Location Based and Energy Efficient Anonymous Routing Protocol for MANET

Snehlata Handrale , Prof. S. K. Pathan

Department of Computer Engineering, University of Pune
Pune , India

***Abstract*— MANET (Mobile Ad-Hoc Network) are characterize self-organizing and independent infrastructures, having dynamic topology which make them an ideal choice for communication and information sharing in network. But MANETs are susceptible to malicious things which aim to tamper and analyze data and traffic analysis by communication snooping .For provide communication security ,in this paper we use anonymous routing protocol, which hide nodes identity ,nodes location and communication route. But only security is not enough for successful routing , routing lifetime is also important factor so for this we contribute energy of nodes.**

***Keywords*— Mobile ad hoc networks, anonymity, routing protocol, energy constraints , node selection.**

I. Introduction

MANETs "Mobile Ad Hoc Network". It is an ad hoc wireless system that can change locations and configure itself. The topology of MANET changes constantly due to the mobility of nodes. Because of that mobility, nodes can move in and out of coverage region of each other, so that some links break while new links between nodes are created. MANETs feature self-organizing and independent infrastructures, which make communication and information sharing in wireless network. In MANETs, there is a malicious activity such as communication eavesdropping or attacking routing protocol to steal the data forwarded through the network. As per security purpose in MANETs anonymity is crucial. For example in military battlefields network, emergency services, commercial and civilian in these areas security is more important. Therefore for this anonymity is best solution. We can provide anonymity in terms of anonymous routing protocol.

Anonymous routing protocols in MANETs provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. In Exiting system anonymity is not provided completely, there is neither source nor destination anonymity. So here a new location based and energy efficient anonymous routing protocol introduced in MANETs which 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 difficult for other nodes to identify the real identities and exact locations of the sources and destinations. For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes in routing . Also, in order to dissociate the relationship between source and destination , 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.

Maintaining an optimized lifetime of a routing path in a network is a very challenging task because the energy of the nodes depends on the model, size, property, and capacity of the battery. Energy in batteries continuously decrease due to node activities such as transmission, reception and overhearing . So for this with anonymity protection this paper focuses on Energy efficient routing. In MANET nodes are battery powered , so for lifetime routing energy must be continuoisly available. For energy purpose here used one threshold value , comparing with this value nodes selection is done for routing, whether the node have sufficient energy for successful routing or not. If not then node will discarded. Another node get selected.

II. Related Work

As anonymity is important factor for MANET, there are many anonymous routing schemes in MANETs are present. By using the different topological information methods, they can be classified into on-demand method or reactive routing methods [2], [3], [4], [5], [6], [7], [8], [9], [10] and proactive routing methods [11].. Table I shows the anonymity protection in different reactive routing methods including hop-by-hop encryption and redundant traffic.

In hop by hop encryption method, a packet is encrypted while transmitting from source to destination, to prevent from tamper or analyze the packet to interrupt the communication or identity of two communication nodes. Hop by hop authentication is used to prevent the adversaries from participating in the routing to ensure the route anonymity [2], [3], [8], [11], [12] [8]. To ensure the discovered routes consist of legitimate nodes and are anonymous to attackers, MASK [8] topological routing is used. In this nodes are encrypted their location updates and send it to the location server. However, the GPSR [2] does not provide the route anonymity because packets always follow the shortest path by using geographic routing. In the AO2P [12] geographic routing algorithm, pseudonyms are used as the nodes identity which protects nodes real identities and a node chooses the neighbor which can reduce the greatest distance from the destination. But AO2P does not provide the anonymity protection to the destination

Table.1. Anonymity Routing Method

Category		Name	Identity Anonymity	Location Anonymity	Route Anonymity
Reactive	Hop by Hop encryption	ANODR	Source , Destination	NA	YES
		AO2P	Source, Destination	Source, Destination	No
		PRISM	Source, Destination	Source, Destination	No
	Redundant Traffic	ASR	Source, Destination	Source, Destination	No
		ZAP	Destination	Destination	No
Proactive	Redundant	ALARM	Source, Destination	Source	No

Redundant traffic based routing protocol uses the redundant traffic, such as local broadcasting, multicast. Multicast is used in the ASR routing algorithm in order to construct a multicast tree to hide the destination node. ZAP [14] uses a destination zone, and locally broadcast to the destination zone to reach the destination without dripping the identity and location of the destination. The redundant traffic method is the very high overhead experienced by the redundant operations or packet leading to high cost is one of the drawback of this method. ZAP performs the destination anonymity whereas it cannot provide the source and route anonymity.

ALARM is under the proactive routing, where each node is broadcast its location information to its authenticated neighbors for route anonymous.

III. Overview Of Attack Model And Secure Routing Protocol

A. Attack Model

There are two types of attacks in MANET, namely External attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from common nodes, which are the part different of network, based on threat analysis several specific attacks that can target the operation of routing protocol in ad hoc network.

1. *Message Reply*: After the attacker interrupted message, it will store the message and re-transmit the message to produce the unauthorized effect because the message is transmitted in the air and easily can be intercepted.

2. *Denial of Service:* Denial of Service attacks means the complete interference of the routing function.

3. *Black hole attack:* The black hole attack means the node exploits the mobile ad hoc routing protocol and attacker carried out away intercepted packets without any forwarding. However the attacker runs the risk with neighbouring node and modified packets originating from some nodes.

4. *Reply attack*: This type of attack explains an attacker introduce network routing traffic that has been captured previously. This attack create problem on the freshness of routes.

B. Secure Routing Protocol

Most of the attacks on routing protocol are due to lack of Encryption. Unauthorized modification of such fields could cause serious security threats. DES for encryption mechanism is used. Each node in the network have a public/private key pair; the certificate is to be valid for certain time period. The protocol overcomes all known vulnerabilities of the existing protocols. It uses DES encryption mechanism to secure the fields of packets. The most severe attacks on MANETs is warm hole attack. This can be overcome applying efficient secure neighbour detection mechanism. To increase the security level of discovered path, route selection is done based on trust level of nodes along the path. In order to secure position coordinates of each node Position verification system is used.

IV. Alert Base System

In order to provide high anonymity protection (for sources, destination, and route) with low cost, propose an Anonymous Location based and Efficient Routing Protocol (ALERT). ALERT can be used in different network models with node movement patterns. Such as random way point model and group mobility model. Using network model information attacker may find out location of nodes. So anonymity may get threaten. Therefore, an anonymous communication protocol is needed which can provide untraceability to strictly ensure the anonymity of sender. As well as attacker try to block the data packets by injecting packets on a routing path. Therefore, route should also be undetectable. And with help of intersection attack on traffic destination node can be detected, So destination node also needs the protection anonymity.

ALERT first dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field into zones. So they get 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 [2] algorithm to send the data to the relay node. In the last step, the data is broadcasted to k nodes in the destination zone, which providing k-anonymity to the destination node. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to support the anonymity protection of the source. ALERT is also resilient to intersection attacks and any node can act as a source or destination. We assumes source and destination node randomly in the different time intervals. For ease of illustration, assume the entire network area is generally a rectangle in which nodes are randomly spread. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT.

A. **Pseudonym and Location of Service**

Dynamic pseudonym is another name or identity given to node. In ALERT pseudonym used as node identifier with replacement of its real MAC address. Nodes MAC address can be used to trace nodes existence in the network. Therefore replacing MAC address with pseudonym is the main advantage of ALERT protocol. This pseudonym is the combination of MAC address and Current time stamp. But if this information is known by attacker then it is easily find out the node. Therefore, to prevent this time stamp can be randomly selected. This pseudonym is not permanent ,it expires after a specific time period so that attacker can not associate the pseudonym with nodes.With this pseudonym there is one problem is changing pseudonym frequently create routing uneasy. Therefore these pseudonym change frequently should be appropriately determined.

B. **The ALERT Routing**

Generally ALERT provides unpredictable and dynamic routing path, which having number of dynamically selected intermediate nodes.

1. First ALERT partitions given network area into two zones as horizontally (or vertically).
2. Then again split every partitions into two zones as vertically (or horizontally). This process called as hierarchical zone partition.
3. After partitioning ALERT randomly select a node in each zone at each step as an intermediate relay node ,in this way ALERT provide dynamically creating an unpredictable routing path.

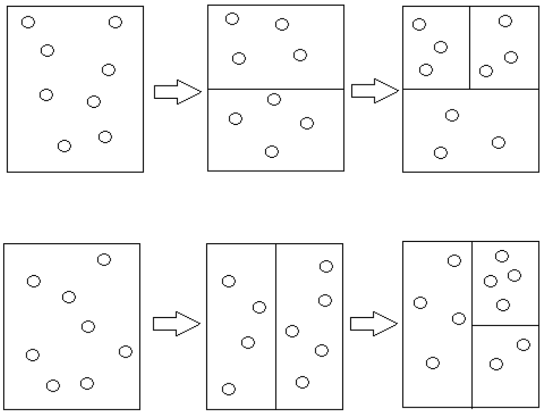

Fig.1. Horizontal and Vertical Routing

Above figs shows both partitioning here we generally network considered in rectangle form. Consider one example of routing in ALERT.

Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. We call this partition process hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

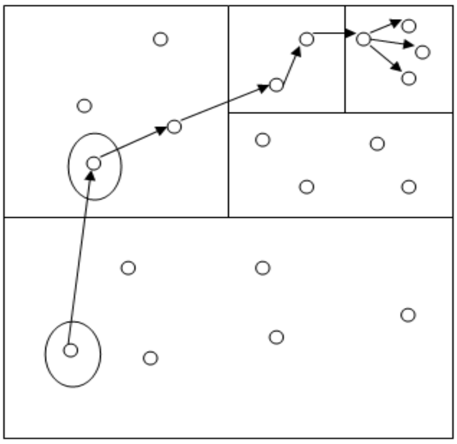

Fig.2. ALERT Routing

In this example we first horizontally partition network then vertically and so on. While this partitioning each data source of forwarder node checks whether itself and destination node are not in same zone. If it is not then partitioning continues. In above fig where the destination node locate that zone is called as destination zone denoted as ZD and that zone having k nodes ,which is used to control the degree of anonymity. While in routing first source node randomly chooses a node in other zone known as temporary destination (TD) and then uses GPSR routing algorithm to send the data to node close to TD. This process continues to reach data to destination node. A node closer to TD known as Random Forwarder (RF) .But in destination zone data is broadcasted in ZD to k nodes which provides k anonymity i.e attacker or observer does not known at destination node.

Here one assumption is taken that destination node with not leave the destination zone during the data transmission to it. So it can successfully receive the full data without any loss. For successful completion of data transmission destination node send a confirmation to source node. If source node not receive to confirm during predefined time period, it will resend packets. As a large no.of hierarchies generated they create more routing hops which increses anonymity degree but also increase the delay.

C.**Location of Destination Zone**

Zone position is made from the upper left and bottom right coordinates of a zone. It is used by each packet forwarder to check wheather it is separated from destination zone or not, To calculate zone position we have H denotes total no.of partitions in order to produce ZD and no.of nodes i.e k and node density ρ ,

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

Where as

G=size of entire network area

Using H and G the position (0,0) & (Xg , Yg) of entire network area and position of destination node d the source can calculate the zone position of ZD.

D.**Packet Format**

For successful routing netween source and destination some information is needed, which is embeds in the packet by source and each packet forwarder node. For ALERT following packet format is use.

RREQ/RREP/NAK	P_S	P_D	L_{z_S}	L_{z_D}	L_{RF}
h	H	K^S_{pub}	$(TTL)_{K^{AN}_{pub}}$	$(Bitmap)_{K^D_{pub}}$	data (NULL in NAK)

Fig.3 ALERT Packet Format

RREQ/RREP/NAK- use to acknowledge the loss of packet.
Ps- Pseudonym of a source.
Pd – pseudonym of a destination.
Lzs & Lzd – are the position of Hth partitioned source zone and destination zone.
h- number of divisions.
H – maximium number of division allowed.

Greedy Perimeter Stateless Routing (GPSR), a novel routing protocol for wireless datagram networks that uses the *positions* of routers and a packet's destination to make packet forwarding decisions. GPSR makes *greedy* forwarding decisions using only information about a router's immediate neighbors in the network topology. When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the *perimeter* of the region. If greedy forwarding is successful then it chooses node which is nearer towards the destination zone to establish routing path between source and destination. This process will repeat for all zones. By keeping state only about the local topology, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations increases. Under mobility's frequent topology changes, GPSR can use local topology information to find correct new routes quickly.

Alert Anonymity

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing [13], [12], [6], which always takes the shortest path, ALERT makes the route between a S-D pair challenging to discover by randomly and dynamically choosing the relay nodes. The resultant different routes for transmissions between a given S-D pair make it difficult for an intruder to observe a fix 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.

Since an RF is only aware of its proceeding node and succeeding node in route, the source and destination nodes cannot be differentiated from other nodes en route. Also, the anonymous path between S and D ensures that nodes on the path do not know where the endpoints are. ALERT strengthens the privacy protection for S and D by the unlinkability of the transmission endpoints and the transmitted data. That is, S and D cannot be associated with the packets in their communication by adversaries. ALERT incorporates the "notify and go" mechanism to prevent an intruder from identifying which node within the source neighborhood has initiated packets. ALERT also provides k-anonymity to destinations by hiding D among k receivers in ZD. Thus, an eavesdropper can only obtain information on ZD, rather than the destination position, from the packets and nodes en route.

The route anonymity due to random relay node selection in ALERT prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In ALERT, the routes between two communicating nodes are constantly changing, so it is difficult for adversaries to predict the route of the next packet for packet interception. Similarly, the communication of two nodes in ALERT cannot be completely stopped by compromising certain nodes because the number of possible participating nodes in each packet transmission is very large due to the dynamic route changes. In contrast, these attacks are easy to perform in geographic routing, since the route between a given S-D pair is unlikely to change for different packet transmissions, and thus, the number of involved nodes is much smaller than in ALERT.

V .Energy Efficient Routing

As we see ALERT routing provides identity , location and route anonymity . But with only anonymity we get routing security , so for continuous routing we need energy of nodes. For energy efficient routing with anonymity nodes energy must be consider.

Here each node in a network serves as a host and/or router partitions network into zones, selecting RFs ,forwarding packets to next relay node or intermediate nodes . These nodes are fitted with and powered by batteries. The depletion of participating nodes' battery power in a routing path will shorten the network lifetime. As charging or replacing batteries on site is a difficult operation, it is necessary to use the available energy efficiently to extend the lifetime of the nodes . Developing an energy efficient routing scheme is one way of achieving optimized performance of nodes.

With ALERT system , first one threshold value of energy in joule is considered. when node get selected for routing that time energy of that node is checked with threshold value of energy. If node have more energy than threshold value then only that node is used for forwarding. Nodes are battery powered therefore we can charge them again when they are discharged. Because of this anonymity could not broke.

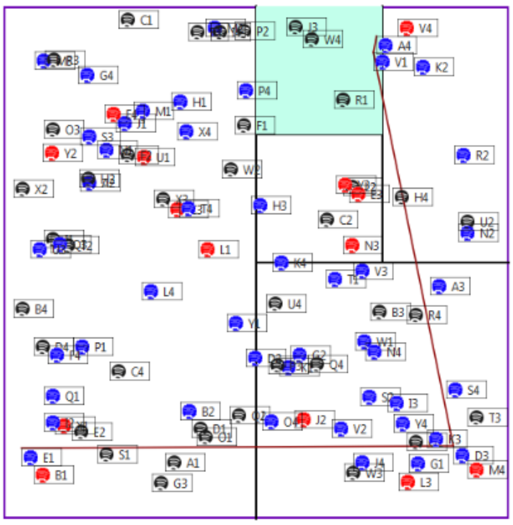

Fig.4.LEARP System

Fig.4. LEARP (Location based and energy efficient anonymous routing protocol) shows ALERT system with energy efficiency. In this ALERT system partitions network into zones and forwards packet as per system. In figure three colors used for node representation , black nodes are having more energy than threshold value , blue nodes are having enough energy for routing but after some time they will get discharged and red nodes are already discharged.In this nodes are recharged therefore they can use in another routing .This is more beneficial for anonymity.

VI.Benefits Of Proposed System

Comparing proposed systems parameters with ALERT system we conclude that

Latency Per Packet Fig.5. shows that Proposed system latency is comparatively less than ALERT system.

Hops per packet Fig.6. shows ,hops per packet are more for proposed system than ALERT system.

Delivery Rate Fig.7. shows proposed system have high delivery rate than ALERT system.

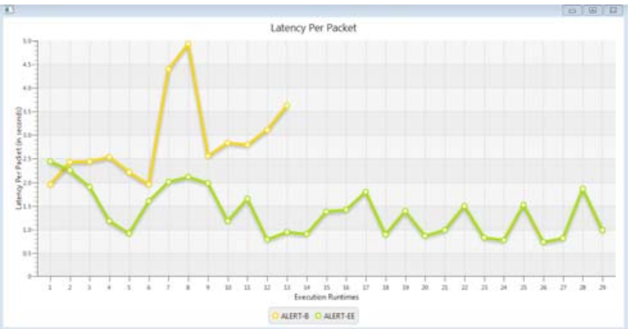

Fig.5.Latency per Packet

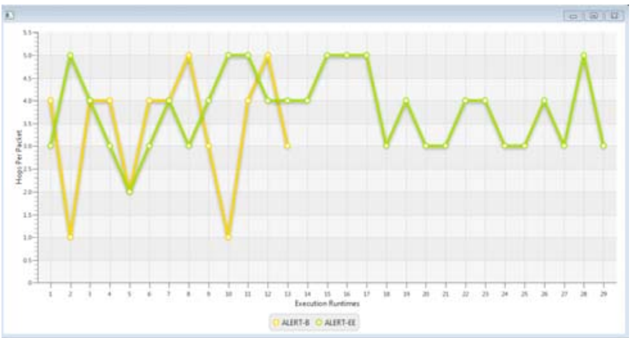

Fig.6.Hops per packet

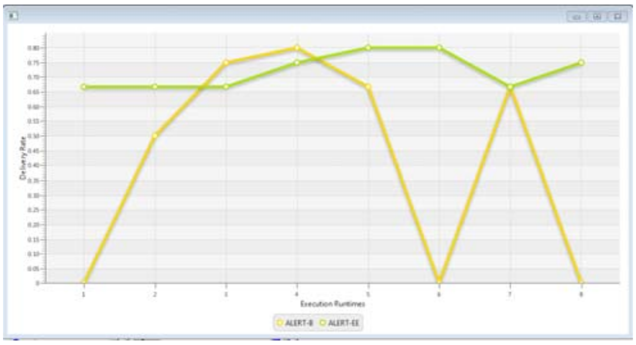

Fig.7.Delivery Rate

As we observe Fig.5. Latency per packet, ALERT system have more latency per packet than proposed system . Using energy efficiency we can improve latency rate. Fig 6. Hops per packet ,shows packet per hops also increased using proposed system. Therefore anonymity of route increases. And Fig.7. Delivery rate, shows proposed system have increased delivery rate than ALERT. So it improve routing efficiency.

VII.Conclusion

There are number of anonymous routing protocols are available for MANET's for sharing the information between source and destination securely. While sharing information between source and destination, the security to source, destination as well as routers is must to prevent the accessing from the unauthorized user. The some existing anonymous protocols provide protection to only source and destination locations or to only route locations. Our proposed anonymous protocol provides security in terms of location and identity anonymity to source, destination as well as routes with energy efficient . 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 has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks. ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line GPSR algorithm. With all this we include energy point which helps ALERT protocol to routing with no failure of energy down problem. Because of this anonymity provide with high energy so that routing is done without failure.

References

[1] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING, JUNE 2013.

[2] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Pr ivacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

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

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

[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] 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.

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

[9] 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.

[10] L. Yang, M. Jakobsson, and S. Wetzel, “Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks,” Proc. Secure comm and Workshops, 2006.

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

[12] 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.

[13] 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.

[14] 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.

[15] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, “The New Casper: Query Processing for Location Services without Compromising Privacy,” Proc. 32nd Int’l Conf. Very Large Databases (VLDB), 2006.

[16] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, “Analyzing the Energy Consumption of Security Protocols,” Proc. Int’lSymp. Low Power Electronics and Design (ISLPED), 2003.