International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

# Anonymous Zone Based Multicast Routing Protocol For Manets

Mr. Sankusu Sharma
Dept. of Computer Engineering
Vidyalankar Institute of Technology
Mumbai, India

Prof. Rinku Shah
Dept. of Computer Engineering
Vidyalankar Institute of Technology
Mumbai, India

***Abstract*—Maintaining anonymity has become an increasingly important issue with the wide use of mobile devices in MANETs. Existing routing protocols based on hop-by-hop encryption or local broadcasting either generate high costs or does not fulfill anonymity requirements of the system. A zone-partitioning based routing protocol known as Anonymous Location-based Efficient Routing proTocol (ALERT), offers to protect both source, destination as well as routing path anonymity at comparatively lower costs. The proposed Anonymous Zone based Multicast Routing Protocol incorporates further enhancements in the existing ALERT protocol and guarantees higher source anonymity. The proposed idea is to hide the source node among its neighbors by Multicasting the packets inside the source-zone, to cover the traffic of the source node. Multicasting packets a number of times within the source zone will help to protect the source node's identity from its compromised neighbors. This mechanism removes the overhead of "Notify and Go" mechanism used in the existing system and makes the system more secure and useful in the real world scenarios.**

***Keywords*—Mobile ad hoc networks; MANETs; anonymity; routing protocol; Zone-based routing; Multicasting; Zone-based Routing.**

## I. INTRODUCTION

Due to the fast developments in mobile ad hoc networks (MANETs), anonymity has become an important issue. Anonymity can be achieved by hiding the identities of data sources, destinations or routing paths. Current anonymous routing methods can be generally classified into three categories: hop-by-hop encryption, which uses asymmetric key or symmetric key to ensure anonymity, but leads to high computing time; local broadcasting, which is also performed at each hop to hide the routing path or source/destination, but consumes much extra hops and causes large energy consumption; anonymity zones, which is similar to local broadcasting, but it is performed in destination to maintain the anonymity of destination.

The proposed Anonymous Zone based Multicast Routing Protocol is based on a low-cost Anonymous Location-based Routing proTocol (ALERT) [1], which provides source node, destination node as well as routing path anonymity. Compared to other existing approaches, ALERT costs less computing energy and time because of the greatly reduced encryption/decryption needs by using Symmetric Encryption instead of Asymmetric Encryption. In addition, the protocol reduces the cost incurred due to broadcasting. ALERT uses geographic routing in every step of our routing process. Moreover, hierarchical zones are dynamically generated and a node is randomly chosen within a zone as a relay node to provide the anonymity.

Alert is more cost efficient with respect to other routing mechanisms. The unique idea of zone partitioning in ALERT, makes the routing path nearly unpredictable to the outside observer, which is the greatest advantage of this system.

## II. EXISTING SYSTEM

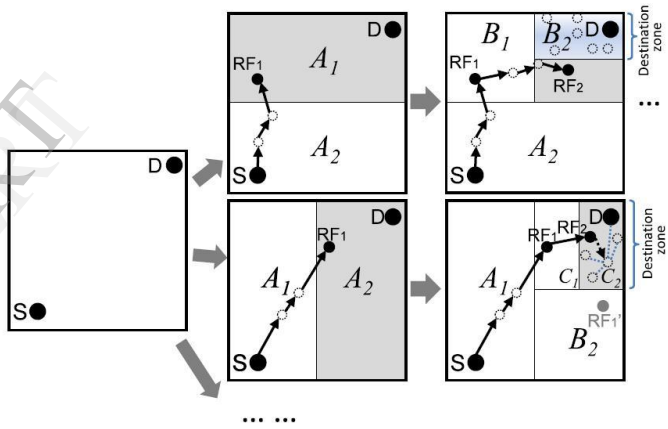


Fig. 1. ALERT Routing Algorithm [1]

For the ease of illustration, the entire network area can be assumed to be a rectangle, in which nodes are randomly distributed. The information of the bottom-right and upper left boundary of the network area is configured into each node when it enters the system. This enables a node to locate the positions of nodes in the entire area for zone partitions.

Consider the upper part in Fig. 1, the given area is horizontally partitioned to form two zones A1 and A2. Zone A1 is further partitioned vertically into zones B1 and B2. Similarly, zone B2 is horizontally partition into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. This partition process is called as hierarchical zone partition.

Using the hierarchical zone partition and randomly choosing an intermediate relay node in the partitioned zone in each step, ALERT generates a dynamic unpredictable routing path for a message. The zone with 'k' nodes, where destination node D resides is known as the destination zone, denoted by $Z_D$. k is used to control the degree of anonymity protection [10] for the destination node.

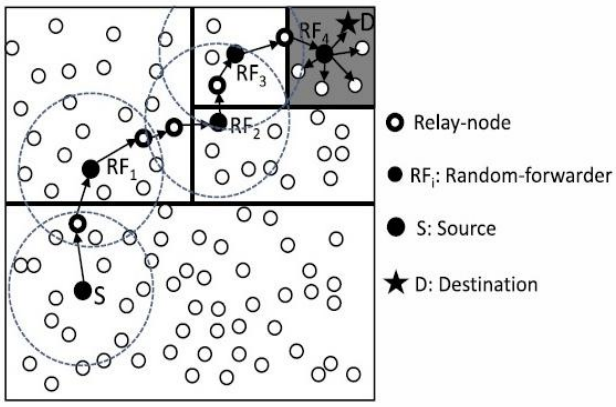


Fig. 2. Routing among zones in ALERT [1]

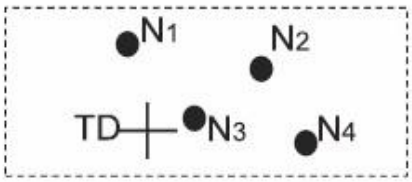


Fig. 3. Choosing a RF according to TD [1]

In ALERT, each data source or forwarder executes the hierarchical zone partition. 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. The node repeats this process until itself and $Z_D$ are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR [16] protocol to send the data to the node closest to TD. This node is defined as a random forwarder (RF). In the last step, the data are broadcasted to k nodes in $Z_D$, providing k-anonymity [16] to the destination.

In ALERT, partitions are created in the alternative horizontal and vertical fashion, in order to ensure that a packet approaches D in each step. In this mechanism, a larger number of hierarchies generate more routing hops increasing the degree of anonymity but it also results in higher transmission delays. To ensure the delivery of packets, the destination acknowledges each packet received, to the source node. If the acknowledgement message is not received by the source within a predefined time period, it resends those packets.

## III. PROPERTY DISCUSSION

The following section discusses the properties as well as the problems with the existing ALERT protocol that can be exploited by the attacker.

### A. *Anonymity in Existing System*

*a) Routing Anonymity:* It ensures that identities of the nodes participating in routing remains unknown. ALERT dynamically splits zones into smaller ones to enable a message to approach the destination. The randomization feature of the routing path is maintained by randomly choosing random-forwarders for routing. Therefore, the path of data transmission is not fixed. Malicious attackers cannot find nodes responsible for routing, because every node in a zone has the chance to route data. Therefore, even when two nodes always transmit data, attackers still cannot find the routing path.

*b) Source Anonymity:* It is to hide source node's identity from any other nodes in the network. In ALERT, every source uses pseudonym as its identity which changes periodically. In addition, the source anonymity is ensured because the source does not embed its precise position in a message, but only the zone information in which it is located. Therefore, even if the attacker can intercept the messages, it cannot identify the position of the source.

*c) Destination Anonymity:* It is to ensure that destination is not known to any other nodes. Rather than specifying the location of the destination node, its vague location is specified as a zone. Since there are *k* nodes in the destination zone, the routing protocol with broadcasting at the last step achieves *k*-anonymity of the destination.

### B. *Problems with Existing System*

ALERT has a strategy to hide the source node among a number of other nodes using "Notify and Go" mechanism [1]. Its basic idea is to let a number of nodes send out packets at the same time as source node in order to hide the source packet among many other packets.

"Notify and go" has two phases: "notify" and "go." In the first "notify" phase, source piggybacks its data transmission notification with periodical update packets to notify its neighbour that it will send out a packet. The packet includes two random back-off time periods; 't' and '$t_0$'. In the "go" phase, source node and its neighbours wait for a certain period of randomly chosen time $\epsilon$ (t, t+$t_0$) before sending out messages. Source node's neighbours generate only several bytes of random data just in order to cover the traffic of the source. t should be a small value that does not affect the transmission latency. A long $t_0$ may lead to a long transmission delay while a short $t_0$ may result in interference due to many packets being sent out simultaneously. Thus, $t_0$ should be long enough to minimize interference and balance out the delay between source node and source node's farthest neighbour in order to prevent any intruder from discriminating source node.

In short, ALERT protocol has following drawbacks:

1. If the neighbouring node of the source is compromised, it can easily identify the source, using the "Notify" messages. This leads to easy detection of the source in the MANETs, thus compromising the entire system.
2. A proper Location Service is not defined in the existing ALERT Protocol.

## IV. PROPOSED SYSTEM

The proposed Anonymous Zone based Multicast Routing Protocol aims to improve the anonymity and efficiency of the existing ALERT Protocol. In the proposed system, the "Notify and Go" mechanism is eliminated, which might lead to the unintentional discovery of the source node from its compromised neighbors, using the "Notify" message.

Instead of "Notifying" each neighbor; the source node multicasts the packets inside the source zone. This multicasting is for selected few neighbours of the source node in the source zone. The selected number of neighbors can be less than or equal to 'n'. The neighbour of the source node also multicast the packet among their neighbours. This process continues till packets are forwarded to sufficient number of nodes to cover the traffic of the source node from the external adversary looking for the source node.'

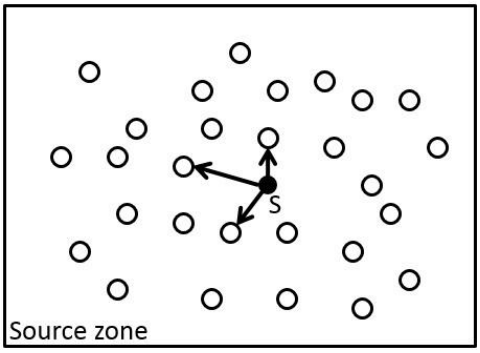


Fig. 4. Source Node multicasting to its n Neighbors

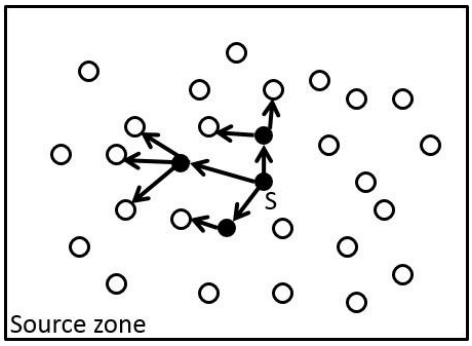


Fig. 5. Neighbors of Source Node multicasting to their Neighbors

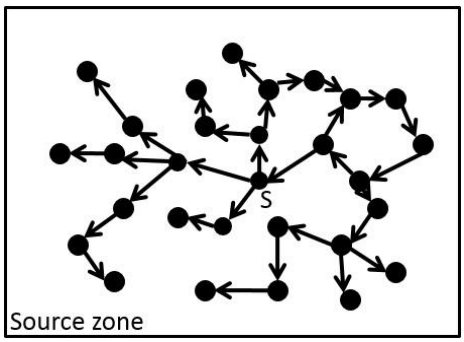


Fig. 6. Source zone after some time interval t

This approach has two advantages namely:

- It reduces the overhead of continuously "Notifying" the neighbors.
- Multicasting protects the source node's anonymity for the compromised neighbour node.

## V. EXPERIMENTAL DESIGN

The proposed protocol will be simulated on NS2.35 simulator under Linux environment. Messages will be randomly generated at the rate of 10 queries/second. The number of nodes will be set to 100, 200 and 400 in a field of 1000m×1000m. Zone will be partitioned into 6 sets in all tests. Simulation will be done at different network scales by varying the number of nodes, node velocity from 0-2m/s and transmission range at 100m.

Comparative analysis of proposed protocol and existing protocols like ALARM (Anonymous Location Aided Routing in Suspicious MANETs) [7] based on hop-by-hop encryption and AO2P (An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks) [8] based on redundant traffic models along with GPSR (Greedy Perimeter Stateless Routing) [16] (baseline protocol) will be done.

The performance of the proposed protocol will be judged on various network transmission parameters like number of participating nodes, number of random forwarders, number of hops/packet, latency/packet, delivery rate, etc.

## VI. CONCLUSION

In this paper, we proposed a low-cost routing protocol that provides efficient routing mechanism for MANETs using low cost Symmetric Cryptography and Zone based Multicasting. Since only zone information of the communicating nodes is embedded in the messages, their anonymity can be protected. Moreover, the use of hierarchical zones and randomly chosen relay nodes ensure an anonymous and random routing path. Also, removal of 'Notify and Go' mechanism protects the source from compromised neighbors.

Future works lies in more thorough simulation, and testing of this protocol under various scenarios and different network attacks. In addition, current method needs a proactive mechanism to better solve various kinds of network attacks.



## REFERENCES

[1] Haiying Shen, Member, Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions On Mobile Computing, Vol. 12, No. 6, June 2013.

[2] Lianyu Zhao, Haiying Shen, "ALERT: An Anonymous Location-based Efficient Routing Protocol in MANETs", 2011 International Conference on Parallel Processing.

[3] Md. Saidur Rahman, Saikat Mondal, Shushanto Kumar Ghosh, Md. Mahbubur Rahman, "A New Approach of Extendable Multicast Routing Protocol in Mobile Ad Hoc Networks", Proceedings of 13th International Conference on Computer and Information Technology (ICCIT 2010) 23-25 December, 2010, Dhaka, Bangladesh.

[4] Lianyu Zhao, Haiying Shen, "Low-cost Anonymous Routing Protocol in MANETs", 978-1-4244-4581-3/09, 2009 IEEE.

[5] 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.

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

[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] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), pp. 10-29, 2001.

[10] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertainty Fuzziness Knowledge-Based Systems, vol. 10, no. 5, pp. 557-570, 2002.

[11] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, "Analyzing the Energy Consumption of Security Protocols," Proc. Int'l Symp. Low Power Electronics and Design (ISLPED), 2003.

[12] 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.

[13] "Ke Liu's NS2 Code," http://www.cs.binghamton.edu/~kliu/research/ns2code/index.html, 2012.

[14] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012.

[15] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

[16] Brad Karp, H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", Mobicom 2000.

[17] 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.

[18] A. Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proc. Network and Distributed System Security Symp. (NDSS), 2001.