Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

MANET: ACHIEVING ANONYMITY PROTECTION BY ALERT MECHANISM

S.Rajaambika[1], R. Balasubramaniam[2], T.K.P.Rajagopal[3]
[123] *Computer Science and Engineering Department, Kathir College of Engineering, Neelambur, Coimbatore-641062.*

Abstract - Mobile Ad-hoc Network (MANET) is self-organizing and independent infrastructures, dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. This makes them an ideal choice for communication and information sharing. In MANETs nodes are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by eavesdropping or attacking routing protocols. Also, limited resource is a problem in MANETs, where each node experiences under an energy constraint problem. Since MANETs complex routing and stringent channel resource constraints impose strict limits on the system capacity. However, existing anonymous routing protocols generate a significantly high cost, which is resource constraint problem in MANETs. It use anonymous routing protocols that hide node identities and routes from outside observers in order to provide anonymity protection and propose an Anonymous Location-based Efficient Routing protocol (ALERT). ALERT initially it partitions the network field dynamically in to separate zones and randomly chooses nodes in zones as intermediate relay nodes, ensuring a non-traceable anonymous route. In this protocol the data initiator/receiver among many initiators/receivers is hidden. Thus, ALERT offers anonymity protection to sources, destinations, and routes. It also provides effective solution to counter inter- section and timing attacks. Experimental results exhibit consistency with the theoretical analysis, and show that ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Many anonymity routing algorithms are based on the geographic routing protocol (e.g. Greedy Perimeter Stateless Routing (GPSR)) that greedily forwards a packet to the node closest to the destination. ALERT provides high level security to sources, routes and destinations. At the end we compare ALERT with other protocols in terms of efficiency and cost.

Keywords— Mobile ad hoc networks, anonymity, routing protocol, geographical routing.

I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) play an increasingly important role in many environments and applications, especially, in critical settings that lack fixed network infrastructure, such as: emergency rescue, humanitarian aid, as well as military and law enforcement. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. 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, so high security anonymous routing protocols are required 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.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Anonymous Location-based and Efficient Routing protocol (ALERT). ALERT 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 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 [9] 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- anonymity to the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks [10]. We theoretically analyzed ALERT in terms of anonymity and efficiency.

II.EXISTING SYSTEM AND PROBLEM DEFINITION

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [1], [2], [3] and redundant traffic. In hop-by-hop encryption only source and destination location will highly secured but routes are not secured so malicious node or attackers can easily retrieve the information by hacking the routing path so this is not an efficient security protocol and some other protocols like ALARM [4] cannot protect the location anonymity of source and destination, SDDR [6] cannot provide the route anonymity, and ZAP[7] only focuses on destination anonymity. Many anonymity routing algorithms are based on geographic routing protocol e.g. Greedy Perimeter Stateless Routing (GPSR) that greedily forwards a packet to the node closest destination. Most of these current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned anonymity protections.

The limited resource is an inherent problem in MANETs, in which each node labors under an energy constraint. MANETs complex routing and stringent channel resource constraints impose strict limits on the system capacity. 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.

III. OVERVIEW OF ATTACK MODELS AND SECURE ROUTING PROTOCOLS.

A. Attack models:

There are two types of attacks in Mobile ad hoc network, namely External attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from shared nodes, which are the part 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 intercepted 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 disruption of the routing function. Specific instances of denial of service attack include the sleep deprivation torture and routing table overflow. In sleep deprivation torture means the consumption of batteries of a specific node by keeping it engaged in routing decision. Another term routing table overflow attack aim is malicious node advertises route that go to non-existent node to authorized nodes available in the network. The attacker tries to create enough routes for disruption the routing. The proactive routing algorithms are more effective to table overflow attack because proactive algorithms is use for discover routing information before it is actually needed.
3. Black hole attack: The black hole attack means the node exploits the mobile ad hoc routing protocol and attacker consumes intercepted packets without any forwarding. However the attacker runs the risk with neighboring node and modified packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of wrongdoing.
4. Reply attack: This type of attack explains an attacker inject 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 absence of Encryption. Unauthorized modification of such fields could cause serious security threats. DES for encryption mechanism is used. Each node in the network maintains a public/private key pair; the certificate is to be valid for certain time period. Each node has T's public key, so it can decrypt certificates of other nodes. The protocol overcomes all known vulnerabilities of the existing protocols. It uses DES encryption mechanism to secure the fields in routing packets. The most severe attacks on MANETs is warm hole attack. This can be overcome applying efficient secure neighbor detection mechanism. To enhance 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 employed.

C. Security architecture for MANETs:

Security issues in mobile ad hoc networks. The designing of security architecture [8] for tackling security challenges mobile ad hoc networks are facing is discussed. The security architecture in a layered view is analyzed for such applying the security architecture in military scenarios. It can be used as a framework when designing system security for ad hoc networks. An efficient secure routing protocol for mobile ad hoc networks guarantees the discovery of correct connectivity information over an unknown network, in the presence of malicious nodes.The term of anonymous location-based routing in certain types of suspicious MANETs. It relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations.

IV. PROPOSED SYSTEM

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an *Anonymous Location-based and Efficient Routing protocol (ALERT).* ALERT 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 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 [9] 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- anonymity to the destination. In addition, ALERT has a strategy to hide the data

initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks [10]. We theoretically analyzed ALERT in terms of anonymity and efficiency. We also conducted experiments to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocols. In summary, the contribution of this work includes:

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.

The block diagram of proposed ALERT system as shown in the fig 1.

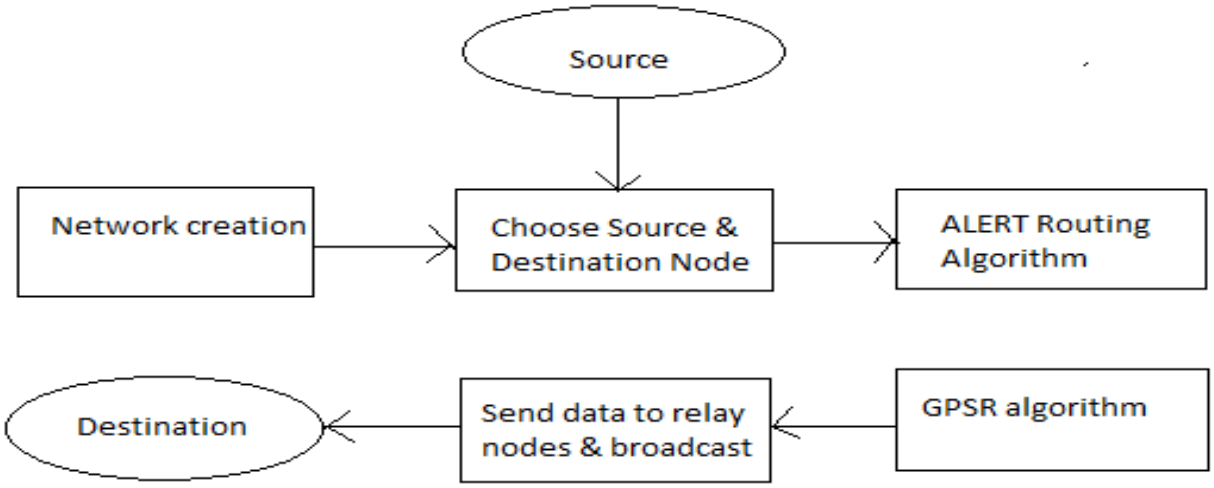

Fig.1. Proposed ALERT system.

The first step in the proposed ALERT system is to establish Ad-Hoc network with *N* number of nodes, because of decentralization feature of Ad-Hoc networks 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, we assume the entire network area is generally a rectangle in which nodes are randomly disseminated. 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

ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes.

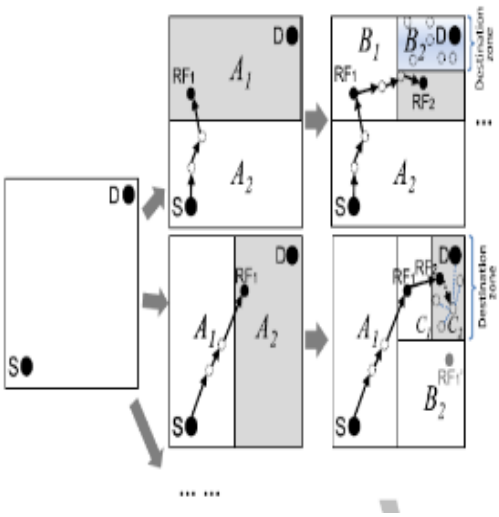

Fig.2. Different network zone partitions.

As shown in the upper part of Fig.2. Given an area, we horizontally partition it into two zones A1 and A2. The number of partitions is determined by $p=log2\ (\rho.G/k)$.where p is number of partitions and ρ is node density, G is size of entire network and k is number of nodes in the destination zone. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 into two zones. 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.

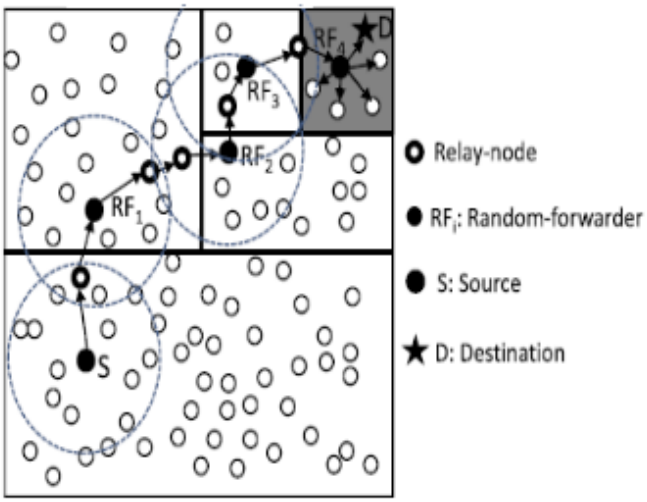

Fig.3. Routing among different zones.

Fig.3. shows an example of routing in ALERT. We call the zone having k nodes where D resides the destination zone, denoted as ZD. k is used to control the degree of anonymity protection for the destination. The shaded zone in Fig.3 is the destination zone. Specifically, in the ALERT routing, 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 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. By TD it chooses a *Random Forwarder (RF)*node, which is nearer to TD node. Through RF node routing path will established as shown in fig.3.

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, where node in greedy forwarding is closest neighbor to destination node. 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.

A. Anonymity protection

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing [13], [2], [3], [11], [12], which always takes the shortest path, 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.

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 unlink ability of the transmission endpoints and the transmitted data [15]. 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. COMPARISION WITH OTHER PROTOCOLS

A. Control overhead Vs. Node Density

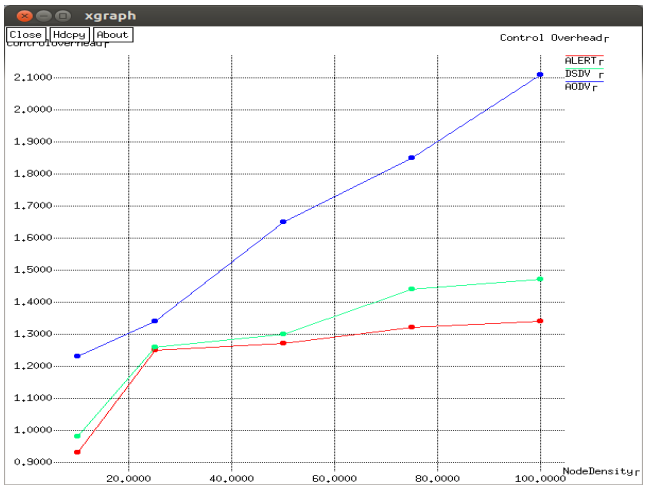

Fig 4. Performance of Control overhead Vs. Node Density

The comparison graph of ALERT, AODV, and DSDV shows that ALERT has minimum control overhead comparing with other two protocols. Thus AODV has control overhead of 2.87 m/sec , DSDV is of 7.01 m/sec whereas ALERT is only 2.68 m/sec.
Thus this shows ALERT is efficient with minimum overhead at maximum node density

B. Packet Delivery rate Vs. Speed of Node

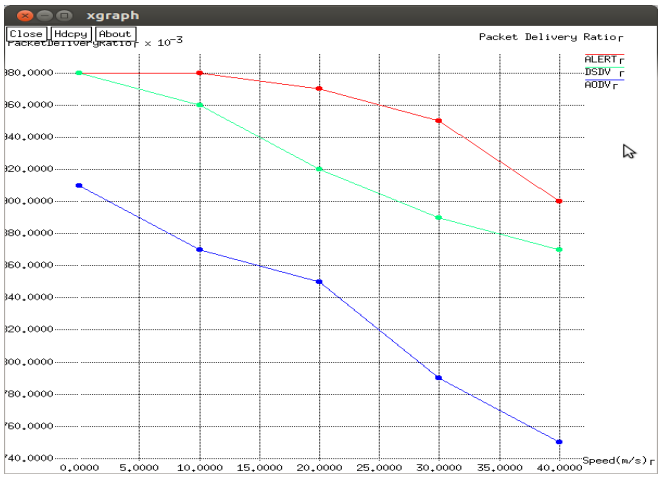

Fig 5. Performance of Packet Delivery rate Vs. Speed of Node

The comparison graph of ALERT, AODV, and DSDV shows that ALERT has maximum packet delivery rate comparing with other two protocols. Thus AODV has packet delivery rate of 5.2 m/sec , DSDV is of 1.97 m/sec whereas ALERT is only 1.32 m/sec.
Thus this show ALERT is efficient with maximum delivery rate at short period of time.

VI. CONCLUSION AND FUTURE WORK

In previous anonymous routing protocols, which relay on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols in the existing system are unable to provide complete anonymity protection to source, destination and to route. In this paper which introduced ALERT mechanism which overcome the existing protocols and is distinguished by its low cost and anonymity protection to source, destination as well route. In order to provide source anonymity it uses 'notify and go' mechanism and uses local broadcasting for achieving destination anonymity. It further strengthens by hiding data initiation/receiver among number of data initiator/receiver. Also ALERT provides an efficient solution to counter intersection attacks and its ability to fight against timing attacks also analyzed. Experiment results show that 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.

As ALERT is not a complete bullet proof to all attacks like other anonymity routing algorithms and routing is the fundamental research issue for this networks and refers to finding and maintaining routes between nodes. Moreover, ALERT involves selecting the best route where many may be available. However, due to the freedom of movement of nodes, new routes need to be constantly recalculated. Intelligent rebroadcasting reduces these overheads by calculating the usefulness of a rebroadcast, and the likelihood of message collisions. Thus future work lies in the Zone based Routing with Parallel Collision Guided Broadcasting Protocol (ZCG) that uses parallel and distributed broadcasting technique to reduce redundant broadcasting and to accelerate the path discovery process, while maintaining a high reachability ratio as well as keeping node energy consumption low. ZCG uses a one hop clustering algorithm that splits the network into zones led by reliable leaders that are mostly static and have plentiful battery resources. The main future work is to send the data on randomly and unpredictable routing path and also many other attacks are available, using to increase the high efficient and we intend to study how the frequency of the pseudonym change influences the level of privacy achieved.

REFERENCES

[1] 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'lSymp.Applications on Internet (SAINT), 2006.

[2] Z. Zhi and Y.K.Choong,"Anonymizing Geographic Ad HocRouting for Preserving Location Privacy," Proc. Third Int'lWorkshopMobileDistributed 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 Conf. Vehicular Electronics and safety (ICVES), 2008.

[4] K.E.Defrawyand G. Tsudik,"ALARM: Anonymous Location Aided Routing in Suspicious MANETs,"Proc.EEEInt'l Conf.Network Protocols(ICNP),2007.

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

[6] 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.

[7] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous GeoForwarding in MANETs through Location Cloaking, "IEEETrans. Parallel and Distributed Systems, vol.19, no.10, pp. 1297-1309, Oct. 2008

[8] Komal Chandra Joshi et al, "Secured Position Aided Ad hoc RoutingSecurityof mobile ad hoc network with five layer security architecture' 'International Journal ITT, India, Dec 2010.

[9] S.Ratnasamy, B.Karp, S.Shenker,D.Estrin, R.Govindan, L.Yin,and F.Yu, "Data-Centric Storage in Sensor nets with GHT,aGeographic Hash Table," Mobile Network Applications, vol. 8, no. 4,pp. 427-442, 2003.

[10] 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.

[11] 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.
[12] 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 Network (LCN), 2004.
[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] 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.
[15] 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.
[16] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Model for Ad Hoc NetworkResearch," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.
[17] 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.
[18] 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.
[19] Karim El Defrawy, "Privacy-Preserving Location-BasedOnDemandRoutingin MANETs" IEEE Journal On Selected Areas In Communications,VOL.29,NO.10,DECEMBER 2011 NO. 2003.

