Location Based Secure Routing Protocol in MANETs

Ms. Deepa K C
2nd year Mtech, Dept of ISE
The Oxford College of Engineering
Bangalore, Karnataka, India

Mrs. Sindhuja
Assistant Professor, Dept. of ISE
The Oxford College of Engineering
Bangalore, Karnataka, India

***Abstract*-Secure routing is the major issue in Mobile Ad Hoc Networks (MANETs).Due to its features of open medium, dynamic topology, infrastructure less, non-centralized authorization. There are a many number of papers on secure routing, only few papers are address anonymity issue. However, for truly secure MANETs anonymity must be crucial part of the overall solution of problem. Existing system cannot offer full security using anonymous mechanisms with low cost. We propose a location based secure routing protocol in MANETs, to achieve anonymity protection with low cost. In location based secure routing protocol offers sender and receiver anonymity and route anonymity to strengthen anonymity protection. We use simulation and analysis to study the anonymity and routing, energy efficiency. And show that location based secure routing protocol achieves comparable anonymity, routing and energy efficiency to GPSR geographical routing protocol. Here, we tend to additionally propose for better receiver anonymity protection performance and achieve high packet delivery ratio using multicasting mechanism.**

Keywords- Anonymity, Location based Anonymous Routing, GPSR, MD5, Security.

I. INTRODUCTION

MANETs are vulnerable to malicious activities such as traffic analysis by communication overhearing and attacking routing protocol. In traffic analysis attack malicious node may obtain transmitted packets, they also monitor information transmission when two nodes are communicating with each other and keep historical communication record of node causes denial-of-services attacks. Also malicious observer might try and block the information packet by act as legitimate nodes in network, intercept the packets on many nodes, and detecting the information transmission direction malicious nodes can trace back to the sender. To avoid these attack propose an location based secure routing protocols in MANETs.

In anonymous routing protocol, identities of the sender and receiver nodes are hidden among many nodes present in network is called source and destination anonymity and In route anonymity which form untraceable route[1], using these mechanisms we can achieve anonymity protection to MANETs. Anonymity protection is important when ad-hoc node want communication privacy. For example, In an online communication, we not only want to hide communication content and disable communication from malicious nodes, but also expect that the identities and location information of sender and receiver in communications are hidden to malicious nodes. Otherwise, malicious nodes uses identities and location information of source and destination node to locate the attacks.

We propose a location based secure routing protocol to achieve high anonymity protection to sender, receiver and route with low cost in terms of encryption time, traffic generation. It uses modified ALERT algorithm, it uses GPS location server to get zone location information and assume entire network area in terms of zone and divides zones dynamically using zone partition algorithm in order to place sender and the receiver into different zone so we can achieve high anonymity protection level and choose relay nodes randomly in other zone which in term form anonymous route and encrypting real identities of sender and receiver, zone position of receiver to provide sender and receiver anonymity. Multicasting mechanism is used to achieve better packet delivery ratio, anonymity protection level. Timing analysis is provided using 'notify and go' lightweight mechanism and multicasting and local broadcasting mechanism is used to avoid counter intersection attack. Uses the GPSR [3] algorithm to send the information to relay node.

The organization of this paper: explanation about the related work in section II, we present the design and analysis of location based secure routing protocol in section III, performance of the location based secure routing protocol is evaluated in section IV, Finally, in section V, the conclusion is given.

II. RLATED WORK

Existing anonymity routing protocols in MANETs may be principally classified into two categories: hop-by-hop cryptography[4] and redundant traffic[5],[6],[9]. Most of the present schemes are limited by specializing in imposing anonymity at a significant cost to precious resources as a result of public key-based cryptography and generate considerably high traffic cost.

A. ANODR[2] achieves source and destination identity anonymity. ANODR not providing route anonymity.

B. MASK [3] protocol offers sender and route anonymity. The big problem here is that MASK exposes the destination ID, which is unacceptable in anonymous routing protocol.

C. In GSPR [4] packets in all time follow the minimum hop count paths so it does not provide route anonymity.

In a long term communication the route can be determined by malicious node.

D. In the AO2P [5] geographic routing algorithm, pseudonyms are used to protect nodes' real identities, and a node chooses the neighbor that can reduce the greatest distance from the destination. So AO2P cannot offer anonymity protection to route.

E. ASR [6] offers source, destination of identity and location anonymity... In ASR does not provide route anonymity protection. ASR follows hop-by-hop authentication so it generates high encryption cost.

F. SEAD [7] uses hop-by-hop encryption methods generate high cost. Because of hop-by-hop public-key encryption or complex encryption schemes.

G. In ZAP [8] redundant traffic-based methods generates very high overhead result to high cost. ZAP cannot provide source or routing anonymity.

H. In ALARM [9] offers source identity and location anonymity, destination identity anonymity. In ALARM using map construction malicious nodes can get destination node locations so it cannot provide destination location anonymity. ALARM does not provide the route anonymity.

I. Mix zones [11] are a zone-based location services. Mix zones achieve anonymous location service by hiding the positions of mobile node in a long period in order to avoid users' movement from being hacked.

J. Anonymous Location-based Efficient Routing protocol (ALERT) [10] to offer high anonymity protection at a low cost. It is not complete bulletproof to all attack.

III. LOCATION BASED SECURE ROUTING PROTOCOL IN MANETs

Network Model

Network models with various node movement patterns such as random way point model and group mobility model. Geographic routing is employed for node communication where MANET deployed in an exceedingly large field so decreases the communication latency. The attackers are often battery steam powered nodes that passively receive network packets and discover activities in their locally. The powerful nodes are act as legal nodes and keep on transmitting packets to the network. Those powerful nodes are regular with the analytical results from their overheard packets.

Dynamic Pseudonym and Location Service

In MANETs, nodes need to retrieves their location information using location server to choose sender and receiver so each node must built in with GPS. Every mobile nodes should contain mobility process in the network. Firstly, find the neighbor location nodes to forward the data from sender to receiver. The nodes are having unique MAC address and time stamp. We are implementing hash technique called MD5[12] Algorithm after finding location. The sender node wants to be sending the information to receiver. Computation complexity can be increased by using randomization for the time stamps. All nodes uses public and private key in this MANET. The secure communication path is established using public key and secure communication by a symmetric key Ks. In geographic routing, a node uses the destination location to find the next hop. Specifically, location service is provided by dedicated location severs or legal normal nodes.

Modified ALERT algorithm

It uses GPS location server to get zone location information and assume entire network area in terms of zone and divides zones dynamically using zone partition algorithm in order to place sender and the receiver into different zone so we can achieve high anonymity protection level and choose relay nodes randomly in other zone which in term form anonymous route and encrypting real identities of sender and receiver, zone position of receiver to provide sender and receiver anonymity. Multicasting mechanism is used to achieve better packet delivery ratio, anonymity protection level. Timing analysis is provided using 'notify and go' lightweight mechanism and multicasting and local broadcasting mechanism is used to avoid counter intersection attack. Uses the GPSR[3] algorithm to send the information to relay node.

Packet Form of Location Based Secure Routing Protocol in MANETs:

Each packet has following information to guaranteed communication between sender and receiver in network

1. The total number of partitioned zone.
2. Encrypted position of zone information
3. The current randomly chosen relay nodes for routing.
4. A bit 0 or 1 is chosen by each Random forwarder in order to partitioning the zones.
5. Group signature.

System architecture

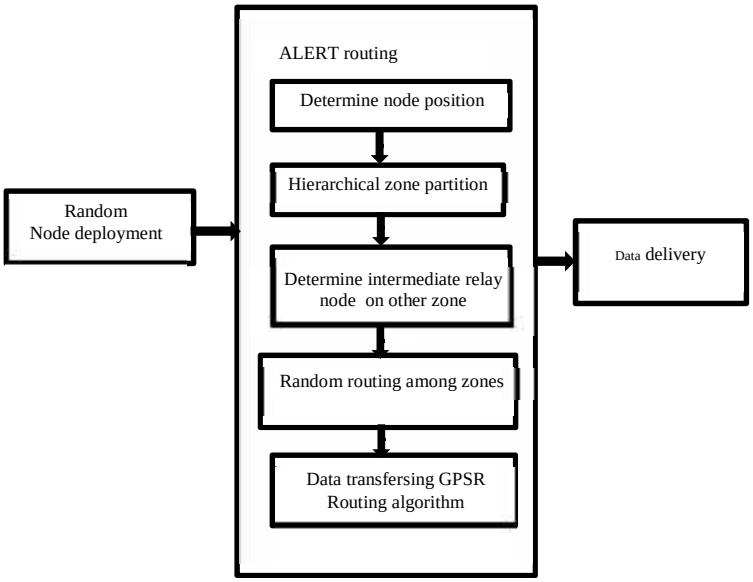


Fig.1. location based secure routing in MANETs

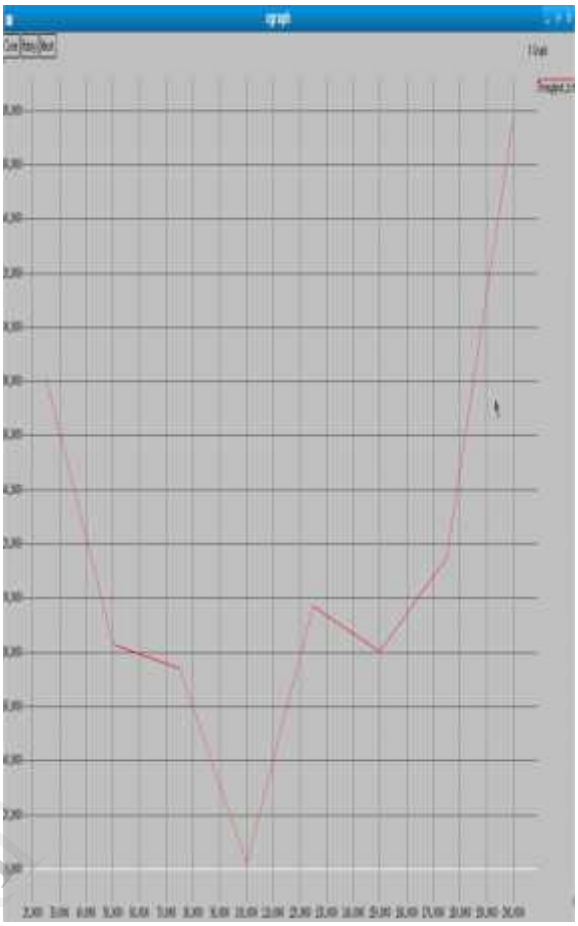
I. PERFORMANCE EVALUATION

The simulations were carried out on NS-2.33 simulator using 802.11 as the MAC protocol with a standard wireless transmission range of 250m and UDP/CBR traffic with a packet size of 512 bytes. The network area in our experiment was set to 2000m X 2000m with 100 nodes moving at a speed of 2m/s. The total number of nodes was set to 25,50,100,175,200 nodes. The simulation duration was set to 50s.

The Parameters considered are,

1. Total number of actual participating nodes in routing to evaluate the ability of randomized routing.
2. Packet delivery ratio - This metric shows number of packets successfully reach to destination.
3. Energy consumption of protocol over simulation time.

Fig. 2 shows the number of actual participating nodes in location based secure routing protocol with 50, 100 ,175 , 200 moving at a speed of 2m/s. Location based secure routing protocol generates more number of actual participating nodes during node communication.



ted

Fig.2. The total number packets transmit

Fig 3 shows Location based secure routing protocol packet delivery ratio increases due to multicasting in a final process.

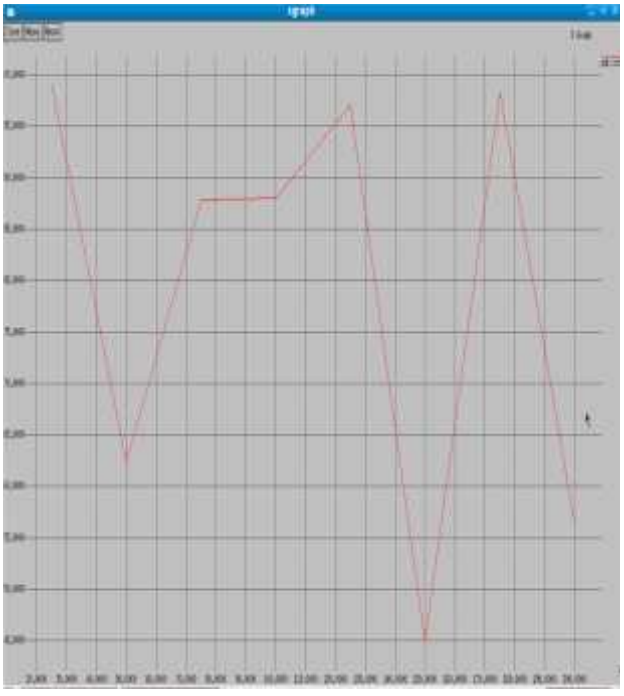


Fig.3.Packet delivery ratio.

Fig.4. shows energy consumption of nodes in location based secure routing protocol.

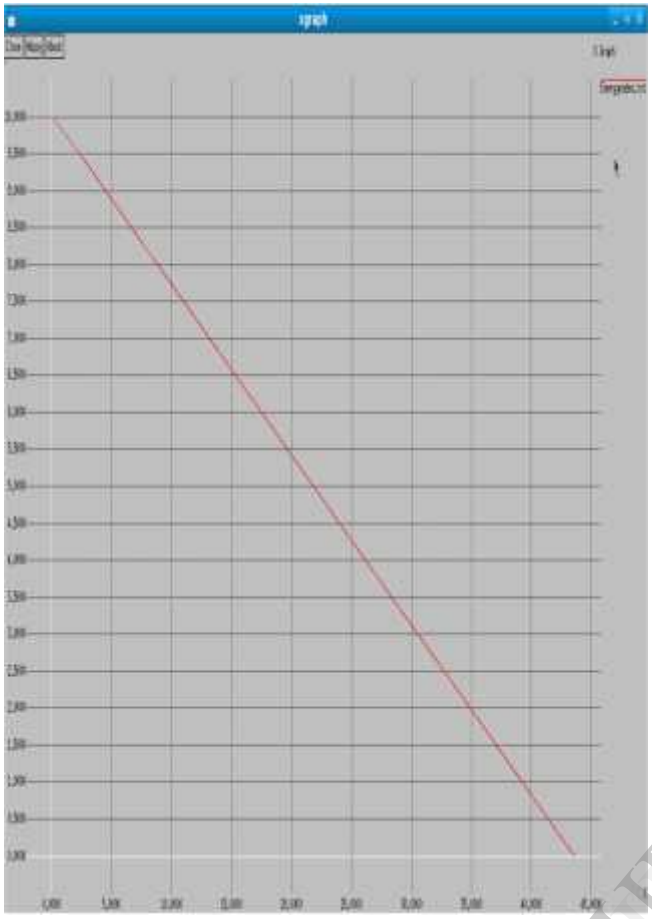


Fig.4.Energy consumption in routing

II. CONCLUSION

Location based secure routing protocol in MANETs is to give anonymity protection to the sender, receiver and routes with low cost. It can prevent some active attacks such as Sybil attacks using MD5 algorithm but it is not bullet proof to all active attacks. It has the "notify and go" lightweight mechanism to avoid timing analysis attacks and use multicasting and local broadcasting to avoid counter intersection attack. Additionally, multicasting mechanism is used in destination zone to achieve better anonymity protection and packet delivery ratio. Future work analyzing the anonymity level at receiver, routing efficiency.

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Mrs. Sindhuja, Assistant Professor, The Oxford College of Engineering, Bangalore, for her exemplary guidance, and constant encouragement throughout.

REFERENCES

[1] .A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31," technical report, 2005.
[2] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003
[3] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.
[4] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.
[5] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.
[6] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.
[7] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.
[8] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.
[9] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.
[10] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.
[11] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW), 2004.
[12] Hash functions: Theory, attacks, and applications Ilya Mironov Microsoft Research, Silicon Valley Campus November 14, 2005

BIOGRAPHY

Deepa k c is currently Pursuing Master of Technology in Computer Network Engineering from the Oxford college of Engineering under Visvesvaraya Technology University (VTU), India and has received BE degree in information science and engineering from VTU University, Bangalore, in 2012. Her research interests are Computer Networks (wireless Networks), security etc. she is a student of the 2nd year mtech, Dept of ISE, the oxford college of engineering, Bangalore, Karnataka, India.

Sindhuja is an Asst professor working in TOCE Bangalore . She has an M.Tech in information technology with specialization in networking in VIT university. Her areas of interest include routing & network security.