A Study on Secure and Zone-based Ad hoc Routing Protocol

Monika Kumar Jethani
Dept. of CSE, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India.

Abstract

An ad hoc network can be vividly defined as a local area network or some other small network, especially one with wireless (or temporary plug in connections), in which some of the network devices are the part of the network only for the duration of a communication. Designing a fullproof security protocol for ad hoc network is the need of the hour.

This is because the ad hoc networks possess unique characteristics such as, lack of central authority, frequent topology changes, rapid node mobility, shared radio channel and limited availability of resources.

Index Terms

Proactive, Reactive, Hybrid, ZRP, SZRP.

I. Introduction

An Ad-hoc network is session the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure.

Its characteristics can pose a challenge to security in the following manner:-

1. Shared radio channel: The radio channel used for communication in ad hoc networks is broadcast in nature and is shared by all nodes in the network so the data transmitted by a node is received by all the nodes within its direct transmission range. This implies a malicious node can easily obtain data being transmitted in the network.
2. Insecure operational environment: The operational environment in which MANETs are generally used, may not be always secure, for example, a battle field. In such environment, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.
3. Lack of central authority: Since MANETs don't have any such central points, these mechanisms can't be applicable to them.
4. Lack of association rules: In MANET, since nodes can leave or join the network at any point of time, if no proper authentication mechanism is used for associating nodes with the network intruders can easily join the network and carry out attacks.
5. Limited availability of resources: Resources such as bandwidth, battery power and computational power are scare in ad hoc networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

Many protocols currently exist for the purpose of secure routing. However, most of these protocols are either proactive or reactive in approach. Both the approaches have their own demerits, for example, the proactive protocols use excess bandwidth in maintaining the routing information while, the reactive ones have long route request delay. Reactive routing also inefficiently floods the entire network for route determination.

1. Table-driven or Proactive Protocols: Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols.

Examples of proactive protocols are: Destination-Sequenced Distance-Vector (DSDV) routing [4], Clustered Gateway Switch Routing (CGSR) [5], Wireless
Routing Protocol (WRP) [6], and Optimized Link State Routing (OLSR) [7].

2. On-demand or Reactive Protocols: Another approach from is reactive or on-demand routing. These protocols depart from the legacy Internet approach.
   Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until the route is no longer used or has expired.

Examples of reactive routing protocols are: Dynamic Source Routing (DSR) [8], Ad hoc On Demand Distance Vector (AODV) routing [9], Temporally Ordered Routing
Algorithm (TORA) [10] and Associativity Based Routing (ABR) [11].

3. Hybrid Protocols: These protocols include the best mix of proactive and reactive protocols.

Examples of hybrid routing protocols are: Zone Routing Protocol (ZRP) [12] and Zone-based Hierarchal Link state routing protocol (ZHLS) [15].

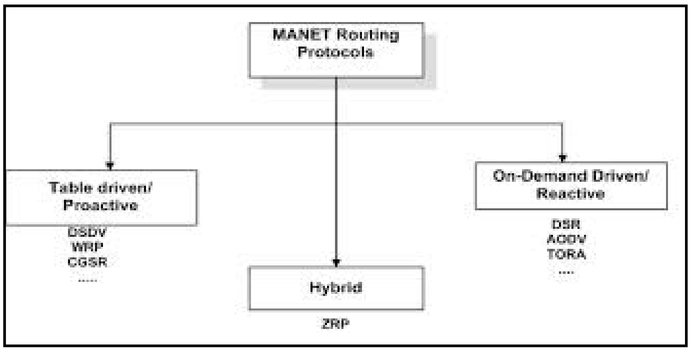

Fig. 1: Classification of MANET Routing Protocols

Optimized Link State Routing (OLSR) Protocol:

Multipoint Relays in OLSR are illustrated below

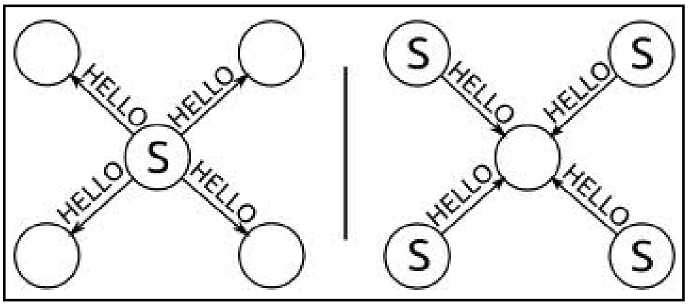

Fig. 2: Multipoint Relays in OLSR

Nodes learn their set of two-hop
neighbours through the periodic exchange of Hello messages. Each node periodically transmits a Hello message that contains a list of neighbours.
Associated with each neighbour is an attribute including the directionality of the link to that neighbour.

Ad hoc On Demand Distance Vector (AODV) Routing:

AODV route discovery can be illustrated as follows

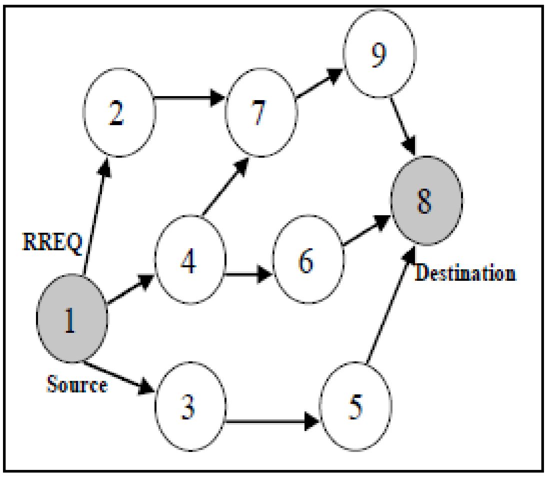

Fig. 3: RREQ in AODV

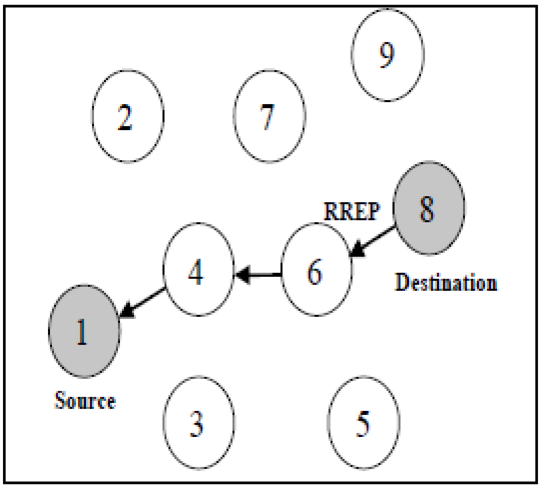

Fig. 4: RREP in AODV

When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located.
Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or the intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ.

Zone Routing Protocol (ZRP):

The Zone Routing Protocol(ZRP) as described in [12] aims at addressing these limitations by combining the best properties of both proactive and reactive approaches and hence it can be classed as a hybrid proactive/reactive routing protocol.
ZRP reduces the proactive scope to a zone centered on each node and reactive approach outside the zone. When a node has a data packet for a particular destination, it checks whether the destination is within its zone or not. If it is within the zone, the packet is routed proactively. Reactive routing is used if the destination is outside the zone.
ZRP Architecture can be diagrammed as follows:-

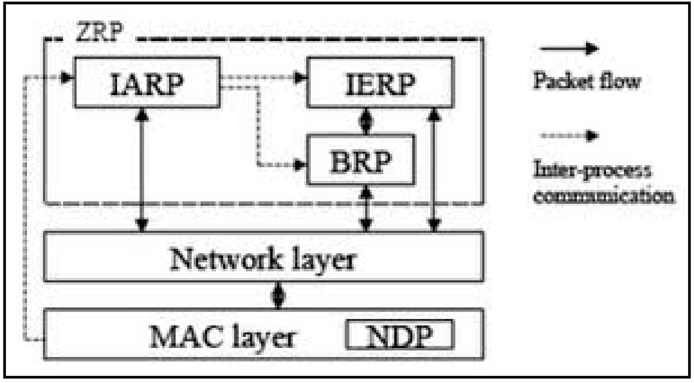

Fig. 5: Architecture of ZRP

IARP : IntrA-zone Routing Protocol
IERP : IntEr-zone Routing Protocol
BRP : Boarder Resolution Protocol
NDP : Neighborhood Discovery Protocol

Secure Zone Routing Protocol (SZRP):

The requirements of a secure routing protocol are as follows:-

1. Routing messages cannot be altered in transit, except according to the normal functionality;
2. Route signalling cannot be spoofed;
3. Fabricated routing messages cannot be injected into the network;
4. Routing loops cannot be formed through malicious action;
5. Routes cannot be redirected from the shortest path by malicious action;
6. Unauthorized nodes should be excluded from route computation and discovery;
7. The network topology must not be exposed by the routing messages either to adversaries or to authorized nodes.

We proposed a secure hybrid ad hoc routing protocol, called Secure Zone Routing Protocol (SZRP), which aims at addressing the above limitations by combining the best properties of both proactive and reactive approaches. The proposed protocol is based on the concept zone routing protocol (ZRP). It employs an integrated approach of digital signature and both the symmetric and asymmetric key encryption techniques to achieve the security goals like message integrity, data confidentiality and end to end authentication at IP layer
The reasons for selecting ZRP as the basis of our protocol are

as follows:

1- ZRP is based on the concept of routing zones, a restricted area, and it is more feasible

to apply the security mechanisms within a restricted area than in a broader area that of the whole network,

2- Since the concept of zones separate the communicating nodes in terms of interior (nodes within the zone) and exterior (nodes outside the zone) nodes,

certain information like network topology and neighbourhood information etc. can be hidden to the exterior nodes,

3- In case of a failure, it can be restricted to a zone.

The security and performance evaluation of SZRP through simulation indicates that the proposed scheme

successfully defeats all the identified threats and achieves a good security at the cost of acceptable overhead.

In ZRP where there is no security consideration, SZRP is designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing.For end to end authentication and message/ packet integrity RSA digital signature mechanism [16] is employed, where as data confidentiality is ensured by an integrated approach of both symmetric and asymmetric key encryption [16].

Like ZRP the proposed protocol performs routing in terms of intrazone [13] and interzone [14] routing. It limits the proactive scope within a zone centered on each node and the reactive approach outside the zone.

Packets are signed and/or encrypted (either using symmetric or asymmetric key approach) depending upon their type i.e. whether the packet is a control or a data packet.

Most of the control packets are only signed. However, all the data packets and those control packets that contain any secret information like a session key between the source and destination node and are signed as well as encrypted. Since the control packets are small in size they are encrypted using the asymmetric key approach.

As the data packets are generally long and symmetric key approach is faster than the asymmetric key encryption we encrypt all the data packets using the symmetric key approach.

Each communicating node has two pairs of private/public keys, one pair for signing and verifying and the other for encrypting and decrypting. For a node X the signing and verifying keys are SKX and VKX respectively while, encrypting and decrypting keys are EKX and DKX respectively.

Among these keys SKX and DKX are private keys whereas VKX and EKX are public keys.

The secure zone routing protocol (SZRP) makes the use of public key certificates [17] for key distribution and management. For the process of public key certification, SZRP assumes the presence of trusted certification servers called the certification authorities (CAs) in the network in addition to the communicating nodes which we call the common nodes (CNs). Each CN before taking part in communication need to be certified by some CA and are granted public keys.SZRP is a two phase protocol. The first phase is the preliminary certification process where each CN fetches their required keys from their nearest CA. The second phase is secure routing phase which uses these keys to perform secure intra-zone or inter-zone routing by applying the process of digital signature and message encryption. The Secure Zone Routing Protocol (SZRP) requires the presence of trusted certification servers called the certification authorities (CAs) in the network.

The CAs are assumed to be safe, whose public keys are known to all valid CNs. Keys are generated apriori and exchanged through an existing, perhaps out of band, relationship between CA and each CN. Before entering the ad hoc network, each node requests a certificate from it's nearest CA. Each node receives exactly one certificate after securely authenticating their identity to the CA.

A common node X receives a certificate from its nearest CA as follows:

CA→ X: certX = [IPX, VKX, EKX, t, e] | signCA

where, signCA = [IPX, VKX, EKX, t, e] SKCA

The certificate contains the IP address of X, the two public keys VKX and EKX of X, one for verifying the signature signed by X and other for encrypting a packet to be send to X, a timestamp 't' of when the certificate was created, and a time 'e' at which the certificate expires, all appended by the signature signCA of CA. All nodes must maintain fresh certificates with their nearest CA.

We have assumed the following things for the design and successful deployment of the proposed protocol.

1-The network links are assumed to be bidirectional.

2- The resources of different ad hoc network nodes may vary greatly, from nodes with very little computational resources, to resource rich nodes equivalent in functionality to high-performance workstations. To make our results as general as possible, we have designed SZRP to support nodes with moderate resources, such as a Palm Pilot or RIM pager.

3- The proposed protocol intends to provide security at IP layer. Hence, for a secure communication across the network protocol stack suitable techniques should be employed to secure MAC and physical layers. A list of such mechanisms is given in [1, 18, 19].

The key management protocol (KMP) is responsible for public key certification proces. It fetches the public keys for each CN by certifying them with the nearest CA. The secure intrazone routing protocol (SIARP) and secure interzone routing protocol (SIERP) uses these keys to perform secure intrazone and interzone routing respectively SIARP is a limited depth proactive link-state routing protocol [2, 3] with inbuilt security features. It periodically computes the route to all intrazone nodes (nodes that are within the routing zone of a node) and maintains this information in a data structure called SIARP routing table. This process is called proactive route computation. The route information to all intrazone nodes collected in proactive route computation phase is used by SIARP to perform secure intrazone routing.

For route maintenance, SIERP at each node keeps track of routes whether they are active or not. When there is no flow of traffic on an existing route for that route's lifetime, the route is deactivated by the node. Data received on an inactive route causes nodes to generate an Error (ERR) message. A node generates an ERR message in either of the following cases:

1-if data is received on an inactive route, or

2-the link of an active

route is broken due to node mobility or some other reasons. The node send the ERR message to the source along the reverse path. All ERR messages must be signed to check the authenticity of the sender as well as the message. For a route between source A and destination X, a node M generates the ERR message for its neighbor N as follows:

M→N : [ERR, IPA, IPX, certM, NM, t] | signM

Where, signM =[ERR, IPA, IPX, certM, NM, t] SKM

This message is forwarded along the path to the source without modification. A nonce and timestamp ensure that the ERR message is a fresh. Since the ERR messages are signed, malicious nodes cannot generate ERR messages for other nodes. The non-repudiation provided by the signed ERR message allows a node to be verified as the source of each ERR message that it sends. The source node drops the duplicate ERR message with same nonce and time stamp.

SZRP can prevent against all types of attacks that include information disclosure, impersonation, modification, fabrication and replay of packets caused by both an external advisory and an internal compromised node.

Comparative Analysis of Routing Protocols is shown below.

CRITERIA	OLSR	AODV	ZRP	ARAN	SZRP
Full Form	Optimized Link State Routing	Ad hoc On Demand Distance Vector	Zone Routing Protocol	Authenticated routing for ad hoc networks	Secure Zone Routing Protocol
Type	Proactive	Reactive	Hybrid	Reactive	Hybrid
Based on	Dijkstra's Algorithm	Destination-Sequenced Distance- Vector (DSDV) routing	IARP(IntrA-zone Routing Protocol), IERP (Inter-zone Routing Protocol),NDP (Neighbour Discovery Protocol) and BRP(Bordercast Resolution Protocol).	-	Zone Routing Protocol
Key Feature	Use of Multipoint Relays	Pure on-demand route acquisition system	Creation of Zones.	Nodes in a managed- open environment exchange initialization parameters before the start of communication.	SZRP is designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing.
Advantages	Reduces the overhead of network floods and the size of link state updates	Minimizes the number of required broadcasts by creating routes on a demand basis	Saves transmission resources	Provide secure communications in managed open environments.	Can operate well on diverse applications of ad hoc networks.
Working	Each node computes its MPR Selectors. he MPR set is selected such that when a node broadcasts a message, the retransmission of that message by the MPR set will ensure that the message is received by each of its two-hop neighbours.	When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbours, which then forward the request to their neighbours, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located	When a node has a data packet for a particular destination, it checks whether the destination is within its zone or not. If it is within the zone, the packet is routed proactively. Reactive routing is used if the destination is outside the zone.	Each node in ARAN receives a certificate after securely authenticating its identity to a trusted certificate server T. Nodes use these certificates to authenticate themselves to other nodes during the exchange of routing messages. The certificate contains the node's IP address, its public key, as well as the time of issuing and expiration. These fields are concatenated and signed by the server T.	First phase is the preliminary certification process where each CN fetches their required keys from their nearest CA. The second phase is secure routing phase which uses these keys to perform secure intra-zone or inter-zone routing by applying the process of digital signature and message encryption.
References	[7]	[9]	[12]	[20]	[16],[17]

II. Result

Secure Zone Routing Protocol under different mobility patterns and traffic scenarios show that the proposed protocol is as efficient as ZRP in discovering and maintaining routes, at the cost of using larger routing packets which result in a higher overall routing load, and at the cost of higher latency in route discovery because of the cryptographic computation that must occur.

However, the impact of the overhead caused is almost insignificant and can be considered negligible as compared to the proposed degree of security, which SZRP provides compared to its other counterparts.

III. Conclusion

The conclusion arises as the proposed protocol intends to provide security at IP layer. Together with existing approaches for securing the physical layer and MAC layer within the network protocol stack, the Secure Zone Routing Protocol (SZRP) provides a foundation for governing a secure communication system for mobile ad hoc networks.

IV. Future Scope

The proposed protocol have assumed that, the Neighbourhood Discovery Protocol (NDP) is implemented as a MAC layer protocol. But in some special cases the MAC layer does not include an implementation of NDP. In such situations the proposed protocol may be modified to provide the functionality of NDP at IP layer.

References

[1] *Imrich Chlamtac, Marco Conti, Jenifer J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challanges", Elsevier Network Magazine, vol. 13, pages 13-64,2003*

[2] E.M. Belding-Royer and C. K. Toh, "A review of current routing protocols for adhoc mobile wireless networks", IEEE Personal Communications Magazine, pages 46–55, April 1999.

[3] Behrouz A. Forouzan, "Data communication and Networking," 2nd edition, Tata McHill publication, 2001

[4] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Commun. Rev., Oct. 1994, pp. 234–44.

[5] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. IEEE SICON '97, Apr. 1997, pp. 197–211.

[6] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183–97.

[7] P. Jacquet, P. Muhlethaler, A. Qayyum, "Optimized Link State Routing Protocol", Internet Draft, draft-ietf-manetolsr-00.txt, November 1998.

[8] D.B. Johnson, D.A. Maltz, "Dynamic source routing in adhoc wireless networks", in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, Dordrecht, 1996, pp. 153–181.

[9] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing", In IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb. 1999.

[10] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. INFOCOM '97, Apr. 1997.

[11] C-K. Toh, "A Novel Distributed Routing Protocol to Support Ad-Hoc Mobile Computing", Proc. 1996 IEEE 15th Annual Int'l. Phoenix Conf. Comp. And Commun., Mar. 1996, pp. 480–86.

[12] Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol (ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[13] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Intrazone Routing Protocol (IARP)", IETF Internet Draft, draft-ietf-manet-iarp-01.txt, June 2001

[14] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Interzone Routing Protocol (IERP)", IETF Internet Draft, draft-ietf-manet-ierp-01.txt, June 2001

[15] M.Joa-Ng and I. T. Lu, "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," IEEE journal on Selected areas in Communications, vol. 17, no. 8, pp. 1415- 1425, August 1999

[16] Behrouz A. Forouzan, "Cryptography and Network Security", Special Indian Edition, Tata McHill publication, 2007

[17] J. J. Tardo and K. Algappan, "SPX: Global authentication using public key certificates", In Proceedings of the 1991 IEEE Symposium on Security and Privacy, pages 232–244, Oakland, CA USA, May 1991. IEEE Computer Society Press.

[18] R. Hauser, T. Przygienda, and G. Tsudik, "Lowering security overhead in link state routing", Computer Networks, 31(8):885–894, April 1999.

[19] P. Michiardi, R. Molva, "Ad hoc networks security", in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.

[20] K.Sanzgir, and B.Dahill, "A secure routing protocol for ad hoc networks",Proceeding of the 10th IEEE International Conference on Network Protocols, 2002, pp.1-10.