Enhancing Protection In Route Anonymity In Manets Using Dyanamic Patition Technique

Ramya J, Nithya TM, Amudha L
Asst.prof, HOD, Asst.prof
Dept. of CSE, K. Ramakrishnan College of engineering, Trichy

***Abstract* – The increase in the development of MANET has been used in various fields such as military,education etc.,The nodes in the manets are Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes such that the observers are protected from anonymity. Anonymity in MANETs includes identity and location anonymity of data sources as well as route anonymity.However, anonymous routing protocols which are used earlier are based on either hop-by-hop encryption or redundant traffic,which leads to high cost or cannot provide full anonymity protection to data sources, destinations, and routes. MANET security is the major concern for the protected communication.Providing anonymity to the routes, source and destination is a major challenge, Therefore, a method to offer high anonymity protection at a low cost is proposed ,which is called Anonymous Location-based Efficient Routing protocol (ALERT). ALERT dynamically partitions the network field into zones and it will randomly choose the corresponding nodes in the zones as intermediate relay nodes, which in turn it forms a non-traceable anonymous route. In addition to this , it also hides the data from sender or receiver among many people to strengthen source and destination anonymity protection. Here the NDP protocol is used along with ALERT protocol for transferring the data between clusters. We theoretically analyze NDP in terms of anonymity and efficiency. The ALERT protocol tolerates this process with low cost Energy Efficient Routing Protocol (EERP) algorithm and uses clustering method to transfer the information between several clusters.**

***Keywords* - Mobile Adhoc networks, anonymous, clusters, NDP, ALERT, EERP**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose".

Further, the recent increasing growth of multimedia applications (e.g., video transmission) imposes higher requirement of routing efficiency. However, existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs. In a MANET employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations.

Contributions

C.-C. Chou [1] et al has proposed a method named Routing. It has been analyzed and then the construction of anonymous protection of route, source and destination node in mobile Adhoc network. Decentralized profiles are created based on the profiles of the co-located users[12].

A framework is proposed by the following steps

ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node

It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions.

1. *Anonymous routing:* ALERT provides route anonymity, identity, and location anonymity of source and destination.
2. *Low cost:* Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.
3. *Resilience to intersection attacks and timing attacks:*
   ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue. ALERT can also avoid timing attacks because of its non-fixed routing paths for a source destination pair.
4. *Extensive simulations:* comprehensive experiments to evaluate ALERT's performance in comparison with other anonymous protocols.

ALERT generates a slightly longer latency than GPSR. ALERT does not aim to find a shortest route. Instead, it deliberately chooses a number of RFs to provide routing anonymity.

II. LITERATURE SURVEY

C.-C. Chou, D.S.L. Wei [1] has proposed a The network topology in a MANET usually changes with time. The routers are free to move randomly and organize themselves arbitrarily and thus the wireless topology of the network may change rapidly and unpredictably. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Anonymity may not be a requirement in civil oriented applications but it is critical in military applications. 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 and destinations, as well as route anonymity.

K.E. Defrawy and G. Tsudik [3] et al. have proposed Most of the routing protocols in MANETs have been designed using a single-interface single-channel (SISC) approach. In this approach, a single-interface and single-channel is commonly used for both incoming and outgoing traffic between nodes along the path. This leads the bandwidth contention and throughput degradation issues. These issues can be tackled by using multi-interface multi-channel (MIMC) approach. In mobile wireless networks, communication typically takes place over time-varying channels. This time-variation or fading is due to several effects such as variations in multi-path interference and shadowing.

Sk.Md.M. Rahman [6] et al. have provided an input to targeted advertising, profiling social network users becomes an important source of revenue. Its natural reliance on personal information introduces a trade-off between user privacy and incentives of participation for businesses and geosocial network providers. Location centric profiles (LCPs), aggregates built over the profiles of users present at a given location. PROFILR is introduced, a suite of mechanisms that construct LCPs in a private and correct manner. It has been combined with iSafe, a novel approach for context aware public safety application. Participating venue owners need to deploy an inexpensive device inside their business, allowing them to perform LCP related activities and verify the physical presence of participating users. PROFILR with the notion of snapshot LCPs is extended and communicated over ad hoc wireless connections. They don't concentrate on geo-social networks. A large number of fake, Sybil accounts cannot be controlled.

COMPARISION WITH OTHER PROTOCOLS

The existing routing protocols such as "*Anonymous location-based aided routing in suspicious MANET's (ALARM)"* provides only route anonymity and it cannot protect location anonymity of source and destination and *"Secure dynamic distribution routing algorithm (SDDR)"* cannot provide the route anonymity, Similarly "*Zone announcement protocol (ZAP)"* focuses on destination anonymity only, but our proposed ALERT systems provides identity and location anonymity of source, destination as well as routes. Following table 1 shows the Existing anonymous routing protocol.

Table1. Summary of existing anonymous routing protocols.

Name of the protocol	Identity anonymity	Location anonymity	Route anonymity
MASK[23]	Source	N/A	Yes
ANODR[24]	Source, destination	N/A	Yes
AO2P[11]	source, destination	Source, destination.	No
PRISM[5]	Source, destination	Source, destination.	No
ALARM[4]	Source, destination	No	Yes
ZAP[7]	Destination	Destination	No

III. PROPOSED WORK

A. Overall Architecture Diagram

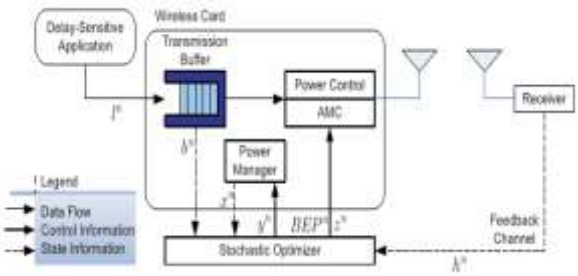

Fig1. Overall Architecture Diagram

B. Concepts Involved

1) Mobile Adhoc Networks

An Anonymous Location-Based Efficient Routing algorithm has been used to find the anonymity from the MANETs. Anonymity node may be drop the data during data transmission from the source to destination. So it cannot receive all data. This

is the major problem of communication between nodes. Anonymous Location.ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue.

2) Zone partitions

It first checks whether itself and destination are in the same zone. The node repeats this process until itself and ZD are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF).

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. ALERT makes the route between a S-D pair difficult to discover by randomly and dynamically selecting the relay nodes. The resultant different routes for transmissions between a given S-D pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes due to the random selection of RFs during the transmission of each packet. Even if an adversary detects all the nodes along a route once, this detection does not help it in finding the routes for subsequent transmissions between the same S-D pair.

IV. RESULTS AND FINDINGS

In the Location centric profiles, we focused on a single profile dimension, *D*.

A. The entire network is considered as a rectangle area in which nodes are randomly spreaded.

B. The network consists of intermediate relay nodes.

C. Hierarchical zone partition splits an entire network into the smallest zones in an alternating horizontal and vertical manner.

D. Data source S first horizontally divides the area into two equal size zones, ie, A1 and A2.S then randomly selects the first Temporary destination TD1 in zone A1 where Z_D resides.

Results

I) Sender partitions the network field in order to itself and destination into two zones.

II) Randomly chooses a node in other zone as relay node is called as Route Forwarder.

III) Hierarchical zone partition splits an entire network into the smallest zones in an alternating horizontal and vertical manner.

IV) S then randomly selects the first Temporary destination TD1 in zone A1 where Z_D resides.

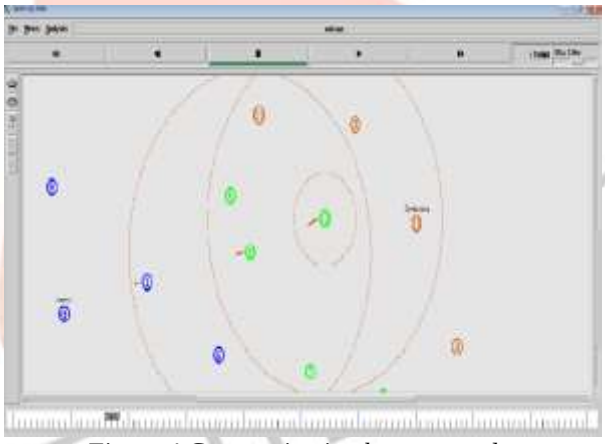

Figure.4 Communication between nodes

V) After RF1 receives packet, it vertically divides A1 into two regions as B1 and B2. ALERT aims at achieving k-anonymity for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in ZD, providing k-anonymity to the destination. Zone position refers to the upper left and bottom-right coordinates of a zone.

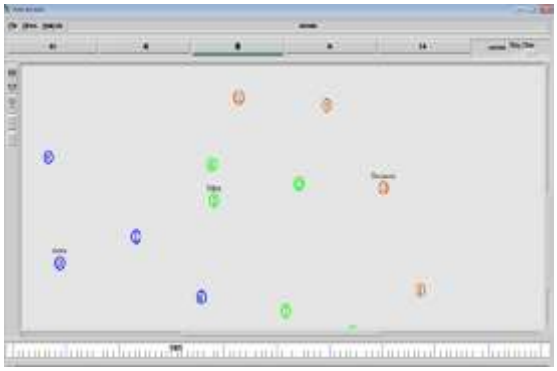

Figure.5 Failure node is detected

VI) The selection of second route

Figure.6 Second route is selected

VII) The provider has to register the personal and professional details to the server and also their services along with the geo-tagged location information. The sender and receiver needs to know about the secret key though which they are going to share the location data. It is of 16-bit secret key which is known to both sender and receiver

Figure.7 Failure node detection

VIII) User1 and User2 exchange their secrets, User1 generates Location to an Encrypted Index (L2I) and index to the encrypted location data from her review of the restaurant.

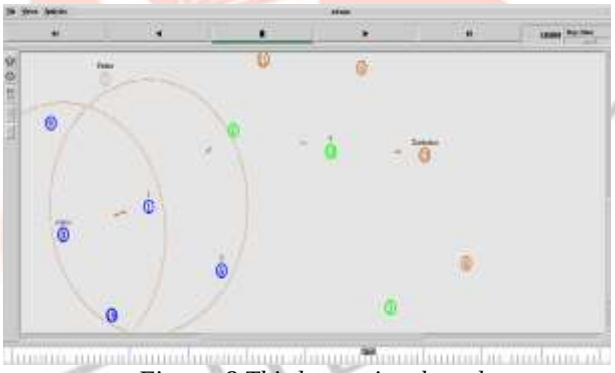

Figure. 8 Third route is selected

IX) Thus, Encryption is performed for sharing the location data and messages

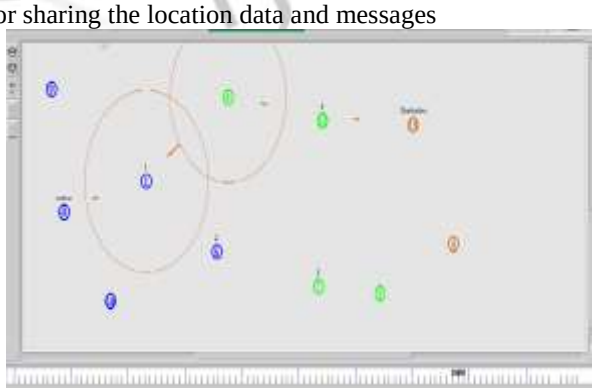

Figure.9 Failure node is used again in MANET

V. CONCLUSION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost.The some existing protocols provide protection to only source and destination locations or to only route locations. Our proposed protocol provides security in terms of location and identity anonymity to source, destination as well as routes. Since ALERT uses dynamic partition and random selection of nodes it establishes a dynamic routing path for different packet transmissions. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. In addition, ALERT and NDP has an efficient solution to counter intersection attacks. The these protocol tolerates this process with low cost Energy Efficient Routing Protocol (EERP) algorithm and uses clustering method to transfer the information between several clusters..Its ability to fight against timing attacks.ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination.

REFERENCES

[1] 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. 2013.
[2]"KeLiu'sNS2Code,"http://www.cs.binghamton.edu/~kliu/research/ns2code/index.html, 2012.
[3] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.
[4] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.
[5] R.Saravanan, V.Kowsalya "High anonymity protection at a High cost in MANETs" Volume 3, Issue 1, January 2012.
[6] 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.
[7] 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.
[8] 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.
[9] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2010.
[10] 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.
[11] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.
[12] Debian Administration, http://www.debian-administration.org/ users/dkg/weblog/48, 2012.
[13] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles," Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006
.[14] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003.
[15] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.