ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Anonymous Privacy-Preserving Routing In Location Based Dynamic Ad-Hoc Networks

G.Gokila[1], Mrs.F.Salma Rosline Mary, M.E[2]., P.Karthikeyan[3], Mr.A.Suresh Babu,M.E.[4]

M.E. Applied Electronics, JJ College of Engineering and Technology, Thiruchirapalli-9[1]

Assistant Professor, JJ College of Engineering and Technology, Thiruchirapalli-9[2]

M.E. Communication System, Hindusthan College of Engineering and Technology, Coimbatore-641032[3]

Assistant Professor, Hindusthan College of Engineering and Technology, Coimbatore-641032[4]

Abstract: Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. ALERT offer high anonymity protection at a low cost. It also has strategies to effectively counter intersection and timing attacks. In this paper, we propose a novel protocol called Position based Opportunistic Routing (POR) which takes full advantage of the broadcast nature of wireless channel and opportunistic forwarding. This protocol reduces the delay of data delivery between the nodes and improves the packet delivery ratio. Both theoretical analysis and simulation results show that POR not only achieves outstanding performances in normal situations but also yields excellent resilience in hostile environments.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) feature self organizing and independent infrastructures, which make them an ideal choice for military uses such as communication and information sharing in battlefields. Although anonymity may not be a requirement in civil-oriented applications, it is critical in military applications (e.g., soldier communication).

Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. For identity and location anonymity of sources and destinations, no one else knows the real identities and exact locations of the sources and destinations except themselves. 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 en route.

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [6], [7], [9], [2], [16] and redundant traffic [3], [4], [5], [8], [12], [14], [15]. Since public-key based encryption and high traffic generate significantly high cost, most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources. In addition, many approaches cannot provide all of the aforementioned anonymity protections. 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. It then randomly chooses a node in the other zone as the next relay node, and uses the Greedy Perimeter Stateless Routing (GPSR) [10] 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. ALERT has a strategy to hide the data initiator among a number. ALERT is also resilient to intersection attacks [11] and timing attacks [11].

Traditional topology-based MANET routing protocols(e.g., AODV, DSR [1]) are quite susceptible to node mobility. One of the main reasons is due to the predetermination of an end-to-end route before data transmission. The discovery and recovery procedures are also time and energy consuming. Once the path breaks, data packets will get lost or be delayed for a long time until the reconstruction of the route, causing transmission interruption. In this paper, a novel Position-based Opportunistic Routing (POR) protocol is proposed, in which several forwarding candidates cache

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

the packet that has been received using MAC interception. If the best forwarder does not forward the packet in certain time slots, suboptimal candidates will take turn to forward the packet according to a locally formed order. In this way, as long as one of the candidates succeeds in receiving and forwarding the packet, the data transmission will not be interrupted. Potential multi paths are exploited on the fly on a per packet basis, leading to POR's excellent robustness.

II. ALERT: AN ANONYMOUS LOCATION-BASED EFFICIENT ROUTING PROTOCOL

A. Attack model

Attackers can be battery powered sensors that passively receive network packets and detect activities in their vicinity. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets.

(1) Capabilities. By eavesdropping, the adversary nodes can analyze any routing protocol and obtain information about the communication packets in their vicinity and positions of other nodes in the network. They can intrude on some specific vulnerable nodes to control their behavior, e.g., with denial-of-service (DoS) attacks, which may cut the routing in existing anonymous geographic routing methods.

(2) Incapabilities. The attackers do not issue strong active attacks such as black hole. They can only perform intrusion to a proportion of all nodes. Thus, both symmetric and public/private key cannot be brutally decrypted within a reasonable time period. Therefore, encrypted data is secure to a certain degree when the key is not known to the attackers.

B. Dynamic Pseudonym and Location Service

In ALERT, each node uses a dynamic pseudonym as its node identifier rather than using its real MAC address, which can be used to trace nodes' existence in the network. To avoid pseudonym collision, we use a collision-resistant hash function, such as SHA 1 [2], to hash a node's MAC address and current time stamp. A node's pseudonym expires after a specific time period in order to avoid adversaries associating the pseudonyms with nodes.

ALERT uses the DISPOSER location service [13] to enable each source node to securely obtain the location and the public key of the destination. The public key is used to enable two nodes to securely establish a symmetric key Ks for secure communication. For example, source node A sends the location request containing destination B's identity to the service. Then the location service returns an encrypted position and the public key of B, which can be decrypted by A using the pre-distributed shared key between A and its location service.

C. Design of the ALERT routing algorithm

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 upperleft 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. As shown in the upper part of Figure 1, given an area, we horizontally partition it into two zones A1 and A2. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 to 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.

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. Specifically, in the ALERT routing, each data source or forwarder partitions the zone it resides in order to separate itself and ZD into two zones. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF). In the last step, the data is broadcasted to k nodes in ZD, providing k-anonymity to the destination.

Zone position refers to the upper-left and bottom-right coordinates of a zone. One problem is finding the position of ZD. Let H denote the total number of partitions in order to produce ZD. Using the number of nodes in ZD (i.e., k), and node density ρ, H is calculated by

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

$$H = \log_2\left(\frac{\rho.G}{k}\right),$$

where G is the size of the entire network area. Using the calculated H, the size G and position (0, 0), (xG, yG) of the entire network area, and the position of D, S can calculate the zone position of ZD. Assume ALERT partitions zone vertically first. After the first vertical partition, the positions of the two generated zones are (0, 0), (0.5xG, yG) and (0.5xG, 0), (xG, yG). S then finds the zone where ZD is located, and divides that zone horizontally. This recursive process continues until H partitions are completed. The resulting zone is the desired destination zone, and its position can be retrieved accordingly. Therefore, the size of the destination zone is G 2H . For example, for a network with size G = 8 and position represented by (0, 0), (4, 2), if H = 3 and the destination position is (0.5, 0.8), the resulting destination zone position is (0, 0), (1, 1) and its size is $\frac{8}{2^3} = 1$

For successful communication between S and D, S and each packet forwarder embeds the following information into the transmitted packet. (1) The zone position of ZD, i.e., the Hth partitioned zone. Each packet forwarder needs this position to check whether it is separated from the destination after a partition and whether it resides in ZD. (2) The encrypted zone position of the Hth partitioned zone of S using D's public key, which is the destination for data response. (3) The randomly selected TD for routing to the next RF. And (4) A bit (i.e., 0/1), which is flipped by each RF, indicating the partition direction (horizontal or vertical) of the next RF. In order to save computing resources, we let the source node calculate the information of (1) and (2) and forward it along the route rather than letting each packet forwarder calculate the values. In order to hide the packet content from adversaries, ALERT employs cryptography. Thus, instead of using public key cryptography, ALERT uses symmetric key encryption for transmitted data.

"Notify and go" has two phases: "notify" and "go". In the first "notify" phase, S piggybacks its data transmission notification with periodical update packets to secretly notify its neighbors that it will send out a packet. The packet includes two random back-off time periods, t and t0. In the second "go" phase, S and its neighbors wait for a certain period of randomly chosen time ∈ [t, t+t0] before sending out messages. S's neighbors 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. Thus, t0 should be long enough to minimize interference and balance out the delay between S and S's farthest neighbor in order to prevent any intruder from discriminating S. This camouflage augments the privacy protection for S by η-anonymity, where η is the number of its neighbors. Therefore, it is difficult for an attacker to analyze traffic to discover S.

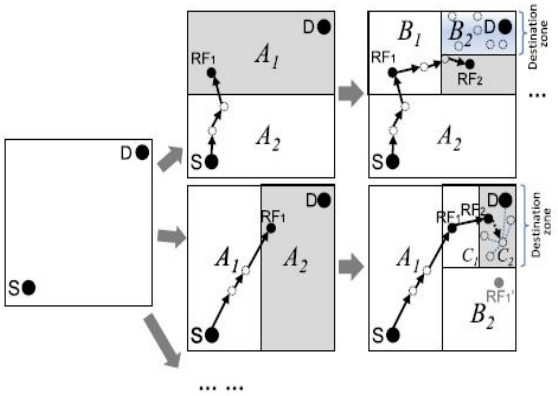

Figure 1: Examples of different zone partitions.

D. Resilience to timing attacks and Strategy to counter intersection attacks.

In timing attacks [11], through packet departure and arrival times, an intruder can identify the packets transmitted between S and D, from which it can finally detect S and D. For example, two nodes A and B communicate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

with each other at an interval of five seconds. After a long observation time, the intruder finds that A's packet sending time and B's packet receiving time have a fixed five second difference such as (19:00:55, 19:01:00) and (20:01:33, (20:01:38). Then, the intruder would suspect that A and B are communicating with each other.

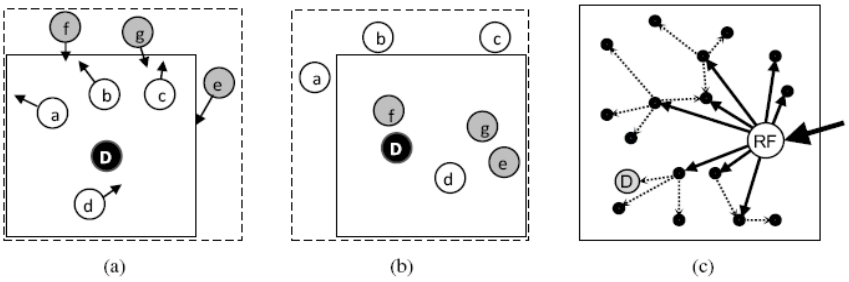

Figure 2: Intersection attack and solution.

Figure 2(a) is the status of a ZD after a packet is broadcasted to the zone . The arrows show the moving directions of nodes. We can see that nodes a, b, c, d, and D are in ZD. Figure 2(b) is the subsequent status of the zone the next time a packet is transmitted between the same S-D pair. This time, nodes d, e, f, g and D are in ZD. Since the intersection of the in-zone nodes in both figures includes d and D, D could be identified by the attacker. Therefore, the longer an attacker watches the process, the easier it is to identify the destination node.

To counter the intersection attack, ZAP [14] dynamically enlarges the range of anonymous zones to broadcast the messages or minimizes communication session time. Fig 2(c) shows the two-step process with the first step in solid arrows and the second step in dashed arrows. We can see that the first step reaches a number of nodes in the destination zone, but the destination is reached in the second step. Because the deliveries of pkt1 and pkt2 are mixed, an attacker observes that D is not in the recipient set of pkt1, though D receives pkt1 in the delivery time of pkt2.

III. PROPOSED METHOD

3.1. Position-Based Opportunistic Routing

Opportunistic routing (OR) takes advantages of the spatial diversity and broadcast nature of wireless networks to combat the time-varying links by involving multiple neighboring nodes (forwarding candidates) for each packet relay[19].

Firstly, we study geographic opportunistic routing (GOR), a variant of OR which makes use of nodes' location information. We identify and prove three important properties of GOR. The first one is on prioritizing the forwarding candidates according to their geographic advancements to the destination. The second one is on choosing the forwarding candidates based on their advancements and link qualities in order to maximize the expected packet advancement (EPA) with different number of forwarding candidates.

In conventional opportunistic forwarding, to have a packet received by multiple candidates, either IP broadcast or an integration of routing and MAC protocol is adopted. In POR, we use similar scheme as the MAC multicast mode described in[20]. The packet is transmitted as unicast (the best forwarder which makes the largest positive progress toward the destination is set as the next hop) in IP layer and multiple reception is achieved in interception.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

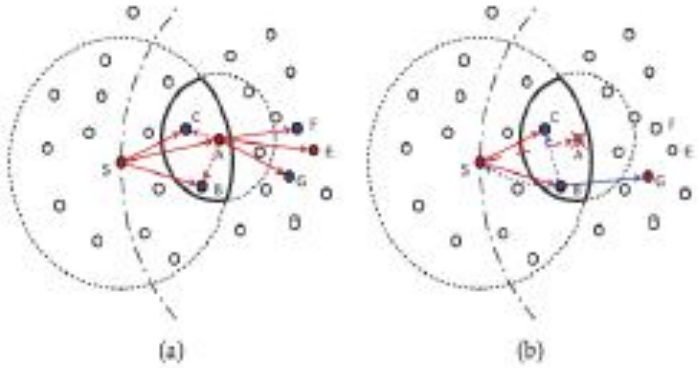

Figure 3. (a) Operation of POR in normal situation. (b) Operation of POR when the next hop fails to receive the packet.

As the data packets are transmitted in a multicast-like form, each of them is identified with a unique tuple (src_ip, seq_no) where src_ip is the IP address of the source node and seq_no is the corresponding sequence number. Every node maintains a monotonically increasing sequence number, and an ID_Cache to record the ID (src_ip, seq_no) of the packets that have been recently received. If a packet with the same ID is received again, it will be discarded. The basic routing scenario of POR can be simply illustrated in Fig. 3. In normal situation without link break, the packet is forwarded by the next hop node (e.g., nodes A, E) and the forwarding candidates (e.g., nodes B, C; nodes F, G) will be suppressed (i.e., the same packet in the Packet List will be dropped) by the next hop node's transmission. In case node A fails to deliver the packet (e.g., node A has moved out and cannot receive the packet), node B, the forwarding candidate with the highest priority, will relay the packet and suppress the lower priority candidate's forwarding as well as node S.

IV. EXPERIMENTAL RESULTS

The experimental results show the simulation results of the topology formation, position-based opportunistic routing, and the operation of POR when the next hop fails to receive the packet. The Qos parameters such as Throughput, Packet Drop, and Packet Delivery Ratio are achieved with their graphs.

A. Operation Of POR

Some of the nodes will be selected as forwarding candidates, only the nodes in the forwarding area will be the backup nodes. The sender and the next hop node select the area to be forwarded.

B. Operation Of POR After Link Failure

Suppose if a node fails to deliver a packet, the nearby nodes in the forwarding candidate which has the highest priority will send the packet forward and avoid the lower priority candidates that is forwarding. If a packet is pulled back from the Mac layer it will not be routed again.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

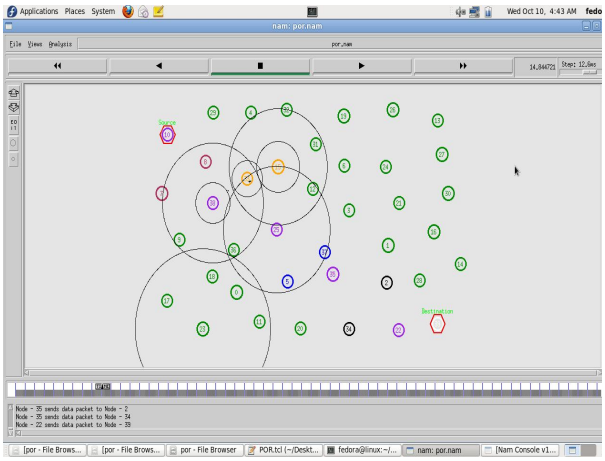

Figure 4. Operation of POR

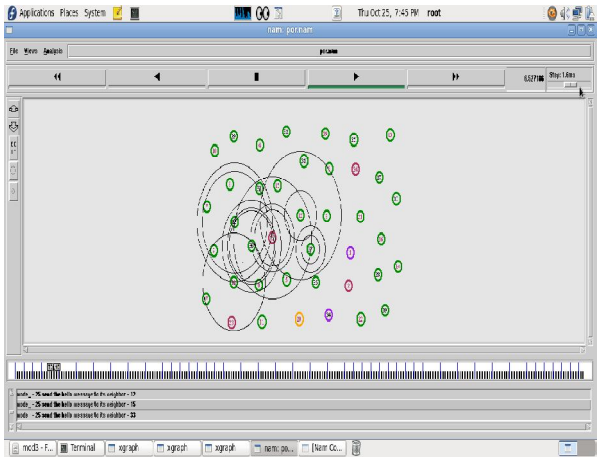

Figure 5. Operation of POR after link failure

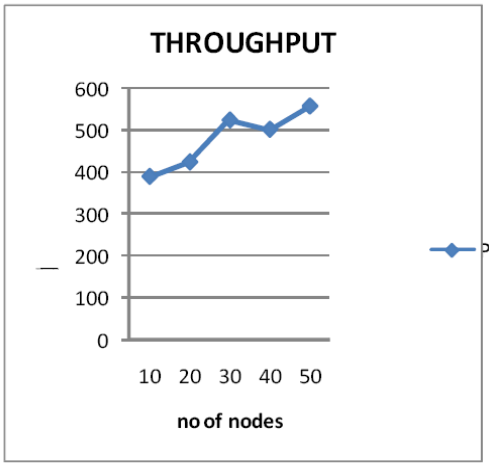

Figure 6. Throughput

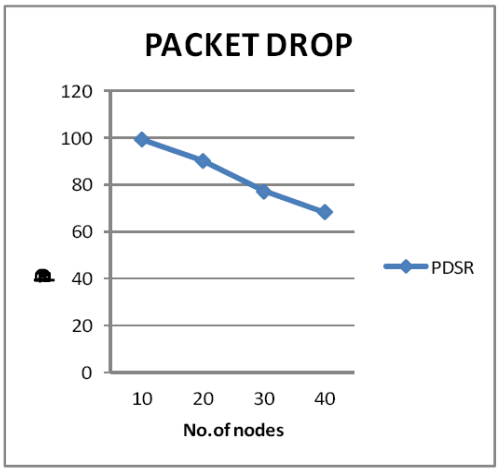

Figure 7. Packet Drop

Over a communication channel, the average rate of successful message delivery is the throughput that is Shown in figure 6. The total number of packets dropped during the transmission is shown in figure 7. As the number of node increases the number of packet drop will also increase. The ratio of the number of data packets received at the destinations to the number of data packets sent by the sources is known as the packet delivery ratio that is shown in figure 8.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

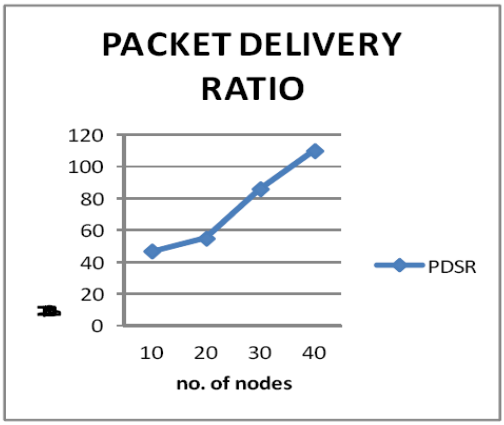

Figure 8. Packet Delivery Ratio

V. CONCLUSION

Some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations and routes. Like other anonymity routing algorithms, ALERT is not completely bullet-proof to all attacks. In this work, the problem of delivering data packets for highly dynamic mobile ad hoc networks is solved. Already existing topology based routing protocols have node mobility. This issue is solved by an efficient position-based opportunistic routing (por) protocol which takes the property of geographic. Through simulation, we further confirm the effectiveness and efficiency of POR: high packet delivery ratio is achieved while the delay and duplication are the lowest. We compare our proposed technique with many traditional algorithms like DSDV in terms of energy saving, which results in our POR is better in energy saving.

REFERENCES

1. 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.
2. 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.
3. I. Aad, C. Castelluccia, and J. Hubaux. Packet coding for strong anonymity in ad hoc networks. In Proc. Of Securecomm, 2006.
4. A. R. Beresford and F. Stajano. Mix zones: User privacy in location-aware services. In Proc. of PERCOMW, 2004.
5. C.-C. Chou, D. S. Wei, C.-C. J. Kuo, and K. Naik. An efficient anonymous communication protocol for peer-to-peer applications over mobile ad-hoc networks. In JSAC, pages 192–203, 2007.
6. K. E. Defrawy and G. Tsudik. Prism: Privacy-friendly routing in suspicious manets (and vanets). In Proc. of ICNP, 2008.
7. K. El Defrawy and G. Tsudik. Alarm: Anonymous locationaided routing in suspicious manets. In Proc. of ICNP, 2007.
8. Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: a secure ondemand routing protocol for ad hoc networks. Wirel. Netw., 11:21–38, 2005.
9. V. Pathak, Y. Danfeng, and L. Iftode. Securing location aware services over VANET using geographical secure path routing. In Proc. of ICVES, 2008.
10. S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu. Data-centric storage in sensornets with GHT, a geographic hash table. Mob. Netw. Appl., 8(4):427– 442, 2003.
11. J. Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In Proc. of WDIAU, pages 10–29, 2001.
12. X. Wu. AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol. IEEE TMC, 2005.
13. X. Wu. DISPOSER: distributed secure position service in mobile ad hoc networks: Research Articles. WCMC, 6(3):357–373, 2006.
14. X. Wu, J. Liu, X. Hong, and E. Bertino. Anonymous Geo- Forwarding in MANETs through Location Cloaking. IEEE TPDS, 2008.
15. B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng. Anonymous Secure Routing in Mobile Ad-Hoc Networks. In Proc. of LCN, 2004.
16. Z. Zhi and Y. K. Choong. Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy. In Proc. Of ICDCSW, pages 646–651, 2005.
17. Mauve M., Widmer A., and Hartenstein H., (Nov./Dec.2001) "A Survey on Position-Based Routing in Mobile Ad Hoc Networks," IEEE Network, vol. 15, no. 6, pp. 30-39.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

18. B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom, pp. 243-254, 2000.
19. E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "SOAR: SimpleOpportunistic Adaptive Routing Protocol for Wireless MeshNetworks," IEEE Trans. Mobile Computing, vol. 8, no. 12,pp. 1622-1635, Dec. 2009.
20. K. Zeng, Z. Yang, and W. Lou, "Location-Aided Opportunistic Forwarding in Multirate and Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 6, pp. 3032-3040, July 2009.