved for hash key estimation. It should be noted here that only trusted packets are delivered, so some packets does fall because of this reason also.

The reduction in packet delivery ratio and increase in end to end delay does not show the effectiveness of the proposed scheme. This change will be obvious as more packets are

sacrificed to keep them secured. Security is achieved at the cost of performance. Efforts are on to reduce the margins by reducing the size of Hash key

5.0 CONCLUSION

The proposed authentication scheme, in essence, is still an asymmetric key based approach, except it shows some properties of lower computational cost and reduced communication overhead comparing with the traditional PKI supported schemes. An attempt has been made to present an overview of the existing security scenario in the Ad-Hoc network environment. Hash Key management has been proposed as one of the best options for security, though other options can also be considered depending upon need of security. As hash key chain is configured as a recursive chain so these keys are noted in route table. Important function is that the routing protocol functions very similar to the existing one when there are no external attacks. Whenever an attack occurs additional packets need to be sent to change the routes established by the malicious control packets. This increased traffic size will have its impact on overhead. The overhead is bound to increase with it, but keeping in view of the better secured routing this will have to be done to achieve desired results. Efforts are on to simulate the proposed scheme with different topologies, more metrics and to compare it with existing secured routing schemes. Proposed scheme is expected to work better in dense environments as selection of path becomes easy in case of failures. Ad hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. Several protocols for secured routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The current security mechanisms, each defeats one or few routing attacks. It is still a challenging task to design routing protocols resistant to multiple attacks.

FUTURE SCOPE

More simulations will be carried out using speed as a function as well. DSR and TORA will also be compared with proposed scheme and implementing this concept into them. Dense environment has been used in this scheme. Efforts are on to make the scheme robust for sparse medium as well.

REFERENCES

[1]. A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and secure source authentication for multicast", In Network and Distributed System Security Symposium (NDSS'01), Feb. 2001.

[2]. T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication 800-48, November 2002.

[3]. William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall New Jersey 2003

[4]. Yonguang Zhang and Wenke Lee, "Intrusion detection in wireless ad-hoc networks", In 6th International Conference on Mobile Computing and Networking(MOBICOM'00), pp. 275– 283, Aug 2000.

[5]. A.Kush, C.Hwang, P.Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE). May 2009, Volume 3. pp 1793-1799,

[6]. B. Dahill, B. N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, Aug. 2001.

[7]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine October 2002.

[8]. Y.-C. Hu, D. B. Johnson, and A. Perrig., "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks" In Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, pp 3-9. IEEE Computer Society, 2002.

[9]. P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[10]. M. Guerrero Zapata. "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing". IETF MANET Mailing List, Available at ftp://manet.itd.nrl.navy.mil/pub/manet/2004.

[11]. P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks" Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks, IEEE Press, 2003, pp. 27–31.

[12]. Y. C. Hu, A. Perrig and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Technical Report TR01-383, Rice University, Dec. 2001.

[13]. A. Perrig, R. Canetti, D. Tygar, and D. Song, "TESLA Broadcast Authentication Protocol, RSA Cryptobytes (RSA Laboratories)", Vol 5, No 2, Summer/Fall 2002, pp. 2-13.

[14]. R. Kravets, S. Yi, and P. Naldurg, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks", In ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001.

Continued on page no. 280