

A SECURE ZONE BASED CLUSTERING PROTOCOL [ZBCP] FOR MOBILE AD HOC NETWORKS [MANETs]

K. Gayathri

Assistant Professor, Department of CS, NGMC, Pollachi.
gayathri.it91@gmail.com

ABSTRACT:

Mobile Ad Hoc Networks (MANETs) are described as a collection of multi hop wireless mobile nodes, infrastructure less connectivity and dynamic topology in nature. Designing a secure protocol for Mobile Ad Hoc Network is a challenging task. There are many protocols proposed for secure routing in MANETs. In this thesis, we proposed a Zone Based Clustering Protocol [ZBCP] which is a hybrid routing protocol and it is a grouping of both proactive and reactive routing technique in MANETs. The implementation of proposed protocol is based on the clustering technique in Zone Based Routing [ZBR]. Routing Disorder [RD] attack is the major issue in Zone Based Routing [ZBR], the Secure Zone Based Clustering Protocol [ZBCP] can provide a basis for the secure communication between mobile nodes.

Keywords: *MANETs, Secure routing protocol, ZBCP routing protocol.*

1. INTRODUCTION:

1.1 Mobile Ad Hoc Network

The wireless technology has been experiencing rapid growth in the past few decades. Wireless networking uses radio frequency to communicate the information. Mobile Ad Hoc Network (MANET) is described as a collection of multi hop wireless mobile node, and dynamic in nature. Since it does not depend on any particular topology, the movements of the nodes are unpredictable. Nodes in the network are used for exchanging data and the nodes are free to move dynamically. MANETs uses shared communication medium and each node in the network act as a routers or hosts. Each node in the network can communicate with all other nodes in the network through wireless medium.

There are large numbers of applications and services run by mobile devices, network connections and data services are most demanding ones. Most of

the connections among the wireless devices are fixed infrastructure-based service, or private networks. For example, connections between two mobile phones are setup by Base Station Controller and Mobile Switching Center in cellular networks.

2. METHODOLOGY:

2.1 PROPOSED SYSTEM

There are many different routing protocols for MANET are already implemented and tested in different simulators. But it has some limitations due to its dynamic nature which leads to mobility in nodes. To overcome the limitations, in this thesis, we proposed a Secure Zone Based Clustering Protocol (ZBCP). It is a hybrid routing protocol, which aims at addressing the drawbacks in existing system of routing protocol by implementing the properties of reactive and proactive routing methodology. The proposed routing protocol is based on the concept of clustering in zone based routing. The thesis describes the design of the proposed protocol and analysis its robustness in the security attacks. Together with existing routing protocol approach for MANETs, Secure Zone Based Clustering Protocol (ZBCP) provides a secure routing operation for mobile node in the network.

Objective:

The main objective of this thesis is based on the following two concepts:

- (i) It aims towards implementing, designing and suggesting a high efficient security for Mobile Ad Hoc Network (MANET) by implementing secure routing and monitor routing disorder attack.
- (ii) The proposed routing protocol ZBCP should be built upon a platform which is not only efficient in security which includes data authentication and integrity but also in practical environment.

3. ZONE BASED CLUSTERING

Zone Based Clustering Protocol [ZBCP] is a hybrid routing protocol to address nodes clustering, and to limit the amount of routing information that broadcast inside the network. The basic concept behind clustering is to cluster the network nodes into a number of overlapping clusters. By clustering the nodes it enables the aggregation of the routing information, and consequently increases the scalability. Specifically, clustering create a possible hierarchical routing in which paths are traced between clusters (instead of among

nodes); this increases the routes duration, thus reduce the amount of routing control overhead.

All nodes in the cluster communicate with cluster head, all inter-cluster communications occur in at most two hops, while intra-cluster communications occurs through the gateway nodes. If a source node wants to send a packet it send it to their cluster head that either distributes the packets inside the cluster, or (if the destination is outside the cluster zone) forwards them to a gateway node, then the gateway forward the packet to the other clusters. By changing the nodes with clusters, existing routing protocols can be openly applied to the network. Only gateways (which act as routers) and cluster heads joined in the propagation of routing.

Protocol Overview

The Secure Zone Based Clustering Protocol [ZBCP] is based on the concept of Zone Routing Protocol [ZRP]. It is build with the concept of clustering the nodes within the zone and it is separated based on the zone range. Each zone in the network will have some fixed range and within the range clusters are formed. Zone Based Clustering Protocol (ZBCP) is described as hybrid routing protocol which combines the

advantages of both proactive and reactive routing approaches and it perform secure routing between mobile nodes. The best components from proactive and reactive approach are combined in this routing protocol.

The main reason for selecting ZBCP for routing mechanism is as follows:

- (i) It is based on the concept of zone clustering (restricted area), and it is more flexible to perform security mechanisms inside the network.
- (ii) Since the concept of zone clustering is to split the nodes in terms of interior nodes (nodes within zone cluster) and exterior nodes (nodes outside the zone cluster).
- (iii) If the intruders try to misuse the nodes, it is restricted within the zone cluster.

Like Zone Routing Protocol [ZRP] the proposed Zone Based Clustering Protocol [ZBCP] performs routing in terms of intra-zone [12] and inter-zone [12] routing. However, the main difference between ZRP and ZBCP is in security aspects. In Zone Routing Protocol [ZRP] there is no security consideration; due to the mobility nature of

nodes in MANET. ZBCP is designed to address all the security concerns like authentication, packet integrity and data confidentiality during both intra-zone clustering and inter-zone clustering. ZBCP is an advanced approach for routing as it is based on clustering algorithm. Figure 1 shows a Zone Based Clustering Protocol [ZBCP]. Cluster head are represented in gray color and gateway present in between the two clusters and each gateway act as a router for node communication.

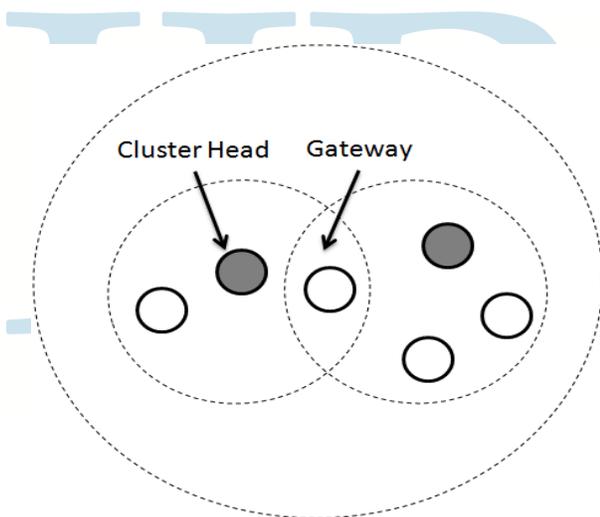


Fig.1 Zone Based Clustering Protocol (ZBCP)

4. SECURE ROUTING IN ZBCP

The main reason for implementing Secure Zone Based Clustering Protocol [ZBCP] is to limit the attacks in existing routing protocols. ZBCP is based on zone clustering (restricted zone), in case of failure

in data transmission, ZBCP does not allow it inside the zone because it is restricted to a zone.

Each packet which is transmitted between nodes are signed or encrypted. All the data packets which contain secret information are encrypted using symmetric key approach. Each node has two pairs of public key/private key. One is for signing and verifying other for encryption and decryption. For all node the signing and verifying keys are S_{key} , V_{key} . Encryption and Decryption keys are E_{key} , D_{key} .

For key distribution and management in secure Zone Based Clustering Protocol [ZBCP] it uses public key certificates. Each node in the network (N_X) before transmitting the data should be certified by CAs (Certification Authorities). CAs provides key generation for node (N_X).

5. CONCLUSION:

In this thesis, we have measured the routing approaches in mobile ad hoc networks for the purpose the security viewpoint. We have analyzed the intimidation against ad hoc routing protocols and the requirements that need to be addressed for secure routing. Existing routing protocols for Mobile Ad Hoc

Networks (MANETs) are either reactive or proactive in nature and they are limited in their approach in terms of offering security across various networking applications. We exposed the advantages of hybrid routing in dealing with these limitations, where the best properties of proactive and the reactive behavior are mixed together to perform secure routing.

In this thesis, we have proposed and designed the analysis of a new secure routing protocol for Mobile Ad Hoc Networks, called the Secure Zone Based Clustering Protocol (ZBCP). The proposed protocol ZBCP is hybrid in nature, which is a combination of proactive and reactive routing and based on the concept of zone routing protocol (ZRP). It provides a result for secure routing in the mobile ad hoc network environment. In designing ZBCP, we carefully fit the economical cryptographic primitives to each part of the protocols to create an efficient protocol that is strong against multiple attacks in the network. The proposed protocol ZBCP gives a better result towards achieving the security objective like data confidentiality, message integrity, and message authentication, by taking an integrated methodology of digital signature and both the symmetric and asymmetric key encryption techniques.

Secure Zone Based Clustering Protocol (ZBCP) is a hybrid routing protocol that supports nodes with sensible resources and does not require major additional work from the nodes within the group. Our simulations show that ZBCP is as efficient as ZRP in discovering and maintaining routes, at the cost of using larger routing packets which result in a highest percentage in 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 would be almost insignificant and negligible as compared to the proposed degree of security, which ZBCP will provide to any network system, if adopted.

The proposed protocol the Secure Zone Based Clustering Protocol [ZBCP] provides security at IP layer. Together with existing approaches to secure the physical layer and MAC layer within the network routing protocol, the Secure Zone Based Clustering Protocol (ZBCP) provides a foundation for governing a secure communication system for Mobile Ad Hoc Networks (MANETs).

6. REFERENCES:

- [1] C. Siva Ram Murthy and B. S Manoj, "Ad Hoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.
- [2] B. G. Claybrook, File Management Techniques. New York: Wiley, 1983.
- [2] Imrich Chlamtac, Marco Conti, Jenifer J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges", Elsevier Network Magazine, vol. 13, pages 13-64, 2003
- [4] S. Dolev, D. K. Pradhan, and J. L. Welch, "Modified tree structure for location management in mobile environments," Comput. Commun., vol. 19, no. 4, pp. 335–345, 1996.
- [3] George Aggelou, "Mobile Ad Hoc Networks", 2nd edition, Mc Graw Hill professional engineering, 2004
- [6] J. S. M. Ho and I. F. Akyildiz, "Dynamic hierarchical database architecture for location management in PCS networks," IEEE/ACM Trans. Networking, vol. 5, pp. 646–660, Oct. 1997.
- [4] Stefano Basagni, Marco Conti, Silvia Giordano and Ivan Stojmenovic, "Mobile Ad Hoc Networks", IEEE press, A John Wiley & Sons, INC. publication, 2003
- [5] 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.
- [6] 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.
- [7] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. IEEE SICON '97, Apr. 1997, pp. 197–211.
- [8] 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.
- [9] 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.