Secure Approach for Location Aided Routing in Mobile Ad Hoc Network

Anamika
Inderprastha Engineering College
Assistant Professor
Computer Science Department

Kalpana Tyagi
Inderprastha Engineering College
M.Tech
Computer Science Engineering

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 and no centralized control. Due to self-configuring and dynamic nature of these networks routing protocol are susceptible to various types of 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 actually does not exist in the network. 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 Θ is kept on route request packet to select optimal path for secure transmission of data packets.

Keywords
MANETs, Black hole attack, Location based communication, Security certificate.

1. INTRODUCTION
The recent advances in computer networking have introduced one of the most valuable wireless technologies for communication, a mobile ad hoc network (MANETs) [1]. Increase in availability and popularity of mobile devices led researchers to extend Mobile Ad-hoc NET working (MANETs) protocols to take advantage of the communication opportunities offered by these devices. MANETs is a distributed system with a collection of dynamic wireless mobile nodes with each of these nodes having their movement throughout the network. The communication between these nodes is via the wireless links by directly or intermediate nodes in a peer-to-peer fashion. Therefore, the success of MANETs communication highly relies on the collaboration of the involved mobile nodes.

The communication takes place in open medium making the MANETs more vulnerable to security attacks [6]. We can use security protocols to reduce the vulnerabilities from various attacks. 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 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 [7, 11, 12]. In such attack a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This hostile node advertises its availability of fresh routes 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 will focus on the basic operation of Location Aided Routing protocol. Subsequently we will analyse how Black hole attack occurs in LARDAR routing protocol and various methods that have proposed to detect and prevent Black hole attack in LARDAR.

2. 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 beaconing to identify presence of neighbors 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 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 mobile nodes maintain path information for destinations only when they need to contact the source node or relay packets. Reactive routing protocols use periodic beaconing to identify presence of neighbors 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 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 [3]. 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.

Many protocols like are anonymous Routing Protocol for mobile ad hoc networks(ALARM) [8], Preserving Location-Based On-Demand Routing in MANETs(PRISM) [9], ALERT have been proposed that are based on LAR and provides security [10]. In this paper, security work is extended for LARDAR Protocol since the request zone is smaller for LARDAR which helps in minimizing power and bandwidth consumption and reduce flooding.

2.1 LARDAR Protocol

2.1.1Expected 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 [4].

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) centered at location L.

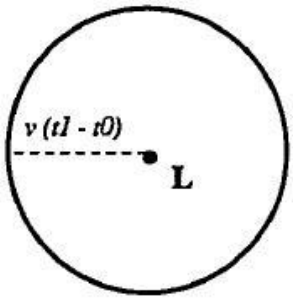

Figure 1: Expected Zone

2.1.2 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 [5] source node tries to minimize the request zone by confining it to the smallest rectangular area containing both sender as well as receiver.

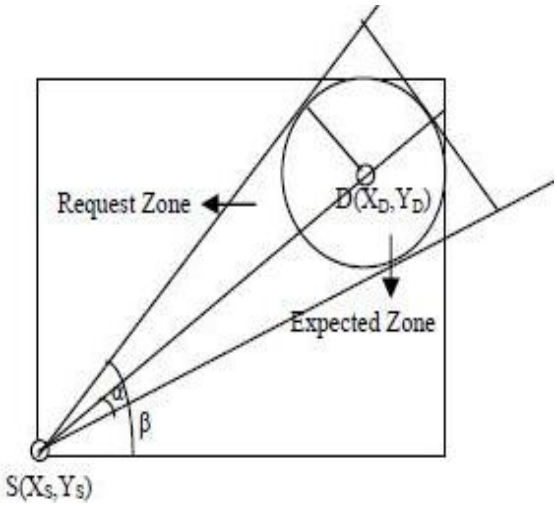

Figure 2: Request Zone in LARDAR

3. 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 neighbors and sets a minimum time delay to receive the RREP. The destination node or one hop neighbor node that have 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 SSC to that 1- hop neighbor.

The node which consists of minimum Θ' will be selected as it forms an optimal route to the destination. So the source node provides SSC to only that 1- hop neighbor node which consists of minimum Θ'. 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 behavior 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.

3.1 Digital Signature

A digital signature is an electronic scheme that can be used to authenticate the identity of the sender of a message [7]. In this there is a trusted certificate which is PKI 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 neighbors by issuing certificate and generate public key. The Certificates are stored in the local repository

of issuer node and to the node that it is issued. Exchange of

Certificates between neighboring 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.

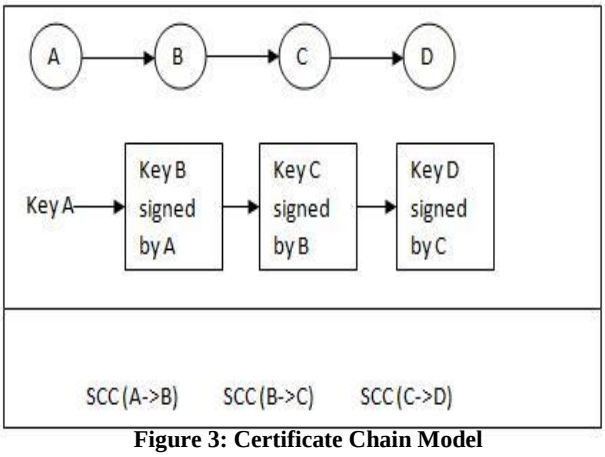

Figure 3: Certificate Chain Model

Example:

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

SC (A→ B) = {IDB, KB, t, ET, S} K_A

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 time delay S value is set to 1 means issuer node is convinced of the security parameters of the subject node and if S=0 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.

3.2 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 the next hop neighbors. 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 from the source by claiming to have the shortest path to the destination.

RREQ would be of the form:

[S_ID, SrcLoc, D_ID, NHN_ID, TTL, Θ]

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]

Example

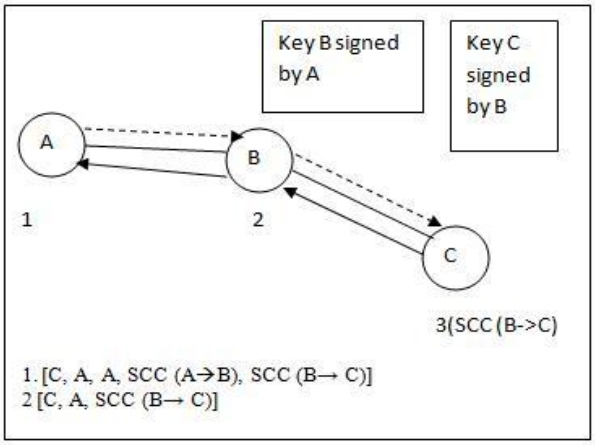

Figure 4: Certified Route from Source to Destination

The RREP from 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 where C is malicious nodes are not by checking the SCC (security certificate chain) issued list. If C is a promiscuous node then it forward the RREP to A by append the SCC (A→ B).

The Forwarded RREP will be in the Form of

{C, A, A, SCC (A→ B), SCC (B→ C)]

All 1 hop neighbors 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 Sv value of the Certificate is not to the satisfactory level that means the certificate is no longer a valid certificate, the Sv is reduced to zero then certificate issued to the node will be revoked otherwise if the node is valid node then the value of Sv is 1.

4. 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, SSC)
Route Reply (RREP) = {S_ID, Θ', DT}
Step 1:
Create expected zone using,

$v(t_1 - t_0)$

Now, create request zone using, Area of TRIANGULAR ZONE, $A_{\Delta ABC} = (d + r)^2 tan\alpha$

Area of RECTANGLE,

$A_{\blacksquare SABC} = (x_d - x_s + r)(y_d - y_s + r)$

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

$$= 1- \frac{(\sqrt{(x_d - x_s)^2 + (y_d - y_s)^2} + r)^2 \tan\alpha}{(x_d - x_s + r)(y_d - y_s + r)}$$

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

Step 2:
Set Delay time. Sv=0.

SN broadcast RREQ to 1-hop neighbor 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' Certify chosen node with SSC

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 neighbor nodes Process continues till DN is reached

Step 3:
DN sends certified RREP appended with security certificate from NHN

All INs append their certificates and forward the certified RREP

RREP reaches SN

SN verifies certificate chain and routes data packets through the secure path.

5. CONCLUSION

This paper has presented the SC-LARDAR, a new ad-hoc routing protocol that provides security against black hole attack that occurs in MANETs. 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 in a request zone based on minimum angle Θ. This limitation will help in reduction in flooding of RREQ packet and in turn helpful in reduction of power and bandwidth consumption. As future work, we intend to develop simulations to analyze the performance of the proposed solution based on the security parameters like packet delivery ratio, memory usage and scope of the black hole nodes.

6. 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] 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.

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

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

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

[7] 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.

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

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

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

[11] 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.

[12] 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.