A reactive protocol for privacy preserving using location based Routing in MANETs

[1]Namrata Marium Chacko, [2]Getzi P. Leelaipushpam

[1, 2]Department of Information Technology, Karunya University
Coimbatore, Tamil Nadu, India

Abstract

Mobile Ad hoc networks (MANETs) are an infrastructure less, self configuring network. These networks can be setup easily anywhere and anytime without any base infrastructure, thus they have proved to be very efficient is rescue related areas like flood and fire. MANETs are now extended to be used in military and law enforcement. MANETs still face the major problem of security and privacy, especially when used in sensitive areas of computing. Secure routing protocols have been developed to provide various levels of security and privacy in the past. This paper presents a Routing scheme based on Location Aided Routing schemes to improve routing facilities along with some enhanced signature schemes to provide privacy and security of data. We prove it by simulation in ns2.

Keywords: *MANETs, Secure routing, Location aided routing, Black hole Attack, Privacy.*

1. Introduction

When MANETs[11] are being used in areas of critical importance such as military operations, rescue operations, law enforcement; privacy and security becomes a major issue. The attacks on MANETs can be broadly divided into four categories Active outsiders, passive outsiders, active insiders and Passive insiders. Thwarting these attackers can be a challenge

.

A. Adversary Model

Attacks can be from Insiders or outsiders.

Outsider attacks: The use of Location routing and group signature scheme keeps attacks from an outsider at the bay. What one should be concerned is of the compromised insider

.

Insider attacks: Nodes can sometimes get compromised and even though they are within the group they may cause problems and leak information to adversary. Insider attacks can be broadly classified into **active insider and passive insider,** a passive insider will only eavesdrop and make no fraudulent movements therefore it is difficult to detect such nodes in a network. The **active insider** poses a great threat to the network as the node has access to most of the traffic in the network and a malicious node can easily leak information to an outsider if working in a cooperative attack.

In our work we concentrate on three types of attacks that can be carried out by the active insider, namely

Blackhole attack: In this type of attack and active insider can lie about having a fresh route to the destination and thus attracting all the packets to itself. Once it receives the packets it simple discards them without forwarding to the destination. This attack results in huge loss of data.

Man-in-The-Middle Attack: The malicious node will remove the keys of a RREQ and add its own keys. It will reply to the sender node as if it is the destination, and then it will generate a new RREQ and forward to the intended destination with its own session key. The MiTM attack can go undetected and the malicious node can easily get hold of information being passed. In this

Location Based attacks: Since we are using Location based routing the possibilities of location based attacks increases. Attacks on location can be further classified as *Distance Fraud, Mafia fraud, Terrorist Fraud* and *Distance Hijacking Attack* [2].

Distance Fraud: In this attack an attacker lies about his actual location, thus attracting traffic to itself.

Mafia Fraud: The attacker tries to modify the distance, by interfering with the communication of different nodes.

Terrorist fraud: This attack involves more than one malicious node. Multiple nodes cooperate to lie about the location of one particular node.

*Distance hijacking attack: t*his is a form of masquerade attack, where in the attacker uses another honest node and deceives the verifier about its location. The attacker waits till all security communications are over and then takes over the communication.

Generally there remains a trade-off between efficiency and security/privacy features. And still the possibility of an active insider attack remains high. Detection of the presence of a malicious insider node will help a great deal to reduce the possibility of loss of important data. Many techniques have been suggested to detect the presence of malicious nodes in the past; in our work we adopt the Round Trip Time technique to detect the presence of malicious nodes.

Organization: The paper is organised as follows. In section II describes the related works, section III the goals and some key features are discussed. Simulation results, future enhancement and Conclusion are in section IV and V respectively.

2. Related Works

There are a numerous protocols addressing the issue of routing in MANETs, routing becomes a challenge as the nodes are mobile, thus resulting in loss of packets, delay and inefficient communication. Also the problem of insecure wireless links poses a threat to communication in MANETs. As mention in section I, there are various possible attacks on MANETs. In this section we discuss the protocols and their features.

The more commonly know protocols such as AODV [14], DSR [3], were proposed to provided more efficient routing in a wireless environment. AODV is a reactive protocol, which facilitate nodes to find links to each other only when there is a need to communicate. DSR works on similar lines of AODV, with the exception that it saves the link information even after communication is terminated. Both the protocols have proved to be a huge success in adapting communication in wireless nodes, but both lack security features to avoid attackers. Various protocols have been suggested to provide security. To overcome this problem of lack of security features, many protocols have been proposed.

Some protocols which provide security features by introducing encryption algorithms and key exchange algorithms, protocols are anonymous Routing Protocol for mobile ad hoc networks (ARM) [4], Secure Position Aided Ad hoc Routing (SPAAR)[1] and On-Demand Anonymous Routing in Ad Hoc networks (ODAR) [6].The ARM protocol proposed by Stefaan Seys and Bart Preneel in [4], aims at overcoming the draw backs mentioned above. The RREQ message is formed such that only the destination can recognize that this RREQ was targeted at it, all other nodes can only verify that it was not targeted at them. The source S and destination D shared a secret key k_{SD} and D has a current pseudonym which only D can recognise. The cryptographic operations are simple and done only by the source and destination node. ARM depends on various assumptions which may not be plausible in a real-time environment, some of the assumptions are, that every node has a permanent ID know by all other node, Source and destination share a secret key and a secret pseudonym and that links between nodes are symmetric.

Secure position Aided Routing [1], implements routing based on location of the nodes in the network. In the route request along with the destination ID also the distance from the source node and the exact coordinates are included, all the information is encrypted with a group encryption key. The receiving node attempts to decrypt, successful nodes indicate that sending node is a one hop neighbour. The route reply contains the RREQ sequence number, destination’s coordinates, velocity, and a timestamp, all encrypted with public key. Fabricated routing messages cannot be injected into the network by malicious nodes, routing messages cannot be altered in transit and routing loops are not formed. SPAAR suffers from a lot of overhead need to encrypt and decrypt at each and every node. It also needs an online server to provide nodes with certificate.

On-Demand Anonymous Routing [6] (ODAR) makes use of bloom filters to achieve strong anonymity against attacks such as address spoofing and route forgery, by concealing the true identity of the traffic. Elements once added to a bloom filter cannot be removed. ODAR initially finds the source route using DSR algorithm. The source hashes the entire route information and puts it into the bloom filter; which is then attached to the packet and forwarded. This algorithm provides three levels of anonymity, node identity is kept anonymous, route details are also anonymous and topology information is also not revealed. When using bloom filters, the possibility of false positives leads to unnecessary packet forwarding. Nodes on the source path can inject packets into the network.

All of the above mention protocols provide security. Besides security; privacy is also an important issue that needs equal attention. Privacy not only refers to confidentiality of the information being passed but also is the property of nodes to remain undetectable by adversaries. Protocols using location centric routing like location aided Routing protocol (LAR) [16], Privacy-

Preserving Location-Based On-Demand Routing in Manets (PRISM)[7], and Anonymous Location-Aided Routing in Suspicious Manets(ALARM) [12], are examples of privacy preserving protocols.

PRISM Protocol

PRISM protocol as suggested by Karim El Defrawy and Gene Tsudik in [7] implements security and privacy, making it an apt protocol to be used in military based applications. To preserve privacy this protocol suggested the use of Location bases routing along with Group signatures and each node possessing a private/public keys. A source node will initiate a route discovery phase when it has data to transmit.

Based on the concept of location aided routing it located the destination, encrypts he packet, insert the source group signature and send the packet. Receiving packets can verify the group signature and destination is identified with the coordinates. The Route reply consists of a session key which will be used for further communication for that particular session. Routes are discarded after communication. This protocol achieves privacy and security against active as well as passive attacks. As the nodes identity is not revealed and the destination node location is encrypted by key known only to valid group members.

3. Goals and Features

Our work is an extension to the PRISM protocol. This section we present some of the assumptions taken into consideration and Goals and features. Before we start explaining the working of our protocol, we present some assumptions. All nodes have prior knowledge of the time needed for Processing and network Delay. Each node is equipped with GPS device and can accurately determine the coordinates of a node. Nodes have capability of carrying out simple mathematical operations and generation of prime numbers.

3.1 Goals

Enlisted below are the main goals of our work

(1) *Security and privacy:* Avoid any kind of information leakage to malicious nodes
(2) *Efficiency*: to achieve Security and privacy without compromising other factors.
(3) *Intrusion detection:* To detect the presence of malicious nodes.

3.2 GPS Based routing

Location added routing [16] refers to the use of location information for routing rather than IP addresses. With the help of GPS, one can obtain the coordinates of a particular node and thus route only in a particular direction. In doing so, the traffic in the network is reduced. This also prevents quite a few numbers of attacks which are based on IP spoofing and masquerading, since no permanent ID are revealed in the packets. An enhancement to LAR routing is GeoAODV routing, where in the authors of [15] suggests a method to reduce the amount of packet flood into the network. According to this method each intermediate node will calculate a flooding angle and determine if it falls into the search area then only will it forward. The flooding angle is calculated as follows:

$$\emptyset = \cos -1 \left(\frac{\overrightarrow{SD}.\overrightarrow{SN}}{|SD| * |SN|} \right) \qquad (1)$$

Where, $\overrightarrow{SD}$ is a vector between source and destination, $\overrightarrow{SN}$ is a vector between source and intermediate node N, while $|SD|$ and $|SN|$ are absolute values of vectors $\overrightarrow{SD}$ and$\overrightarrow{SN}$, respectively. Our work adopts this technique to make routing more efficient by reducing the number of packets flood into the network.

3.3 Round Trip Time (RTT)

Round trip time is defined as the interval between the sending of a packet and the receipt of its acknowledgement in [13]. It includes network propagation delay and the sender and receiver processing times. The RTT is use by many protocols to send the timeout value for retransmission of packet if the packet is not acknowledged. In our work we propose using the RTT as a threshold to detect the presence of malicious nodes, explained in section III.

3.4 Group signature

Group signature is scheme was first introduced by Chaum and Van Hejst in [5] as a public key signature with additional privacy features. This scheme is used for large and dynamic groups to sign a valid message. The components include a group manager who is responsible for distributing the private and public keys. Each node has a secret long term identity which is mapped to its private key and only the group manager knows the relation.

The protocol we propose has the same basic working as PRISM protocol. We try to reduce routing overhead by introducing GPS based routing and also detect the presence of malicious nodes which lie about their location by calculating the Round Trip Time (RRT).

4. Proposed Work

The basic working of the paper is similar to that of PRISM protocol.

(1) All nodes acquire public and private keys base on the Group signature scheme [reference paper] from the group manager

(2) When a node decides to communicate, it first locates the destinations coordinates, using LAR scheme it will calculate the approximate Radius and the flood angle of the destination node. The source then creates a Route request message (RREQ), and broad casts it in the calculated direction only. The RREQ contains the destination location (DST-AREA) along with the flood angle (ϕ), a temporary public key (PK_{TMP}), a time-stamp (TS_{SRC}) and a group signature ($GSIG_{SRC}$), $GSIG_{SR}$. Fig. 1 shows the RREQ packet format with various fields.

Message-type=RREP
H(RREQ)
$E_{PKTMP}(K_S)$
$E_{(Ks)}$ (DST_{LOC})
$GSIG_{DST}$

Figure1: RREQ Packet Format

(3) Once the packet is forwarded the node starts a timer "T". This timer is used as a threshold for determining the time taken by the reply message. Based on this the source node can determine if the reply contains a valid Destination location.

(4) Upon receiving a RREQ, each node will first verify the time stamp. Then it will determine if it has processed the RREQ previously. If not, then the node uses its coordinates and the flooding angle to determine if it belongs to the search region.

(A) If not, the intermediate node keeps a hashed copy and re-broadcasts the RREQ. Without modifying any fields of the RREQ packet.

(B) If the node is within the search region, it verifies $GSIG_{SRC}$. If invalid, the RREQ is discarded. Else, it stores the entire RREQ (including GSIGSRC).

(5) When the destination receives the RREQ, it composes a route reply (RREP) which contains: h(RREQ), a new random session key KS and (3) the exact destination location. Both (2) and (3) are encrypted under PKTMP obtained from the RREQ. The RREP also includes the group signature – GSIGDST of all fields. The packet format of RREP is shown in fig 2.

Message-type=RREQ
DST-AREA + flood angle (ϕ)
PK_{TMP}
TS_{SRC}
$GSIG_{SRC}$

Figure 2: RREP Packet Format

(6) The RREP is forwarded on the revers route, by intermediate nodes, each node stores a h(RREQ),h(RREP)and timestamp of entry creation.

(7) When the RREP is received, the source first verifies the group signature. If invalid, the RREP is discarded. Next, the source calculates the RTT based on the coordinates provided in the RREQ, as follows

DISTANCE D$= \sqrt{(Sy - Sx)^2 - (Dy - Dx)^2}$

RTT=2(D/SPEED)

Total time needed TT= RTT + Processing time + Network delay

Now the source node can compare the timer from the timer "T", started in step (3) and the calculated "Total tine needed ". If there is a huge difference then the packet is dropped and alert for a malicious node can be signalled.

(8) This completes the route setup process. Once the route is established, each source-destination data message specifies the tuple<h (RREQ), h(RREP)> as a unique route identifier. In the opposite direction, <h(RREP), h(RREQ)>is used as a route identifier. If the route breaks, a route error (RERR) message similar to that in AODV is generated

4. Simulation and Results

The proposed protocol was implemented in NS2.34, a discrete event simulator. The results of the simulation were plotted graphically and these will be explained in this section. We study the effect of the protocol on network Throughput, end to end delay, jitter, packet delivery ration and we also compare the number of nodes relieved using OLSR protocol to that of our proposed protocol. We have used CBR traffic pattern and the parameters are given in Table I.

Table I: Simulation Parameters

Sr. No	Parameter	Value
1	Routing Protocol	AODVand PRISM
2	MAC Layer	802.11
3	Terrain Size	1000x1000
4	Nodes	150
5	Node Placement	Random
6	Mobility Model	Random Way point
7	Data Traffic	CBR
8	Simulation Time	600 seconds
9	Pause Time	10

We now present the graphical presentation of the results. Figure 3, show below, depicts the end-to-end Delay for the proposed protocol and the existing AODV protocol. End to end delay is the time taken for a packet to be transmitted across the network from source to destination. the end to end delay include the transmission delay, propagation delay and the processing delay From the graph it can be observed that there is a decrease in the delay for the proposed protocol. The use of location aided routing helps to direct the traffic towards the source and thus reduce the delay in the network.

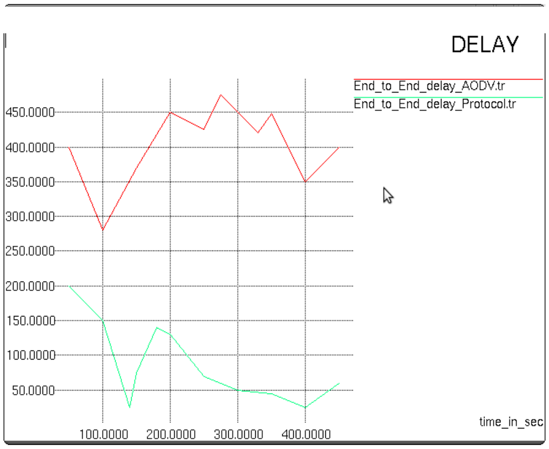

Figure 3. Average End-to-End Delay for the protocol

The protocol has proven to be efficient by reducing the delay in the network and the jitter. When the packets are routed directly to the DIST-AREA, the number of packets in the network reduces, thus decreasing the number of packets in the network and thus increasing the rate of successful packet delivery. At the same time the network throughput is also increased. Figure 4, depicts the throughput of the proposed protocol in comparison to AODV protocol.

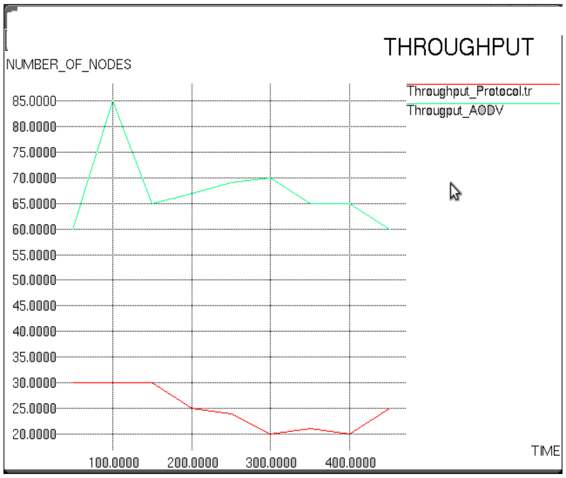

Figure 4. Graph for Throughput

Figure 5 shows a graph in which the number of nodes whose location is revealed using the Location aided routing as compared to the AODV protocol. Hence can be concluded that privacy of nodes are preserved to a certain extend. The number of location revealed using AODV is higher as the number of route request increases. But in the case of the proposed protocol the number of nodes location revealed is lesser.

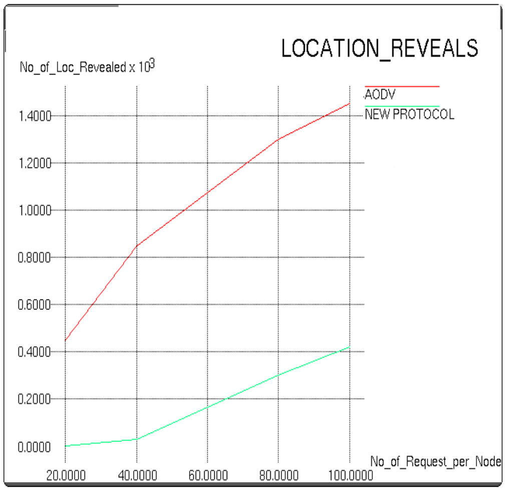

Figure 5. Location revealed.

As can be deduced from the above simulation results that the proposed protocol is sufficiently secure and provides privacy. The use of location information and simple encryption scheme, within the group keeps the nodes location and information safe from possible outsider attcks.One should be worried about passive insiders. The security is preserved by using the Session key between the source and destination, thus the passive insider cannot access the information.

The use of Round trip time, detects the presence of a lying node and also possible presence of malicious nodes. Since the RTT is calculated with nearly accurate precision the presence of an attacker can be detected as soon as possible.

5. Conclusion and future work

Use of MANETs in mission critical applications calls for more secure and efficient routing of packets. With the use of simple cryptographic techniques strong enough security can be provided against intrusive attackers. But a major challenge that persisted is the need privacy against insider nodes. There have been many protocols proposed to preserve the privacy of a node in the network like PRISM, ALARM. Our proposed protocol, preserves privacy of nodes and also detects the presence of malicious nodes.

This proposed system is an intrusion detection system. Only detection is done in this paper, for future work detection and prevention can be done. One can consider detection and prevention of man in the middle, cooperative black hole attack and all kinds of location fraud.

References

[1] S. Carter and A. Yasinsac, “Secure position aided ad hoc routing,” Proc. IASTED International Conference on Communications and Computer Networks (CCN02), pp. 329–334, 2002.

[2] Cremers,C. ;Rasmussen,K.B. ; Schmidt,B. ; Capkun,S, “Distance Hijacking Attacks on Distance Bounding Protocols” 2012 IEEE Symposium on Security and Privacy (SP), pp. 113 – 127.

[3] http://tools.ietf.org/html/rfc4728

[4] S. Seys and B. Preneel, “Arm: anonymous routing protocol for mobile ad hoc networks,” Int. J. Wire. Mob. Comput., vol. 3, no. 3, pp. 145–155, 2009.

[5] D. Chaum and E. V. Hejst, “Group signatures,” EUROCRYPT,1991.

[6] R. Chen, and L. Bao, “Odar: On-demand anonymous routing in ad hoc networks,” Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on, pp. 267–276, Oct. 2006.

[7] Karim El Defrawy and Gene Tsudik, “Privacy-Preserving Location-Based On-Demand Routing in MANETs” IEEE journal on selected areas in communications, vol. 29, no. 10, december 2011

[8] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” in Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 90–100.

[9] “RCF2501-Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, http://www.faqs.org/rfcs/rfc2501.html

[10] Jun-Zhao Sun,”Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing”

[11] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[12] K. El Defrawy and G. Tsudik, “Alarm: Anonymous location-aided routing in suspicious manets,” IEEE ICNP 2007, pp. 304–313, Oct. 2007

[13] http://en.wikipedia.org/wiki/Round-trip_delay_time

[14] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” in Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 90–100.

[15] H. Asenov, and V. Hnatyshin, "GPS-Enhanced AODV routing," in Proceedings of the 2009 International Conference on Wireless Networks.

[16] (ICWN'09), Las Vegas, Nevada, USA (July 13-16, 2009) Young-Bae Ko and Nitin H. Vaidya, “Location-Aided Routing (LAR) in mobile ad hoc networks” Wireless Networks, vol. 6, pp. 307–321 307, 2000.

First Author Namrata Marium Chacko has completed her B.E degree in Computer science in the year 2011 and is currently perusing the Master Degree in the field of Network and Internet at Karunya University.

Second Author Getzi P. Leelaipushpam has completed her ME degree and currently perusing Ph.D from Karunya university and is presently working as Assistant Professor in the department of Information technology of Karunya university.Has 5 Years Work Experience Her Areas of Specialization are Computer Networks and Cloud computing