Scalable ALARM: Anonymous Location Aided Routing in Hostile MANETs

[1] Geethu Mohandas, [2] Dr Salaja Silas

[1, 2] Department of Information Technology, Karunya University
Karunya Nagar, Coimbatore 641114,India

Abstract

Hostile MANETs are significant because of their applications in military and law enforcement area where the identity of the nodes cannot be revealed since there is a risk of tracing and locating them with their identities, which makes the network vulnerable to attacks. Therefore communication between nodes should be performed with the help of location information which mitigates the risk of exposure. Security and privacy in location based communication within suspicious MANETs can be enforced using the group signature scheme along with the ALARM protocol which can provide authentication of nodes, data integrity and intractability but lacks scalability due to excessive broadcasting of link state information. This study proposes, HOLSR addresses the scalability problem by providing a resilient approach to enhance the scalability feature of ALARM protocol.

Keywords: *MANETs, security, privacy, scalability, HOLSR.*

1. Introduction

MANET is an infrastructure less dynamic network of mobile devices having self-configuring capability. These mobile nodes [9] are able to move in either direction freely and the connection between them alters intermittently. The applications of MANETs are in the area of military, civilian environment, emergency operation and disaster recovery. The routing between nodes in MANET is of two types, they are identity based routing and location based routing. In location based routing, node location is found by using GPS technique.

This method is used in the areas where high security must be established. In hostile environments, adversaries will be trying to track the nodes if their communication is done via identity based routing so that, location based routing is used to hide their real identity. Routing protocols are categorized as proactive (table-driven) and reactive (on-demand) protocols.

Reactive protocol is based on route requests and replies, i.e. whenever a node wants to communicate with another the source node sends route requests and follows route discovery process [5]. AODV is the commonly used reactive protocol.

Proactive protocols have route readily available regardless of their necessity [5]. Proactive protocol is of two types; distance vector and link-state. Distance Vector (DV) protocol offers weak levels of security relatively and cannot be used in areas where high security is needed [5]. Link State (LS) protocol prevents the need for route discovery hence this protocol is applicable to environments having strict delay constraints. Optical Link State Routing (OLSR) is one of the finest link state protocols used for routing, which works based on Multi Point Relays (MPRs), only the selected first hop neighbors forwards packets. This eliminates the drawback of excessive broadcasting because only selected nodes forwards. Link state can offer more security since origin authentication and integrity of LS updates can be easily supported.

In hostile MANET's security and privacy features must be considered, because the environment undergoes attacks from both outsiders and insiders. Attackers try to perform malicious actions to the critical data, finally causes compromise to confidentiality and integrity. To achieve privacy and security group signatures can be employed, which is just like traditional public key cryptographic system having additional privacy features. Group signature scheme is employed by group manager that is based up on its group members.

2. Related Work

C. Adjih et. al 2003 had proposed "LSR: Link State Routing", a proactive protocol [1] which was based distributed database concept and each node periodically updated its links to the neighbors. The link information was again forwarded until all nodes in the network had same information but this protocol had not included any security features and LSR lack scalability due to excessive broadcasting. Guoyou He, 2006 had proposed "Destination-Sequenced Distance Vector (DSDV)" [7], a proactive protocol eliminated the disadvantages of distance vector routing scheme by the addition of sequence numbers to routing entries. Protocol kept its path to all other known nodes and updated these details frequently. But the protocol created the problem of overhead.

C. E. Perkins et.al had proposed “Adhoc On Demand Distance Vector Routing (AODV)”, a basic reactive protocol [13]. AODV worked in two phases. Phase one was the route discovery phase where the source node created the route requests and forwarded it to the neighbors. On receiving route request the nodes created route reply and send it back reverse route. The second phase was route maintenance wherein links are updated using hello and route error messages. Jacquet. P et.al had proposed Optimized Link State Routing Protocol (OLSR) [2], a proactive method which reduced overhead of link state protocol. OLSR was based on Multi Point Relays (MPRs) and was efficient in highly dense network.

Young-Bae Ko et. al had proposed “Location Aided Routing (LAR)”, a scheme which used location information[11] for improving routing in MANETs and which mainly used in highly hostile environments. Location was found based on GPS systems and expected zone, request zone were figured for finding route to a specific destination. Wen-Hwa Liao1 et. al had proposed “GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID”, which was a location based proactive protocol for geocasting[8]. The protocol attained high data arrival rate and eliminated traffic in the networks. The protocol divided area of the mobile networks into square grid of size d*d and routing is done only within the specified area.

Carter S et al. had proposed “SPAAR: Secure Position Aided Ad Hoc Routing”, a reactive location based protocol [3] had security capability could be used in non high risky environments. In the protocol position was protected from unauthorized nodes. Nodes accepted request from one-hop neighbors alone. Karim El Defrawy et.al 2011 had proposed “Privacy-Preserving Location-Based On-Demand Routing in MANETs [PRISM]”, a location aided reactive protocol based on AODV used in hostile environments. This gave protection against outsider and insider attackers based on a group signature scheme. PRISM [4] worked based on route requests (RREQ) and route replies (RREP) in specified geographical area. The disadvantage of the protocol was that it didn’t have prior knowledge about the topology.

Karim El Defrawy et. al 2011 had proposed “Anonymous Location-Aided Routing in Suspicious MANETs: ALARM”, a location based proactive protocol[5], used in hostile environments.

Protocol protected against both outsider and insider attacks by using group signature mechanism. Nodes broadcasted location announcement messages (LAM) for periodical announcement of its current location to other nodes. Group Manager was responsible for the establishment group signature scheme.

The proactive protocols used in MANETs are divided into two: distance vector and link state protocols. Proactive protocols eliminate the need for route discovery. The distance vector protocol [5] having weak levels of security. Link State protocols are suitable for real-time applications having strict delay constraints. OLSR is an optimized version of link state protocol eliminates broadcasting by every node. This is achieved in OLSR by using multipoint relays, a subset of first hop neighbors only forwards control messages to others. Using OLSR modest sized MANET’s scalability can be achieved. By the usage of HOLSR protocol scalability of the system can be greatly increased.

The performance of flat routing protocol OLSR puts down as the raise in number of nodes on account of a more number of topology control messages within the network. OLSR doesn’t distinguish the capability of its member nodes, hence which doesn’t make use of nodes with higher capacities. OLSR is scalable only up to 70 nodes due to diffusion of all network nodes of all link state information.

3. Scalable ALARM

The Hierarchical Optimized Link State Routing (HOLSR) [6] protocol has been proposed to enhance scalability of OLSR used in mobile adhoc networks. It organizes network in logic levels and nodes in clusters. In these clusters it uses normal OLSR to distribute traffic information. The primary advantages are effective utilization of higher capacity nodes and stepping down the topology control traffic. The framework of HOLSR makes reduction in computational cost for routing since any collapsed link makes only nodes within the same cluster need to recalculate their routing table as nodes of other clusters are unaffected.

In the protocol nodes are organized according to their capacities [6] and nodes with more number of interfaces are selected as cluster heads. Cluster identification messages are used to organize a HOLSR network into clusters. It is a proactive protocol having two phases: i) topology formation and ii) topology map acquisition. Within each cluster optimal routes are calculated via information contained in Hello and Topology Control messages. Membership information is advertised from nodes in one cluster to others done by applying Hierarchical Topology Control (HTC) messages. In HOLSR node exchange of Hello and TC inside the clusters creates cuts the percentage of traffic broadcast inside the network**.**

The system explains about a protocol used in hostile mobile networks. Proposed system is a proactive protocol having security capability based on group signature scheme. The basic working of the scalable ALARM protocol is completely same as that of ALARM protocol [5].

Scalable ALARM

Step1: Nodes are classified into clusters according to their capacities and node having more interfaces is taken as cluster head within each cluster.

Step2: Group manager initializes underlying group signature scheme and adds all legitimate nodes as group members.

Step3: Determine the nodes private and public key pair and which is send to the group manager which calculates group public key and send to the group members

Step4: Time is divided into equal intervals and key pairs are generated in the beginning of each time slot.

Step5: Each node generates Location Announcement Message (LAM) containing location, timestamp, temporary public key and group signature computed of these parameters shown in figure 1.

Step6: The LAM messages are forwarded to its neighbors and each node receiving the LAM message does the following,

a) Checks whether it has received the LAM message before
b) Verifies the group signature and time stamp
c) If both the above conditions are satisfied, LAM messages are forwarded to its neighbours and acquiring all these LAMs, nodes will get details of the network topology.

Step7: When a node wants to communicate with a specific location it checks to see if any node exists in that location , if so node send message to the destinations present pseudonym. Message format is shown in figure 2[5].
Pseudonym = node location||group signature

a) The message is encrypted with session key using a symmetric cipher
b) Session key in turn encrypted with public key of the destination included in the latest LAM
c) Session key is retrieved soon after a message received and uses that to decrypt the message.

Message-Type : LAM
Location
Time-Stamp[TS]
Temporary Cryptographic Key [PK-TMP]
GSig[Location||TS||PK_TMP]

Figure1. LAM format [5]

Message-Type : DATA
SRC_TMPID={Location||Gsig}
DST_TMPID={Location||Gsig}
$E_{PKDST}(K_s)$
GSig[Location||TS||PK_TMP]

Figure2. DATA message format [5]

Nodes intermittently forwards LAM messages to distribute topology information among nodes. Source node finds path based on shortest path algorithm or location-aided routing algorithm. For example a node at location 6 with pseudonym (TmpID6={Location6||GSig6}) wants to communicate with a node at location 2 pseudonym (TmpID2={Location2||GSig2}), then the sender node finds the route and then generates a session key to encrypt the data, which in turn encrypted with the destination nodes public key and gathers data message with source node as TmpID6 and destination as TmpID2.

4. Simulation Results

NS-2 is an event driven packet level network simulator. NS is an Object-oriented Tcl (OTcl) script interpreter. NS-2 has expanding uses including evaluating the performance of existing network protocols, to evaluate new network protocols before use, to run large scale experiments not possible in real experiments, to simulate a variety of ip networks.

Table1. Simulation Parameters

Simulation Area	1000m X 1000m
Simulation Time	1000 sec
Routing Protocols	OLSR and HOLSR
Number of Nodes	50
Node placement	Random
Mobility Models	Random Walk and Random Waypoint

Using HOLSR computational cost can be greatly reduced i.e., in the case of broken link only nodes inside the cluster need to be recalculate their routing table while nodes in different clusters are not affected. HOLSR is used in ALARM protocol in order to reduce route computational and scalability improvement. Computational cost is calculated against varying speed and area and is plotted in the graph shown below. As shown in figure1 HOLSR having low computational cost compared to OLSR because link recalculation area is minimized to the particular cluster rather the whole network.

Area is taken in the X axis and which is measured in meters and Computation cost is taken in the Y axis. As seen in the graph as area increases number of nodes increases and computation cost also increases. But compared to OLSR protocol cost is lower in HOLSR protocol.

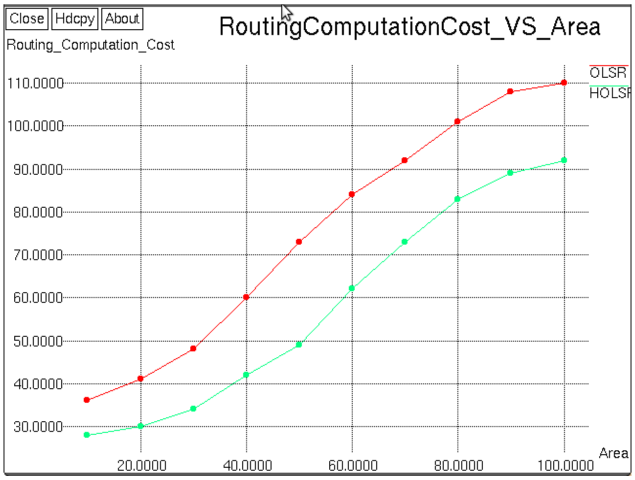

Figure 4.Comparison of routing cost between OLSR and HOLSR

Area is taken in the X axis and is measured in meters. As seen in the graph as area increases, throughput decreases. OLSR protocol has lower throughput than HOLSR protocol as a result of the comparison graph.

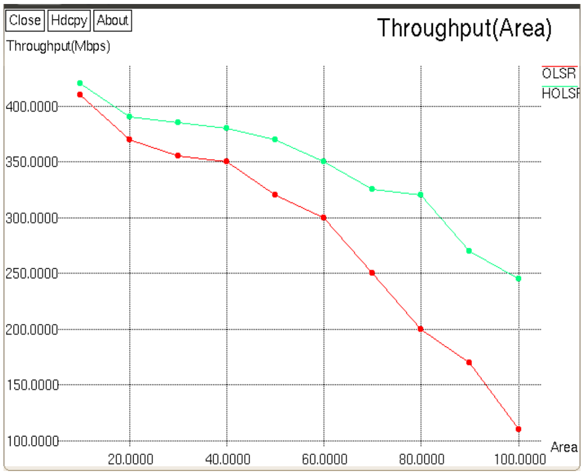

Figure5. Comparison of Throughput VS. Area between OLSR and HOLSR

5. Conclusion

Hostile MANET's security is an important area and on account of that anonymous location aided proactive protocol is developed to protect against both outsider and insider attacks using group signature scheme. But the protocol lacks scalability and this is rectified with using HOLSR protocol as base protocol for routing in the architecture. As seen in the graph routing computational cost is greatly reduced in the HOLSR and throughput comparatively higher in HOLSR while comparing with OLSR.

Acknowledgements

The authors wish to thank Karunya University for providing infrastructure for carrying out the simulation and financial support. The authors thank the senior professors and the technical experts for providing valuable suggestions to improve the quality of the research paper.

References

[1] Adjih C, Baccelli E., Jacquet P, "Link State Routing In Wireless Ad-Hoc Networks", Milcom'03, 2003, Pages 1274-1279

[2] Clausen T, Jacquet. P, Laouiti A, Muhlethaler. P, Qayyum A, and Viennot L," Optimized link state routing protocol for ad hoc networks," 2001, pp. 62–68

[3] Carter S and Yasinsac A, Secure position aided ad hoc routing, (2003)" Proc. IASTED International Conference on

Communications and Computer Networks (CCN02)", pp. 329–334

[4] Gene Tsudik , Karim El Defrawy, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE Journal on Selected Areas In Communications, Vol. 29, No. 10, December 2011.

[5] Gene Tsudik, Karim El Defrawy," ALARM: Anonymous Location-Aided Routing in Suspiciou ANETs" IEEE Transactions on Mobile Computing, Volume: 10, Issue: 9 Page(s): 1345 - 1358, September 2011.

[6] Gimer Cervera1, Michel Barbeau1, "Preventing the Cluster Formation Attack Against the Hierarchical OLSR Protocol",FPS'11 Proceedings the 4th Canada-France MITACS conference on Foundations and Practice of Security, Pages 118-131

[7] Guoyou He," Destination-sequenced distance vector (DSDV) protocol", Technical report, Helsinki University of Technology, Finland.

[8] Jang-Ping Sheu, Kuo-Lun Lo1,Wen-Hwa Liao1, Yu- Chee Tseng2,"GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID", Journal of Internet Technology, Vol. 1--2 (2000), pp. 23-32.

[9] Jun-Zhao Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", Info-tech and Info-net, 2001, Proceedings, ICII 2001-Beijing, 2001International Conferences on,volume3, pages: 316-321

[10] Nitin H. Vaidya ,Young-Bae Ko,(2000) "Location Aided Routing (LAR) in mobile ad hoc networks" Wireless Networks, vol. 6, pp. 307–321 307, 2000

[11] Robin Kravets, Prasad Naldurg, Seung Yi," Security - Aware Ad hoc Routing for Wireless Networks", Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, Pages 299-302

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