RESEARCH ARTICLE OPEN ACCESS

Security Certified LARDAR Protocol in Mobile Ad Hoc Network

Kalpana Tyagi [1], Anamika [2]
M.Tech [1], Assistant Professor [2]
Department of Computer Science and Engineering
Inderprastha Engineering College
Ghaziabad - India

ABSTRACT
Mobile Ad-hoc Networks (MANETs) are self-managing network which consists of distributed nodes that communicate with each other through wireless links with no fixed infrastructure. Due to dynamic nature of these networks routing protocol are susceptible to various attacks. The black hole attack is one of the noticeable security threats in MANETs. In black hole attack the packet is redirected to a node that is claiming of having shortest route to the destination node but instead it intercepts the data packet and retains it. This paper, presents an approach to overcome black hole in MANETs. In proposed work nodes validate each other by issuing security certificate in digital form to all the other nodes in the network. The proposed method is to be adapted on Location Aided Routing Protocol with Dynamic Adaptation of Request Zone (LARDAR) protocol. This method is capable of detecting and removing black hole nodes in the MANETs. In addition information about angle is kept on route request packet to select optimal path for secure transmission of data packets. The simulation result shows that SC-LARDAR is more secure and bandwidth efficient than the prior methods in terms of packet delivery ratio, routing overhead, throughput etc.
Keywords:- Black hole attack, Location based routing, MANETs, Security Certificate.

I. INTRODUCTION

Mobile ad hoc network (MANETs) [1] became a valuable wireless technology and has gained a lot of advancement in recent years. These devices offer communication opportunities and also increase availability and popularity of mobile devices which led researchers to extend Mobile ad hoc networking. MANETs is a distributed system with a collection of self-managing wireless mobile nodes where each node moves throughout the network in a random way. The communication between these mobile nodes is via the wireless links either directly or by intermediate nodes in a peer-to-peer manner. Therefore, the success of MANETs communication highly relies on the collaboration of the involved mobile nodes. The communication between the mobile nodes takes place in open medium making the MANETs more vulnerable to security attacks [7].

We can use various security protocols to reduce the vulnerabilities from various types of attacks that occur in MANETs. So in this paper we investigate “Black hole” attack security problem in the Ad hoc network routing protocol, and the corresponding security routing mechanism. Due to the importance of Mobile ad hoc network in the communications, the future research should focus on the development of secure routing protocol for data transmission in the network.

The "Black hole" attack is aimed at the routing protocol [8, 12, 13]. In such attack a malicious node advertise itself as having the shortest path to the destination node in order to intercept the packet of source node. This hostile node advertises the availability of fresh route to the destination node irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. Then this malicious node can choose whether to drop the packets or forward it to unknown address.

In this paper, we intended an approach Security Certified-Location Aware Routing with Dynamic Adaptation of Request Zone. We will focus on the basic operation of LARDAR protocol. Subsequently we will analyze how Black hole attack can be detected and prevented in LARDAR to make it secure and reliable. Simulation results shows that SC-LARDAR protocol has lower routing overhead and higher packet delivery ratio and throughput.

II. RELATED WORK

Routing protocols for wireless ad hoc networks are categorized as: Table-driven (or Proactive),On-demand (or Reactive/Source Initiated) and Hybrid Routing Protocols [2]. The table driven routing protocol can be further categorized into link-state and distance-vector protocols. Reactive routing protocols use periodic approach to identify presence of neighbours that leads to unnecessary bandwidth consumption, causes network

overhead and introduces latency. As a result, we state that reactive routing protocols are unsuitable for the problem at hand.

In Proactive routing protocols [3] every mobile node in the network keeps a routing table that contains the list of all available destinations and the number of hops to each. Periodic transmissions of updates of the routing tables help maintaining the topology information of the network. If there is any new significant change for the routing information, the updates are transmitted immediately. Therefore, proactive routing protocols are not suitable for large networks, as Excessive communication overhead due to periodic and triggered updates of routing information throughout the network. When network grows the size of the routing tables and the bandwidth required to update them also grows.

In Reactive routing protocols [3] mobile nodes maintain path information for destinations only when they need to contact the source node or relay packets. This in return ensures that routes are determined and maintained for nodes those require sending of data to a particular destination.As a result, we state that reactive routing protocols are unsuitable for the problems.

In this method of routing the nodes are alienated into regions based on hierarchy. A node can converse with nodes at the same hierarchical level or the nodes at a lower level and directly under it. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The major weakness of these routing protocols are, it depend on meshing parameters and nesting addressing scheme.

The Geographic routing takes into account the physical location of a destination node [4]. GPS conveys location information of each node present over the network. With location information message can be routed to the destination without knowledge of the network topology or a prior route discovery which ultimately reduces the search space and limit the flooding area. Using this physical location of the nodes power and bandwidth consumption to transfer data can be reduced and efficiency can be improved as in GPSR, LAR, and LARDAR etc.

In LARDAR [6], a dynamic adaptation of request zone approach is used. This approach finds the newest location information of destination node which will be carried in the route request packet and helps in finding the destination node address.

Many protocols like are Anonymous Routing Protocol for Mobile ad hoc networks(ALARM) [9], Preserving Location-Based On-Demand Routing in MANETs(PRISM) [10], ALERT have been proposed that are based on LAR and provides security [11]. In this paper, security work is implemented for LARDAR Protocol which also provides low bandwidth consumption and low energy utilization.

A. LARDAR Protocol

Expected Zone:

Expected Zone is the region where source node S consider that the destination node D may contain some time t assuming that node S knows that the node D was at location L at time t0 and current time is t1 [5].

From the viewpoint of S, expected zone of node D is the region that node S expects to contain node D at time t1 based on the knowledge than node D was at location L at time t0. Now, If S knows that D travels with average speed v, then S assumes that the expected zone is the circular region of radius v (t1- t0) centred at location L.

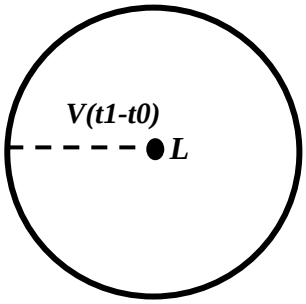

Fig1: Expected Zone

Request Zone:

Request zone is the area where the request packets are sent or broadcast to find a path from source to destination. In LARDAR [6] source node tries to minimize the request zone by confining it to the smallest rectangular area containing both sender as well as receiver.

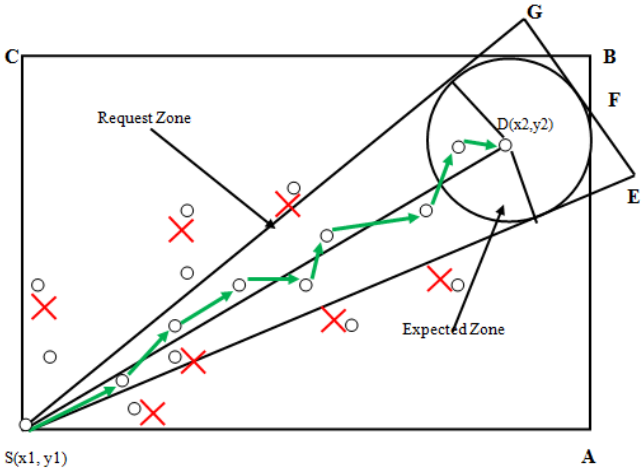

Fig 2: Request Zone in LARDAR

III. PROPOSED WORK

SC-LARDAR is extension of LARDAR protocol where route discovery process original route discovery process followed by an authentication phase When a source node desires to transfer data to a destination node, it first broadcasts a RREQ to next 1-hop neighbours and sets a minimum time delay to receive the RREP. The destination node or one hop neighbour node that has minimum angle and valid route to the destination replies to the RREQ. In

this case if the source node receives RREP immediately without any time delay, then the source suspects the RREP initiator to be black hole node. If RREP comes after the time delay then the node is consider as legitimate node. Then source node provides SCC to that 1- hop neighbour.

The node which consists of minimum Θ' will be selected as it forms an optimal route to the destination. So, the source node provides SCC to only that 1- hop neighbour node which is having minimum Θ' value. All intermediate nodes perform the same procedure until the final destination is reached. Then the destination node sends authenticated messages appended with certificates taken from the corresponding node's repository. When source node receives the packet, it checks the whole certificate chain. If the route is protected source node starts sending data packets through this route and in case of a legitimate node turning malicious over a period of time, the node's behaviour would be recorded and once recorded the certificate would not be renewed after its expiry time, thus isolating the node from further participation in the network activities. So due to this only legitimate node will be left in the network because malicious node would not be able to produce the certificates to be appended with the RREP message.

A. *Digital Signature*

A digital signature is an electronic scheme that can be used to authenticate the identity of the sender [7]. In this there is a trusted certificate which is PKI (Public Key Infrastructure) authenticated by a chain of nodes. The mobile nodes can directly issue certificates to nodes that are in radio range of each other. A certificate is a binding between a node, its public key and the security certificate is issued on the basis of security parameters of the node. Every node in the network authenticates its neighbours by issuing certificate and generate public key. The certificates are stored in the local repository of issuer node and to the node to which certificate is issued. Exchange of certificates between neighbouring nodes takes place periodically. Local exchange of certificates in one hop leads to low communication cost. If different nodes have same public key or the certificates are conflicting, it is possible that a malicious node has issued a false certificate. If certificates issued by any node are found to be incorrect, then that node may be assumed to be malicious.

Example:

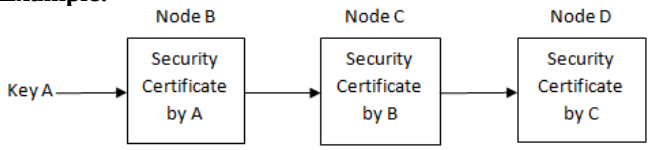

Fig 3: Certficate Chaining

Let node B is within the radio range of node A, node A issues a certificate to B.

SCC (A→ B) = {IDB, KB, t, ET, S} KA

The certificate contains the identity of node B, the public key of B generated by applying one way hash function to IP address or MAC address of the node B , the time at which certificate is issued, time after which certificate will be expire and security level of the node, signed by the public key of A.

The public key is calculated by applying a one way hash function H, to the identity of the node. The identity may be either IP address or MAC address.

KB = H (IDB)

Initially the security level S value is set to 1 means issuer node is convinced of the security parameters of the subject node and if S value is reduced to 0 then security is found to be compromised, node bearing a certificate is set aside as malicious node. When the ET value expires every security certificate becomes invalid. However if the certificate is still required, it has to updated by the issuer again by checking the security parameters.

B. *Authentication*

The authentication phase is followed by certification phase. When source node A wants to find a route to destination D for data transfer, it broadcasts a RREQ to its next hop neighbours. The destination node or any other node that has a valid route to the destination now replies to the RREQ. Any malicious node may reply to the request before the set delay time.

RREQ would be of the form:

[S_ID, SrcLoc, D_ID, NHN_ID, TTL, Θ]

Example

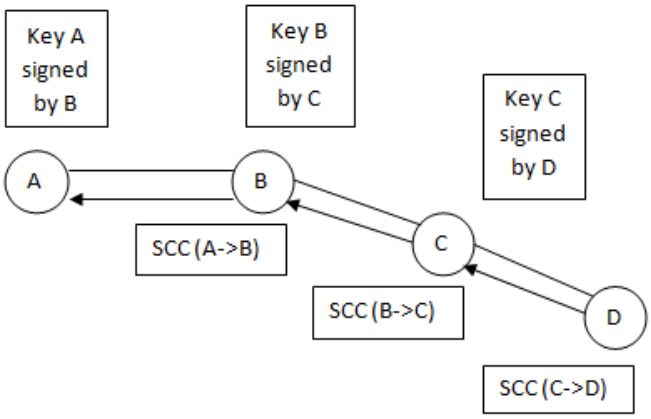

Fig 4: Certified Route from Souce to Destination

To conquer this black hole attack, source node initiate data transfer after receiving authenticated RREP from the destination. The destination node sends authenticated

messages appended with certificates taken from the corresponding node's repository.
Authenticated RREP would be of the form [S_ID, Θ', NHN_ID, SCC]

The RREP from valid node C would be
[C, A, SCC (B→ C)]
When RREP reaches node B, it checks its routing cache to see if SCC (B→ C) is there. It checks whether C is malicious node or not by checking the SCC (Security Certificate Chain) issued list. If C is a promiscuous node then B also forward the RREP to A append with SCC (A→ B).

The Forwarded RREP will be in the Form of
{C, A, A, SCC (A→ B), SCC (B→ C)]

All 1 hop neighbours at every step perform the same procedure until the A is reached. When node A receives the RREP, it checks the whole certificate chain. If there is no problem with the certificate chain, node A trusts the route and starts sending data packets through this route. On the other hand, if the issuing node feels that the subject node is compromised, it will not provide the certificate update. If the S value of the certificate is not to the satisfactory level that means the certificate is no longer a valid certificate, the S is reduced to zero then certificate issued to the node will be revoked otherwise if the node is valid node then the value of S is 1.

C. Route Recovery

If a route failure is detected by the node while moving towards the destination, it must recover the route immediately. There are some alternatives of route recovery which helps in identifying the broken route. The first alternative is the broken node sends a packet in the form of route error to inform the source node that a route failure has occurred. After receiving a route error packet, the source node re-initiates a route discovery procedure to search a new path. Another alternative is to initiate a route discovery process by the broken node, called local search, to repair the broken path. This local search method reduces the overhead of route recovery as well as the latency of the route rediscovery. While the local search failed, it does route recovery by the first alternative.

IV. ALGORITHM

Parameters
Source id-=S_ID
Source location= SL
Destination id= D_ID
Time to live= TTL
Next hop node id=NHN_ID
Delay time=DT

Route Request (RREQ) = {S_ID, SL, D_ID, NHN_ID, TTL, Θ, SCC)
Route Reply (RREP) = {S_ID, Θ', DT}

Step 1:
Create expected zone using,
$v(t_1 - t_0)$
Now, create request zone using Fig 2,
Area of TRIANGULAR ZONE, $A_{\Delta SEG} = (d + r)^2 \tan \alpha$
Area of RECTANGLE,
$A_{\square SABC} = (x_2 - x_1 + r)(y_2 - y_1 + r)$

Reduced request zone ratio, R= 1-$(A_{\Delta SEG} / A_{\square SABC})$

$$=1-\frac{(\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}+r)^2 \tan \alpha}{(x_2-x_1+r)(y_2-y_1+r)}$$

Where,$\alpha = \sin^{-1}(\frac{r}{d})$, r=$v(t_1 - t_0)$

Step 2:
Set Delay time. S=0.
SN broadcast RREQ to 1-hop neighbour If (1 hop is DN) THEN
DN return RREP
SN transfer packet to DN Else if
1-hop returns RREP with Θ'
If RREP of any node is immediate. Do not issue security certificate. Else
Choose node with minimum Θ' and then
Certify chosen node with SCC
Request id and security parameters of NHN
Generate public key of NHN based on id Issue Certificates encrypted with public key
Store certificates in route cache
Exchange Certificates with neighbour nodes Process continues till DN is reached

Step 3:
DN sends certified RREP appended with security certificate from NHN
All INs append their certificates forward the certified RREP
RREP reaches SN
SN verifies certificate chain and routes data packets through the secure path.

V. SIMULATION

We have developed simulation for our routing protocol SC-LARDAR. Here, we tried to compare the performance of SC-LARDAR with LARDAR that was implemented by Tzay-Farn Shih, Hsu- Chun Yen. The implementation of LARDAR followed the specification proposed in [6]. The

packet delivery ratio, routing overhead and throughput for different network size is investigated by simulation.

In our simulation, all network nodes were located in a physical area of size 900 × 700 m to simulate actual mobile ad hoc networks. The network sizes were generated according to a uniform distribution. A node selects next hop node which is secure and having minimum angle w.r.t baseline, and then it moves in the direction of the destination in a uniform speed and it reaches its destination, the node stays there for a specified pause time period.

In this model, a node selects only one hop neighbour node and moves towards that destination at a speed between the pre-defined maximum and minimum speed. The minimum speed for the simulations is 0m/s while the maximum speed is 50m/s. The radio bandwidth of each mobile node was 2 Mbps. The simulation time is 200sec. The malicious nodes are selected randomly.

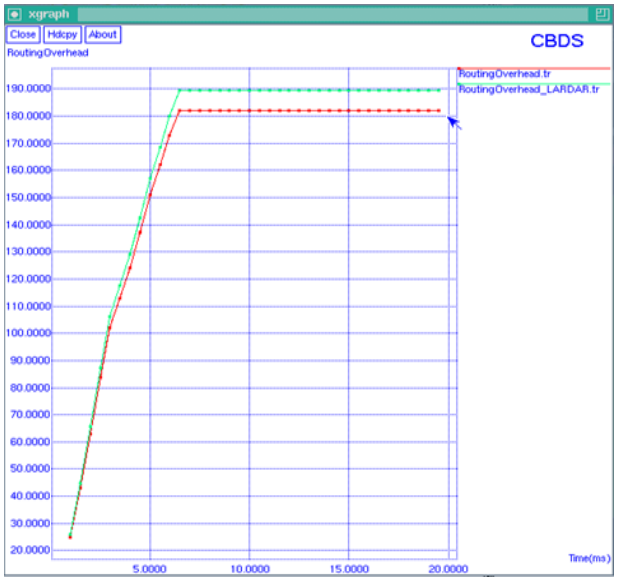

Fig 5: Packet Delivery Ratio

The packet delivery ratio of SC-LARDAR and LARDAR is illustrated in Figure 5. In this figure, we can find that the packet delivery rate of SC-LARDAR is slightly higher than LARDAR (as red line shows SC-LARDAR and green shows LARDAR). The packet delivery ratio of SC-LARDAR and LARDAR is decreased with the increase of network size for the increase collision.

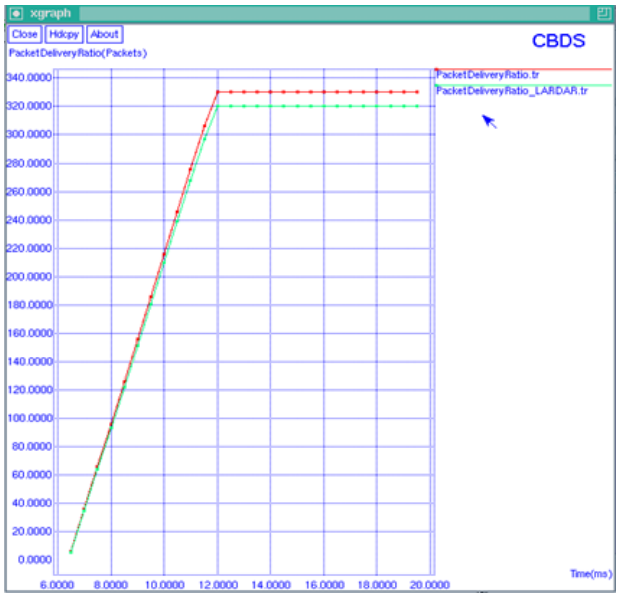

Fig 6: Routing Overhead

Figure 6 show the distribution of routing overhead for different network size. The routing overhead was calculated as the total number of control packets transmitted in the route discovery procedure. The control packets included the route request packet and route reply packet for SC-LARADR and LARDAR. The number of control packets of both routing protocols increased when the network size enlarged. With a higher number of nodes, the density of node within the request zone increased, so the routing overhead also increased. The simulation result shows that SC-LARDAR always had a lower routing overhead than LARDAR. Because LARDAR defines a request zone in which all nodes will be considered for data delivery of packet from source to destination rather in SC-LARDAR a secure path is created from source to destination which induces a lower routing overhead.

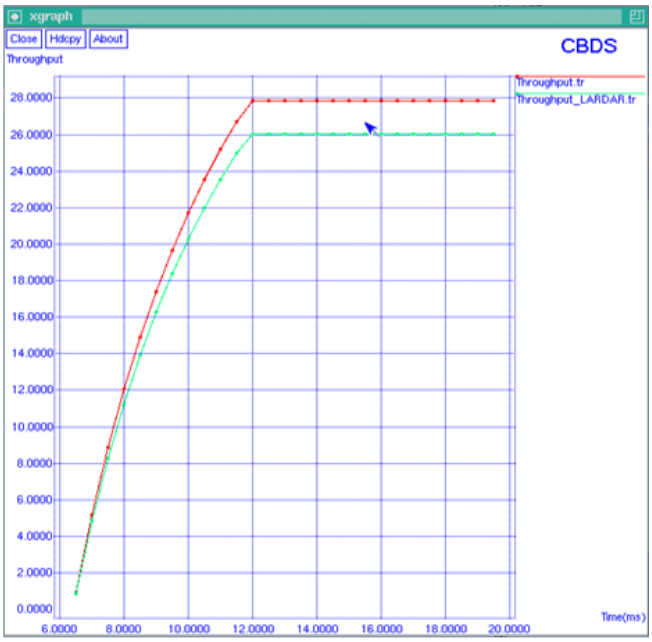

Fig 7:Throughput

The throughput is defined as the total amount of data received by the receiver from the sender divided by the time it takes for the receiver to get the last packet. The throughput is measured in bits per second (bit/s or bps). Here, simulation results show that SC-LARDAR shows higher throughput than LARDAR. As an explanation of good throughput in SC-LARDAR is that which uses limited bandwidth and limited energy.

VI. CONCLUSION

We use location information of mobile nodes to confine the route searching space into smaller range. This paper has presented the SC-LARDAR, a new ad-hoc routing protocol that provides security against black hole attack that occurs in MANETs. This proposed protocol is an efficient routing scheme that provides efficiency and security to LARDAR protocol. SC LARDAR dynamically discovers the route between nodes only as needed; the design is based on the basic operation of the LARDAR protocol. The proposed protocol can be used to find secured route to transmit data packet in request zone based on minimum angle Θ. This will help in reduction in flooding of RREQ packet and in turn helpful in reduction of bandwidth consumption.

In future, we intend to increase the end to end delay in our network. This proposed mechanism can also be applied for securing the network from other routing attacks by just changing the parameters in accordance with the nature of attacks.

REFERENCES

[1] S. Gangwar, K. Kumar, "Mobile Ad hoc Networks: A detailed survey of QoS Routing Protocols", Vol. 2, International Journal of Distributed and Parallel Systems, 2011.

[2] Dr. P.K. Suri, Dr. M.K. Soni, Parul Tomar, "Routing in Mobile Ad hoc Network: A Review", International Journal of Advances in Computing and Information Technology, 2012.

[3] Naveen Bilandi, Lokesh Sachdeva, Aakash Setia, Suresh Kumar, "Performance Analysis of Proactive and Reactive Routing Protocols In MANET", International Journal of Advanced Research in Computer Science and Software Engineering, May 2012.

[4] Atekeh Maghsoudlou, Marc St-Hilaire, Thomas Kunz, "A Survey on Geographic Routing Protocols for Mobile Ad hoc Networks", Carleton University, Systems and Computer Engineering, Technical Report SCE-11-03, October 2011.

[5] Young-Bae Ko, Nitin H. Vaidya, "Location Aided Routing (LAR) in Mobile Ad-Hoc Networks", International Journal of Computer Network and Communication, 2000.

[6] Tzay-Farn Shih, Hsu-Chun Yen, "Location-aware Routing Protocol with Dynamic Adaptation of Request Zone for Mobile Ad Hoc Networks", Wireless Network, 2008.

[7] Sachin Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", International Journal of Multidisciplinary and Current Research, Vol. 2, January 2010.

[8] K. Selvavinayaki, K. K. Shyam Shankar, Dr. E. Karthikeyan, "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs", International Journal of Computer Applications, 2010.

[9] Karim El Defrawy, Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", International Conference on Local Computer Network, IEEE, September 2011.

[10] Karim El Defrawy, Gene Tsudik, "PRISM: Privacy-Friendly Routing In Suspicious MANETs", IEEE International Conference, ICNP, 2008.

[11] Haiying Shen, Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", Transactions On Mobile Computing, IEEE, Vol. 12, June 2013.

[12] Fan-Hsun Tseng, Li-Der Chou, Han-Chieh Chao, "A Survey of Black Hole Attacks in Wireless Mobile Ad hoc Networks", Human Centric Computing And Information Sciences, 2011.

[13] E. A. Mary Anita, V. Vasudevan, "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining", International Journal of Computer Applications, 2011.