International Journal of Engineering Research & Management Technology ISSN: 2348-4039

September- 2014 Volume 1, Issue-5

Email: editor@ijermt.org www.ijermt.org

# Enhancement of SZRP Hybrid Routing Protocol Using OPNET Simulator

**Gurwinder Singh Jatana**
M.Tech (CE) Student
Department of Computer Engineering
Punjabi University Patiala
Punjab, India

**Jaswinder Singh**
Assistant Professor (CE)
Department of Computer Engineering
Punjabi University Patiala
Punjab, India

## ABSTRACT
This paper is a contribution in the field of security analysis on mobile ad-hoc networks, and security requirements of applications. Limitations of the mobile nodes have been studied in order to design a secure routing protocol that thwarts different kinds of attacks. Our approach is based on the Zone Routing Protocol (ZRP); the most popular hybrid routing protocol. The importance of the proposed solution lies in the fact that it ensures security as needed by providing a comprehensive architecture of Secure Zone Routing Protocol (SZRP) based on optimization using AACO, secure neighbour discovery, secure routing packets, detection of malicious nodes, and preventing these nodes from destroying the network. In order to fulfil these objectives, both efficient key management and secure neighbour mechanisms have been designed to be performed prior to the functioning of the protocol.

**Keywords:** MANETs, OPNET, ZRP, SZRP, AACO etc.

## I. INTRODUCTION
The attractive features of ad-hoc networks such as open medium, dynamic topology, absence of central authorities, and distributed cooperation hold the promise of revolutionizing the ad-hoc networks across a range of civil, scientific, military and industrial applications. However, these characteristics make ad-hoc networks vulnerable to different types of attacks and make implementing security in ad-hoc network a challenging task. The main security problems that need to be dealt with in ad-hoc networks include: the identity authentication of devices that wish to talk to each other, the secure key establishment of keys among authenticated devices, the secure routing in multi-hop networks, and the secure transfer of data [1]. This means that the receiver should be able to confirm that the identity of the source or the sender (i.e., one hop previous node) is indeed who or what it claims to be. It also means that the receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit. In this paper, we propose securing one of the most popular hybrid protocols: zone routing protocol (ZRP). For details on the basic operation of ZRP, see [2]. Conventional ZRP is not secure and does not consider security requirements. We modify it by using four stages as shown in Fig. 1. First, we use an efficient key management mechanism that is considered as a prerequisite for any security mechanism. Then, we provide a secure neighbour detection scheme that relies on neighbour discovery, time and location based protocols [3, 4]. Securing routing packets is considered as the third stage which depends on verifying the authenticity of the sender and the integrity of the packets received.

## II. ROUTING IN MOBIE AD HOC NETWORK
One of the most exciting and challenging aspects of ad hoc network is the routing issue. Most of the routing protocols are designed for wired and structured network. It is often very hard to adopt these protocols for ad hoc network. Broadly routing protocols can be classified into three groups: reactive, proactive and hybrid. This is summarized in the following figure:

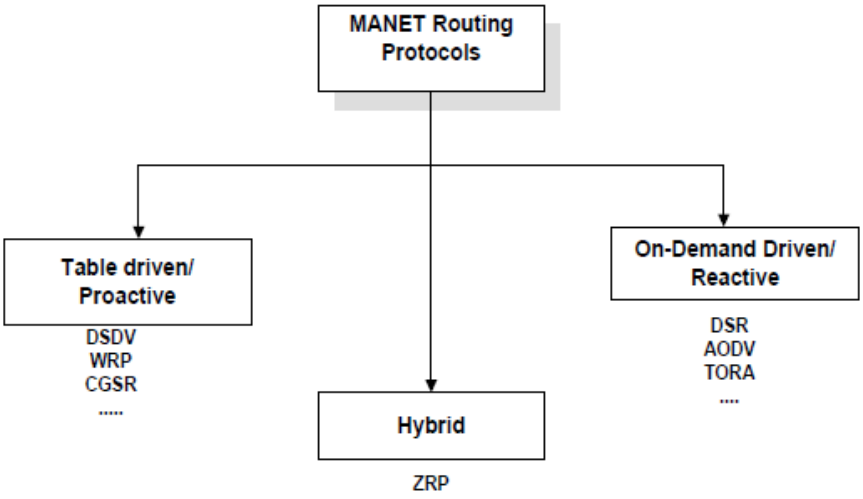


Fig 1: Classification of routing protocols

### A. ROACTIVE ROUTING PROTOCOLS

In table-driven or proactive protocols, the nodes maintain an active list of routes to every other node in the network in a routing table. The tables are periodically updated by broadcasting information to other nodes in the network such as the Destination Sequenced Distance Vector routing protocol (DSDV)[2].

### B. REACTIVE ROUTING PROTOCOLS

In contrast to table driven routing protocols, on demand routing protocols find route to a destination only when it is required. The on-demand protocols have two phases in common – route discovery and route maintenance. In the route discovery procedure, a node wishing to communicate with another node initiates a discovery mechanism if it doesn't have the route already in its cache. The destination node replies with a valid route. The route maintenance phase involves checking for broken links in the network and updating the routing tables. One of the most popular reactive protocols is Ad hoc On-demand Distance Vector routing protocol (AODV) [3].

### C. HYBRID ROUTING PROTOCOLS

Hybrid routing protocols inherit the characteristics of both on-demand and table-driven routing protocols. Such protocols are designed to minimize the control overhead of both proactive and reactive routing protocols. The best example of hybrid routing protocols is the Zone Routing Protocol (ZRP)[4].

## III. SECURITY GOALS

To secure the routing protocols in MANET, researchers have considered the following security services [5][6][7]:

**Availability** guarantees the survivability of the network services despite attacks. A Denial-of-Service (DoS) is a potential threat at any layer of an ad hoc network.
**Confidentialit**y ensures that certain information be never disclosed to unauthorized entities. It is of paramount importance to strategic or tactical military communications.
**Integrity** ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.
**Authentication** enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information.
**Non-repudiation** ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

## IV. ISSUES IN SECURING THE ROUTING PROTOCOL

Securing the routing protocols for ad hoc networks is a very challenging task due its unique characteristics [8]. A brief discussion on how the characteristics causes' difficulty in providing security in ad hoc wireless network is given below.

Shared radio channel: Unlike the wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc networks is broadcast in nature and shared by all nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So a malicious node can easily obtain data being transmitted in the network.

Insecure environment: The environment in which MANET is generally used may not be always securing, for example, a battle field. In such environment, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks. Lack of central authority: In wired networks or infrastructure based wireless networks it would be possible to monitor the network traffic through routers or base stations and implement security mechanisms at those points. Since MANET don't have any such central points, these mechanisms can't be applicable to them.

Lack of association rules: In MANET, since nodes can leave or join the network at any point of time, if no proper authentication mechanism is used for associating nodes with the network intruders can easily join the network and carry out attacks.

Limited availability of resources: Resources such as bandwidth, battery power and computational power are scare in ad hoc networks.

## V. SECURE ROUTING PROTOCOLS FOR ADHOC NETWORKS

Following is the brief description of the security protocols in MANET.

### A. SAODV

The Secure Ad-hoc On-Demand Distance Vector (SAODV) proposed by Zapata [9]is an extension of the AODV routing protocol. It can be used to protect the route discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation. The protocol operates mainly by using new extension messages with the AODV protocol. In these extension messages there is a signature produced by digesting the AODV packet using the private key of the original sender of the Routing message. The Secure-AODV scheme is based on the assumption that each node possesses certified public keys of all network nodes. Ownership of certified public keys enables intermediate nodes to authenticate all in-transit routing packets. The originator of a routing control packet appends its RSA signature and the last element of a hash chain to the routing packets. As the packets traverse the network, SAODV protocol gives two alternatives for ROUTE REQUEST and ROUTE REPLY messages. In the first case when a ROUTE REQUEST is sent, the sender creates a signature and appends it to the packet. Intermediate nodes authenticate the signature before creating or updating the reverse route to that host. The reverse route is stored only if the signature is verified. When this packet reaches the final destination, the node signs the ROUTE REPLY with its private key and sends it back. The intermediate and final nodes, again verify the signature before creating or updating a route to that host. The signature of the sender is also stored along with the route entry. The second case is also similar to the first one with the only disparity being that the ROUTE REQUEST message has another signature that is always stored along with the reverse route.

### B. SEAD

The Secure and Efficient Ad hoc Distance vector routing protocol (SEAD) [10] is based upon the DSDVSQ routing protocol (which is a modified version of DSDV routing protocol). It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and sequence number in the routing table. More specifically, for authenticating a particular sequence number and metric, the node generates a random initial value $x \in (0,1)^p$ where p is the length in bits of the output of the hash function, and computes the list of values h0,h1,h2,h3,…,hn, where h0=x , and hi = H(hi-1) for $0< i \leq n$ , for some n. As an example, given an authenticated hi value, a node can authenticate hi-3 by computing H (H (H (hi-3))) and verifying that the resulting value equals hi. Each node uses one authentic element of the hash chain in each routing update it

sends about itself with metric 0. This enables the authentication for the lower bound of the metric in other routing updates for that node. The use of a hash value corresponding to sequence number and metric in a routing update entry prevents any node from advertising a route greater than the destination's own current sequence number. The receiving node authenticates the route update by applying the hash function according to the prior authentic hash value obtained and compares it with the hash value in the
Routing update message. The update message is authentic if both values match. The source must be authenticated using some kind of broadcast authentication mechanism such as TESLA [11]. Apart from the hash functions used, SEAD doesn't use average settling time for sending triggered updates as in DSDV in order to prevent eavesdropping from neighboring nodes.

### C. SZRP

The Secure Zone Routing Protocol (SZRP) is based on the concept of Zone Routing Protocol (ZRP) [12, 13]. It is a hybrid routing protocol that combines the best features of both proactive and reactive approaches and adds its own security mechanisms to perform secure routing. SZRP is designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing. For end to end authentication and message/packet integrity RSA digital signature mechanism is employed, where as data confidentiality is ensured by an integrated approach of both symmetric and asymmetric key encryption [14]. SZRP requires the presence of trusted certification servers called the certification authorities (CAs) in the network. The CAs are assumed to be safe, whose public keys are known to all valid CNs(common nodes). Keys are generated a priori and exchanged through an existing, perhaps out of band, relationship between CA and each CN. Before entering the ad hoc network, each node requests a certificate from it's nearest CA. Each node receives exactly one certificate after securely authenticating their identity to the CA. The methods for secure authentication to the certificate server are numerous and hence it is left to the developers; a significant list is provided by [15].

## VI. SIMULATION EXPERIMENTS

We used standard simulator tool OPNET for simulation. A scenario is set up for simulation to evaluate the performance of three secure protocols SZRP and proposed algorithm. This scenario is run 4 times with different values of the number of nodes ranging from 25 to 100. In scenario the comparison of the scheduling schemes by taking 35 subscriber stations which is shown below.

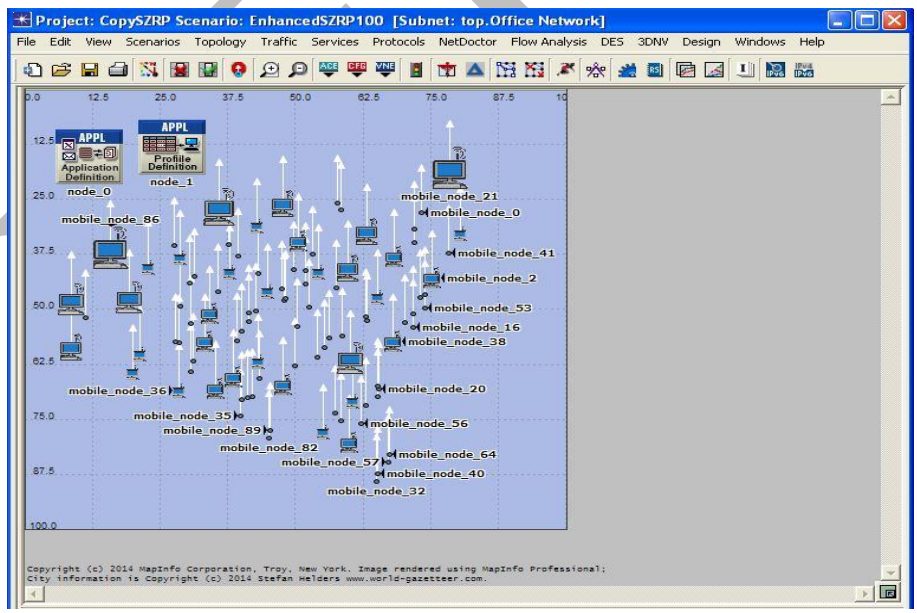


Fig 2 Simulation Scenario

**A. Simulation parameters**

| Parameters | Values |
|---|---|
| Simulator | OPNET 14.0 |
| Protocol examined | SZRP, Enhanced SZRP |
| Simulation time | 400 seconds |
| Topology size | 1000m x 1000m |
| Buffer size (bits) | 256000 |
| Data rate (bps) | 11 Mbps |
| Mobility pattern | Random way point |
| Mobile nodes | 25,50,75,100 |

Tab 4.1 Simulation parameters

**B. Performance metrics**

Throughput: Throughput is the average rate of successful data packets received at the destination. It is the measure of how fast we can actually send the packets through the network. It is measured in bits per second (bits/sec or bps) or data packets per second.

Load: Load in the wireless LAN is the number of packets sent to the network greater than the capacity of the network. When the load is less than the capacity of the network, the delay in packets is minimum. The delay increases when the load reaches the network capacity.

Data Dropped: Data dropped is the count of number of bits per second which are dropped during the travelling of signals from source to destination. Data can be dropped due to unavailability of access to medium.

Delay: The packet end-to-end delay refers to the time taken for a packet to be transmitted across the network from source to destination. In other words, it is the time a data packet is received by the destination minus the time a data packet is generated by the source.

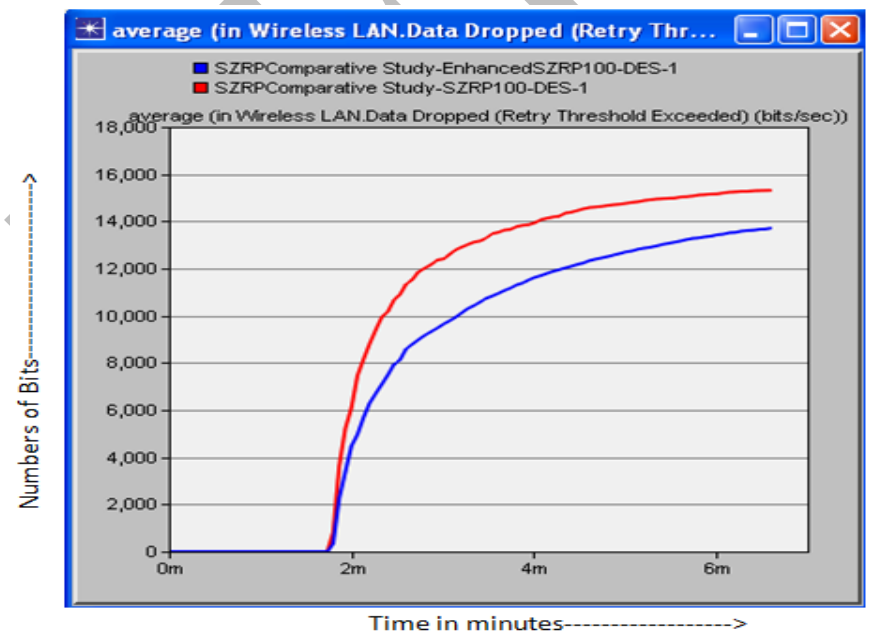


Fig 3: Data Dropped

Figure 3 represented the data dropped in the proposed algorithm i.e. enhanced SZRP and SZRP. From the figure it is clear that the data dropped in the proposed algorithm is much less than that of SZRP.

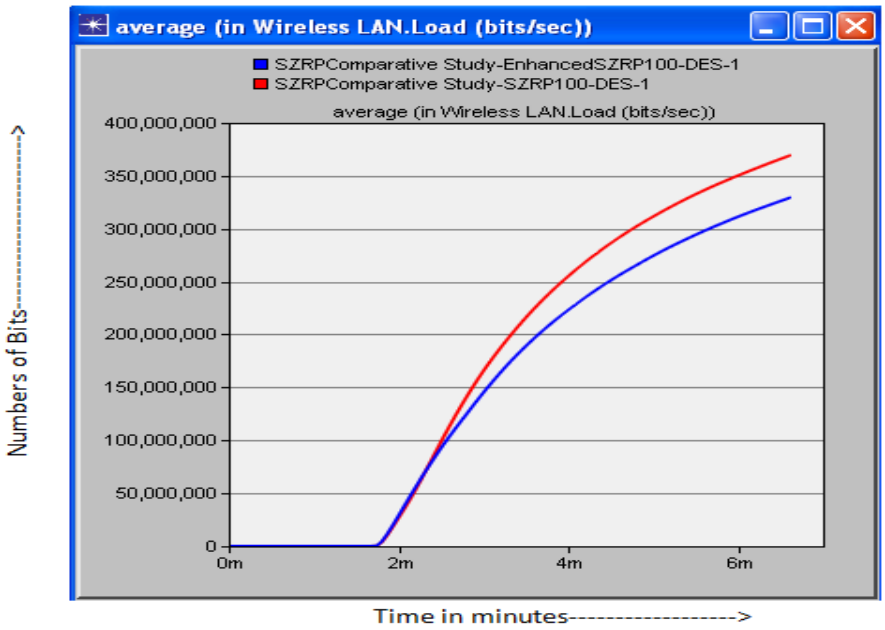


Figure 4 represented the load in the proposed algorithm i.e. enhanced SZRP and SZRP. From the figure it is clear that the load in the proposed algorithm is less than that of SZRP.

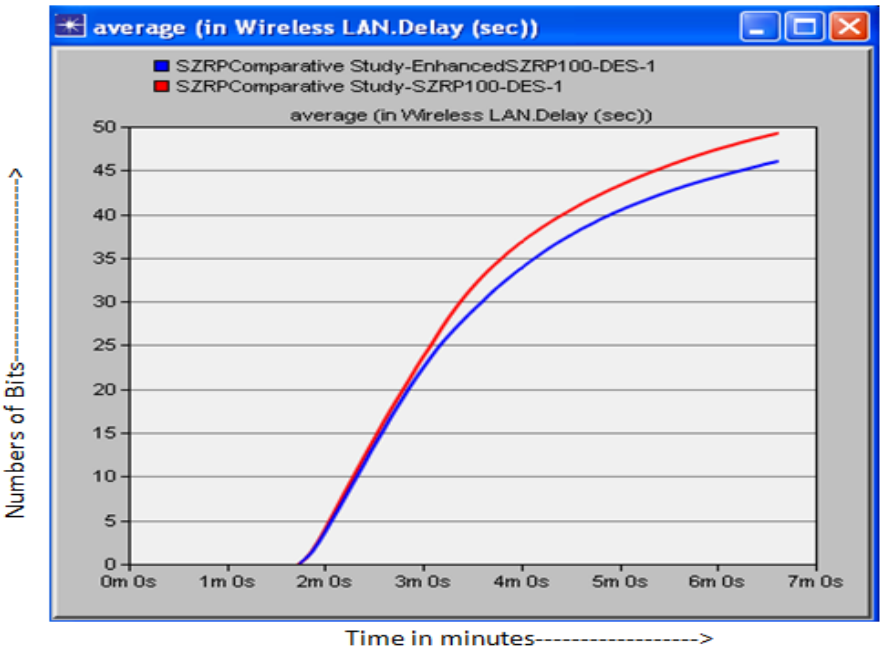


Figure 5 represented the load in the proposed algorithm i.e. enhanced SZRP and SZRP. From the figure it is clear that the delay in the proposed algorithm is less than that of SZRP.

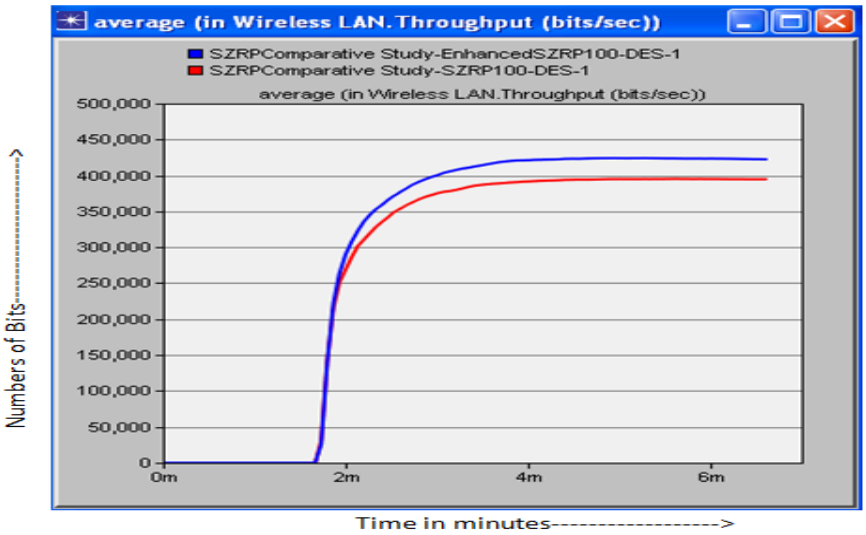


Fig 6: Throughput

Figure 6 shows the data dropped in enhanced SZRP and SZRP in MANET in 100 nodes. From the graph it can easily depicted that the throughput in enhanced SZRP is increased than that of Existing SZRP protocol.

## VII. CONCLUSION

The two most important issues in mobile ad hoc networks are the performance and security. Each mobile node in a MANET acts as a router by forwarding the packets in the network. Hence, one of the challenges in the design of routing protocols is that it must be tailored to suit the dynamic nature of the nodes. In this paper we investigate the performance and security of proposed algorithm and SZRP secure MANET routing protocols and it is found that the proposed algorithm has less data dropped, load and delay and throughput is increased as compare to the SZRP protocol.

## VIII. REFERENCES

1. Nitin H. Vaidya,"Mobile Ad Hoc Networks: Routing, MAC and Transport Issues", University of Illinois at Urbana-Champaign, Tutorial presented at: INFOCOM 2004 (IEEE International Conference on Computer Communication).
2. C. Perkins and P. Bhagwat, Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In Proc. of the ACM SIGCOMM, October 1994.
3. C.E. Perkins, E. Royer, and S.R. Das, "Ad hoc on demand distance vector (AODV) routing," Internet Draft, March 2000.
4. Haas Z.J, " A new routing protocol for the reconfigurable wireless network". In Proceedings of the 1997 IEEE 6th International Conference on Universal Personal Communications, ICUPC '97, San Diego, CA, October 1997; pp. 562 -- 566.
5. Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad. "Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network". , CRC PRESS Publisher, 2003.
6. A Study of Secure Routing in MANET: various attacks and their Countermeasures Abari Bhattacharya , Prof. Himadri Nath Saha , IEMCON , Jan 2011
7. Security in Wireless Ad Hoc Networks , Eric Lee ,Science Academy Publisher, United Kingdom , Vol. 1, No. 1, March 2011
8. C.Siva Ram Murthy and B. S. Manoj. "Ad hoc wireless networks: Architecture and Protocols". Prentice Hall Publishers, May 2004, ISBN 013147023X.
9. M. Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proceedings of the ACM Workshop on Wireless Security (WiSe), ACM Press,2002, pp.1-10.
10. Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks Journal, 1, 2003
11. William Stallings. "Network Security essentials: Application and Standards", Pearson Education , Inc 2003, ISBN 0130351288.
12. 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.
13. Jan Schaumann, "Analysis of Zone Routing Protocol", Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002
14. Behrouz A. Forouzan, "Cryptography and Network Security", Special Indian Edition, Tata McHill publication, 2007
15. J. J. Tardo and K. Algappan, "SPX: Global authentication using public key certificates", In Proceedings of the 1991 IEEE Symposium on Security and Privacy, pages 232