International Journal of Multidisciplinary Approach and Studies

ISSN NO:: 2348 – 537X

A Survey on Performance Based Security Analysis of Geographical Routing Protocols In MANET

Shanthi . H. J* & Dr. E. A. Mary Anita**

**Research Scholar, AMET University, Chennai*
***Professor, S.A Engineering College, Chenna*

ABSTRACT

The routing protocols in MANET are substantially investigated by researchers. The lack of dependency in routing initialization and secure communication for geographic routing protocols attracts considerable attention. In this paper we review the existing secure geographic routing protocols of MANET and provide a qualitative comparison of them.

We compare and contemplate the features, vitality, and vulnerability of these approaches and highlight indispensable research challenges that are imperative to address and will have substantial advantages. The fallout of the analysis will significantly be a guide for anyone willing to develop into research on secure geographical routing algorithm to provide MANETs. We indicate the security gaps and challenged threats will allow design new secure network algorithms.

Keywords: *Location based protocols, Geographical routing, LAR, DREAM, ALERT, Secure Geographical protocols*

I. INTRODUCTION

MANETs are dynamic, self-configuring, and infrastructure-less groups of mobile devices. They are usually created for a specific adhoc purpose with no permanent function [1]. They can be constructed and deconstructed without central management system. This attractive scenario of leads to MANET research and focused on developing an efficient routing mechanism in highly dynamic and resource constrained network. Much of algorithms does not concentrate on location based routing. Further these protocols assume the trusted and cooperative environment. Hence presence of malicious node in the network makes the network vulnerable to various kinds of attacks.

The MANET has various applications in various fields. The applications from ascertain from civilian wireless networks to disaster management. The adhoc networks in conference rooms and campuses to emergency conditions like disaster management and fire, battlefield, intelligent transport system for vehicle to vehicle communication and personal area networks linking laptops, cell phones, wearable systems and PDAs [15].

The location-based services are popular, because they are driven by the availability of modern mobile devices with integrated position sensors. The geographical nodes know their location using positioning device like global positioning system (GPS) [3]. The locations of immediate neighbours and destination node are estimated through it to forward the message. The GPS takes the help of satellites and use them as reference point to calculate. These protocols can be used in Wireless sensor Network, VANET, Rooftop networks and other ad

hoc networks. The rest of paper is organized as follows. The section 2, presents overview of existing routing protocols and we have outlined the geographical routing protocols. In Section 3, we have discussed the methods adopted by geographical routing. In Section 4 we have evaluated their characteristics and their limitation. In Section 5 we conclude our discussion.

II. OVERVIEW OF PROTOCOLS

There are different types of secure routing protocols for MANET. The main four categories are,

1. Proactive protocol
2. Reactive protocol
3. Hybrid protocol
4. Geographical positioning protocol

Proactive routing protocols are also called as table driven routing protocols. Every node in the network maintains one or more route table. The changes in the route table will be sent to all nodes by other nodes through broadcasting so that they are updated regularly. E.g. DSDV, WRP etc.

Reactive protocols are also known as Demand Driven protocols. The nodes look to set up routes based on demands. The reactive protocol will try to establish a route when a node wants to communicate with another node that has no route. The end to end delay is more in reactive protocols. E.g. DSR, AODV etc.

The hybrid routing protocol is combination of proactive and reactive protocols. It was designed to decrease the latency caused by route discovery in reactive routing protocols and the control the overhead of proactive routing protocols. E.g. ZRP, SHARP etc.

In a geographical location information of the nodes was gathered by the positioning devices like GPS present in the network. This helps to identify a node without searching the entire network. The transmit decision is based on the location information and it is vulnerable, can hacked easily. There is necessity for secure location information for exchange of information [3]. Recently several secure ad hoc routing protocols are proposed in geographical routing with various attacks. The attacks are of two types, one is malicious user node and other is compromised user node. An attacker who is not belonging to the network and not have valid cryptographic key is a malicious user node. An insider who is capable of initiating several kind of attacks in the network is compromised user node and generally hard to detect by other entities.

The Location Aided Routing LAR [5]is popular reactive protocol using location information to identify the expected zone. The request zone is rectangular area which includes sender and receiver. The search area is wider which leads to increase in overheads.

S. Basagni et al. [6] proposes DREAM (A Distance Routing Effect Algorithm for Mobility) which is proactive protocol maintaining the each nodes location in routing table. Each node broadcast the packet with its location such that location table maintained accurately

The CONFIDANT [13] protocol is a secure demand routing protocol which makes misbehavior nodes unappealing for other nodes to communicate. This protocol is based on

selective selflessness. The nodes keep track of the malicious nodes and maintains forbidden list. The service from the forbidden list is not entertained. The protocol uses trust mechanism. The trust relationships are based on observation on reported routing and forwarding of forbidden list.

El Defrawy, Karim et al[7] proposed ALARM Anonymous Location-Aided Routing in Suspicious MANETs is designed to analyse the privacy-preserving and provide secure link state based routing. The protocol constructs the topology snaps and uses cryptographic techniques to give protection against the passive and active inside and outside attacks.

Malgi et al. [9] proposed SC_LARDAR (Security Certificate Location Aided Routing Protocol with Dynamic Adaptation of Request Zone) protocol which concentrates on black hole attack. The protocol has reduced the flooding and power consumption.

The Energy Efficient Location Aided Routing (EELAR) [14] is variation provided for LAR to reduce the energy consumption of mobile node batteies by limitting the search area. Further the control packet overhead is reduced significantly.

The Greedy Perimeter Stateless Routing (GPSR) [8] Protocol forwards packets with decision using the routers immediate neighbour in topology. The packets are forwarded on a greedy basis by selecting the node closest to the destination and provide the short path.

The Anonymous Location-Based Efficient Routing Protocol in MANETs (ALERT) [2] protocol dynamically partitions the network field and hides the initiator and receivers to strengthen anonymity protection. It further offers lower cost and routing efficiency.

The Secure and Efficient Distance Effect Routing Algorithm for Mobility (SE_DREAM) [10] protocol is discovers the malicious nodes in transmitting zone by evaluating the traffic flow between the nodes. The challenges of routing protocol designed for Ad Hoc wireless faces problem of mobility nodes, resource constraints, error-prone channel state and hidden and exposed terminal problems [12].

III. TECHNIQUES OF GEOGRAPHICAL ROUTING PROTOCOLS

In the previous section, we have classified of routing protocols in MANETS. We have further surveyed the geographic routing protocols. Position based routing or geographic routing is used to eliminate the limitations of topology based routing. It gives the better performance in dynamic topologies because the packets are forwarded to its destination with respect to its position. We further discuss the methods and major characteristics adopted by the geographical routing protocols.

LAR

The LAR uses positional information to flood a route request packet for destination node in request zone to entire ad hoc networks. A source requests their neighbours for route to destination before transmitting a routing in forwarding zone. Based on reply the forwarding and the expected zone adapt during transmission. The intermediate nodes do not update the source with recent location on the destination. This leads to floods with route requests but since the intermediate are not allowed to respond it has the benefits of malicious nodes disruption is reduced. The request zone is a rectangular area with the source and expected

zone of destination. The x and y axis are parallel to sides form rectangular zone. In route discovery source transmits the route request message on all four corners of request zone, intermediate node decides whether to transmit the message or not. The MAC layer implementation does not exist hence the route errors are generated when a route breaks.

DREAM:

This protocol uses distance effect on two separating nodes based on mobility. The moving nodes send their mobility updates autonomously with their mobility rate. The source selects the neighbors that are in the direction of destination. The each node repeats the same till the forwarding message reaches the destination. The selection of neighbors is crucial within an angle. The radius of expected region around the source is set t1-t0 max, where t1 is current time, t0 is time stamp of source and destination and vmax is maximum speed of a node that may travel in the network. A circle is defined around source and Destination with angle. This protocol reduces uses of bandwidth and transmission power with accuracy since it updates its routing table frequently [11]. This protocol provides loop free routes and adaptive to mobility making them robust.

CONFIDENT

The CONFIDANT design assumes the design of network layer with base on DSR. This protocol has four components: the monitor, the reputation system, the path manager, and the trust manager. The monitor records the neighbor nodes communication. The trust manager accounts with incoming and outgoing ALARM messages. These are the warning messages to warn about malicious nodes to other nodes. The reputation system helps in exchange of black list and avoids the centralized rating. This type is used in online auctioning systems. Each node maintains reputation value for each node in network and combines all various functional reputation values. The global reputation value hides the malicious node behavior. The distributed nature leads to inconsistency in reputation value. The difficulty in this system leads to false advertising high values or false low rating about another node. Hence the simple local reputation mechanism is efficient than the complex reputation mechanism.

ALARM*:*

ALARM uses nodes' locations to securely broadcast and construct topology snapshots and to forward data. This protocol uses advanced cryptographic techniques. The first step is initialization of group manager with group signature and enrolls all the legal nodes as group members. The each member creates their own unique private key. Each of the node disseminate a Location Announcement Message (LAM), which containing their location (GPS coordinates), time-stamp, temporary public key and a computed group signature. The each node constructs geographical map of network and connectivity graph. When the node wants to communicate it checks to see it exists near. The message is encrypted with session key using symmetric cipher cryptography principle, which further encrypted with current public key. The sender computes shared key and encrypts with session key which is tested at destination. The each node gets entire view of network and the actual path is computed with shortest path or any other location routing algorithm.

ALARM provides both security and privacy features, including protection against passive and active insider and outsider attacks. The simplicity and effectiveness is advantage of the protocol.

GPSR

Greedy forwarding is efficient and highly suitable for dynamic ad hoc network topology. The accuracy of destination is must or the packets cannot be delivered. When the protocol is compared with DSR packet delivery is high and less overhead. This works in two modes Greedy mode, when forwarding and Perimeter in recovery phase. To calculate a path, GPSR uses a greedy forwarding algorithm that will transmit the information to the final destination using the most efficient path possible. If the greedy forwarding fails, perimeter forwarding will be done with routes in region around the perimeter. The algorithm aims to find the nearby router which is also the nearby to the final destination. A node remembers the location of neighbors within one-hop. The Routing decisions are dynamically made. When the network is dense Greedy forwarding will fail. When the Greedy Forwarding algorithm fails, the Perimeter Forwarding algorithm will follow. It follows the right-hand rule to traverse the edges of the void and find a path using the topology's perimeter. The Perimeter Forwarding Algorithm uses a little longer path to the destination so the perimeter forwarding algorithm less efficient and cannot be used divide. Both together will help to find best path in topology.

ALERT

ALERT partitions the network field into zones and chooses the nodes randomly as intermediate relay nodes. This helps in formation of non-traceable route, which hides the source, receiver giving strength to anonymity protection. The source executes horizontal partition and checks whether the destination in the same zone. If it falls it divides zone alternatively in horizontally and vertically otherwise chooses position in other zone to make temporary destination and uses GPSR routing to send data close to temporary destination. This protocol also uses symmetric cryptography and decrypts its own public key. The main achievement is of this protocol is restricting the node's view to its neighbour alone and constructing same initials and forwarded message, which makes intruder difficult to detect whether it's a source or forwarding node. The ALERT uses TTL (Time to Live) field in each packet to reduce excessive traffic by restricting TTL =0. This protocol provides good secure anonymity routing with low cost.

SC_LARDAR

This protocol overcomes black hole attack by issuing the security certificate adapted on Location Aided Routing Protocol with Dynamic Adaptation of Request Zone. This also helps to select ideal path for transmission. It works as extension of LARDAR protocol using route discovery process followed by an authentication. The source broadcasts RREQ to its neighbours with minimum time delay to receive. The digital signature is used to identify the authentic sender. Every node validates its neighbour by issuing certificate and generating public key. The certificate have separate local repository with issuer and node issued. The exchange of certificates periodically takes place with one hop low communication cost. The conflict arise when malicious node issue false certificate and node is assumed to be malicious. This secured route transmits based on minimum angle. This helps in reduces flooding and bandwidth consumption.

SE_DREAM:

The protocol reduces misbehaving nodes in forwarding zone using traffic flow analysis between nodes. The protocol further uses cryptography to produce secure data transmission.

The protocol is implemented on DREAM protocol for routing. The traffic matrix is constructed for two individual nodes and traffic analysis is done with calculated predefined threshold value to find the misbehaviour list. When the malicious node reaches the threshold revocation message is generated. Each node has its own public key shared among network. This signature is appended with revocation message and on receipt checks whether the equation holds true. When the equation holds, the node is cancelled from forwarder zone list. Thus the forwarding zone is free from malicious node.

IV. ANALYSIS AND DISCUSSION

All the protocols are tested with performance metrics such as protocol overhead, end to end delay and packet delivery in under the baseline case. The DREAM protocol has a average end-end delay and packet delivery ratio. The DREAM protocol provide more robust to mobility when compared with LAR.

It also provides high packet delivery ratio to LAR[12]. The ALERT protocol provides anonymity whereas ALARM does not provide complete anonymity. The ALERT protocol is compared with GPSR and ALARM protocol. The ALERT protocol does not take shortest path on contrast ALARM provides shortest route. The encryption of ALERT is simple than ALARM. The latency is high in ALERT. The number of hops for GPSR and ALARM are similar. ALERT provides higher delivery rate then GPRS protocol. The CONFIDENT protocol works has the extension of Dynamic Source Routing (DSR). It is able to control the malicious node to certain extent when compared with DSR with slight overhead. The SE_DREAM protocol is extension of DREAM which provides security to DREAM in efficient manner. The throughput and packet delivery ratio is high. All the protocols provide small end to end delay.

TABLE I. Comparison Of Protocols

Protocols	Type	Security	Merits	Demerits
LAR	Reactive	No	Uses multipath strategy Shortest path metric	Uses Flooding In Control message Overhead increase with distance
DREAM	Proactive	No	Reduced Overhead	Packet loss is high Consumes Higher bandwidth
CONFIDENT	Reactive	Yes	Uses reputation method	Packet drop is high
ALARM	Proactive	Yes	With group signature it provide anonymity	Resistant to passive and active Attacks Prevents Sybil attack but not location fraud Does not offer Scalability in larger network
GPSR	Proactive	Yes	Data overhead is	It induces great

			low	traffic. Failure of central node bring the network down
ALERT	Reactive	Yes	Uses Symmetric key encryption Generates longer path Lower Energy Consumption	Preserves security and privacy Avoid dead-end problems
SC_LARDAR	Reactive	Yes	Digital Certificate	Packet delivery ratio is not considered Detects and removes black hole Excess overload
SE_DREAM	Proactive	Yes	Packet Delivery ratio is high	Effective to reduce flooding attack Overhead is high

V. CONCLUSION

Various security parameters like integrity, overhead, authentication, confidentiality and utility **were analyzed. Security methods adopted are discussed for all the protocols**

REFERENCES

i. Shanthi, H. J., and EA Mary Anita. "Heuristic Approach of Supervised Learning for Intrusion Detection." Indian Journal of Science and Technology 7.S6 (2014): 11-14.

ii. Haiying Shen, Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocols in MAnets" Transactions in Computing, IEEE, Vol. 12, June 2013.

iii. Sharama S. and Singh S., "A Survey of Routing Protocols and Geographic Routing Protocols Using GPS in MANET," Journal of Global Research in Computer Science(JGRCS), Volume 3, ISSN-2229-371X, December 2012.

iv. Kumar, Arun, et al. "Location-Based Routing Protocols for Wireless Sensor Networks: A Survey." Wireless Sensor Network 9.01 (2017): 25.

v. Ko, Young-Bae, and Nitin H. Vaidya. "Location-aided routing (LAR) in mobile ad hoc networks." Wireless networks 6.4 (2000): 307-321

vi. Basagni, Stefano, et al. "A distance routing effect algorithm for mobility (DREAM)." Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking. ACM, 1998.

vii. K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2007.

viii. Karp B, Kung HT , GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. ACM MOBICOM 2000, pp. 243–254

ix. Tyagi, Kalpana. "Secure Approach for Location Aided Routing in Mobile Ad Hoc Network." International Journal of Computer Applications 101.8 (2014).

x. Shanthi, H. J., and EA Mary Anita. "Secure and Efficient Distance Effect Routing Algorithm for Mobility (SE_DREAM) in MANETs." Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16'). Springer International Publishing, 2016.

xi. Shanthi, H. J., and EA Mary Anita. "Performance analysis of black hole attacks in geographical routing MANET." (2014).

xii. Kehar, Priyanka, and Pushpendra Kumar Pateriya. "A STUDY ON OPTIMIZING THE EFFICIENCY OF LOCATION AIDED ROUTING PROTOCOL (LAR)." International Journal of Computer Science and Information Security 14.4 (2016): 81.

xiii. Buchegger, Sonja, and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol." Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. ACM, 2002.

xiv. Vijayakumar, H., and M. Ravichandran."Efficient location management of mobile node in wireless mobile ad-hoc network." Innovationsin Emerging Technology (NCOIET), 2011National Conference on. IEEE, 2011.

xv. Agrwal, Dharma P and Quing-An Zing. Introduction to wireless and mobile system. Cengage learning,2015