APSAR: Anonymous Position base Security Aware Routing Protocol for MANETs

Priyanka Malgi
Departement of electronics and
Telecommunication Engineering
S.P.I.T.Andheri
Mumbai

Dayanand Ambawade
Departement of electronics and
Telecommunication Engineering
S.P.I.T.Andheri
Mumbai

ABSTRACT

In major scenarios of mobile ad hoc networking (MANET), nodes communicate to each other based on public identities. But while considering applications such as military and law enforcement domains nodes should not expose their identities and node movements should be untraceable. So, alternately, nodes need to communicate based on their current locations or positions. While doing so; there is a challenge for nodes to maintain anonymity protection from outside observers or malicious attackers. Full anonymity protection can be achieved only when; sources, destinations and routes all are protected. In this work, To offer anonymity protection, we propose an Anonymous Position-based security aware routing protocol (APSAR). Experimental results exhibit consistency with the theoretical analysis, and show that APSAR achieves better route anonymity protection compared to other anonymous routing protocols. Also, APSAR achieves comparable routing efficiency to the GPSR geographical routing protocol.

General Terms

Congestion Window Size, Packet Size, NS-2

Keywords

Ad hoc Anonymity, Geographic routing, Security

1. INTRODUCTION

The new age of Information Technology is a drastic change from traditional regular desktop computing, where there is a need for isolated workstations communicate to each other through shared servers in a fixed network, to an environment where a large number of different platforms communicate over multiple network platforms. In this environment the devices adapt and reconfigure themselves individually and collectively, to support the requirements of mobile users. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid 1990s.[1]. Mobile ad hoc networks (MANETs) are autonomous collection of mobile nodes which communicate over relatively bandwidth constrained wireless links. MANETs differ from wireless networks, such as cellular networks, MANETs are self-organizing and adaptive; they can therefore construct and deconstruct without the need for any central management system. So MANETs are very attractive for scenarios requiring rapid network deployment, such as search and rescue operations. These nodes are free to move about arbitrarily. MANETs exhibit very interesting properties: they are self-organizing, decentralized and support mobility. Hence, they are very good candidates for tactical networks in military applications. There are many challenging security issues which need to be addressed before MANETs are ready for widespread commercial or military deployment. Major security problem is the issue of secure routing in the presence of selfish or malicious nodes, which selectively drop packets they are required to forward and in so doing, these selfish or malicious entities can cause various communication problems.

1.1. Routing Challenges and design issues

Wireless cellular system has been in use since 1980s.Wireless system operates with the aid of a centralized supporting structure such as an access point. These access points help the wireless users to keep connected with the wireless system, when they roam from one place to other. In wireless system the device communicate via radio channel to share resource and information between devices.. Recent advancement of wireless technologies like Bluetooth, IEEE 802.11 introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) which operate in the absence of central access point. It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network. User has great responsibility to design such a network at cheapest cost and minimum time. MANETs shows distinct security threats, such as[1]

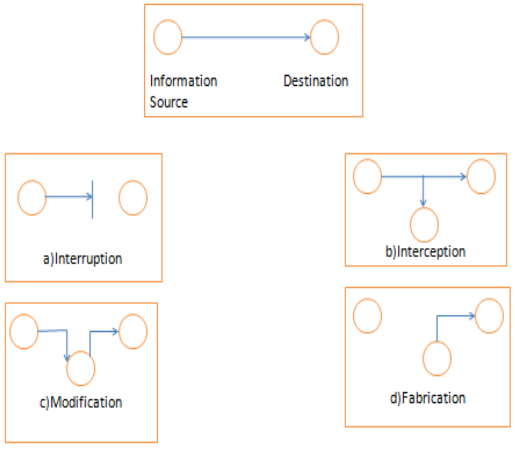

Figure 1. Security Threats

Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability.

Examples:

- Destroying some H/W (disk or wire).
- Disabling file system.

Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality.

Examples:

- Wiretapping to capture data in a network.
- Illicitly copying data or programs.

Modification: An unauthorized party gains access and tampers an asset. This is an attack on integrity.

Examples:

- Changing data files.
- Altering a program.
- Altering the contents of a message
- Security Attributes

1.2 Security of a MANET can be inspecting by analyzing the certain attributes. These are:

1. Availability

- The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This attribute is affected by DOS.

2. Integrity

- Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways
- Malicious altering
- Accidental altering
- A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

3. Confidentiality

- Confidentiality means that certain information is only accessible to those who have been authorized to access it.

4. Authenticity

- Authenticity is essentially assurance that participants in communication are genuine and not impersonators .It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity.

5. Authorization

- Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

6. Anonymity

- Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the systems software.
- This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities

In this proposed work we are working with one of the Security Attribute which is Anonymity. Pfitzmann and Hansen define anonymity in [2] as ”the state of being not identifiable within a set of subjects”. In MANET

data communication, anonymity means that the identities of source, destination and the route of a data message cannot be linked to any node within the network. A related requirement is unlink ability [2], i.e. it is necessary to ensure that data packets from a single data flow cannot be linked in order to trace the origin and the destination of this flow. Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [3], [4], [5], [6],[14] and redundant traffic [7],[8], [9], [10], [11], [12], [13]. Most of the existing solutions are limited by providing anonymity at a high cost because public-key based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide ll of the aforementioned anonymity protections. For example, ALARM [5] cannot protect the location anonymity of source and destination and ZAP [13] only focuses on destination anonymity.

To offer anonymity protection at a low cost, we propose an Anonymous Position-based security aware routing protocol (APSAR). Experimental results exhibit consistency with the theoretical analysis, and show that APSAR achieves better route anonymity protection considering other anonymous routing protocols. Also, APSAR achieves comparable routing efficiency to the GPSR geographical routing protocol.

The remainder of this paper is organized as follows. In Section 2, we present and discuss the design of the APSAR routing protocol. In Section 3, Experimental performance of the APSAR protocol in comparison with GPSR is evaluated. In Section 4, we describe related anonymous routing approaches in MANETs. The conclusion and future work are given in Section 5.

2. ANONYMOUS POSITION BASED SECURITY AWARE ROUTING PROTOCOL

2.1 Zonal Environment

Consider a MANET in a large area where geographic routing is applied for communication. The position of a sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide untraceability is needed to ensure the anonymity of the sender when the sender communicates with the remaining

network. Moreover, an attacker or malicious observer or malicious node may try to block or modify the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even tracback to the sender by detecting the data transmission direction. Therefore, the route should also be undetectable or untraceable.
A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity. In this work, the attackers can be battery powered nodes 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.

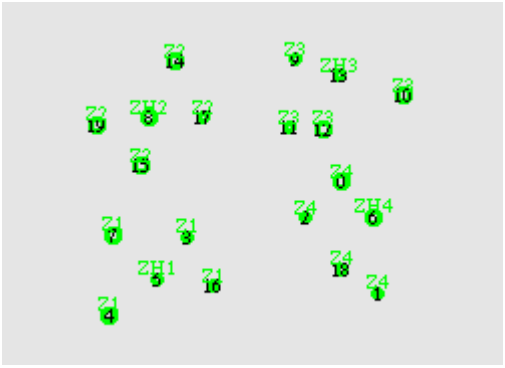

Figure 2. Examples of different zone partitions

2.2 APSAR routing algorithm

1. Node Initialization: Node environment is created for total 20 nodes
2. Zone Creation wherein the network area or total 20 nodes' environment is divided into 4 zones.
3. Zone Discovery Process wherein each node discovers its zonal head and exchanges routing related information.

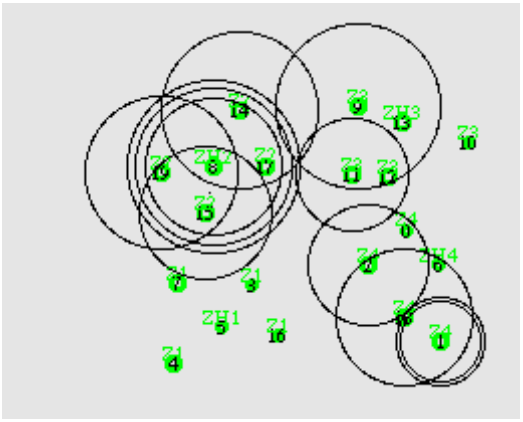

Figure 3. Routing among zones

4. Key Generation for transmitting data securely
5. Source node starts data transmission to destination
6. It selects first neighbor in zone and transmits data securely using encryption to first neighbor
7. This neighbour then forwards packet to next zone till it is received by destination zone.
8. Finally the destination node retrieves all data received successfully using decryption

2.3. Packet Format

Dz: Destination zone

Td: Temporary destination

Pf: Packet forwarder

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 Dz, i.e., the Nth partitioned zone.

(2)The encrypted zone position of the Nth partitioned zone of S using D's public key, which is the destination for data response.

(3)The current randomly selected Td for routing.

(4)A bit (i.e.0/1), which is flipped by each Pf, Indicating the partition direction(horizontal or vertical) Of the next Pf.

Table 2.1:Routing table

Node	one hop neighbour
Node(11)	(12)
Node(11)	(13)
Node(11)	(14)
Node(11)	(15)
Node(11)	(16)
Node(11)	(17)
Node(11)	(18)
Node(11)	(19)
Node(12)	(13)
Node(12)	(14)
Node(12)	(15)
Node(12)	(16)
Node(12)	(17)
Node(12)	(18)
Node(12)	(19)
Node(13)	(14)
Node(13)	(15)
Node(13)	(16)

Node(13)	(17)	
Node(13)	(18)	
Node(13)	(19)	
Node(14)	(15)	
Node(14)	(16)	
Node(14)	(17)	
Node(14)	(18)	
Node(14)	(19)	
Node(15)	(16)	
Node(15)	(17)	
Node(15)	(18)	
Node(15)	(19)	
Node(16)	(17)	
Node(16)	(18)	
Node(16)	(19)	
Node(17)	(18)	
Node(17)	(19)	
Node(18)	(19)	

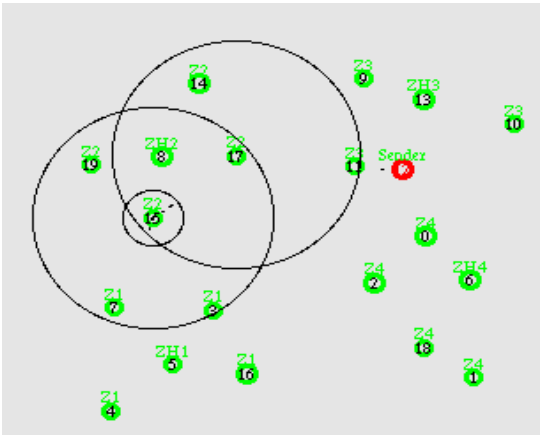

Figure 4. Sender transmitting data

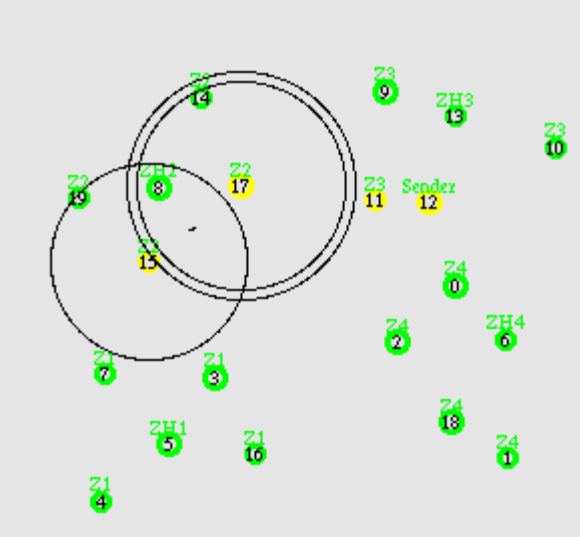

Figure 4. Final Route Estimation

2.4 Anonymity Protection

APSAR offers location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing , which always takes the shortest path, APSAR 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 SD pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the *Pf* set changes due to the random selection of *Pfs* 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. Additionally, since an *Pf* 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. APSAR strengthens the privacy protection for *S* and *D* by the *unlink ability* of the transmission endpoints and the transmitted data [1]. That is, *S* and *D* cannot be associated with the packets in their communication by adversaries. The route anonymity due to random relay node selection in APSAR prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In APSAR, 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 APSAR 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.

3. PERFORMANCE EVALUATION

In this section, we provide experimental evaluation of the APSAR protocol. It proves the superior performance of ASR in providing anonymity with low cost of overhead. Recall that anonymous routing protocols can be classified into hop-by-

hop encryption and redundant traffic. ASR is geographic routing, so we compare ASR with the baseline routing protocol GPSR [16] in the experiments. In GPSR, a packet is always forwarded to the node nearest to the destination. When such a node does not exist, GPSR uses perimeter forwarding to find the hop that is the closest to the destination.

3.1 Parameters

The tests were carried out on NS-2.34 simulator using 802.11 as the MAC protocol with a standard wireless transmission. UDP/CBR traffic [15].
We use the following metrics to evaluate the routing performance in terms of effectiveness on anonymity protection and efficiency:

1. **Latency per packet**: This is the average time elapsed after a packet is sent and before it is received. It includes the time cost for routing and cryptography. This metric reflects the latency and efficiency of routing algorithms.

2. **Delivery rate**: This is measured by the fraction of packets that are successfully delivered to a destination. It shows the robustness of routing algorithms to adapt to mobile network environment

3. **Throughput**: Throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

4. **Drop-ratio:** Packet loss or drop occurs when one or more packets of data travelling across a network fail to reach their destination. The fraction of lost packets increases as the traffic intensity increases. Therefore, performance at a node is often measured not only in terms of delay, but also in terms of the probability of packet loss.

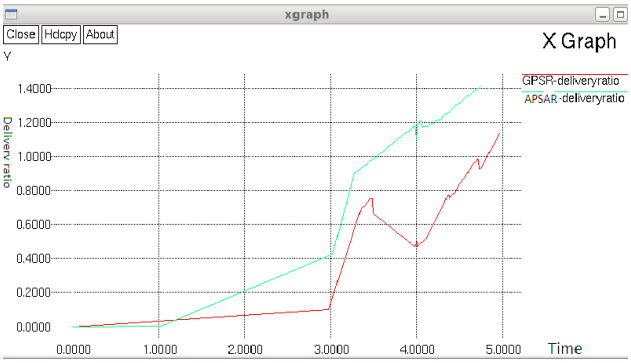

Figure 5. Delivery ratio/rate

Figure 5shows the comparison between APSAR and GPSR for the parameter **Delivery ratio/rate** versus **Time.** We see that packet delivery ratio for APSAR is much better than GPSR.As time on X axis goes on increasing packet delivery ratio also goes on increasing in better manner. This is due to the reason that APSAR is having better anonymity protection for Source, Destination and the entire route; as the nodes in next single hop are selected randomly gives better packet delivery.

Figure 6.Latency

Figure 6 shows the comparison between APSAR and GPSR for the parameter **Latency** versus **Time.** We see that Latency for APSAR is much lower than GPSR; as time on X axis goes on increasing..This is due to the reason that APSAR is having better anonymity protection for Source, Destination and the entire route; as the nodes in next single hop are selected randomly gives better packet delivery. As packet delivery rate is better in turn it also helps reducing latency.

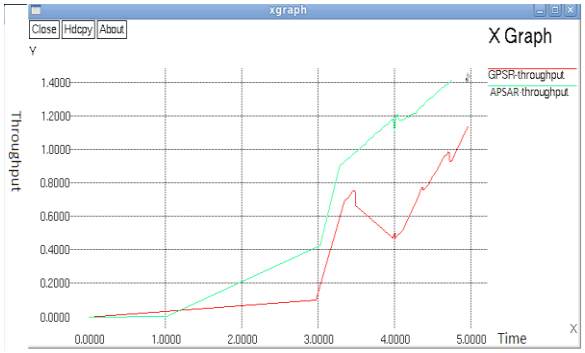

Figure 7.Throughput

Figure 7 shows the comparison between APSAR and GPSR for the parameter Throughput versus Time. We see that packet delivery ratio and Latency for APSAR is much better than GPSR; which in turn helps improving Throughput As time on X axis goes on increasing Throughput also goes on increasing in better manner.

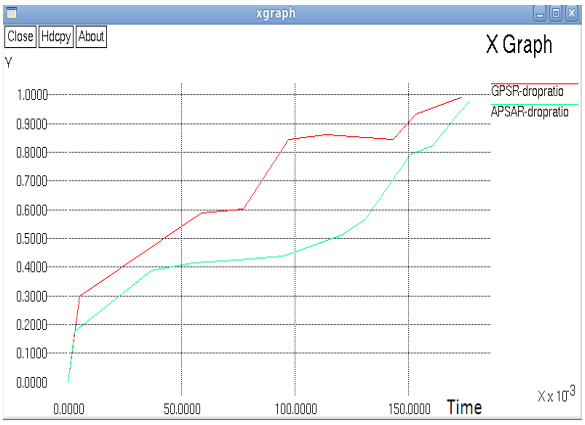

Figure 8.Drop-ratio

Figure 8. shows the comparison between APSAR and GPSR for the parameter Drop-ratio versus Time. We see that packet drop-ratio for APSAR is much better than GPSR.

4. RELATED WORK

Table 1**.** Summary of existing anonymous routing protocols

Name	Identity Anonimity	Location Anonimity	Route Anonimity
MASK[18]	**Source**	**n/a**	**Yes**
ANODR[19]	**Source, Destination**	**n/a**	**Yes**
AO2P[10]	**Source, Destination**	**Source, Destination**	**No**
PRISM[6]	**Source, Destination**	**Source, Destination**	**No**
ALARM[5]	**Source, Destination**	**Source**	**no**

Anonymous routing schemes in MANETs have been studied in recent years. Taking example of ALARM [5] uses proactive routing, where each node broadcasts its location information to its authenticated neighbors so that each node can build a map for later anonymous route discovery. However, this map construction leaks destination node locations and compromises the route anonymity. But in APSAR as we have seen nodes are randomly selected based on next single hopping. So this is not broadcasting location information prior but after the packet is forwarded to desired node or forwarder. So without leaking out location information of source as well as Pf (Packet Forwarder) trustfully packet transmission is done.

5. CONCLUSION AND FUTURE WORK

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. APSAR is distinguished by its better route anonymity protection. Experiment results show that APSAR can offer high anonymity protection when compared to the base-line GPSR algorithm. Still like other anonymity routing algorithms, APSAR is not completely bullet-proof to all attacks. Future work lies in modifying APSAR in an attempt to fight stronger, active attackers and to be proved by related theoretical and simulation results.

6. REFERENCES

[1] Henric Johnson,Blekinge Institute of Technology, Sweden, Introduction:Computer and Network Security.

[2] A Ptzmann and M. Hansen, " Anonymity, Unlinkability, Undetectability,Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology", *Tech. Rep*., February 2008.

[3] Z. Zhi and Y. K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy", *In Proc. of ICDCSW*,2005.

[4] V. Pathak, D. Yao, and L. Iftode, "Securing location aware services over VANET using geographical secure path routing*", In Proc. of ICVES*,2008.

[5] K. El Defrawy and G. Tsudik, "Alarm: Anonymous location-aided routing in suspicious manets", *In Proc. of ICNP*,2007.

[6] K. El Defrawy and G. Tsudik, "Prism: Privacy-friendly routing in suspicious manets (and vanets)", *In Proc. of ICNP*, 2008.

[7] Y-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure ondemand routing protocol for ad hoc networks", *Wirel. Netw*.,2005.

[8] I Aad, C. Castelluccia, and J. Hubaux, "Packet coding for strong anonymity in ad hoc networks", *In Proc. of Securecomm*,2006.

[9] 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", *In JSAC*,pages 192203, 2007.

[10] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol", *TMC*,2005.

[11] 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.

[12] A R. Beresford and F. Stajano, "Mix zones: User privacy in locationaware services", *In Proc. of PERCOMW*,2004.

[13] Y. Zhang, W. Liu, and W. Luo, J. Liu, X. Hong, and E. Bertino,"Anonymous Geo- Forwarding in MANETs through Location Cloaking",*TPDS*,2008.

[14] Sk. Md. M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks", *In Proc. of SAINT*, 2006.

[15] http://www.isi.edu/nsnam/ns/

[16] http://www.cs.binghamton.edu/kliu/research/ns2code/index.html.

[17] T.Camp,J.Boleng,andV.Davies, "A survey of mobility models For adhoc network research", *WCMC*, 2002.

[18] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng,"Anonymous Communications in Mobile Ad Hoc Networks", *In Proc.of INFOCOM*,2005.

[19] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on demand routing protocol with untraceable routes for mobile adhoc networks",*Proc. of MobiHoc*,pages 291302, 2003

[20] L. Zhao and H. Shen," Alert: An anonymous location-based efficient routing protocol in manets",*Proc. of ICPP*,2011.