

**A SECURITY IN ZONE ROUTING PROTOCOL FOR MANET**

Arvind Dhaka \*

Raghuveer Singh Dhaka \*

Priyank Singh Hada \*

---

**ABSTRACT**

*MANET is a collection of wireless mobile nodes, which dynamically form a temporary network without using any existing network infrastructure or centralized administration. Mobile nodes communicate each other via radio waves. MANET are often called infrastructure less network. This security solution provides secure routing and effective key management mechanism. Their main applications are Military applications, Emergency systems, Wireless mess networks and wireless sensor networks. In this paper, we proposed a secure hybrid ad-hoc routing protocol, called Advance Zone Routing Protocol (AZRP), by combining the best properties of both proactive and reactive routing approaches. The proposed protocol is based on the zone routing protocol (ZRP). It used the approach of digital signature and both the symmetric and asymmetric key encryption techniques to achieve the security goals like message integrity, data confidentiality and authentication at IP layer. The proposed scheme successfully defeats all the identified threats and achieves a good security at the cost of acceptable overhead. Together with existing approaches for securing the physical and MAC layer within the network protocol stack, the Advance Zone Routing Protocol (AZRP) can provide a foundation for the secure operation of an ad hoc network.*

**Keywords:** MANET, ZRP, AZRP.

---

\* Department of Computer Science & Engineering, Central University of Rajasthan, Ajmer.

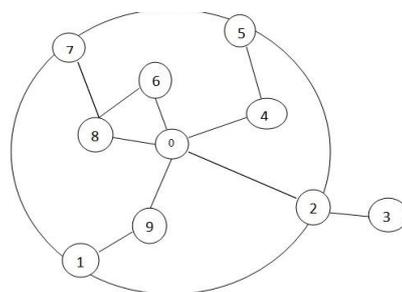
## 1. INTRODUCTION

New area of communication is the communicating devices like personnel digital assistants (PDAs), pagers, laptops and cellular phones are the way for mobile connectivity. The wireless devices are achieved via fixed infrastructure-based service or private networks. In the infrastructure-based networks takes time and high cost to set up the necessary infrastructure. The mobile devices connect to each other through flexible and powerful network which is called Mobile ad-hoc network. Wireless network for mobile nodes is called a wireless ad hoc network or a mobile mesh network. Nodes are communicate wireless links. Both host and router is used to forwards the data to some other node. Ad-hoc network are used military operations, emergency disaster and interaction between attendees at a meeting or students during a lecture. The characteristics of ad hoc networks present a host of research areas related to security, such as, key management models, secure routing protocols, intrusion detection systems and trust based models. This work is used for secure routing.

## 2. ZONE ROUTING PROTOCOL (ZRP):

This type of Routing Protocol is used to combining the properties of both proactive and reactive approaches. In mobile ad-hoc network all nodes are communicate to each other. When a node sent the data packet for a particular destination, it checks whether the destination is within its zone or not. If data packet is within the zone, then the packet is routed according proactive Routing approach. If the data packet is outside the zone then Reactive routing approach is used.

A zone is the area of local neighborhood of that node. The “size” of a zone is determined by a radius of length  $\beta$  where,  $\beta$  is the number of hops to the perimeter of the zone. Their various overlapping zones that contain a different size. An example routing zone is shown in Figure 1 where the routing zone of 0 includes the nodes 8–2, but not node 3 because it is outside of the zone..



**Fig 1: Routing zone of node S with zone radius  $\beta = 2$**

The nodes of a zone are divided into peripheral nodes and interior nodes. Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius  $\beta$ . The nodes whose minimum distance is less than  $\beta$  are interior nodes. In Figure 1, the nodes 4–9 are interior nodes, the nodes 5–1 are peripheral nodes and the node 3 is outside the routing zone. Note that node 7 can be reached by two paths, one with length 2 and one with length 3 hops. The node is however within the zone, since the shortest path is less than or equal to the zone radius.

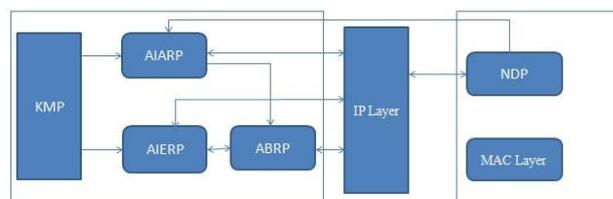
### 3. SECURITY GOALS:

- (a)Confidentiality
- (b)Integrity
- (c)Availability
- (d)Authenticity
- (e)non-repudiation

### 4. ADVANCE ZONE ROUTING PROTOCOL (AZRP):

#### Protocol Overview:

Advance Zone Routing Protocol (AZRP) is a hybrid routing protocol that combines the best features of proactive and reactive routing approaches and provide security. The reasons for selecting ZRP is as follows: (i) Easy to apply the security in a restricted area. (ii) ZRP separate the communicating nodes in terms of interior (nodes within the zone) and exterior (nodes outside the zone) nodes. (iii) In case of a failure, the proposed protocol performs intra-zone [18] and inter-zone [19] routing. For Digital Signature Algorithm (DSA) is used.



**Fig 2 Architecture**

The architectural design of AZRP is shown in Figure: 2 There are some new modification in the previous routing protocol [16]. It is used for design both secure routing (intra-zone and inter-zone) and effective key management. For public key certification used the key management protocol (KMP) process. KMP process is used to transfer the public keys for each node with the nearest CA. AIERP(Advance Inter-Zone Routing Protocol) provide secure route discovery and route maintenance services. For minimization of the delay AIERP uses

the Advance border resolution protocol (ABRP). It is used for secure route discovery packets sets up a reverse path back to the neighbor node.

## 5. CONCLUSION :

In this Paper, we presented a new design of secure ad hoc routing protocol(hybrid routing). We analyzed the robustness of the protocol and found that, the proposed protocol gives us a better solution by taking an unique approach of digital signature using symmetric and asymmetric key encryption technique.

## 6. REFERENCES

1. Kamanashis Biswas and Md. Ali, "Security threats in Mobile ad hoc networks", University essay from Blekinge Tek nisha Ho gskola/Sektionen for Teknik (TEK), 2007.
2. Ming Yu; Mengchu Zhou; Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology Vol-58, Issue 1, Jan. 2009 , pp.449 – 460.
3. George Aggelou, "Mobile Ad Hoc Networks", 2nd edition, Mc GRAW Hill professional engineering, 2004
4. Imrich Chlamtac, Marco Conti, Jenifer J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challanges", Elsevier Network Magazine, vol. 13, pages 13-64, 2003
5. E. Baccelli, J. A. Cordero, P. Jacquet: Using RNG for Reliable Database Synchronization in MANETs. Proc. of the 5th IEEE Workshop on Wireless Mesh Networks. June 2010.
6. Behrouz A. Forouzan, "Data communication and Networking," 2nd edition, Tata McHill publication, 2001
7. 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.
8. C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. IEEE SICON '97, Apr. 1997, pp. 197–211.
9. 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.
10. P. Jacquet, P. Muhlethaler, A. Qayyum, "Optimized Link State Routing Protocol", Internet Draft, draft-ietf-manetolsr- 00.txt, November 1998.

11. A. Laouiti, A. Qayyum, and L. Viennot, "Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks," in Proceedings of the 35th Annual Hawaii International Conference on System Science (HICSS' 2002), Waikoloa, HI, January 2002.
12. 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.
13. 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.
14. V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. INFOCOM '97, Apr. 1997.
15. 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.
16. 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.
17. Jan Schaumann, "Analysis of Zone Routing Protocol", Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002
18. Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Intrazone Routing Protocol (IARP)", IETF Internet Draft, draft-ietf-manet-iarp-01.txt, June 2001
19. Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Interzone Routing Protocol (IERP)", IETF Internet Draft, draft-ietf-manet-ierp-01.txt, June 2001
20. Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks", IETF Internet Draft, draft-ietf-manet-brp-01.txt, June 2001