Enhancing Privacy Preservation using S-ALERT Protocol to Diminish Routing Attacks in MANETs

Pooja P. Borekar
Dept. of Computer Engineering Dr .D. Y. Patil SOET Pune,
Savitribai Phule Pune University
Maharashtra, India

Nilav Muhkerjee
Dept. of Computer Engineering Dr .D. Y. Patil SOET Pune,
Savitribai Phule Pune University
Maharashtra, India

ABSTRACT
An innominate communication method in MANETS is categorized into proactive method, re-active method and anonymous routing method. Re-active routing is further divided into two methods, which includes superfluous traffic and routing hop-by-hop encryption. Whereas MANETs has various choices in respect to anonymous routing protocols, to provide location innominate safety to information, source node and destination node. However, a previous innominate routing protocol fully depends on station by station encryption or superfluous traffic which generates a heavy cost and offer low anonymity protection. Hence to offer a very high innominate protection, S-ALERT is pro-posed. Basic idea behind S-ALERT is to divide the whole network into number of nodes and then allocate each node a unique Id, so that we can differentiate source node and destination node. Followed by dynamic partition of network into zones and then randomly choosing nodes in zones as random forwarder, which forms a non trace-able innominate route. Along with, it also hides the source/destination node among many source/destination, in order to give very high safety to source node and destination node. It is observed that S-ALERT gives better as compared to other protocols. Hence S-ALERT protocol achieves full anonymity protection and that to at very least cost.

General Terms
Dynamic Partitions, Anonymous Routing.

Keywords
Mobile-Ad-Network, Anonymity Routing Protocols, Zone Partitions, Geographical Routing.

1. INTRODUCTION
In the last 15-20 years, there is tremendous changes in Mobile Ad Hoc Networks (MANETs) have found various wireless applications, which are used in various areas of day to day life such as military, research, education, emergency services, and disaster relief and so on. MANET is self composing, self construct and infrastructure less network which consist of n number of mobile fork which does not consist of cables. In MANETs various nodes are connected without wires, node is laptops, mobile phones and many more. Here the framework is not fixed and changes as topology changes. MANETs is widely used today because it offers us with many features and overcome many of existing system problem. Main issue in MANETs is that the nodes are exposed to attacks and hence attacker can easily analyze data and traffic by intercepting or attacking routing protocol. Secure Ad Hoc network routing protocols comprises of two main problems, first that they are difficult to design and second that they are highly dynamic to Ad Hoc network. On other hand anonymous routing protocol are essential in MANETs for reliable communication there by keeping safe node identities and protecting them from various types of attacks. Anonymity includes location anonymity and route anonymity. Location anonymity means protecting location of source nodes, destination nodes as well as route anonymity. That means it will be very hard for other nodes as well as attackers to obtain original and exact information of source and destination nodes. In route anonymity it will be hard enough to trace the path carrying data from source node to destination node.

Anonymous routing provides secure and safe communication between two nodes in network by hiding nodes original information and prevents these nodes from traffic analysis attacks of adversaries. However, a previous innominate routing protocol fully depends on station by station encryption or superfluous traffic which generates a heavy cost and offer low anonymity protection. Hence to offer a very high innominate protection, S-ALERT is pro-posed. Basic idea behind S-ALERT is to divide the whole network into number of nodes and then allocate each node a unique Id, so that we can differentiate source and destination node. Followed by dynamic partition of network into zones and then randomly choosing nodes in zones as random forwarder, which forms a non trace-able innominate route. Along with, it also hides the source/destination node among many source/destination, in order to give very high safety to source node and destination node. Hence S-ALERT Protocol achieves full anonymity protection and that to at very least cost.

This paper is organized as follows: Section 2; is related work done. Section 3; describe existing anonymous routing protocol and its drawbacks, along with motivation and problem definition. Section 4; describes proposed S-ALERT protocol along with its four module explanations. Section 5, explains mathematical modeling. Section 6; summarizes the performance of protocol in comparison with other anonymous routing protocol along with few results. Section 7; states conclusion followed by acknowledgement and references.

2. RELATED WORK
Anonymous routing in MANETs is been studied in recent years. Due to its usage in various fields it can be classified into reactive routing and proactive routing [5]. There are various anonymous routing protocol [5], [10], [11]. Existing protocols are mainly of two types' step-by-step encryption and superfluous traffic [6], [8]. All this generate a huge cost and offer with low protection. An Anonymous on Demand Routing was designed to overcome the passive attacks. It is reactive routing and identify free routing scheme that means route is established only when needed. This protocol provides with node protection, route protection as well as location, but is robust against various attacks. Not suitable for real time application. Further innominate protocol is innominate safe scatter (ASR) [17] protocol ensures identity protection of source node destination node, and location privacy. But fails to provide route anonymity, means the path which carries data from source node to destination node can be attacked and data

can be leaked. Further An ad hoc on-demand position-based private routing (AO2P) [7] came which is reactive routing type protocol and based on hop-by-hop encryption, which offers location anonymity to source node, destination node and identity anonymity. It fails to provide route protection. PRISM [6] uses a location-centric, instead of an identity centric, communication paradigm. Therefore, it does not assume any knowledge of long-term node identifiers or public keys. PRISM requires neither pre-distributed pair wise shared secrets nor on-line servers of any kind. As an on-demand protocol, PRISM is also very different from ALARM [5], even though the latter uses group signatures and is also location centric [4]. ZAP [16] an anonymous rerouting protocol that adopts fuzzy positions to positions to create AZ for destination anonymity. In the AZ produce set of innominate, to protect original destination. In MANETs nodes are nothing but mobiles, and hence protection in protocols is dynamic, unlike the case of wired networks. Various protocol have introduced like PD-ZAP, G ZAP, and RR-ZAP protocols.

Anonymous Location Aided Routing (ALARM) [5], a proactive routing protocol was introduced to solve number of problems in MANET. ALARM [5] provides secure and smooth communication in both suspicious and hostile networks. Provide with just identity protection to source node and destination node along with location protection to just source node. With drawback that it won't provide route anonymity. Hence here we have survey that one or the other protocols provide with identity protection, location protection to source node, destination node and the route protection, none of the protocols provide all features together.

In response to provide high protection and that to at least cost we propose an Secure Anonymous Location based and Efficient Routing Protocol (S-ALERT) offers with both privacy and security features, including data integrity, anonymity, tracking-resistance and also offers protection against passive and active insider and outsider attacks. Basic idea behind ALERT is to dynamically partition the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. Along with, it also hides the initiator/receiver among many initiators/receivers so as to provide high anonymity protection to source and destination. In all Anonymous Location-based Efficient Routing protocol provide protection to sources, destinations, and routes.

3. EXISTING SYSTEM AND PROBLEM DEFINITION

Existing system mainly consist of ALARM protocol or ALS protocol or MASK. All the protocols specified consist of many drawbacks. It generates a huge traffic which leads to collision of data packets. Other can be loaded routing table and wastage of memory. Further all this problems came into picture and hence there was need to overcome these problems to provide with safe and smooth communication.

Drawbacks

- Previous anonymous routing methods produce a very high cost.
- Fails to provide full protection to source node, destination node, data and routes carrying data.

3.1 Motivation

Consider a situation where MANET is used in battlefield. By studying the traffic patterns, enemies can get the original message transmitted which will lead to attacks on our solider by knowing their exact location, even getting the entire message being transmitted/ blocked and attack on commander nodes. Also preventing communication from malicious entities and eavesdropping. Hence we must come up with system that provides secure communication by hiding node identities and preventing traffic analysis attacks from outside observers in MANET.

Hence S-ALERT is used which has various strategy to hide data initiator among a number of initiators to strengthen the anonymity protection of the source. S-ALERT offers with both privacy and security features, including data integrity, anonymity, tracking-resistance and also offers protection against passive and active insider and outsider attacks.

3.2 Problem Statement

Existing innominate routing protocols generate\ high cost. It fails to offer full safety to source node, destination node and the path which carry data packets. This previous approaches had many drawbacks and are not feasible for various technology. Hence S-ALERT is been proposed which overcome all the limitation and aims to provide full anonymity to each factors.

Anonymous Location based Efficient Routing protocol is proposed which offers

- Great innominate safety at a low cost,
- Innominate safety to source node, destination node, and routes,
- Plan to easily overcome intersection and timing attacks.

4. PROPOSED SYSTEM

Main contribution in existing system is to offer with anonymity protection and to come up with strategy for timing and intersection attacks. And there by making a smooth and safe communication between source node and destination node. Here we came up with new anonymous routing protocol, which have good performance results with respect to other anonymous routing protocols. Hence the protocol proposed is S-ALERT.

4.1 S–ALERT Routing

In order to offer high innonimate protection (to source nodes, destination nodes, and route) that to with low cost, we came with new and efficient protocol name as Secure Anonymous Location-based and Efficient Routing protocol (S-ALERT). Basic and short idea behind S-ALERT is that it first, dynamically partitions a whole network into number of zones which is called as zone partitions and then randomly selects nodes in zones as intermediate relay nodes, to form a path which is non-traceable anonymous route. Second, in each routing step, sender or data forwarder partitions the network field each time in order to separate itself and destination node into two separate zones. Third, it then randomly selects a node in the other zone as the next relay node and uses the concept of GPSR [15] algorithm to forward the data to the relay node.

Fourth, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination.

In summary, the contribution of S-ALERT includes:

- Anonymous routing: S-ALERT provides with route innonimate, identity, and location innonimate of source node and destination node.

- Low cost: Rather than depending on step- by- step encryption and superfluous traffic, S-ALERT mainly uses randomized routing of one message copy to provide anonymity protection.

4.2 Algorithm Steps

1. Entire network area is assumed as rectangle.
2. Number of nodes to form a network is decided.
3. Each node in network is assign a unique Id. (so that source node and destination node are distinguished) Source and destination node is decided.
4. Entire network is partitioned into horizontal and vertical partitions.
5. Generate data packet according to format.

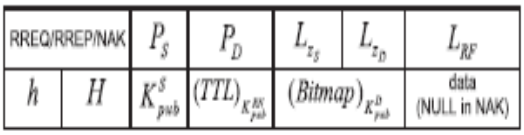


Fig 1: Packet Format of S-ALERT

6. Repeat step 4, until source node and destination zone are in different zones.
7. RF (random forwarder) is selected from each zone to carry data packets followed by encryption process.
8. MAC address of source node is encrypted.
9. Source node send data packet to RF, RF then send it to another RF of another zone.
10. Repeat step 7 until data packet is reached to destination zone, in destination zone data packet is flooded and reached to destination node.
11. At destination side decryption process is done and original data is gained.
12. Stop the process when data is reached to destination node safely.

4.3 System Architecture

The block diagram of proposed S-ALERT system as shown in the Fig. 2

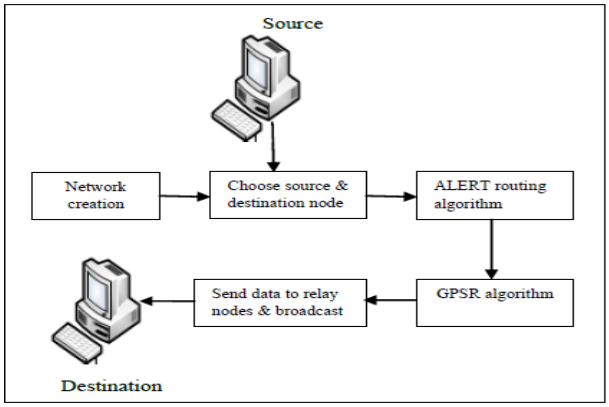


Fig 2: System Architecture

System architecture is divided into four modules

a) Network Construction
b) Zone Partition
c) Source Anonymity
d) Destination Anonymity

Let explain each module in details

4.3.1 Network Construction -

A network creation is to distribute whole network into number of nodes. Each node in network is assigned unique ID. Here, unique ID, is used for identify the source node and destination node. We first introduce two functions to calculate the two side lengths of the hth partitioned zone which are mentioned below

a (h, lA) = lA/2[h/2]
b (h, lB) = lB/2[h/2]

4.3.2 Zone Partition -

Separate source and destination by dynamically partition the network .It will generate an unpredictable routing path for a message. Zones are partitions into alternating horizontal and vertical manner. This method is called hierarchical zone partition [16]. Generally ALERT provides unpredictable and dynamic routing path, which having number of dynamically selected intermediate node. S-ALERT partitions given network area into two zones horizontal or vertical. Then again split every partition into two zones as vertically (or horizontally). This process called as hierarchical zone partition [16], [17]. Fig.3 and Fig.4 shows picture view of horizontal and vertical partitioning.

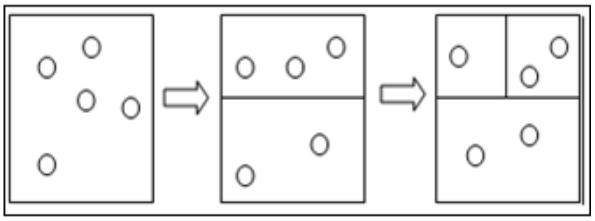


Fig 3: Horizontal Partitioning

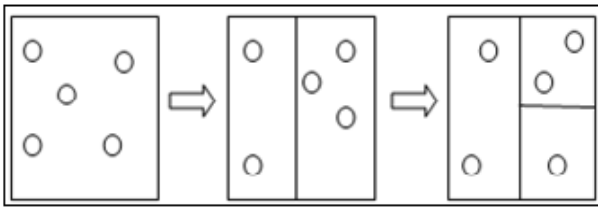


Fig 4: Vertical Partitioning

4.3.3 Source Anonymity -

To strengthen the innominate anonymity protection of the source nodes, a mechanism called notify and go is proposed. Main idea behind it is to let number of nodes send packets at same time as that of source node S, so that source node packet can be hidden among other packets. S-ALERT utilizes a TTL field in each packet to prevent the packets issued in the first phase from being forwarded in order to reduce excessive traffic [20]. Only the packets of S are assigned a valid TTL, while the covering packets only have a TTL = 0. S decide the next terminal destination (TD), it then forwards the packet to next relay node, based on GPSR protocol. Each and every node that receive packet but are unable to find valid TTL, will try to decrypt it using its private key. Only nodes with valid TTL field will decrypt it while all other nodes will drop the packets.

4.3.4 Anonymity -Destination

To counter the intersection attacks, in the destination zone broadcast packet to a set of m nodes out of k nodes. The m nodes hold the packet pkt1 until the arrival of the next packet pkt2.Upon receiving the next packet; the m nodes conduct one-hop broadcasting to enable other nodes in the zone.

S-ALERT Advantages

- To provide innominate protection to source node, destination node, and routes,
- Various strategies to efficiently counter intersection and timing attacks,
- To offer high innominate protection at a low cost.

5. MATHEMATICAL MODELLING

S = {K, D, A, R, Zd, p, k, H, la, lb}

Let's define each term in detail

S = Set of Whole System.
K = Set of Keys.
D = Set of Various Database.
A = Set of ALERT Routing Algorithm.
R = Set of Results.
Zd = Destination Zone.
p = Node Density.
k = Number of Nodes in Zd.
H = Total Number of Partitions in Zd.
la, lb = Side Lengths of Rectangle.

In proposed system analysis, we assume network as a rectangle, having side lengths with la, lb. First we calculate two side length of rectangle

$$a\ (h, lA) = lA/2[h/2]$$

$$b\ (h, lB) = lB/2[h/2]$$

Secondly, we will calculate H, denote total number of partitions. H is calculate by below formula

$$H = \log2\ (p.G/k)$$

Here G is size of network which we assume as rectangle. Based on H we calculate size of destination zone that is G/2H.

6. RESULTS AND COMPARISIONS

This section consists of the bar graphs which show performance of S-ALERT algorithm. Net beans and JDK tools are used to build the model and test the system of algorithm based on assuming network area as rectangle. The database is comprised of users and server contained within a MySQL schema. MySQL is a very powerful program in its own right. It handles a large subset of most expensive and powerful database packages. All the graphs show the performance in terms of execution time and transmission delay.

Below Fig.5 shows graph of location anonymity with respect to other anonymous routing protocols. It clearly shows that S-ALERT protocol offer with very high location anonymity as compared to other anonymous routing protocols. PRISM is one which provides quite better location anonymity.

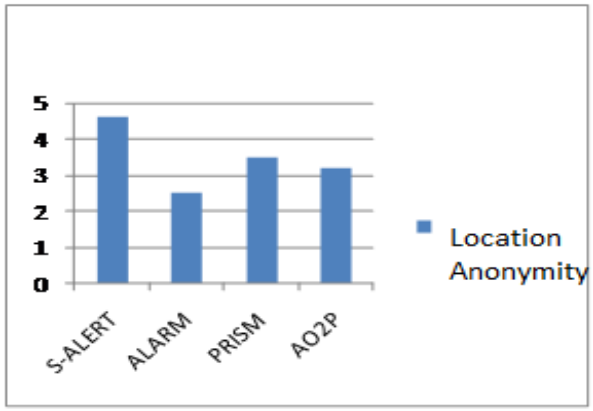


Fig 5: Location Anonymity of S-ALERT

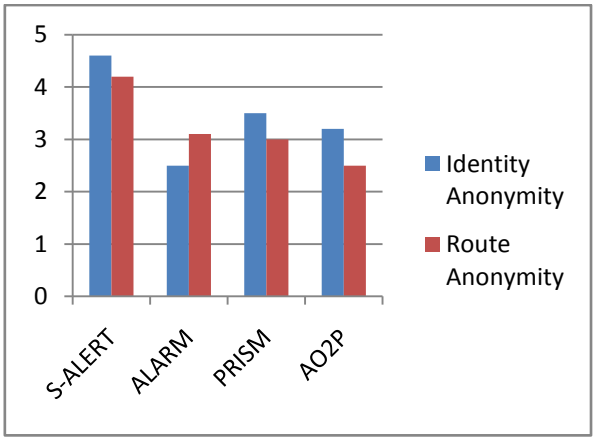
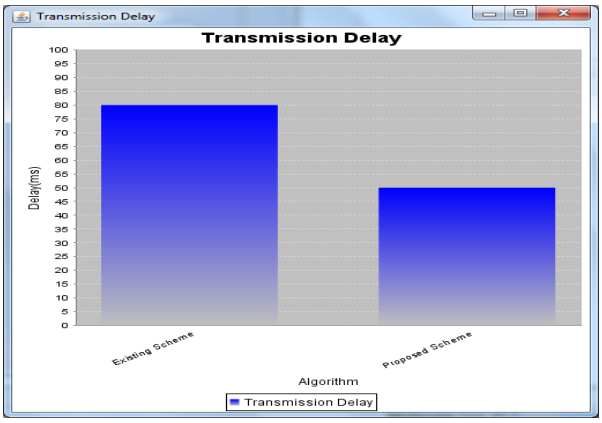


Fig 6: Identity and Route Anonymity of S-ALERT

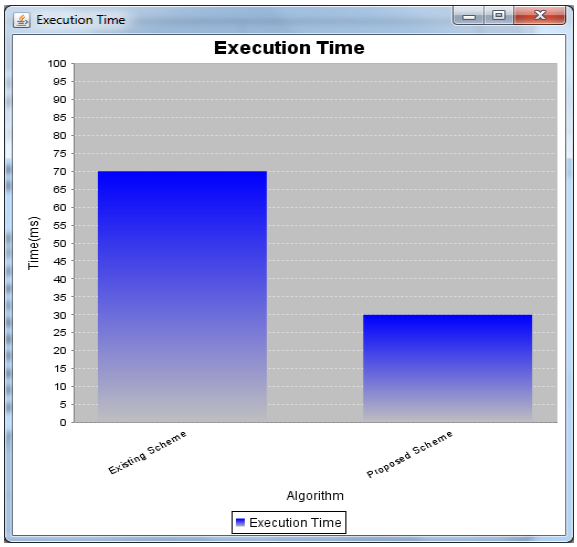
Fig 6. Shows clear comparison of S-ALERT protocol with other anonymous routing protocol. S-ALERT uses dynamic partitions to provide route anonymity and hence offer very high route anonymity. For identity anonymity it use concept of dynamic pseudo name.

In this section, performance is evaluated of S-ALERT protocol, which shows good performance with respect to existing system. Here we have considered two parameters, based on which performance is evaluated. The two parameters consider are transmission delay and execution time.



Graph clearly shows that transmission delay is much less with respect to existing system. Due to very less delay in

transmission the overall performance of proposed system is increased.



Below Table 1 show comparison of S-ALERT protocols with other anonymous routing protocols. Table 1 clearly shows that S-ALERT offers with innominate protection to all factors like source node, destination node and route carrying data. And thereby making the communication secure.

Table1. Comparison of S-ALERT Protocols with Other Anonymous Routing Protocols

Name of protocol	Location Anonymity	Identity Anonymity	Route Anonymity
S-ALERT	**Source, Destination**	**Source, Destination**	**Yes**
ANDOR	Source, Destination	N/A	Yes
MASK	Source	Source, Destination	No
AO2P	Source, Destination	Source, Destination	No
ALARM	Source, Destination	No	Yes
ZAP	Destination	Destination	No

7. CONCLUSION AND FUTURE SCOPE

Aim of proposed system is to provide full protection to identity of source node, destination node and data packets. 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. And to also provide with counter measures to prevent from timing attacks and intersection attacks. S-ALERT is mainly recognize by its very low cost and providing full innominate protection to source nodes, destination nodes, data as well as routes carrying data. S-ALERT further strengthens the innominate protection of source and destination by hiding sender/receiver among a number of data sender/receiver. In addition, S-ALERT has various measures for various attacks.

Future work lies in; first making S-ALERT system bulletproof to types of attacks. Hence it should have counter measures to be safe from all attacks which harm it. Second S-ALERT system is not feasible for network models [11], [22], so there is need to make some changes in S-ALERT. It can also achieve comparable routing efficiency to the base-line GPSR algorithm. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks.

8. ACKNOWLEDGMENT

It gives me a great pleasure and immense satisfaction to present this special topic. I express my deep sense of gratitude and humble thanks to my college Principal, HOD and project guide for their valuable guidance throughout the presentation work. I sincerely thanks to my colleagues, the staff and family members who directly or indirectly helped me and made numerous suggestions which have surely improved the quality of my work.

9. REFERENCES

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

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

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

[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] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[10] 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.

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," Proc. ACM MobiCom, 2000.

[18] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[19] 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.

[20] 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.

[21] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.

[22] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int' Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.

[23] 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.

[24] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy,"Efficient and Robust Pseudonymous Authentication in VANET", Proc. ACM Intl Workshop Vehicular Ad Hoc Networks (VANET 07), pp. 19-28, Sept. 2007.

[25] E. Schoch, F. Kargl, T. Leinmu ller, S. Schlott, and P. Papadimitratos,"Impact of Pseudonym Changes on Geographic Ad Hoc Routing",Proc. Third European Workshop Security and Privacy in Ad Hoc and Sensor Networks (ESAS 06), vol. 4357, pp. 43-57, 2006.

[26] 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.

[27] X. Hong, M. Gerla, G. Pei, and C.C. Chiang,"A Group Mobility Model for Ad Hoc Wireless Networks",Proc. Second ACM Intl Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.

[28] (ISLPED), 2003. L. Sweeney,"k-Anonymity: A Model for Protecting Privacy",Intl J. Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5,pp. 557-570, 2002.

[29] J. Li, J. Jannotti, D.S.J. De, D.S.J. De Couto, D.R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing",Proc. ACM MobiCom, 2000.

[30] L. Y. Xue, B. Li, and K. Nahrstedt,"A Scalable Location Management Scheme in Mobile Ad-Hoc Networks",technical report, 2001 J. Li, J. Jannotti, D.S.J.