ijecs
open access
www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 10, October 2014 Page No. 8519-8522

Improved Routing Performance in MANET Using Anonymity Algorithm

Ms. Kanchan P.Kamdi , Mr. Rahul Dhuture, Mr. G. Rajesh Babu

(Student TGPCET Nagpur)
Department of Computer Science & Engineering Tulsiramji Gaikwakd –Patil college of Engineering & technology mohgaon wardha road Nagpur,
Maharashtra,India
kanchan.kamdi@gmail.com
(Assistant Professor TGPCET Nagpur)
Department of Computer Science & Engineering Tulsiramji Gaikwakd –Patil college of Engineering & technology mohgaon wardha road Nagpur,
Maharashtra,India
rmdhuture@gmail.com
(Assistant Professor TGPCET Nagpur)
Department of Computer Science & Engineering Tulsiramji Gaikwakd –Patil college of Engineering & technology mohgaon wardha road Nagpur,
Maharashtra,India
grajeshbabu.37@gmail.com

ABSTRACT - MANET is a type of wireless ad-hoc network that usually has a routable networking environment. Mobile Ad Hoc Networks use unidentified routing protocols that hide node identities and routes from outside observers to provide anonymity protection. Our existing anonymous routing protocols depending on either hop-by-hop encryption, redundant traffic either produce high cost or it cannot provide privacy protection to data sources, destinations, and routes. We propose a new location based routing protocol which offers high privacy protection at low cost to sources, destinations, and routes. It also has approaches to effectively counter intersection and timing attacks. The proposed plan ensures the privacy of both route and nodes which westudy and simulate the result. This existing protocol achieves better route privacy protection and its lower cost compared to other unidentified routing protocols, and also improving the routing efficiency compared to other geographical routing protocol.

Index Terms - *Manets, privacy, routing protocol, geographical routing*

I. INTRODUCTION

A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers (an associated hosts) connected by wireless links - the union of which forms an arbitrary graph Mobile Ad Hoc Networks feature self-organizing and independent infrastructures, which make them an ideal choice for military uses such as communication and information sharing in battlefields. However, the innate on-air nature of MANETs makes them vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. MANET routing focused on security issues, less attention has been devoted to privacy. Privacy doesnot mean confidentiality of communication (i.e., data)among MANET nodes.

Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity.

Identity and location anonymity of sources and destinations means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations. For route anonymity, it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped .

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Most of the current approaches are limited by focusing on enforcing privacy at a high cost to existing resources because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned privacy protections. For example, existing ALARM cannot protect the location privacy of source and destination. SDDR protocol cannot provide route privacy, and ZAP protocol only focuses on destination privacy. Many privacy routing algorithms are based on the geographic routing protocol .

To provide high privacy protection for sources, destination, and route with low cost .We propose an Anonymous Location-based Routing protocol. These routing protocol dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable unknown route. Specifically, in each routing step, a data sender partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR [15] algorithm to send the data to the relay node. In the last step, the data is broadcasted to k

nodes in the destination zone, providing k-privacy to the destination. It also has a strategy to hide the data sender among a number of senders to strengthen the privacy protection of the source. The proposed routing protocol is also resilient to intersection attacks and timing attacks .

We theoretically analyzed proposed system in terms of privacy and efficiency. We also try to do experiments to evaluate the performance of proposed system in comparison with other privacy and geographic routing protocols.

II. RELATED WORK

.

K.E. Defrawy ,G. Tsudik [2] proposes on privacy aspects of mobility. Unlike most networks, where communication is based on long-term identities (addresses), we argue that the location centric communication paradigm is better-suited for privacy in suspicious MANETs.

Karim El Defrawy and Gene Tsudik [3] proposes the ALARM framework which supports anonymous location-based routing in certain types of suspicious MANETS ALARM relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations.They show through simulation that node privacy under this framework is preserved even if a portion of the nodes are stationary, or if the speed of movement is not very high.

V. Pathak, D. Yao, and L. Iftode [4] proposes the design of the GSPR secure geographic routing protocol. The overhead of location authentication is investigated under various scenarios through network simulation. Results show that although the presence of malicious nodes increases the routing path length, a data delivery rate of larger than 80% is sustained even if 40% of the nodes are malicious.

Sk.Md.M. Rahman, M. Mambo [5] proposes a new position-based routing protocol which keeps routing nodes anonymous, thereby preventing possible traffic analysis. Time variant Temporary Identifier Temp ID is computed from time and position of a node and used for keeping the node anonymous. Only the position of a destination node is required for the route discovery, and Temp ID is used for establishing the route for sending data: a receiver hand shake scheme is designed for determining the next hop on-demand with use of the Temp ID. hey evaluate the level of anonymity and performance of proposed scheme.Also they clarified the achievement of anonymity and security

Z. Zhi and Y.K. Choong [6] proposes to preserve location privacy based on the idea of dissociating user's location information with its identity.They also propose an anonymous geographic routing algorithm which includes three components to avoid the explicit exposure of identity and location in communication without compromising the efficiency guaranteed by geographic routing.

III. PROPOSED METHODOLOGY

A. Network Models

We use two different network models, random way point model and group mobility model. With the random way point model as the default setting, we also compare the performance of anonymous based routing protocol in the group mobility model. In the group mobility model, we set the movement range of each group to 150 m with 10 groups and to 200 m with five groups .

B. Dynamic Pseudonym and Parameter Testing:

The tests were carried out on network simulator using 802.11 as the MAC protocol with a standard wireless transmission range of 250 m and UDP/CBR traffic with a packet size of 512 bytes. The test field in our experiment was set to a1000 m1000 m area with 200 nodes moving at a speed of 2 m/s, unless otherwise specified. The density was set to 50, 100, 150, and 200 nodes per square meters. The duration of each simulation was set to 100 s unless otherwise indicated.

C. Actual Participating Nodes

The cumulated actual participating nodes in proposed anonymous location based routing protocol, GPSR, ALARM, and AO2P, with 100 and 200 nodes moving at a speed of 2 m/s, respectively. Since ALARM and AO2P are similar to GPSR in the routing scheme and thus have similar number of actual participating nodes, we use GPSR to also represent ALARM and AO2P in discussing the performance difference between them and proposed routing protocol.

D. The Destination Anonymity Protection:

The number of remaining nodes with partitions and a 2 m/s node moving speed when the node density equals 100, 150, and 200, respectively. The figure shows that the number of remaining nodes increases as node density grows while it decreases as time goes on.

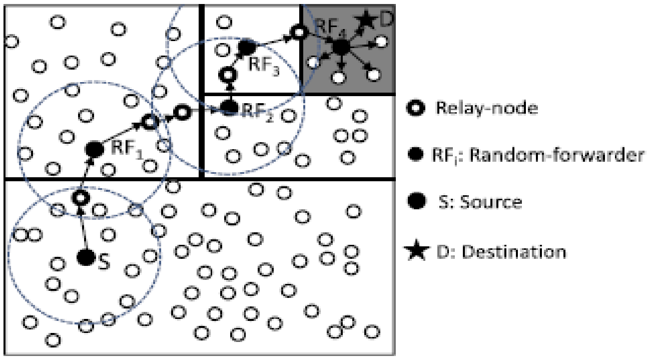

Figure. 1 Routing among the zones.

E. Routing Performance:

The routing performance of Anonymous location based routing protocol compared with GPSR, AO2P, and ALARM in terms of latency, number of hops per packet, and delivery rate. We also conducted tests with and without destination update in location service to show the routing performance of different methods as shown in fig below which shows the actual packet delivery ratio in %. We are trying to improve the packet delivery ratio to 98% to 100%.

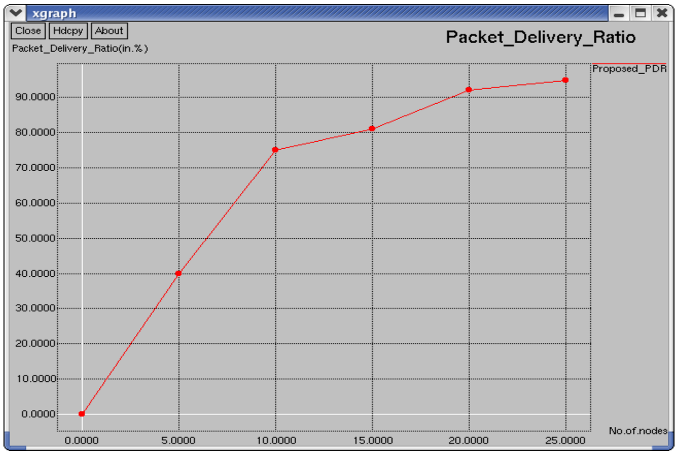

Fig. 2 Packet Delivery Ratio

IV.IMPLIMENTATION

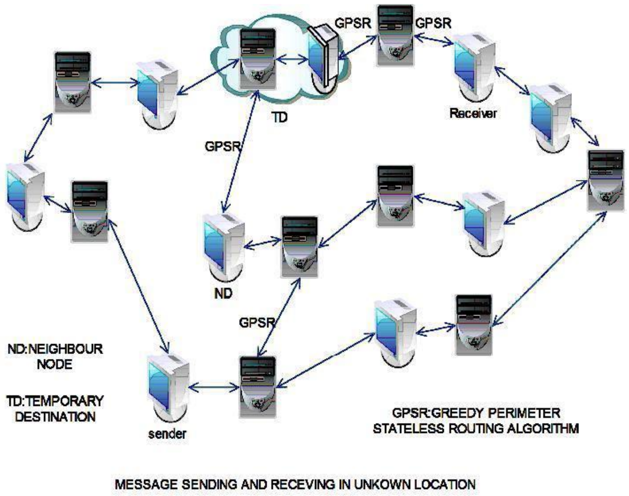
GPSR
GPSR
TD
Receiver
GPSR
ND
GPSR
ND:NEIGHBOUR NODE
TD:TEMPORARY DESTINATION
sender
GPSR:GREEDY PERIMETER STATELESS ROUTING ALGORITHM
MESSAGE SENDING AND RECEVING IN UNKOWN LOCATION

Fig 3 General Architecture of creating temporary destination nodes

The main idea behind the project is to provide destination anonymity protection from outsider attracters. By introducing temporary destination in the network to change the attention of the malicious node. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide un traceability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity. In this work, the attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. the assumption below apply to both inside and outside attackers.

In capabilities Their computing resources are not unlimited; thus, both symmetric and public/private key cannot be brutally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers. In this design, the tradeoff is the anonymity protection degree and transmission delay. A larger number of hierarchies generate more routing hops, which increases anonymity degree but also increases the delay.

After performing parameter testing with respect to some factors the packets are transmitting to the destination through GPSR algorithm which is a shortest path algorithms which allows nodes to figure out who its closest neighbors that node are also close to the final destination node that node is selected for the packets transmission between source and destination

A. Simulation performance

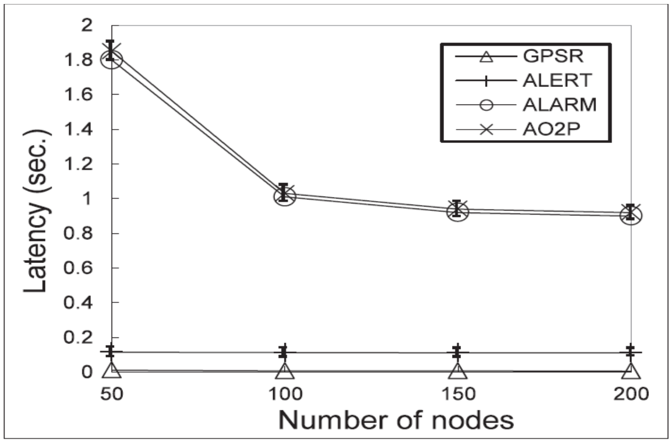

Fig 4 Latency of different nods.

The above Fig.4 shows presents the latency per packet versus the total number of nodes (i.e., node density). Recall that ALERT does not take the shortest path in routing, while ALARM and AO2P take the shortest path in routing. It is intriguing to see that the latency of ALERT is much lower than ALARM and AO2P. This is caused by the time cost of encryption. ALERT is based on symmetric key encryption for packets, which takes shorter time than the public key encryption used in ALARM and AO2P. Also, ALERT encrypts packets once, while AO2P needs to encrypt packets in each hop in routing and ALARM needs to periodically authenticate neighbors. In ALARM and AO2P, the latency caused by the public key cryptography outweighs the benefit of short latency using the shortest path. Therefore, even though ALERT generates more routing hops than AO2P and ALARM.

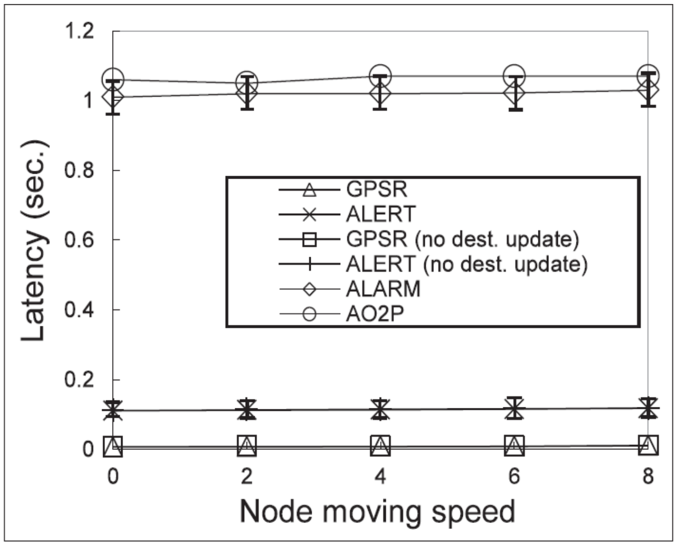

Fig 5: Different node moving speed

Fig.5 shows the latency versus node moving speed varied from 2 to 8 m/s. We can also observe that AO2P generates marginally higher latency than ALARM, both of them produce dramatically higher latency than GPSR and ALERT, and ALERT produces slightly higher latency than GPSR due to the same reasons in Fig. 14a. When with destination update, experimental data indicate GPSR and ALERT have relatively stable latency with respect to node moving speed. This is because the destination node location can always be updated in time, so the routing path is always the shortest regardless of the moving speed. When without destination update, the experimental results shows that GPSR increases from 7 to 11 ms and ALERT increases from 11 to 12 ms though the phenomenon is not obvious in the figure. When a forwarding node fails to forward a message to the destination, it continues to forward the packet to other nodes until the path length reaches the TTL ¼ 10. Thus, the number of hops in a route increases, leading to longer routing latency.

V. CONCLUSION:

Existing anonymous routing protocols, depending on either hop-by-hop encryption or redundant traffic, it produces high cost. And also, some routing protocols are unable to provide complete source, destination, and route privacy protection. Proposed anonymous location based routing protocol is distinguished by its low cost and privacy protection for sources, destinations, and routes. Also we will try to improve the packet loss ratio to 98%.

REFERENCES

[1] Location-Based Efficient Routing Protocol in MANETs"IEEE Transaction on mobile computing Vol. 12,No.6,June 2013.

[2] HaiyingShen, Lianyu Zhao, "ALERT: A Anonymous K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.

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

[4] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

[5] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.

[6] 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.

[7] 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.

[8] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[9] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.