Implementation of SEZRP in MANET using Secure Code Technique

Karishma Kottarwar
Department of Computer Technology
YCCE, Nagpur, India

Nilima Jichkar
Department of Computer Technology
YCCE, Nagpur, India

***Abstract*— Mobile ad-hoc network (MANET) become popular because it gives access anywhere anytime. These networks are self organizing, infrastructure-less, decentralized, dynamic topology. Routing plays an important role for construction of ad hoc networks. Security is one of the main issues in MANET. In the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. Therefore a system is required for securely routing the packets. This system will include Secure Enhanced Zone Routing Protocol (SEZRP). It requires key is generated and provided as input to the secure hash algorithm (SHA-2) to calculate the secure hash code. This secure hash code is distributed among each node in ad-hoc network before it starts transmission of information. The secure routing protocol routes packets from source to destination by providing authentication, non-repudiation, integrity to the system. Result states the performance analysis of SEZRP against the non-secure version of ZRP in the presence of malicious nodes.**

***Keywords*—Zone Routing Protocol, MANET, Secure Enhanced Zone Routing Protocol.**

I. INTRODUCTION

Mobile ad hoc network become popular due to its fundamental characteristic like self manageable, infrastructure less, easy, quick and cost effective deployment, decentralized etc [2]. MANET is a collection of wireless computational devices which has a ability of working as a host as well as router and it can move anywhere in the physical environment [3][4]. Ad hoc network are used in many application particularly when the deployment of access point or fixed base station is very difficult or impossible [5]. These types of network are widely used in battlefield, military, earthquake, disaster relief operation, etc.

There are various routing protocols have been designed for MANET. Routing protocols are broadly classified in three categories which are Proactive, Reactive and Hybrid routing protocols. Zone Routing Protocol is a hybrid routing protocol. Hybrid routing protocol uses advantage of both proactive and reactive routing protocols. Security of routing packets is required in many application of MANET. MANET is vulnerable to various attacks like DOS, black hole, impersonation etc due to the fundamental characteristics of MANET. Maintaining the confidentiality and integrity of the message is very difficult in MANET [6][7][8].

This paper includes enhanced secure routing architecture which detects and protects from malicious actions by third parties. It introduces authentication, non-repudiation, and message integrity to routing in an ad hoc environment as a part of a security policy. The cryptographic secure code will use to prevent most of the attacks and detect malicious behavior. Use of preliminary distribution of secure hash code process will be done followed by a route instantiation process that guarantees point to point authentication for every instance. Route discovery in protocol is accomplished by broadcasting a route discovery message from a source node that is replied to by the destination node.

As mentioned earlier, the authenticated routing protocol is based on the Zone Routing Protocol. Proactive routing is used inside the zone and Reactive routing is used outside the proactive routing zone. Protocol uses cryptographic secure code to bring message-integrity, non-repudiation and authentication to the route discovery process. Nodes use this code to secure the node and authenticate them to other nodes during the exchange of routing messages.

The rest of this paper is organized as following: Section II gives a brief introduction of ZRP routing protocols. The proposed technique is described in Section III. Section IV gives the details of simulation results and performance analysis. Section V gives the conclusion of this research work.

II. ZONE ROUTING PROTOCOL

The Zone Routing Protocol combines the advantages of proactive and reactive approaches into a hybrid scheme, taking advantage of proactive approach within a zone, and using a reactive approach for communicating in different zone.

Zone Routing Protocol consists of several components, which provide the full routing benefit to ZRP. Each

component works independently of the other and they use different techniques in order to maximize efficiency. Figure I illustrate the different protocols and their interactions.

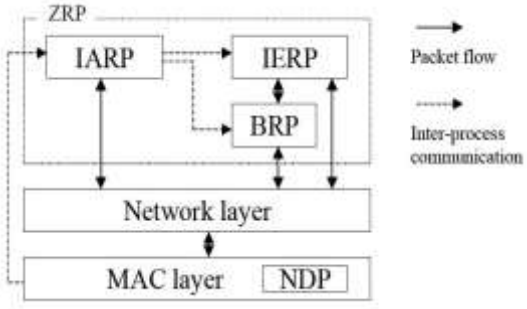

Figure I. ZRP Architecture

A. *Intra Zone Routing Protocol(IARP)*

ZRP assumes that local neighbour discovery is provided by the neighbour discovery protocol (NDP) and implemented on the link-layer. So, the first protocol to be part of ZRP is the IntraZone Routing Protocol, or IARP. This protocol is used when the source node and destination node are in the same zone. The IARP component makes use of proactive protocol for routing the packets.

The node continuously updates the routing information in order to determine the peripheral nodes (border nodes) as well as maintain a list of possible routes to reach the destination. The IARP allows for route optimization through the removal of redundant routes, shortening the routes if a route with fewer hops has been detected, and bypassing the link-failures through multiple hops.

Route discovery in IARP is very efficient and routes to destination are immediately available, due to its proactive nature. In order to not over utilize the available bandwidth resources, the IARP is restricted to routing within the zone, which is why it is referred to as a "limited scope proactive routing protocol".

B. *InterZone Routing Protocol(IERP)*

The InterZone Routing Protocol, or IERP is a reactive routing component of ZRP which takes advantage of known local topology of a node's zone and it enables communication with nodes in other zones.

Route queries are issued on demand within the IERP that is only when a request for a route is made. The delay caused by the route discovery is minimized by the use of border casting technique (in which the node submits the query only to its peripheral nodes). A node does not send the query back to the nodes that made a request even if they are peripheral nodes.

C. *Border cast Resolution Protocol (BRP)*

The Border cast Resolution Protocol is used in the ZRP to direct the route requests initiated by the IERP to the peripheral nodes, removing redundant queries and maximizing efficiency. For this, it utilizes the list provided by the IARP to construct a border cast tree. BRP is only a packet delivery service it is not a routing protocol like IARP and IERP.

The BRP keeps track of which nodes received a query, so that it can prune the border cast tree of nodes that have already received the query. Border cast tree get constructed when a node receives a query packet for a node that does not lie within its routing zone, so that it can forward the packet to its neighbours. These nodes reconstruct the border cast tree upon receiving the packet so that they can determine whether or not it belongs to the tree of the sending node. If it does not, continues to process the request and determines if the destination lies within its routing zone. After that it takes the appropriate action, upon which the nodes within this zone are marked as covered.

Two levels of Query Detection are provided by BRP to detect when a routing zone they belong to has been queried. In first level of Query Detection QD1, the nodes detect the query and notes which zone have been covered as they relay the queries to the peripheral nodes. In networks that use a single broadcast channel, a node can determine this information by listening to the traffic broadcast to other nodes. This approach is referred to as QD2.

The BRP can be seen as the join which ties together the IARP and the IERP for taking full advantage of the proactive and reactive components where they are best used, in the context of ZRP.

III. SEZRP USING SECURE CODE TECHNIQUE

In ZRP before entering to routing zone, the secure code must be generated and distributed among each node. Each node receives exactly one secure code after securely authenticating its identity. For example node A receives a code as follows:
A: fccc241cac177dc8e7b58d13b3de25edaa943bfd

The above secure code is generated by using secure hash algorithm (SHA-2). The system date is taken as input to the secure hash algorithm and generates almost unique fixed size 256 bit hash code. Figure II illustrate the mechanism of generating hash code.

Figure II. Mechanism of generating hash code

A. Neighbour Discovery

Neighbor discovery module in IARP allow nodes to discover who is in their n-hop neighborhood where n is the radius of the zone. This is achieved by NDP in which all nodes advertise their 1-hop neighborhoods to each other. A node accepts HELLO messages from trusted neighborhood.

B. Route Discovery

The reactive route discovery is used to discover new routes as they are needed. If a node requires a route to a destination in IERP, it broadcasts a Route Request message, which contains the addresses of source node and destination node. Source node A begins route discovery to destination X by broadcasting to its neighbors a route request packet (RREQ):
A→broadcast: [RREQ, MAC_ADDRX] codeA
Where,
RREQ : Route Request Packet.
MAC_ADDRX : MAC address of Destination node, X.
codeA : fccc241cac177dc8e7b58d13b3de25edaa943bfd

The RREQ packet includes a packet type identifier (RREQ), destination X's MAC address, A's code. When a node receives a RREQ message, it sets reverse path back to the source node by recording the neighbour from which it received the RREQ. Therefore a reply message will need to forward back to the source.

Let the receiving node is B. After receiving the RREQ packet, node B sends ACK packet with secure hash code of its own back to the node A. Node A first extracts the node B's secure hash code after receiving the ACK packet; it will then match the secure code of B with secure code of its own. If it matches then the node B is not malicious, otherwise it is considered as malicious node.

There are three conditions for checking malicious node that is: 1) If the ACK packet not comes from the receiving node after attempts of resending packets, it is considered as malicious, 2) If ACK packet comes and hash code is not attached with it, it is considered as malicious node, and 3) If ACK comes and hash code is also presents but not match with the senders hash code, it is considered as malicious node. Figure III shows the flow diagram of the system.

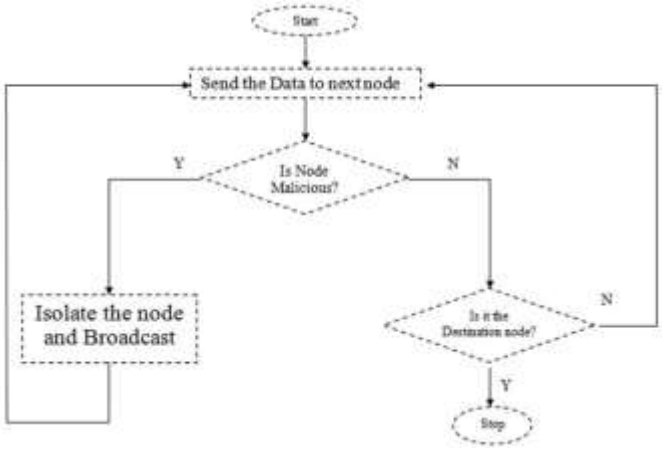

Figure III. Flow Diagram of System

Node B is considered as authorized node to take participate in routing the RREQ packet, node B will append its hash code to the packet and broadcasts the message to each of its neighbours.
B→broadcast: [RREQ, MAC_ADDRX] codeB

Let the neighbour of B be C. Upon receiving ACK packet from node C, node B first extracts the secure hash code of node C and then validates the secure hash code of node C with its own hash code. If the secure hash code matches node C then removes B's code, records B as its neighbour and appends its own code. C then broadcasts the RREQ packet to its neighbours. Each intermediate node repeats the same steps as C between the paths.
C→broadcast: [RREQ, MAC_ADDRX] codeC

C. Route Setup

The message eventually is received by the destination X who replies to the first RREQ that it receives for a source. Now node X creates the Route Reply Packet (RREP) and sends back to the source node A. Malicious nodes have no chance to redirect traffic with the attacks, because messages are verified at each hop.

Along the reverse path back to the source, destination node unicasts a route reply (RREP) packet. Let the first node that receives the RREP packet sent by node X be node D.
X→D: [RREP, MAC_ADDRA] codeX

Route Reply Packet includes a packet type identifier (RREP), the MAC address of A, the secure code belonging to X. The RREP receive by the nodes forward the packet back to the previous neighbour from which they received the original RREQ. Along the reverse path back to the source each node appends its own code before forwarding the RREP

packet to the next hop. Let node C is the D's next hop to the source.
D→C: [RREP, MAC_ADDRA] codeD

Each node checks the secure code of the previous node as the RREP is returned to the source. It avoids attacks by malicious nodes along the path. The source node then receives the RREP packet, and it verifies the destination's secure code.

D. Dealing with Erratic Behaviour

The route is plainly deactivated in the route table when no traffic has occurred on an existing route for that route's lifetime. Data received on an inactive route causes nodes to generate an Error (ERR) message. The use of ERR messages is to report to nodes that links in active routes are broken due to node movement.

This message is forwarded without modification toward the source along the path. It is extremely difficult to detect when ERR messages are made-up for links that are truly active and not broken. A node that send out a large number of ERR messages that should be avoided depending on the ERR messages are valid or untrue.

E. Key Updation

In this event a secure code needs to be updated, the nodes which are already having secure hash code refresh their code with the help of system date after specific time interval.

IV. RESULTS AND PERFORMANCE ANALYSIS

The simulations were performed using widely used network simulator tool (NS2) version 2.33 on Ubuntu 14.04 [1]. In simulation performance of ZRP and SEZRP are compare in terms of packet delivery ratio and average throughput in the presence of malicious nodes.

This analysis is shown using excel charts. For two cases we analyze the performance-

A. Packet Delivery Ratio

The ratio of total packet received to total packet sent is Packet Delivery Ratio (PDR). That means the ratio of total number of data packets successfully collected at destination to the packet generated by CBR traffic sources.

B. Average Throughput

The total data transmits in a period of time and its unit is Kbps is the Throughput of network.

Table I shows the list of simulation parameter which are used in simulation.

TABLE I. SIMULATION PARAMETERS

Simulator	NS2(v-2.35)
Simulation Time	25 ms
Number of Nodes	22
Area Size	1000x1000
Transmission Range	500m
Maximum Speed	0-20 m/s
Maximum No. of Connection	10
Application Traffic	CBR
Packet Size	1024 bytes
Traffic Rate	4 packet/sec
Node Mobility Model	Random Way-point

Secure Hash Algorithm (SHA2) takes system date as input and generates hash code as output. The generated hash code is assigned to all nodes in MANET before transmission of information gets starts. Figure III shows transmission of information started by server1, server1 sends packet to node 5. Node 5 sends the acknowledgement (ACK) back to server1 and server1 checks the ACK if there is hash code present, if present it then match hash code of itself with the received hash code. If it matches then the node which sends ACK is not malicious, otherwise it will be considered as malicious node. Node 5 is considered as authorised node because it's hash code match with server 1's hash code.

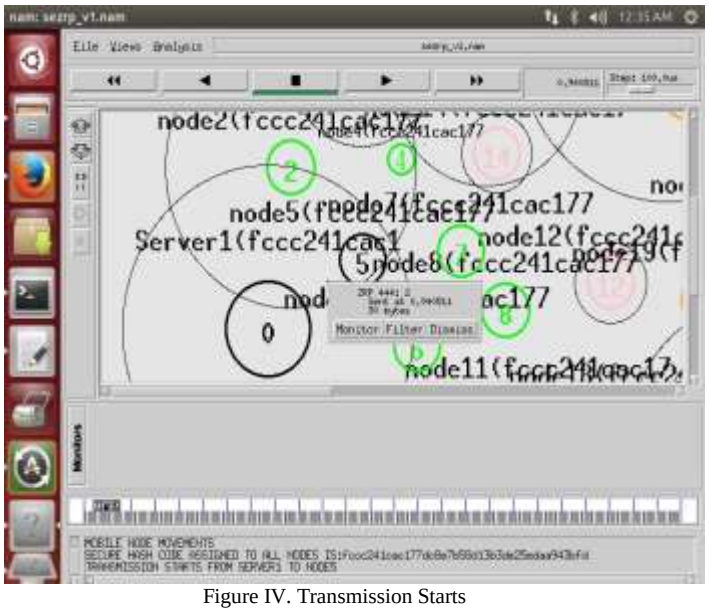

Figure IV. Transmission Starts

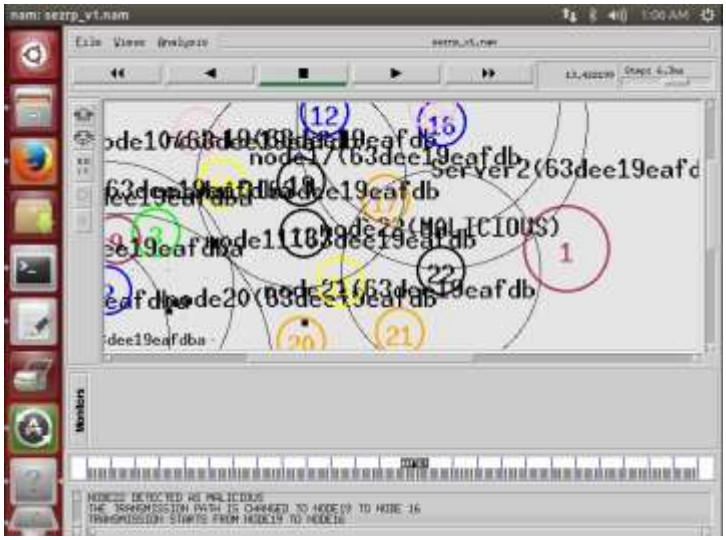

Figure V. Node 19 sends packet to Node 22

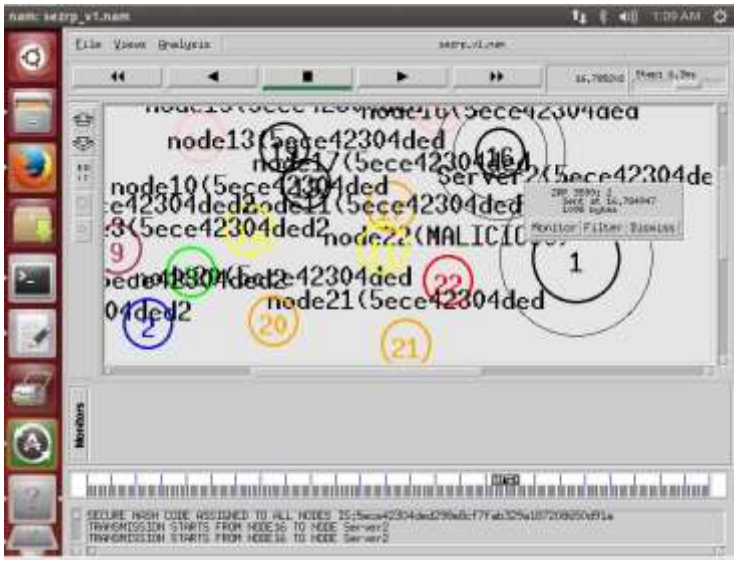

Figure VII. Node 16 sends packet to destination node

Figure VI. Node 19 change route from Node 22 to Node 16

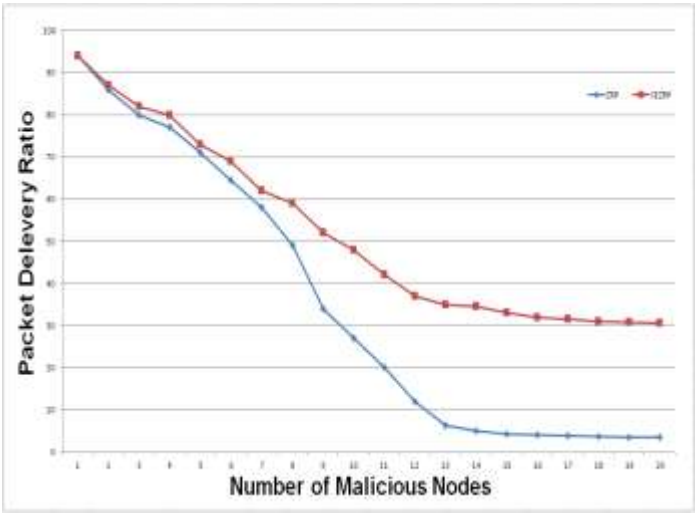

Figure VIII. Packet Delivery Ratio

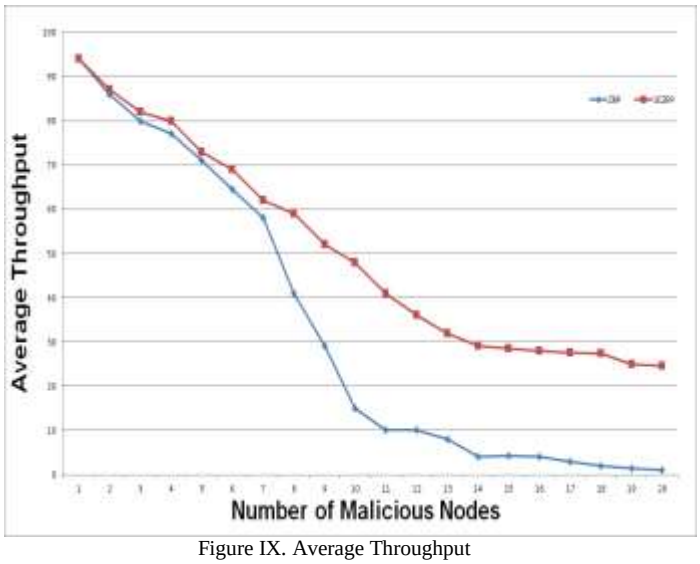

Figure IX. Average Throughput

Likewise transmission further goes on. Now node 19 sends packet to node 22, as node 22 comes in the way of sending packet to destination node as shown in Figure IV. ACK returned by node 22 to node 19 has no hash code attached with it, hence node 22 is considered as malicious. When a node is detected as malicious, the route gets changes from that node to other node. Here route gets changes from node 22 to node 16 which is shown in Figure V. Node 16 sends ACK to node 19 and again security check performs and after authenticating the node, node 16 sends packet to its neighbour node which is a destination node. Figure VI shows that node 16 sends packet to destination node which is denoted as server2. Server2 then sends reply packet back to sender node via possible available route. Also from figures III, V, VI we can see that hash code gets updated by nodes after specific time interval, here time interval is set as 5 milliseconds (ms). Figure VII and Figure VIII shows the performance analysis for packet delivery ratio and average throughput in the presence of malicious nodes respectively.

V. CONCLUSION

In this paper SEZRP with security code technique is proposed to achieve integrity, security and to identify the malicious nodes in MANET. Results and Discussion section includes the working of SEZRP and performance analysis between ZRP and SEZRP. The packet delivery ratio and average throughput are better in case of SEZRP than ZRP in the presence of malicious nodes. Hence, SEZRP enhances ZRP by incorporating security to it and also in the presence of malicious node SEZRP gives better performance factor.

In future, an enhanced version of SEZRP will be implemented to avoid attacks that may be performed against this version of SEZRP. An environment with the presence of attackers will be simulated using NS-2 simulator to study the behaviour of the current protocols and the enhanced one against all possible attacks.

ACKNOWLEDGMENT

The author is highly gratified to her respected guide Prof. N. M. Jichkar for admirable guidance and support to complete this paper. Author is also thankful to Project Development Lab, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur (India) for providing essential facilities to complete this manuscript in present nature. The author would like to thank Prof. N. M. Jichkar (Lecturer, Dept. of CT) and family members for financial and moral supports throughout their technical education.

REFERENCES

[1] Shyam Singh Rajput, and Dr. Munesh C. Trivedi, “Secure zone routing protocol in MANET using authentication technique”, 2014 Sixth International Conference on Computational Intelligence and Communication Networks, pp. 872-877, 2014.

[2] Y. Zhang, and B. H. Soong, “Performance of mobile networks with wireless channel unreliability and resource inefficiency,” IEEE Transactions on Communications, vol. 5, no. 5, pp. 990-995, 2006.

[3] S. Chakrabarti, and A. Mishra, “Qos issues in ad hoc wireless network,” IEEE Communications Magazine, vol. 39, no. 2, pp. 142-148, 2001.

[4] B. Xu, S. Hischke, and B. Walke, “The role of ad hoc networking in future wireless communications,” in Proc. of the IEEE International Conference on Communication Technology(ICCT), vol. 2, pp. 1353-1358, 2003.

[5] S. K. Sarkar, T. Basavaraju, and C. Puttamadappa, “Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications,” Auerbach Publications, MA, USA, 2007.

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A secure routing protocol for ad hoc networks,” in Proc. of the 10th IEEE International Conference on Network Protocols, pp. 78-87, 2002.

[7] M. Yu M. Yu, M. Zhou, and W. Su, “A secure routing protocol against byzantine attacks for MANETs in adversarial environments,” IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449-461,2009.

[8] L. Abusalah, A. Khokhar, and M. Guizani, “A survey of secure mobile ad hoc routing protocols,” IEEE Communications Surveys and Tutorials, vol. 10, no. 4, pp. 78-93, 2008.

[9] Harjeet Kaur, Varsha Sahni, and Dr. Manju Bala, “A survey of reactive, proactive, and hybrid routing protocols in MANET: a review”, International Journal of Computer Science and Information Technologies, vol. 4, no. 3, pp. 498-500, 2013.

[10] Sarvesh Tanwar, and Prema K. V., “Threats & security issues in ad hoc network: a survey report”, International Journal of Soft Computing and Engineering ISSN: 2231-2307, vol. 2, no. 6, pp. 138-143, 2013.

[11] Manoj Yadav, Sachin Kumar Gupta, and R. K. Saket, “Experimental security analysis for SAODV vs SZRP in ad hoc networks”, 2014 Sixth International Conference on Computational Intelligence and Communication Networks, pp. 819-823, 2014.

[12] Bounpadith Kannavong, Hidehisa Nakayama, Yoshiaki Nemoto, Neikat, and Abbas Jamalipour, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless Communications, vol. 14, no. 5, pp. 85-91, Oct 2007.

[13] Sandeep Kaur, and Supreet Kaur, "Analysis of zone routing protocol in MANET", International Journal of Research in Engineering and Technology, vol. 2, no. 9, pp. 520-524, Sept 2013.

[14] Niklas Beijar, "Zone Routing protocol (ZRP)", Networking Laboratary, Helsinki University of Technology, 2002.