An Efficient Location Based Anonymous Secure Routing Protocol for Mobile Ad hoc Network

E. A. Mary Anita*, R. Geetha, D. Mohana Geetha

Computer Science and Engineering, S.A. Engineering College, India

*Corresponding author: maryanita@sace.ac.in

Abstract:
Security is a major problem in the shared wireless medium of mobile ad hoc networks since it gives a way to the adversaries to launch various devastating attacks on the target network. To reduce this passive eavesdropping we propose an efficient approach for providing security for data and network. Initially, anonymity protection is provided to source, route and destination. Due to this the attacker finds it difficult to discover the source and destination. The path of packet flow is hidden from the attacker. This anonymity is provided at a low cost with improved efficiency. Also, high packet delivery ratio is achieved with the use of proactive geographical routing protocol (GRP), which is also known as position-based routing protocol. Our simulation results prove that packet delivery ratio is enhanced to a larger extent, thereby maintaining a trade-off between efficiency and security.

Keywords:
Anonymity; Geographical Routing Protocol (GRP); Mobile ad hoc networks (MANET); Trust

1. INTRODUCTION

Wireless network is an emerging technology which poses many challenges with respect to security. From the networking perspective, security threats may occur at different layers of the ISO/OSI model: Routing Layer, MAC Layer and Physical Layer. It is identified that a number of security threats might affect the operation of wireless networks. A large number of sensor network applications [1] are security critical and therefore processing and flow of the data in the network must be recorded. Typical security-critical applications include intelligent security systems in smart buildings, detection and tracking in the battlefield, and secure pervasive computing.

Mobile ad hoc network is an emerging area of mobile computing and is gradually becoming a new paradigm of wireless network. Its attractiveness includes easy deployment, fast network setting up, and less dependence on infrastructure. Each user directly communicates with an access point or base station. A mobile Ad hoc network, or MANET [2], does not rely on a fixed infrastructure for its operation. The Networks in MANET are deployed in random distribution. In mobile ad-hoc networks, each wireless node communicates only with a few adjacent wireless nodes to enable a low-power communication. To support multi-hop communication in ad hoc networks, many routing protocols have been designed.
protocols can be classified into table-driven (or proactive) and on-demand (or reactive) ones. There are many reasons that lead to the popularity of ad hoc networks:

1. Cost savings: Because there is no need to purchase or install access points of wireless LANs, a considerable amount of money is saved when deploying ad hoc networks.

2. Rapid setup time: Ad hoc networks only require installation of radio NICs in users’ devices. Therefore, the time to set up an ad hoc network is much less than that needed to install an infrastructure.

3. On-the-fly network: Because there is no infrastructure needed in ad hoc networks, deployment is simple. A node can join a network anytime and build a network on-the-fly.

In table driven routing protocols, nodes need to exchange routing information regardless of communication requests. Such protocols attempt to maintain consistent, up-to-date routing information for each node to reach every other node in the network. Therefore, they require each node to maintain one or more tables to store routing information. Additionally, any change in network topology may need to be propagated to the whole network to maintain a consistent network view. The destination-sequenced distance-vector (DSDV) routing protocol is a representative example. In DSDV, each node maintains a forwarding table in which each entry contains a destination address, the next hop to the destination, the number of hops to the destination, and a sequence number. Nodes will periodically exchange the contents of their forwarding tables. To relay packets, an intermediate node simply has to look its forwarding table to find out the next hop to the destination.

On-demand [3] protocols are more popular for ad hoc routing. The main feature of such protocols is that nodes exchange routing information only when there are communications waiting. This can reduce routing overhead compared to the table-driven protocols. When a node attempts to communicate with another node, it floods a route request (RREQ) packet in the network. Nodes receiving the RREQ packet will send back a route reply (RREP) packet to the source if they know how to route to the destination; otherwise, they forward the RREQ packet to other nodes.

Mobile nodes are prone to major threats than fixed nodes in MANET. Nodes in mobile ad hoc network communicate in a single-hop or multi-hop fashion, where intermediate nodes between a pair of communicating nodes act as routers. In mobile ad hoc networks, network operations are carried out by all available nodes, and such dependency is the fundamental reason for all the security problems [4] that specifically belong to ad hoc networks. During the past few years, lots of research has been done in ad hoc networks. Most of the research has focused on routing. Security issues have received relatively less attention, and these issues must be addressed. To overcome the existing problem, we propose an approach which uses proactive GRP protocol. In order to maintain the position of the neighboring nodes, the routing table is updated instantly. The information from source to destination always follows a random path and vice versa. Our simulation result proves that packet delivery ratio is enhanced to a larger extend. Thereby trade-off is maintained between packet delivery ratio and security.

The existing systems [1, 5] either concentrate on security or on data delivery ratio. The existing system uses the GPSR [6] algorithm to get the position information of the source and destination. This gives anonymity protection [6] to the source, destination and the transmitting route. The location servers [7] have been used to transmit the private keys. In this the public key encryption is used in transmitting the keys. This leads to some security issues. Existing system uses the zone based partitioning mechanism where the given land area [8] is divided into different virtual zones with respect to the nodes. Through this zone partitioning [9] and the GPSR algorithm the data packets are transmitted. The main disadvantage in the existing system is that it leads to delay since it uses the reactive protocol. The reactive protocols are only initiated when the request is given. So the packets will be flooded to find the exact path, this may lead to a situation where the data packets are send to the unnecessary nodes and letting them know the details which should be actually secured.

Since the reactive routing provides delay in finding the right path to the destination the final result will
lead to less data delivery ratio. This only gives security to the data but the data delivery rate is low. Here in the existing system there is no trade-off between the security and data delivery ratio.

Due to the delay in the reactive protocol there can be chances where the Man in the Middle attack may be possible. Due to the delay the hacker who has long time observation in the system can find the route and so the Man in the Middle attack is possible here.

2. RELATED WORK

C.-C. Jay Kuo and Chao-Chin Chou [5] proposed a MANET Anonymous Peer-to-peer Communication Protocol (MAPCP), for P2P applications over mobile ad-hoc networks (MANETs). MAPCP employs broadcasts with probabilistic-based fooding control to establish multiple anonymous paths between communication peers. It requires no hop-by-hop encryption/decryption along anonymous paths and, hence, demands lower computational complexity and power consumption than those MANET anonymous routing protocols.

Carla-Fabiana Chiasserini [7] proposed local link connectivity information mobile in ad-hoc networks, which is extremely important for route establishment and maintenance. Periodic Hello messaging [10] is a widely-used scheme to obtain local link connectivity information. In MANETs, any node in a route can move away or be turned off, which negatively affects route maintenance and throughput may cause delays in data dissemination, and so on. It is vitally important for a node in a MANET to discover live neighbor nodes through Hello messaging or a link layer feedback mechanism. Based on the event interval of a node, the Hello interval can be enlarged without reduced detects ability of a broken link, which decreases network overhead and hidden energy consumption.

Fraser Cadger [11] proposed geographic routing which offers a radical departure from previous topology-dependent routing paradigms through its use of physical location in the routing process. Geographic routing protocols have been designed for a variety of applications ranging from mobility prediction and management to anonymous routing and from energy efficiency to QoS. Within security, anonymous geographic routing appears to be a promising area of developing frameworks that facilitate efficient geographic routing without compromising privacy and security. As well as providing security, another aspect of geographic routing is location accuracy as inaccurate position information caused by location errors and unpredictable mobility can have disastrous effects on geographic routing protocols.

Gene Tsudik [12] proposed the protocol called PRISM (privacy-friendly routing in suspicious Manets) protocol. It provides privacy to the network both from inside and outside adversaries. It also supports anonymous reactive routing in suspicious location-based Manets. PRISM has three main building blocks: 1. Well-known AODV routing protocol, 2. any group signature scheme, 3. Location information. It prevents node tracking by providing group signatures to authenticate nodes and ensures integrity of routing messages. The proposed technique is used to protect the nodes from the inside and outside adversaries. The node achieves privacy and the information cannot be hacked by any adversary. The node searches its neighbor only when it is in need to send the information and the privacy is preserved in order to protect the information from the adversaries.

Kui Ren [13] proposed the stronger privacy preserving network using an unobservable secure on-demand routing scheme (USOR). The previous approaches do not offer complete unlink ability and unobservability property. But, USOR provides complete unlink ability and unobservability to all types of packets. USOR uses group signature and ID-based encryption for route discovery. It protects user privacy against inside and outside adversaries. USOR not only provides strong privacy protection but it is also more resistant against attacks due to node compromise. The proposed technique is used to provide route anonymity to the transmission. There is no link between the sender and receiver, so the adversary cannot
track the path between the sender and receiver.

Mahbub Hassan [14] proposed an Adaptive Position Update (APU) for Geographic Routing where nodes need to maintain up-to-date positions of their immediate neighbors for making effective forwarding decisions. Periodic broadcasting of beacon packets that contain the geographic location coordinates of the nodes is used by geographic routing protocols to maintain neighbor positions. Greedy Perimeter Stateless Routing Protocol (GPSR) [5], shows that APU can significantly reduce the update cost and improve the routing performance in terms of packet delivery ratio and average end-to-end delay in comparison with periodic beaconing and other recently proposed updating schemes. Results indicated that the APU strategy generates less or similar amount of beacon overhead as other beaconing schemes but achieve better packet delivery ratio, average end-to-end delay and energy consumption.

The Literature review focuses on the various adaptive routing schemes which does not focus much on anonymity.

3. PROPOSED SYSTEM

The proposed system uses the proactive routing with the GRP routing algorithm. The Geographical routing protocol is used in finding the locations of the source and the destination. This routing mechanism will not reveal the source and destination even to the network. GRP first divides the network into maintainable workspace such that particular nodes in each zone will not go out of the boundary of that particular zone. If any node has moved to another node it should register to the network. The partitioning here is governed by the network itself.

And the proactive routing is used in the transmission of the data packets to the destination from source with the help of the nearest neighbors. The proactive routing protocol maintains a routing table to keep track of the information about their own neighboring nodes. This will help in the immediate access of the nearest neighbor in the situation of a demand. This table will consist of all the information about the neighbor nodes and their position with respect to the destination. The routing tables are being updated periodically since it is a mobile network with all the nodes in mobility.

Anonymity Protection

The anonymity protection for the source, route and destination is provided as follows: in order to hide the source packet among many other packets, the source and its neighbor nodes forward the packet at the same time which provides anonymity protection to the source. Only the direct neighbors in the particular zone of the source know about the source. Others will know only the zone identification and not the nodes. Even if any node wants to know the source it needs to come in the zone only after the verification and registration by the protocol. So the threat for the identification of the source is reduced.

Each packet has a TTL field which defines the time span to reach its destination. The original source will have a valid TTL field while the other nodes will have the TTL field as 0. If a packet is received with the TTL as 0 it is dropped without opening. Only if there is a valid TTL field the packet is opened. If in the given time the packet is not delivered it will be dropped and the packet will be resent.

Source and its neighboring nodes forward the packets in different random paths. Due to the use of random paths there is no proper link between source and destination thereby providing route anonymity. Proactive protocol uses the position table which keeps track of its neighbors. Once the destination ID is found in the position table, the packet is forwarded to all the nodes in the position table.

The formatting table for initiating the communication is shown in Table 1.

In the position table, S_map is the source which sends the packet. TTL defines the life span of the packet. \( N_{nodes} \) are the neighboring nodes. \( R_{node} \) is the selected node for transmission. CTS/RTS is clear to send/request to send in which 0 defines the node is busy and 1 defines node is ready to receive. \( D_{id} \) is the
Table 1. Formatting Table for Communication

<table>
<thead>
<tr>
<th>$S_i$</th>
<th>TTL</th>
<th>$N_{nodes}$</th>
<th>$R_{node}$</th>
<th>CTS/RTS</th>
<th>$D_{id}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>2</td>
<td>N1, N2, N4, N10</td>
<td>N1</td>
<td>1</td>
<td>D</td>
</tr>
</tbody>
</table>

destination node

Advantages in the Proposed System

The proposed system uses the proactive protocol which gives various advantages in the event of maintaining the trade-off between the security and the data delivery ratio.

Since it uses the proactive routing protocol the delay which is produced by the reactive protocol has been overcome (i.e.) the reactive protocol gets activated only the demand is given due to this the route is only detected after there is demand. This will lead to flooding problem. The data packets will be sent to all the nearby nodes to find the right path for transmission which will be a threat to security since the unwanted nodes will be getting the data packets. The proactive protocol always keeps track of the nearby nodes since there is no need for the flooding to occur.

Since the proactive uses a position routing table which periodically updates its nearest neighbors there will be no delay in delivering the packets to the destination and also in finding the route. So the data delivery ratio is being increased.

Security is also enhanced by partitioning the network area into zones and governing the nodes inside that particular area. This will give higher security in the nodes since no data can be shared with unknown nodes. Even if any node is compromised, also there will be less probability for an attack to be successful since no node in the network knows the source and the destination except the active node.

SYSTEM ARCHITECTURE

Figure 1 shows the network which consists of mobile nodes. In the network, all nodes are free to move (i.e.) mobile in nature. Any node can send a packet which is referred to as a source and can receive a packet called as the destination. There is no permanent position of one node. It is difficult to detect the position of a specific node at any time. Any node can send a packet which is referred to as source and any node can receive a packet called as destination.

The Figure 2 contains the routing table of source and destination node. The source sends the packet to the nearest neighbor which in turn sends it to its nearest neighbor and so on. In the same way the packet is forwarded to the destination. Each node contains the routing table, which consists of its neighbor nodes and its position from it. The source has its routing table which shows that the next nearest neighbor is N1. Likewise the process iterates till it reaches the destination. The destination again finds another route in order to send acknowledgement to the source. For this purpose destination needs the routing table.

Figure 3 shows how the packet is forwarded from the source to the destination. The source forwards the packet to the node N1 which is nearer to it and node N1 forwards it to the node N4 which is close to the node N1. The above process is continued until the node reaches the destination. Therefore, the route for packet delivery is, “source, N1, N4, N5, N8, N13, N14, N15, and destination”.

The entire network is divided into zones as shown in Figure 4. The nodes within one zone cannot enter the other zone without requesting the authentication from GRP (Geographic Routing Protocol). The mobile nodes search for its nearest neighbor within the zone and forwards to it. The node near the boundary of one zone forwards the packet to the node in the boundary of another zone. The process iterates till it reaches the destination.

Trust computation by the Intermediate source $S_i$ about its neighbors in the set $NS_i$
Trustworthy behavior

If the intermediate source $S_i$ detects that a neighbor node $i \in NS$ has successfully forwarded a packet towards destination $d$, it will increase the trust level of node $i$ as shown in (1).
Figure 3. Random Paths

Figure 4. Zone Based Partitioning

\[ T_{\text{new}} = \begin{cases} 
T_{\text{old}} + \Delta_t & \text{if } T_{\text{old}} + \Delta_t < 1 \\
1 & \text{otherwise,} 
\end{cases} \]  

(1)

where NS is the set of neighbors of the intermediate source \( S_i \) and \( \Delta_t \) is the predefined appreciation value e.g., 0.01.

Untrustworthy behavior
When intermediate source $S_i$ detects that a neighbor node $i \in \text{NS}$ has dropped a packet, it will decrease the trust level of node $i$ as shown in (2)

$$
T_{\text{inew}} = \begin{cases} 
T_{\text{old}} - \delta_i & \text{if } T_{\text{old}} - \delta_i > 1 \\
0 & \text{otherwise,} 
\end{cases}
$$

(2)

where NS is the set of neighbors of the intermediate source $S_i$ and $\delta_i$ is the specified penalty for each suspicious behavior.

$\Delta_t$ is added to the existing trust which specifies the appreciation if a node is trustworthy and $\delta_i$ is a penalty which is subtracted from the existing trust when the node behaves maliciously in the network.

Algorithm 1: Anonymous secure routing

1. Procedure
2. Begin
3. Network is divided into zones
4. Input:
   - Intermediate Source $S_i$
   - Intermediate Destination $D_i$
   - Trust worthy neighbor $T_i$
   - Set TTL=Minimum Threshold
5. Output:
   - Secure Anonymous Path
6. If(TTL>0) then
7. $S_i$ calculates trust worthiness of $T_i$
8. $S_i$ forwards the RTS to closest $T_i$ node($D_i$)
9. If(CTS received) then
10. Forward the packet
11. Else
12. Goto step 7
13. If( ACK received ) then
14. If ( $D_i$ decrypts packet) then
15. Destination reached
16. Goto step 23
17. else
18. $D_i=S_i$
19. Else
Algorithm 1 explains the identification of secure anonymous routing. It provides anonymity protection to source, route and destination. Due to this the attacker was unable to discover the source and destination. The path of packet flow is hidden from the attacker. This anonymity is provided at a low cost with improved efficiency. It provides security through trust computation which eliminates the malicious nodes in between the routing path from forwarding the packets. If the packet cannot be delivered to the destination before its TTL value becomes 0, then it is dropped. Also the efficiency of routing is improved along with low cost.

4. PERFORMANCE EVALUATION

We evaluate the routing performance of our algorithm through simulations. We implement it in OPNET, a popular network simulator for MANETs.

Consider the mobile nodes are moving in different directions and with different speed. These nodes are configured using the mobility configurations. This will hold the information about all the nodes which are under its control. Each mobility nodes will have an attribute setting those and all have to be defined while creating the network.

This contains the code for the random mobility of the nodes. In this the state variables are initialized and the status is obtained for each variables. Here it checks for the mobility status and then parse the mobility model profile one by one. After parsing the next line decides which node picks which profile. Finally it creates child node for each profile.

The GRP protocol which we are using in this is used to reduce the delay. From Figure 5 we can clearly say that the average delay is reduced. Initially the delay is high but within 20 seconds it decreases and after that it maintains a constant delay.

Figure 6 describes about the variance in the load. The graph shows a change in the flow initially because the proactive geographical routing protocol takes time to update the table when the initial request is received later on the graph maintains a constant flow. The load is represented for the number of bits carried per second.

Figure 7 describes the packets which are delivered successfully between the nodes. The throughput here is represented for the number of bits delivered with respect to the time. Initially the throughput is low and it is raised immediately later the time goes on it is steadily maintained, because during the initial state the routing table is updating the information about neighbor. The malicious nodes are avoided in the routing path by taking trust value of the nodes into account. This makes the throughput high. After updating the table all the packets are delivered successfully hence the through is steady without any high deviations.

The overall traffic sent and received is similar which is shown in Figure 8. While the routing table is getting updated the deviation is more in traffic sent and received. Later on there is only a slight deviation in traffic received. The traffic flow is represented as bits per second.
Figure 5. Variation in Delay

Figure 6. Variation in Load
5. CONCLUSION

Trade off is maintained between the data delivery ratio and security. This is achieved by means of proactive GRP routing protocol. The security is enhanced by dividing the whole area into zones so that the nodes in any particular zone is maintained within the zone itself. Any new node cannot enter the zone without the authentication from the GRP protocol. Thus secured routing is maintained. The proposed system maintains a trade-off between security (anonymity protection) and data delivery ratio (packet delivery ratio). Since the proactive protocol is used there will be less delay due to the maintaining of the position routing table which keeps track of all the nearest neighbors periodically. This helps in avoiding
the Man in the Middle attack. Future works may focus on improving immunity towards other active attackers and demonstrating comprehensive theoretical and simulation results.

References


About This Journal

ISA is an open access journal published by Scientific Online Publishing. This journal focus on the following scopes (but not limited to):

- Access Control
- Authentication and Authorization
- Database Security
- E-Commerce Security
- Encryption and Decryption
- Grid Security
- Information Hiding and Watermarking
- Information Privacy
- Intrusion Detection
- Network Security
- OS Security
- Security Engineering
- Security for Personal Information
- Security Models
- Security Protocols

Welcome to submit your original manuscripts to us. For more information, please visit our website: http://www.scipublish.com/journals/ISA/

You can click the bellows to follow us:

- Facebook: https://www.facebook.com/scipublish
- Twitter: https://twitter.com/scionlinepub
- LinkedIn: https://www.linkedin.com/company/scientific-online-publishing-usa
- Google+: https://google.com/+ScipublishSOP

SOP welcomes authors to contribute their research outcomes under the following rules:

- Although glad to publish all original and new research achievements, SOP can’t bear any misbehavior: plagiarism, forgery or manipulation of experimental data.
- As an international publisher, SOP highly values different cultures and adopts cautious attitude towards religion, politics, race, war and ethics.
- SOP helps to propagate scientific results but shares no responsibility of any legal risks or harmful effects caused by article along with the authors.
- SOP maintains the strictest peer review, but holds a neutral attitude for all the published articles.
- SOP is an open platform, waiting for senior experts serving on the editorial boards to advance the progress of research together.