Providing Privacy & Security for Location Aided Routing in MANETS

Rathi.R *
School of information technology and engineering,
VIT university,vellore,India

Visvanathan.P,
Computer science and engineering ,
Ganathipathi tulsis engineering college,India

***Abstract* - In mobile adhoc network each node acts as a router to forward the data to other nodes within the network. In certain domains such as law enforcement, search-and-rescue, node identities might not be as important as node locations. Going a step further, if the operating environment is hostile, node identities should not be revealed, so establishing communication between nodes based on its location plays a significant role in these cases. By applying Location Aided Routing, tracking the node movements even without knowing its identity becomes impossible or at least very difficult. In this paper, a framework is created for Location Aided Routing (LAR) which provides strong privacy and security, and the routing protocol used is secure link state based routing. The privacy features of the system includes node anonymity and resistance to tracking, the security features include node authentication and location integrity. Furthermore, a group signature scheme and certain cryptographic techniques have been used for providing privacy and security**.

***Keywords* - MANET, Location Announcement Message (LAM), Neighbour Identification, Group Signature, LAR, Proactive Routing.**

I. INTRODUCTION

An adhoc network is a framework in which devices or stations communicate directly with each other, without the use of an access point. Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist. A Mobile Ad-hoc Network (MANET) is a wireless communication network formed by mobile wireless devices such as smart phones, electronic book readers etc. All nodes in the MANET have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment. The nodes can join or leave the network anytime, making the network topology dynamic in nature. In certain areas like military, search and rescue, internet connection sharing MANET plays a significant role, new innovations in MANET domain are highly valued by these people. In military and law enforcement scenarios, location aided routing has become an important issue because node identity should not be exposed and to identify the node which is nearest to us. For establishing an efficient Location Aided Routing in MANETs two things are essential, node location is very important i.e knowledge of the physical as opposed to logical or relative topology, it avoids wasteful communication and focuses on nodes located within a specific area. Secondly, critical settings must contend with security and privacy attacks, because security attacks might attempt to distribute false or impede propagation of genuine routing information; whereas privacy attacks aim to track nodes as they move. The proposed system provides strong privacy and security. The communication between the nodes is based on its current location. Topology discovery is done in advance by using proactive routing protocol. It has a group signature scheme which prevents the network from outsiders attack**.** The best path from source to destination is identified by calculating the shortest path.

The rest of this paper is organized as follows: We discuss Related Works in Section 2, Routing Protocols and Adversarial Attacks in Section 3, Proposed Work in Section 4, Future Enhancements in Section 5, Conclusion in Section 6 and References in Section 7.

II. Related Works

There are several researches which have been carried out in the field of MANETs for past two decades. The first research on Location Aided routing was carried out in the year 1998, from that time several enhancements and new extensions have been done to increase the efficiency of LAR. Location Aided Routing in suspicious MANETs [1] discusses, a mobile ad hoc network consists of wireless hosts that may move often. Movement of hosts results in a change in routes. By using location information, the proposed Location-Aided Routing (LAR) protocols limit the search for a new route to a smaller "request zone" resulting in a significant reduction in the number of routing messages. It follows Distance Vector (DV) routing protocols to identify the routes. Distance vector (DV) protocols inherently offer relatively weak levels of security. A single compromised node can easily create any number of phantom node location entries and propagate them to the entire MANET, thus "poisoning" everyone's DV tables. An Optimized Link State Routing Protocol for Ad hoc Networks [2], discusses about one of the most effective route discovery technique. The protocol is based on the link state algorithm and it is proactive in nature. It employs periodic exchange of messages to maintain topology information of the network at each node. It provides optimal routes in terms of number of hops, which are immediately available when needed. In [3] and [4], they provide an efficient short group signature scheme that is secure and based on strong Diffie-Hellman assumption. Compared with other group signature scheme, this scheme has a much shorter public key length and signature length, and needs less computation. The main objective of using a group signature scheme is to prevent the network from outsiders attack. In [6] it mainly focuses on privacy aspects of the system. It argues that the location-centric communication paradigm is better-suited for privacy in suspicious MANETs. They construct an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries. The drawback with PRISM is that it follows reactive routing; topology discovery is done in a hit-and-miss fashion. In PRISM, a node has no prior topology knowledge; it has to first determine its geographical area with a route-request message (RREQ).

III. ROUTING PROTOCOLS & ADVERSARIAL ATTACKS

A. *Routing Protocols*

In Re-active Routing**,** it does not take initiative for finding routes. It establishes routes "on demand" by flooding a Query. Some examples of Reactive Routing protocol includes Ad-hoc On Demand Distance Vector routing (AODV), Dynamic Source Routing (DSR) etc. In Pro-active Routing**,** routes are set up based on continuous controlled traffic. All routes are well maintained and available when required. When the network topology changes the protocol responds by propagating updates throughout the network to maintain a consistent view. Some examples of Proactive Routing protocol includes Optimised Link State Routing (OLSR), Destination Sequence Distance Vector (DSDV) etc. So Pro-active protocols are preferred if the size of the MANET network is big, it provides better scalability.

B. Adversarial Attacks

Three kinds of attacks which may occur in a suspicious MANET network. They are: Passive Outsider Attack**:** A passive outsider aims to compromise privacy, i.e. to track nodes. It does not engage in any active attacks like injecting, modify and replay to any messages. Active Outsider Attack: An active outsider can inject, modify and replay messages. Its goals can include disruption of routing, node impersonation, and creation of phantom nodes. Passive Insiders Attack: A passive insider possesses all cryptographic keys used for network-wide encryption /authentication. It can listen silently to all exchanged messages, and outwardly behaves correctly by following all rules and protocols. But it does not send fraudulent messages, does not attempt to impersonate other nodes, and does not delete or modify other nodes traffic. Active Insiders Attack: An active insider can modify, inject, and replay "genuine" messages. In more traditional MANET settings, the identity of each node is known and the power of the active insider is constrained, since its activity can be detected and/or traced. However in LAR, an active insider can easily modify or inject seemingly genuine routing messages, thus masquerading as other nodes. We consider two kinds of active insider attacks: Sybil attack and Location fraud. In Sybil attack, adversary creates one or more phantom nodes by generating fake routing control messages ostensibly from these nodes locations. In Location fraud, adversary lies about its own location. This can be harmful in situations where node communication is location-centric.

IV. PROPOSED WORK

The proposed system is to develop a Location Aided Routing framework that provides strong privacy and security features. The LAR framework is been set up as discussed below.

The location aided routing framework varies slightly for Online and Offline scenario, the online scenario has some additional techniques involved. In Offline scenario, each node enters a network by mentioning its distance and range. The distance D is manually entered by the node, and it's the distance traversed by the node from the starting point. The range of a node is the circular area with D as the centre point and range value as its radius, and that is the area where the node has the ability to communicate with other nodes. Each time when a new node enters a network, it sends "hello" message to other nodes which allows detecting it. Once a node detects "hello" message from another node, it maintains a contact record to store information about the neighbour. The Cluster Head (Group Manager) is elected based on Battery, Memory and Mobility. The neighbour node details and their related information are stored and maintained by each node. In military or a rescue scenario, when a node is in problem and it needs to get help from any of the other nodes within the network, in such a case it can easily identify its nearest node since they are listed as neighbours. So communication becomes easier with LAR framework. The drawback with Offline scenario is node locations are not updated automatically. If a node moves from one place to another, then it has to exit the network and enter once again by mentioning its new distance and range.

In Online scenario, LAR framework is setup based on location and range. The location of a node can be obtained by using small and inexpensive GPS receivers. The range of the node is obtained manually as in offline scenario. A new idea of Location Announcement Message (LAM) is introduced in online scenario. In LAM, time is divided into equal slots. At the beginning of each slot, each node generates a temporary public-private key-pair. Each node broadcasts a Location Announcement Message (LAM), containing its location, time-stamp, temporary public key, and a group signature computed over these fields. Each LAM is flooded throughout the MANET. On receiving a new LAM, a node first ensures that it has not received the same LAM before; it then verifies the time-stamp and group signature. If both are valid, the node rebroadcasts the LAM to its neighbours. Having collected all current LAMs, each node constructs a geographical map of the MANET and a corresponding node connectivity graph.With the help of LAM, the node's locations are updated periodically and automatically within a MANET network.

To provide privacy and security a Group Signature Scheme is used. Group signature can be viewed as traditional public key signature but with additional privacy features. In a group signature scheme, any member of a large and dynamic group can sign a message, thereby producing a group signature. A group signature can be verified by anyone who has a copy of a constant-size group public key. A valid group signature implies that the signer is a genuine group member.

The group manager (GM) initializes the underlying group signature scheme and enrols all legitimate MANET nodes as group members. The need for group signature scheme is to provide strong privacy and security features, and it is obtained by using several cryptographic techniques. During this phase, each member (node) creates a unique private key, which is not revealed to anyone. This key is needed to produce valid group signatures. It also creates a corresponding public key, which is revealed only to the GM. In addition, each member learns the common group public key that is subsequently used to verify group signatures. In case of a dispute and for offline forensics, GM is responsible for opening any contested group signatures and determining actual signers. Depending on the specific group signature scheme, GM might also handle future joins for new members as well as revocation of existing members. However, in most envisaged MANET scenarios, membership is likely to be fixed, i.e., all joins can be done in bulk, before deployment.

Whenever a node desires to communicate with a certain location, it checks to see if any node currently exists at (or near) that location. If so, it sends a message to the destination's current pseudonym. This message is encrypted with a session key using a symmetric cipher. The session key is, in turn, encrypted under the current public key included in the destination's latest LAM. When the destination receives the message, it first recovers the session key and uses it to decrypt the rest.

The proposed system is effective against several adversarial attacks, protection against passive outsiders is obtained by group signature scheme, because without knowing the group public key the outsider cannot have access to the nodes. In active outsider attack it tries to inject, modify and replay messages, but only legitimate nodes have the copy of a group signature. Group signatures are essential for sending messages, so the group signature scheme also protects the network from active outsiders attack. In the proposed system communication between nodes are not based on their permanent identities, but based on their current locations; and location of nodes tend to change periodically based on node movements. So tracing a node is highly impossible in the proposed system and is secure against passive insiders attack.

V. FUTURE ENHANCEMENTS

When the number of nodes in a MANET network is less, then the system works effectively, but when there are 1000 and more nodes then the system gets slow. The Location Announcement Message (LAM) is sent from one node to all other nodes in a network. Similarly each node in a MANET network sends the LAM to all other nodes within MANET. So the network gets flooded with LAM messages reducing the speed of the system. The Multi Point Relaying technique is used as a future enhancement to reduce the traffic within a MANET network.

VI. CONCLUSION

The proposed LAR protocol supports location-based routing in suspicious MANETS. The system relies on group signatures to construct one-time pseudonyms used to identify nodes at their present locations. The protocol works with any group signature scheme and any location-based forwarding mechanism. We evaluated the overhead and scalability of proposed protocol, it shows that it performs close to other protocols (e.g., OLSR) optimized to reduce control traffic. We also evaluated the system's tracking-resistance with different mobility models via simulations. The system is a viable and practical approach to routing in mission-critical location-based MANETS where security and privacy requirements must be reconciled and resistance to both outsider and insider attacks is needed.

VII. REFERENCES

[1] Young-Bae Ko and Nitin H. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks" Wireless Networks, 2000. Pg no 307–321.

[2] Jacquet, P.; Muhlethaler, P.; Clausen, T.; Laouiti, A.; "Optimized link state routing protocol for ad hoc networks" Multi Topic Conference, 2001 IEEE International , Pg no 62-68.

[3] Wang Shaohui; Wang Meiqin; Shandong Univ., Jinan, "An Efficient Group Signature Scheme without Random Oracles" International Conference on Computational Intelligence and Security Workshops, 2007. Pg no 807-810.

[4] Dan Boneh; Xavier Boyen; Hovav Shacham; "Short Group Signatures" Advances in Cryptology—CRYPTO 2004, Springer-Verlag.

[5] New Directions in Cryptography. Invited Paper. Whitfield Diffie and Martin E. Hellman.

[6] El Defrawy, K.; Tsudik, G.; "PRISM: Privacy-friendly routing in suspicious MANETs" IEEE International Conf on Network Protocols, 2008. Pg no 258-267.

[7] El Defrawy, K.; Tsudik, G.; "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs" IEEE Transactions on Mobile Computing, September 2011. Pg no 1345-1358.