A SECURE IMPROVED ZONE ROUTING PROTOCOL (SIZRP) FOR AD-HOC NETWORKS

[1]Jyoti*, [2]Priyanka

[1-2]Assistant Professor in Computer Science
P.I .G. Government College for Women, Jind, Haryana, India

***Email ID**: [1]jsihmar10@gmail.com, [2]ms.redhu@gmail.com*

Accepted: 14.04.2023 **Published**: 28.04.2023

Keywords: MANET, ZRP, IARP, IERP, BRP, Improved ZRP (ZRP1), NS2.33

Abstract

Ad hoc networks (MANET) are self-organizing wireless networks composed of mobile nodes. Zone Routing Protocol (ZRP) is a hybrid routing protocol used to reduce control overhead of proactive routing protocol and to decrease the latency of reactive routing protocol and suitable for networks with large span and diverse mobility patterns having adaptive behaviour. In ZRP, the proactive routing is performed for the nodes within the zone and reactive routing for the nodes that are outside the zone. Abstract- Ad hoc networks (MANET) are self-organizing Improved ZRP (ZRP1) improves the performance of ZRP by controlling broadcasting by peripheral nodes. ZRP1 is less secure. The present work modifies the ZRP1 by using key authentication and trust based routing. The proposed works add trust based intra zone routing (IARP) and key authentication based inter zone routing (IERP). The key filed id added to ZRP data packet format. The key authentication is used for IERP; if it is used for IARP routing then overhead will get increased. IARP uses trust based security. The trust value is assigned to each node. The trust value of a node increases with successful transmission and decreases with unsuccessful transmission. Ns2.33 network simulator has used for obtaining the simulation results; this process improves security while maintaining the performance.

Paper Identification

**Corresponding Author*

I. INTRODUCTION

Mobile Ad hoc networks (MANET) are wireless networks that have no fixed infrastructure. Each node forwards traffic from other nodes which also act as a router in ad-hoc networks [1]. MANET has been becoming popular due to multiple applications provided by these networks. However, change in the topology in ad-hoc is inherent. The reasons for the change in topology may be are low transmission power. Because of interference and fading due to high operating frequency in an urban environment, the links are unreliable. Ad hoc networks have low bandwidth links because of difference in transmission capacity; some links may be unidirectional. Due to link Instability and mobility of node, the topology of ad-hoc networks changes and routing become difficult [2] [3]. MANET routing protocols are mainly classified into proactive and reactive. Proactive protocols are table driven protocols in which each node stores its routes to all the destination nodes. Advantage of proactive protocol is that there occurs no delay in packet delivery since routes to destination are immediately available. Disadvantage is storage and updating of routing information. Reactive protocol on the other hand doesn't store the routing information instead it finds the route to destination only when the request arrives. Advantage is that overhead of route updating and maintenance is less but delay of delivering packet get increased due to time taken for finding route to the destination [4]. All these leads to hybrid MANET routing which combines the best features of both proactive and reactive routing protocols. In hybrid MANET routing protocol routes within a zone are immediately available and for the destination which is outside the zone, it goes for on demand (reactive) approach [6]. Security of a network is an important factor in constructing any network. In traditional wired networks and infrastructural wireless networks, central servers are available to provide security services for the users inside the networks system. A network has to achieve security requirements in terms of authentication, confidentiality, integrity, availability and non repudiation [7]. The current ad hoc secure routing protocols can be broadly divided into two categories: cryptographic based systems and trust based systems. Cryptographic based systems are further divided into asymmetric and symmetric cryptographic. Both require the existence of an online trusted third party, for example a certification authority, in order to facilitate the acquisition and verification of public keys of the nodes that participate in the ad hoc networks [8]. Much more work has been done for performance improvement of ZRP1. An algorithm is given in this paper for improving the performance of ZRP1.

The rest of paper is organized as follows. In section II ZRP and ZRP1 is described. In section III, new protocol Secure Improved ZRP (SIZRP) is proposed. In section IV, simulation results are discussed. Finally conclusion and future work are given in section V.

II. Zone Routing Protocol and Improved ZRP (ZRP1)

In ZRP, a node proactively maintains routes destination within a local neighbourhood, which is considered as a routing zone. A node routing zone is defined as a collection of nodes whose minimum distance hop from the node is no greater than a parameter referred to as the zone radius. Each node maintains its own routing zone, but routing zones of neighbourhood nodes overlap. For constructing of a routing zone the information of neighbour is needed [9].

The routing process in ZRP protocol is as follows:-

1. A node which has data to transmit, first it checks the destination in its zone.
2. If the destination is present in its zone then it uses proactive routing within zone using routing table information.
3. If destination is outside the zone, it initiates route discovery procedure.
4. In this process the source node generates route request packet (RREQ). Network either uses flooding or uses boarded-casting routing protocol (BRP). In case of flooding every other node receives the RREQ packet, whether they are in the local zone of source node or outside of it. However in case of BRP, source node sends the RREQ packets to the nodes which are at the border of its zone. Now these border nodes flood the packets in rest of network.
5. If a node receives RREQ packet and it is the final destination, it generates the route reply (RREP) sends it back to the node, form where the request came using the same path. This procedure of sending the RREP packet is continued till these packets are received by source nodes. In this way RREP packet follow the same path from which RREQ packets traversed the path.
6. Once the route is established, data transfer take place through the same path [9].

Improved Zone Routing Protocol

ZRP has some drawbacks. In ZRP, when source node broadcasts the query the query packets in the network, some node which are zone member of broadcaster node also receive the packet and forward them. There is no need to forward the query packets by these nodes because their route information already listed in broadcaster's routing table. Only peripheral nodes should forward the query packet. If interior member of the zone forwards the query the query packets, there will be large number of forwards query

packet in the network which are useless; decrease system performance. In order to remove these useless packets, first the position of nodes is checked before forwarding the query packets. If the node is in the zone of that node which has forwarded query packet and also not a border node, it then goes to IDLE STATE and discard the query packet. However if the node is the zone member and border node, it forwards the query performance [10].

III. PROPOSED ALGORITHM

ZRP1 protocol combines the features of both proactive and reactive routing protocol, the performance of this protocol is better. The main drawback of ZRP1 is the security as improved ZRP is less secure. The proposed algorithm modifies the ZRP1 by using key authentication and trust based routing. The proposed works add trust based intra zone routing and key authentication based inter zone routing. The end to end authentication in the inter zone routing is done by using key. The key filed is added to the ZRP data packet format. The key authentication is used only for inter zone routing, if it is used for intra zone routing (IARP) then overhead will get increased. IARP uses the trust based security. The trust value depends upon the number of successful transmission done by the node. The trust value of a node increases with successful transmission and decreases with unsuccessful transmission. This process improves security while maintaining the performance.

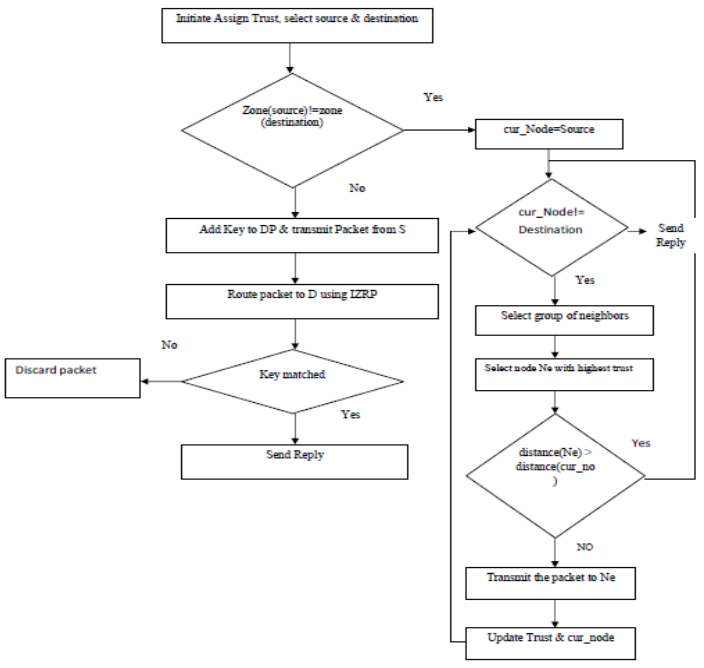

Figure 1 Flow Diagram of SIZRP

IV SIMULATION RESULTS

For obtaining the simulation results NS2.33 network simulator is used. Simulation is defined as "Imitating or estimating how events might occur in a real situation". NS-2 is an event driven simulator that can be implemented in Linux based platform. There are two languages used in NS-2; C++ and OTCL.

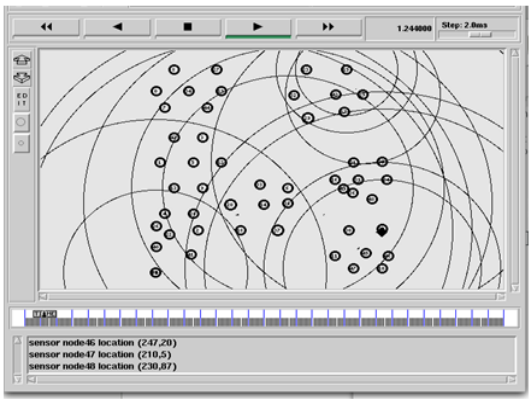

Figure 2 Scenario used for simulation

Figure 2 shows the scenario used for the simulation parameters are mentioned in table 1. In the scenario, network size of 30 nodes with zone radius 2, 5, 10, 30, 35. Three routing protocol ZRP, ZRP1, SIZRP is taken for simulation. The performance is compared on the basis of Packet Delivery Ratio, Routing Load, and End to End Delay.

Simulation area	10000X10000
Node communication range	250m
Data rate	2mb
Mobility model	Random Way point
No of nodes	30
Radius	2,5,10,30,35
Max node speed	50
Media Access mechanism	802_11
Packet Size	512
Simulation time	100

Table I Simulation parameters for network with varying zone radius

Figure 3 shows the Packet Delivery Ratio as a function of zone radius in the network; number of nodes is fixed 30. PDR is ratio of packets delivered to destination and total number of data packet sent by source. The enhancement in PDR is observed at each zone radius. PDR changes with changes in the zone radius. The zone radius changes result but after a certain value performance gets constant. This is due to facts that all nodes already get covered within the zone. Moreover, in every case the performance of SIZRP is better than ZRP1 in terms of PDR.

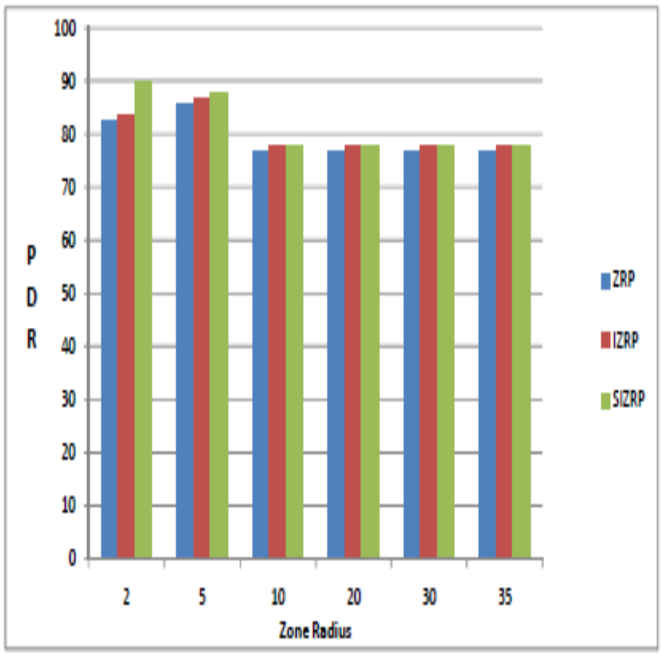

Figure 3 PDR V/s Zone Radius

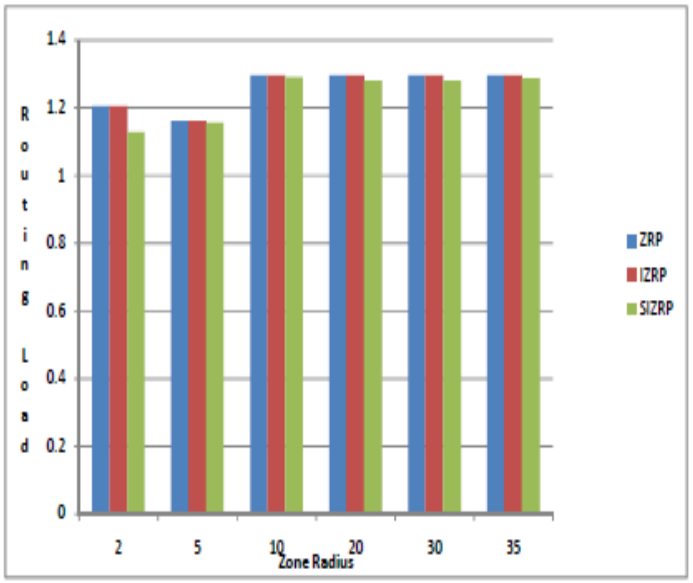

Figure 4 Routing Load V/s Zone Radius

Figure 4 shows the routing load versus zone radius; number of nodes is 30. Routing Load is ratio of total number of routing packets to the total number of received data packet at destination. It is found that routing load is less in SIZRP than ZRP1. For example for zone radius 20 in network it is 1.28021 SIZRP and 1.298 for ZRP1.

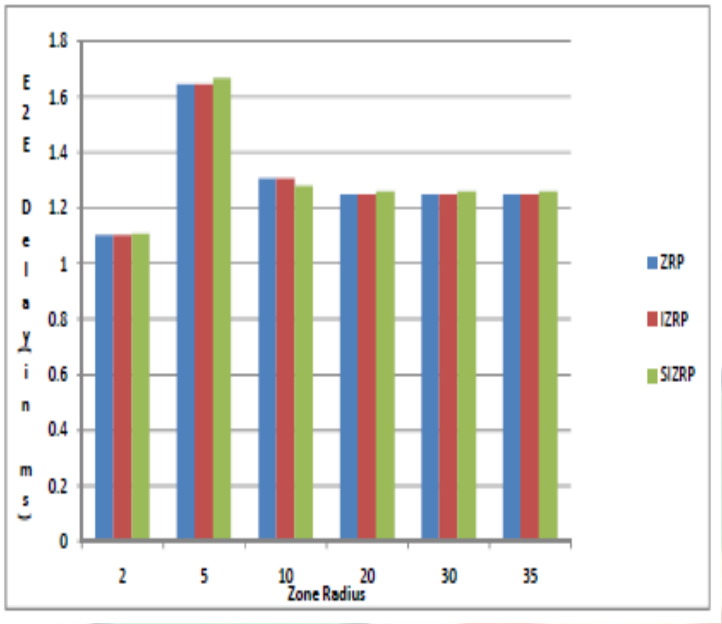

Figure 5 End to End Delay V/s Zone Radius

Figure 5 shows End to End Delay versus Zone Radius; number of nodes is 30. E2E is interval time between time at which packet is sent and time at which packet is received. It is found that E2E delay is almost same in SIZRP than ZRP1. This is due to adding one extra key filed in ZRP data packet format.

V. CONCLUSION AND FUTURE SCOPE

ZRP combines two different routing methods into one protocol. Intra zone routing uses proactive approach to maintain up to date routing information to all the nodes within the zone. In this paper, an extension to ZRP1 with the use of security is proposed. This new routing protocol is called as Secure Improved Zone Routing Protocol (SIZRP). The proposed algorithm is implemented in NS2.33 and results shows that there is increase in Packet Delivery Ratio and decrease in Routing Load, End to End Delay. This confirms the better performance of modified protocol. In future this protocol can be extended by artificial intelligence. This protocol can be analysed over other IEEE standard like 802.15.4 or 802.15.6 etc.

REFERENCES

[1]. H. Osanai, A. Koyama, L. Barolli “An Implementation and Evaluation of Zone Based Routing Protocol for Mobile Ad-hoc Networks”, *International Conference on Network-Based Information Systems*, 2011

[2]. Z.J. Haas and M.R. Pearlman, “The Performance of Query Control Schemes for the Zone Routing Protocol”, *IEEE/ACM Transaction on Networking*, Vol.9, No.4, pp. 427-438, 2001

[3]. Pearlman, R. Marc, Haas et al. "Determining the Optimal Configuration for the Zone Routing Protocol", *IEEE Journal on Selected Areas in Communications*, Vol. 17, No. 8, 1999

[4]. A.S. Tanenbaum, "Computer Networks" third edition, prentice-hall of India private limited, New Delhi

[5]. V. Kumar, Y. Vasudeva, Reddy, et al. "Current Research Work on Routing Protocols for MANET: A Literature Survey", *International Journal on Computer Science and Engineering*, Vol. 2, No. 3, 2010

[6]. S. Taneja, A. Kush, "A Survey of Routing Protocols in Mobile Ad-hoc Networks", *International Journal of Innovation, Management and Technology*, Vol. 1, No. 3, 2010

[7]. L. Zhou and Z.J. Haas, "Securing ad-hoc Networks", *IEEE Network*, Vol. 13, No. 6, pp. 24-30, 1999

[8]. Y. Eirefaie, L. Nassef, I. A. Saroit, "Enhancing Security of Zone Based Routign Protocol Using Trust", *The 8th International Conference on Informatics and Systems (INFOS)*, pp. 32-39, 2012

[9]. L. Barolli, Y. Honma, A. Koyama et al. "A Selective Border-Casting Zone Routing Protocol for Ad-hoc Networks", *Proceedings of 15th International Workshop on Database and Expert System Applications (DEXA'04) IEEE*, 1529-4188/04

[10]. S. K. Pathak, R. Upadhyay, U. R. Bhatt, "An Efficient Query Packets Forwards Algorithms in ZRP Protocol", *International Conference on Issues and challenges in Intelligent Computing Techniques (ICICT) IEEE*, pp. 592-595, 2014