An overview of Zone Routing Protocol

Aasim Zafar

Information Systems Department, Faculty of Computing and Information Technology,

King Abdulaziz University, Jeddah, Saudi Arabia

Abstract –This paper analyses Zone Routing Protocol (ZRP) that employs location aware routing and incorporates security into itself. It takes into account various aspects of routing which overall improves the routing performance. The use of location information limits the search to a desired area and also reduces the number of routing packets. The existing routing protocols are highly vulnerable to the attacks. We have considered the security criteria and discussed the ad hoc routing security in ZRP

Keywords: Zone Routing Protocol, Security, MANET

---♦-------------------------------------

INTRODUCTION

In recent years wireless communications and portable computing devices have gained a widespread popularity. This has triggered the research on the design of Mobile Ad hoc Networks (MANET). The dynamic topology of the network poses a great challenge in the design of ad hoc networks. Each of the existing protocols has one or the other limitations. The existing protocols are generally categorized into proactive, reactive and hybrid.

Zone Routing Protocol (ZRP) [19] is a hybrid scheme that combines both proactive and reactive routing into a single framework to achieve scalability and improve efficiency. It divides the entire network into zones of different size. The Intrazone Routing Protocols (IARP) [2] are the proactive protocols that maintains the route within the zone whereas the Interzone Routing Protocols (IERP) [3] are the reactive protocols that are responsible for the communication between the zones.

However, the combination of both routing strategy still poses challenges due to the constant changing topology. For example, a packet destined for a node may be lost, if the previous route no longer exists and may require route discovery starting from the scratch.

Location aware routing assist in eliminating these limitations to a large extent [9]. It limits the search by the use of Global Positioning System (GPS) and location information, thereby, minimizing the time and effort in route discovery. One thing that must be noted here is that the location aware service can be used only with IERP, which requires on-demand route discovery since the functionality of local routing is provided by IARP.

Another challenge faced by the existing routing protocol is that ad hoc networks are highly vulnerable to attacks. Privacy and reliability are highly desirable in communication. Any intermediate node can compromise or any malicious node can drop the packets that are destined to other nodes. Secure routing in MANETs depends upon the trustworthiness of the participating nodes.

RELATED WORKS

Mobile Ad Hoc Network has significantly gained the attention of researchers. A large number of routing protocols have been proposed in order to overcome the challenges posed by MANET. Most of the proposed routing protocol today are either proactive (i.e. table driven) or reactive (i.e. on-demand). Some hybrid protocols have also been proposed. However none of the hybrid protocols incorporate location information or security. Neither any QoS extensions have been made. In this section we provide an overview of the work done in field of ZRP, location aware information, security and QoS.

The Zone Routing Protocol (ZRP) was the first hybrid routing protocol. ZRP defines a zone around each node of radius ρ, where ρ is number of hops to peripheral nodes. It makes use of IARP for routing within zone and IERP for routing between zones. It provides efficient route discovery through border casting [6]. [1] Gives analysis of ZRP. [6] gives the optimal configuration for routing in ZRP. Independent Zone Routing (IZR) [7] is an enhancement of the zone routing framework, which allows adaptive and distributed configuration for the optimal size of routing zone.

SHARP [16] finds a balance point between proactive and reactive routing by adjusting the degree to which the route information propagated proactively versus the degree to which it needs to be discovered reactively. It creates proactive zone around hot destinations.

The existing ZRP routing algorithm does not take into account the physical locations of the nodes participating in the network.

However, many other routing algorithms are proposed that uses location information. [8] Proposes algorithm to reduce route discovery overhead using location information. Dommety and Jain [17] briefly suggest use of location information in ad hoc network. GRID [18] tries to exploit location information in route discovery, packet relay and royte maintenance. [10] maintains location information of each node in routing tables and sends data message in the direction computed based on these routing tables. [9] gives a survey on the location services and forwarding strategies.

OVERVIEW OF ZRP

As mentioned earlier ZRP provides a framework to the existing protocols. It combines the advantage of both proactive and reactive scheme. ZRP divides the network into zones of variable size, size of the zone is determined by radius of length ρ, where ρ is the number of hops to the perimeter of the zone and not the physical distance.

Since most of the communication takes place between the nodes that are in close proximity of each other, ZRP takes advantage of proactive protocols to discover the routing information within the zone. This is called as Intrazone Routing Protocol (IARP). Also, changes on the other side of network have less impact on local neighbourhood [1], reactive protocols are used to discover the routes between the zones. This is called as Interzone Routing Protocol (IERP). The description and analysis of zone routing protocol in detail is in [1].

A node uses IARP [2] to communicate with its neighbour nodes that are within its zone. It is table driven protocol and it continuously updates the routing information to determine the peripheral nodes and to maintain the map in order to route the packets efficiently within the zone. Peripheral nodes are the nodes whose minimum distance to the node is exactly equal to zone radius.

Because each node maintains its own routing zone, the zones of neighboring nodes heavily overlap. IARP allows for local route optimization by removing redundant routes and using the routes with fewer hops if any exists. Each node is assumed to maintain routing information only for the nodes within its zone. Hence, scope of IARP must be limited to ρ. This can be achieved by assigning time-to-live (TTL) initially to ρ-1 and decrementing it at each hop so that it becomes zero when it reaches the peripheral node.

IERP [3] is on-demand protocol that allows route discovery for nodes that are in other zones. It sends route request query when a route for a particular node is desired. However to minimize the delay it makes use of Border casting, where the node submit the queries to its peripheral nodes instead of local nodes.

Whenever a node wants to send a packet to another node it first checks whether the destination is within its zone, as the node knows route to all other nodes in its zone. If a route exists, it sends the packet to the desired destination. If the route is not found, it then border casts a route request to all its peripheral nodes. Each peripheral node then looks for the destination within their respective zone and repeats the same process until the destination is found.

Border cast routing protocol (BRP) used in ZRP allows efficient query to border cast the route request initiated by IERP, only to peripheral nodes. The node constructs a border cast tree using the routing zone topology, pruning those nodes that have always been covered. BRP is discussed in detail in [4].

However, since the routing zones heavily overlap, a node can be a member of more than one routing zone. Problem will arise when a node receives the same query multiple times. [5] describes to overcome some of these problems and to overcome the traffic.

To notify the node that the routing zone they belong to have been queried two levels of query detection are introduced. The first level of query detection (QD1) allows intermediate nodes, which forward the queries to the peripheral nodes to detect these queries. The second level of query detection (QD2) allows a node to determine this information by listening the transmission (eavesdropping) if network use a single broadcast channel. Once the nodes are aware that the routing zone they belong, have been queried, they can minimize the packet by dropping the packets. This process is called as Early Termination (ET). Also, they make use of Loopback Termination (TL) in which the routes that loopback into querying nodes are eliminated. Selective border casting [1] can also be used in order to further eliminate the unnecessary border casting.

Given the hybrid nature of the ZRP, performance can be increased by finding the optimal size of the routing zone radius ρ for the given network – which may vary from case to case depending upon the circumstances [6]. For example, in a stationary network like number of people attending conference it would be possible to increase ρ to a large number, without too much of penalty, taking advantage of the easily available routes maintained by proactive routing protocols. [6] proposes two approaches to estimate optimal zone radius “min searching” and “traffic adaptive” which are designed to minimize the amount of control traffic based directly on the control traffic measurements themselves.

POSITION BASED ROUTING

Position based routing require that information about the physical position of the nodes must be available. It reduces the search for routing by minimizing the area of search.

Global Positioning System (GPS) enables a node to determine its position. [20] Outlines various other type of positioning service that can be used in place of GPS.

A location service is used by the sender to determine the position of the destination, so that the sender can include the destination address in the header of the packet which it wants to send. *In ZRP, it is clear that location aware routing is used by IERP, not IARP.* IARP is table driven and it has predetermined path to every node its zone and hence, does not require position based routing.

In order to learn the current position of a specific node, IERP takes help of location service. Location service can be classified as centralized and decentralized [9]. In centralized location service mobile nodes register their current position with the server. When a node wants to send a packet to a destination whose address it does not know it contacts the server of its network. Centralized network has a drawback that since the topology is dynamic, it is difficult to guarantee that atleast one server is present in a given ad hoc network. Moreover it would be difficult to obtain the position of the server in the network. This would result in chicken and egg problem.

As mentioned earlier that location aware services will be used by IERP, which is on-demand, we concentrate on decentralized location services. Some of the prominent decentralized location services, like Distance Routing Effect Algorithm for Mobility (DREAM), Quorum based location service, Grid Location Service, Home Zone, etc are outline in [9].

[8] makes use of expected zone and requesting zone to limit the search to the specified area. Results of [8] showed that using location information results in significantly lower routing overheads, as compared to an algorithm that does not use location information. *Expected zone* from sender’s point of view is the region it expects to contain the destination node at any time ‘t’. The sending node defines *‘request zone’* for the route request. A node forwards a route request only if it belongs to the request zone.

When location information is used in ZRP, IERP has to be modified in order to limit the route request search only to the request zone. Earlier in ZRP when a node has to send a packet to the destination, which is not in its routing zone, it constructed the border cast tree and sent the route request to the peripheral nodes. *We propose an algorithm, when such a situation occurs, the node first defines the request zone, construct the border cast tree and then send the route request to those peripheral nodes that belong to request zone.*

SECURITY IN ZRP

MANET does not have a fixed infrastructure. Hence, the nodes themselves perform routing. Since any node entering in the network can perform routing, the nodes may not be trustworthy. A malicious node may enter the network and degrade the performance, or may discover valuable information by listening to the routing traffic. [11] Discusses some of the criteria and suggests solution for a secure routing protocol. From the standpoint of security, an optimal routing protocol should fulfill the criteria like Certain discovery, Isolation, Light Weight Computation, Location Privacy, Self-Stabilization, and Byzantine Robustness.

In order to accomplish these criteria we must know the different types of attacks and vulnerabilities, an ad hoc network is prone to. We broadly classify the attacks into *passive* and *active* categories. [11], [12] outlines some of the attacks and gives the security analysis.

ZRP attempts to accomplish ‘certain discovery’, using IP address as the identities of the nodes. However a malicious node can advertise itself as having any IP address and the address can be changed instantly. Some kind of cryptography must be employed to ensure route validity.

In order to increase the battery life, algorithm must use ‘lightweight computation’. IARP in ZRP are proactive routing protocols. ZRP allows changing the zone radius to control the number of nodes within the zone and therefore the heaviness of the IARP computations. On the other hand IERP of ZRP is fully reactive which helps in decreasing computation complexity since reactive algorithms requires only forwarding the received messages and storing some routing state.

‘Location Privacy’ must be provided by the routing protocol. ZRP provides some crude location security by dividing network into zones and can attempt to conceal their internal organization from outside world.

‘Self-stabilization characteristics of ZRP can be analyzed according to the choice of the routing protocol for both IARP as well as IERP. [11] suggests some possible ways of protecting routing information integrity from malicious nodes.

- **IPsec:** Different assumptions about cryptographic keys are made in different cases. IPsec can provide protection against the creation of forged nodes. If none of the nodes in a network share cryptographic keys with one another, any malicious node can obtain itself the identity of another node and can route the packets to itself. IPsec Authentication Header (AH) [13] and the Encapsulating Security Payload (ESP) [14] could be used for secure routing. However, this scheme fails if any of the trusted nodes are compromised.

- **Non-Disclosure Method (NDM):** In NDM, a number of independent security agents (SA) are distributed over the network. Each of these SA maintains a pair of asymmetric keys. If a node S wishes to transmit a message to D, without disclosing its location, it sends the message using a number of SAs. When the SA receives the encrypted message, it decrypts the outermost encapsulation and forwards it to the next security agent. Each SA knows only the address of the previous and next hop. NDM may not be possible for routing because of the amount of overhead it introduces. NDM is given in detail in [15].

- **Redundant Path:** Another solution for increasing route robustness is the use of redundant paths mentioned in [16]. If one of the route fails due to malicious node in the path, another one of the discovered routes could be used. However the usefulness of this protection is limited, since an attack cannot always be detected by the route endpoints, which is necessary to switch to other route.

CONCLUSION

We have discussed ZRP by providing an overview of its working and use of position based routing. A brief analysis of security related issues have been discussed. This discussion helps in understanding the ZRP and further improving the performance of ZRP by suggesting new algorithm.

REFERENCES

1. Schauman, J.,”Analysis of Zone Routing Protocol”, December,2002.

2. Haas, Z. J., Pearlman, M. R., and Samar, P., “Intrazone Routing Protocol (IARP)”,,IETF Internet Draft, draft-ietf-manet-ierp-02.txt, July 2002.

3. Haas, Z. J., Pearlman, M. R., and Samar, P., “Interzone Routing Protocol (IERP)”, IETF Internet Draft,draft-ietf-manet-ierp-02.txt, July 2002

4. Haas, Z. J., Pearlman, M. R., and Samar, P.,”Broadcasting Resolution Protocol (BRP)”, IETF Internet Draft,draft-ietf-manet-ierp-02.txt, July 2002.

5. Sinha, P., Krishnamurthy, S. V., and Dao, S., “Scalable Unidirectional Routing with ZRP extensions for MANET”, In proceedings of WCNC, pp.1329-1339, 2002.

6. Pearlman, M. R., Haas, Z. J., “Determining the optimal configuration for the ZRP”, IEEE journal on selected areas in communications, vol. 17, no. 8, Aug 1999.

7. Samar, P., Pearlman, M. R., Haas, Z. J., “Independent Zone Routing – an adaptive hybrid routing framework for ad hoc wireless networks”, IEEE/ACM transactions on networking, vol. 12, no: 4, August 2004.

8. Ko, Y. B., and Vaidya, N. H., “Location Aided Routing (LAR) in MANET”, Wireless Network 6 (2000), pp. 307-321.

9. Mauve, M., Widmer, J., and Hartenstein, H., “A survey on Position Based Routing in Mobile Ad hoc Network”, Network, IEEE 15 (6), 30-39.

10. Basagni, S., Chalmatac, I., Syrotiuk, V. and Woodward, B., “A Distance Routing Effect Algorithm for Mobility (DREAM). In proc. of the 4th annual ACM/IEEE Int. Conf. On Mobile Computing and Networking (MOBICOM)’1998 pp.76-84.

11. Lundberg, J., “Routing Security in Ad hoc Networks”, seminar on network security, HUT TML 2000.

12. Wang, W., Lu, Y., and Bhargava, B.K., “On Security Study of Two Distance Vector Routing Protocols for Mobile Ad hoc Networks”, in proc. of

IEEE Annual Conf. On pervasive computing and communication (Per Com) 2003.

13. Kent S. and R. Atkinson, R., "IP Authentication Header", RFC 2402, Nov 1998.

14. Kent S. and R. Atkinson, R., "IP Encapsulating Security Payload (ESP)", RFC 2406, Nov 1998.

15. Fasbender, A., Kesdogan, D., and Kubitz, O., "Variable and scalable security: protection of location information in Mobile IP technology for the Human Race", IEEE 46th Vehicular Technology Conference, 1996.

16. Ramasubramanyam V., Haas Z. J., Sirer E.G., "SHARP: A Hybrid Adaptive Routing Protocol for MANETs", Mob Hoc '03, June 1-3 2003, Amapolis, Maryland, USA.

17. Dommetty, G. and Jain, R., "Potential Networking Application of Global Positioning System (GPS)", Technical Report, TR-24, The Ohio State University 1996.

18. Liao, W.H., Tseng, Y.C., and Sheu, J.P., "GRID: A Fully Location Aware Routing Protocol for Mobile Ad Hoc Networks", Selected Areas in Communications, IEEE Journal on 18 (9), pp. 1647-1657, 2000.

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

20. Hightower, J. and Gaetano Boriello, G., "Location systems for ubiquitous computing", Computer, 34 (8), pp.57-66, August 2001.