A Study of Efficient Anonymous Routing Protocols in MANET

Anupriya Augustine
M Tech Scholar
Department of Electronics and Communication
Vimal Jyothi Engineering College, Kannur

Jubin Sebastian E
Assistant Professor
Department of Electronics and Communication
Vimal Jyothi Engineering College, Kannur

ABSTRACT
Mobile Ad Hoc Network (MANET) is a type of wireless network without a fixed topology consist a set of self organized nodes which are randomly, frequently and unpredictably mobile. MANET has a wide range of applications in civilian and military systems because of its infrastructureless nature and rapid self configuration capability. MANET is an open environment and it is susceptible to many security attacks due to dynamic topology and lack of centralized monitoring authority. Anonymous routing protocols conceal the identities about the route, source and destination to provide security and privacy from intruder's attacks. This paper provides an overview of most efficient anonymous routing protocols in MANET and examines the security efficiency of these protocols. The parameters consider for the comparative study of these protocols are the number of actual participating nodes in the network, latency in packet transmission, packet delivery rate and the transmission cost. The protocols taken in to account include, AO2P, ALARM and ALERT.

General Terms
Ad hoc On-demand Position based Private Routing Protocol, Anonymous Location Aided Routing, Anonymous Location-Based Efficient Routing Protocol.

Keywords
Mobile Ad Hoc Networks, security, anonymity, routing protocols.

1. INTRODUCTION
Without fixed topology collection of mobile nodes forming an instant network is called ad hoc network. In this network nodes perform as both router and host simultaneously, it will move out or join in the network freely. Ad hoc network does not have any base infrastructures such as in the conventional networks. In the computing industry the importance of Wireless network is become very high. Wireless network are adapted to enable mobility to a great extend. There are two types of network, they are Infra-structured network and ad-hoc network. In Infra-structured network have the network with fixed and wired gateway. In ad hoc networks, where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range.

MANET is very attractive in tactical and military applications because of rapidly deployable and self-organizing configurability. Like tactical communications in a battlefield, where the environment is unfavorable, but fast network establishment self reconfiguration and security-sensitive operations are absolutely essential. For providing security for MANET so many anonymous [1] routing protocols are developed.

2. ROUTING IN MANET
Routing protocols in MANET are divided in to three main groups (see ***Figure 1***). They are reactive, proactive and hybrid routing protocols. Depending on the mechanism used for routing purposes, they are mainly included in to two categories; they are hope by hope encryption and redundant traffic.

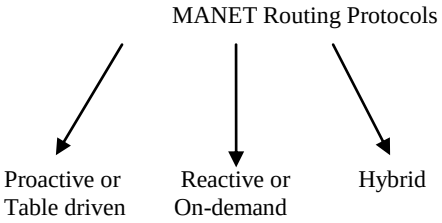

Fig 1 MANET Routing Protocols classification

2.1 Proactive or Table-driven Routing Protocols
Proactive routing protocols also called table driven routing protocols. In this type of protocols a table contains all the latest and consistent information of all the nodes in the network. Periodic information about the dynamics of the nodes is updated in the table for an active network. Routing table information is used for the data transmission in the network. Protocols in this category experiences lower latency.

2.2 Reactive or On-demand Routing Protocols
Another group of MANET routing protocol is reactive or on-demand routing protocol. In this type the protocol establishes a route if and only if a node wants to route data packets. Route discovery process increases.

2.3 Hybrid Routing Protocols

The third class of MANET routing protocol is the hybrid protocols. It combines the advantages of both proactive and reactive routing protocols and reduces the limitations of these two. Hybrid type reduces the traffic overhead in proactive and transmission latency in reactive protocols.

3. ROUTING ATTACKS IN MANETS

Active cooperation of all the nodes is required to provide routing between the source and destination in the network. Ad hoc networks are vulnerable to different types of attacks due to dynamic, distributed infrastructureless nature of MANETs, and lack of centralized authority [2].

The attacks to be faced by MANETs are very high those to be faced by the traditional wireless networks. MANETs are susceptible to both passive eavesdrops as well as active malicious attacks due to the accessibility of the wireless channel to both the genuine user and attacker. The main problem in the implementation of complex security algorithms are the limited power backup and limited computational capability of the individual nodes. Frequent network reconfigurations because of the nodes mobility create more chances for attacks.

Different types of attacks on MANET are passive and active attacks.

In passive attack the attacker listens and taps the communication between two nodes. Passive attacks are adverse for the security and privacy of communication. Operation of the communication channel is not disturbed by the passive attacker. But the attacker explores some valuable information about the communication channel. Topology of the network or the relationship between the nodes is used by the passive attacker to find out the network map. This can create some active attacks in the network.

Active attacker can inject unwanted information in the communication channel. It can also listen and modify the information in that channel. Active attackers can replay, modify or deletes some packets from the network. In a replay attack, the attacker resends a packet that was already transmitted. In modify attack, the attacker can modify the active packets with unwanted information which causes incorrect updates of the routing table. So the packets are transmitted to wrong destinations. Active attacks create network congestion problems.

The well known routing attacks in MANETs are discussed below.

3.1 Flooding Attack

It is also known as Routing Table Overflow. In this attack the attacker node send more information to the network which causes overflow of the routing tables.

3.2 Black Hole Attack

In this attack, the attacker nodes reply false route information for the route request. If the malicious route is established then the current active route is routed through this new attacker route and the data in the network may be misused or discarded.

3.3 Wormhole Attack

In this attack two attacking nodes cooperate between each other. Capturing routing traffic is down by one attacker at one point of the network and tunnels it to another point in the network. A private high speed communication link is shared between the two attackers. The network is selectively injected the tunnel traffic by the attackers. Then the routes established under the control over the wormhole link. The wormhole attacks distort the topology of the network.

4. ANONYMOUS ROUTING PROTOCOLS

In the past years number of anonymous routing protocols are proposed for MANET [3] - [15] the following four phases are included most commonly.

For to providing anonymity to source destination and route anonymous routing protocols are essential in MANET. The attacker can try different path to hack the data between the source and destination also able to find the identity of source and destination. There are different anonymous routing protocols are used in MANET to provide anonymity.

4.1 AO2P: Ad Hoc On-Demand Position Based Private Routing Protocol

In AO2P route discovery is done by using only the position of the destination. Other information such as forwarding nodes positions are hiding from the network. Real identities of source, destination and forwarding nodes are confidential. Date packet transmission uses the pseudo identifiers of the source, destination and forwarding nodes. ***Figure 2*** shows the route discovery of AO2P.

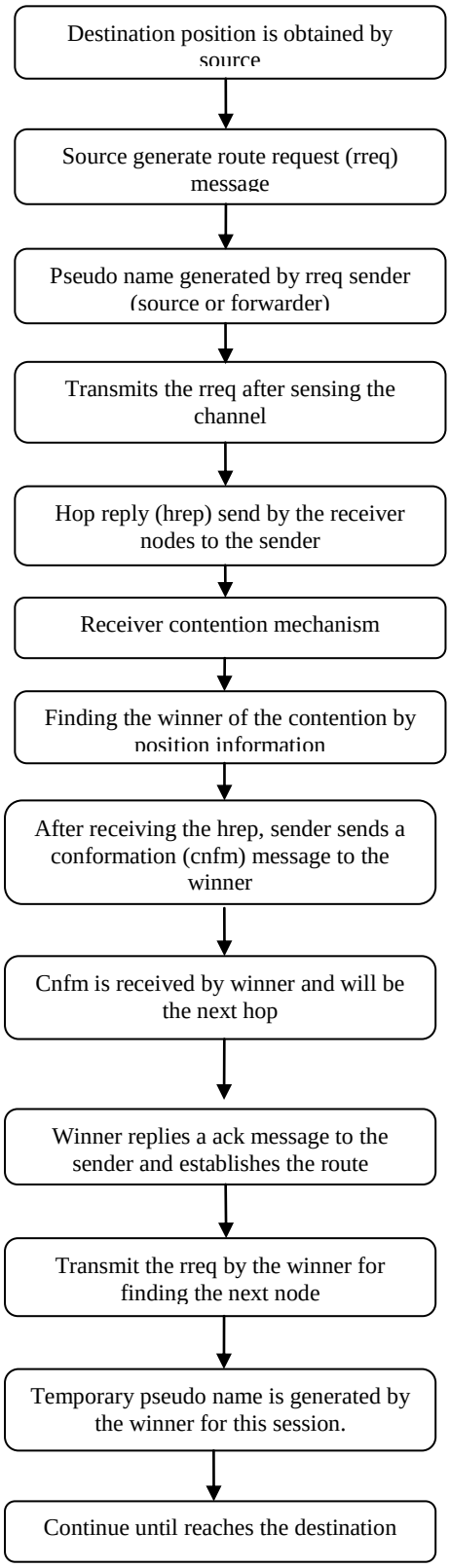

Fig 2: Route discovery in MANET

Route is established by receiver contention scheme. In this protocol receivers (node receiving the rreq message) are included in different class. The receiver which is closer to the destination is in the higher priority class. Highest priority receiver is the destination node. A node in the network obtains its position through GPS. Every node has a region around a fixed center called virtual home region (VHR). Position information of the node is updated to the servers in the VHR. This distributed secure position service is named as DISPOSER which improves the position security.

R-A02P is another method to provide more destination anonymity. In this position of a reference point is used for establishing the route instead of destination position.

4.2 ALARM: Anonymous Location Aided Routing

ALARM provides secure communication and privacy in both suspicious and hostile networks with reasonable efficiency. The ALARM [17] is a privacy preserving and secure link state based routing protocol. Node anonymity and protection from tracking are objectives of privacy. Security means nodes authentication and integrity of locations secure data forwarding in ALARM is by using the node's current locations.

Identification of nodes at certain locations in ALARM is relies on group signature to create pseudonyms. Security against active and passive attacks and privacy features are provided by ALARM. It is due to the integration of advanced cryptographic techniques such as group signature in this protocol which gives some features including authentication of node, integrity of the data, untraceability and anonymity. Group signature is another form of public key signature with further privacy features. The group manager (GM) helps to identify the nodes which are provided with the group signature. This technique contributes additional security for the MANET. The procedures in ALARM are given below.

4.2.1 Initialization

Group signature scheme is started by the GM. A private key is generated by all the group members and this key is concealed from other nodes. Group signature is produced from this private key. Each node also creates a public key and is revealed only for GM. Group public key is common to all members in the group.

4.2.2 Operation

1. Time duration is divided into slots having length T. A node creates a temporary public private key pair, PK-TMPs and SK-TM at the beginning of every time slot.
2. Location co-ordinates, public key, group signature and time stamp of all the group members are contains in a location announcement message (LAM). This LAM is broadcasted in to the MANET. This procedure is shown in ***figure 3***.
3. After receiving a LAM the node check this LAM is already received or not. If it is received at the first time, node authenticates the group signature and the time-stamp. If this is valid, then the LAM is broadcasted again and collects all current LAMs of each node in the network. A node connectivity graph and geographical map can be made from this information. It is shown in ***figure 4.***
4. Communication between a node and a node at another location is operated by first checking that whether there is a node at that location. If a node is present, then the temporary ID of the destination is obtained by transmitting a message to the destination's current location. A session key is used

to encrypt the data and this session key is also encrypted under the public key. The receiver node decrypts session key first and then decrypts the message.

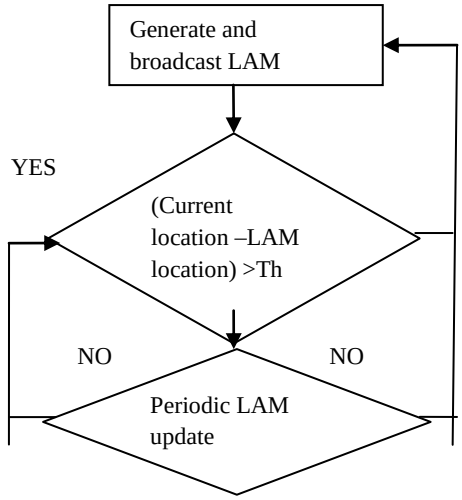

Fig 3: ALARM Sender Process

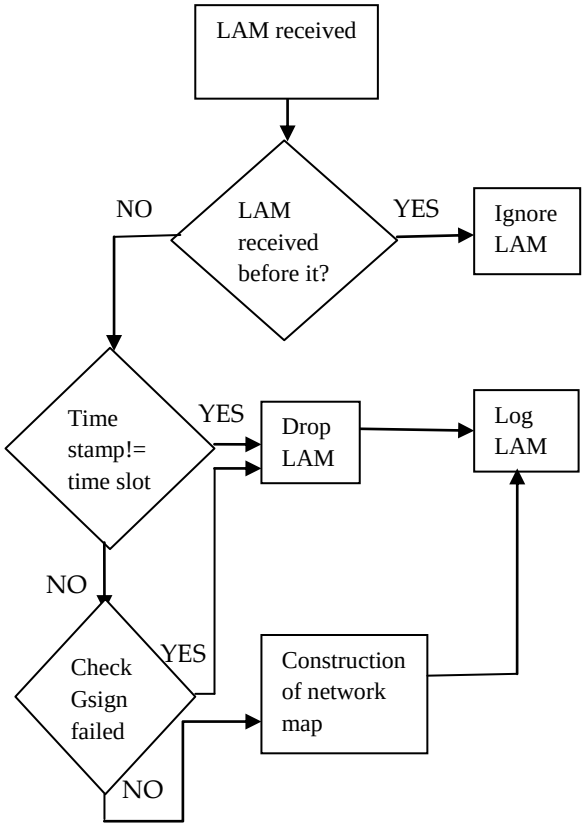

Fig 4: ALARM Receiver Process

4.3 ALERT: Anonymous Location-Based Efficient Routing Protocol

Route identity, source identity and destination identity are the main goals of anonymous routing protocols. The existing hop by hop encryption or redundant traffic concepts for providing anonymity results high cost. Hierarchical partition is the main technique used in ALERT [18]. The network is partitioned dynamically in to vertical and horizontal zones in ALERT. The algorithm used for data transmission is Greedy perimeter stateless routing (GPSR). Different mobility models such as random way point model and group mobility model can be used for ALERT. Communication latency is reduced to a great extend by using ALERT.

ALERT restricting a node's visibility only to its neighbors. Here the same initial and forwarded messages are created. So an attacker cannot identify whether a node is a source or a forwarding node. All this factors contributes to the achievement of anonymity.

Another mechanism used in ALERT to provide anonymity is the "notify and go". In this a number of nodes send information at the same time as the source sends packets. This hides the source among other nodes and provides high anonymity protection for the source. The number of nodes in the destination zone provides destination anonymity. The number of nodes in destination depends on the node density and destination zone size. ALERT is also providing protection from intersection attacks and timing attacks.

5. PERFORMANCE COMPARISON

The comparison of the three protocols are worked out based on some parameters such as the number of actual participating nodes, latency in packet transmission, packet delivery rate and transmission cost.

5.1 Number of Participating Nodes in the Network

ALARM and AO2P is based on the GPSR method. Next hop in GPSR scheme is always the node which is nearest to the destination. If such a node does not present, then GPSR practice perimeter forwarding to find the next hop. ALARM and AO2P uses the GPSR baseline for routing purposes. ALERT generates different routes between each source and destination pair since it produces many actual participating nodes. The actual participating nodes in ALERT also include the random forwarders. It contributes high routing anonymity in ALERT. GPSR always proceeds through the shortest paths. So the number of actual participating nodes is less compared to ALERT.

Increased number of participating nodes in ALERT creates more randomized routes between source and destination. So it is very difficult to detect this routes and it provides great anonymity for the route. When the node density increases, shorter routes are easily obtained in GPSR. So the number of actual participating nodes is almost steady with the increase in node density. The GPSR routing paths in ALARM and AO2P are easily identified by the attackers. This reveals that ALERT provides more anonymity than the AO2P and ALARM.

5.2 Latency in Packet Transmission

Latency is defined as the time difference between the packet transmission and receiving. Latency includes the time for both routing and cryptography. ALARM and AO2P take the shortest path for routing of packets. ALERT does not take the GPSR mechanism. Even thought ALERT not establishing the shortest path, the latency of ALERT is very much lower than ALARM and AO2P. More routing hops are generated in ALERT than AO2P and ALARM. But the latency in ALERT is significantly lower than the other two. This is because of the time needed for the public key encryption of ALARM and AO2P. ALERT follows symmetric key encryption only once which reduces the latency. ***Figure 5*** shows the delay of different protocols.

The transmission between two random forwarders in ALERT is depends on GPSR, it helps to reduce the latency further more. ALARM requires a periodic authentication of adjacent nodes and AO2P requires an encryption in each node. This process outweighs the low latency due to shortest path in ALARM and AO2P.

AO2P has a contention phase and it increases the path length. So AO2P has latency higher than ALARM. Increase in node density decreases latency of ALARM, AO2P and ALERT. Improved node density creates more relay nodes and shorter paths. Latency of ALARM and AO2P can be reduced to an extent by reducing the public key encryption operations.

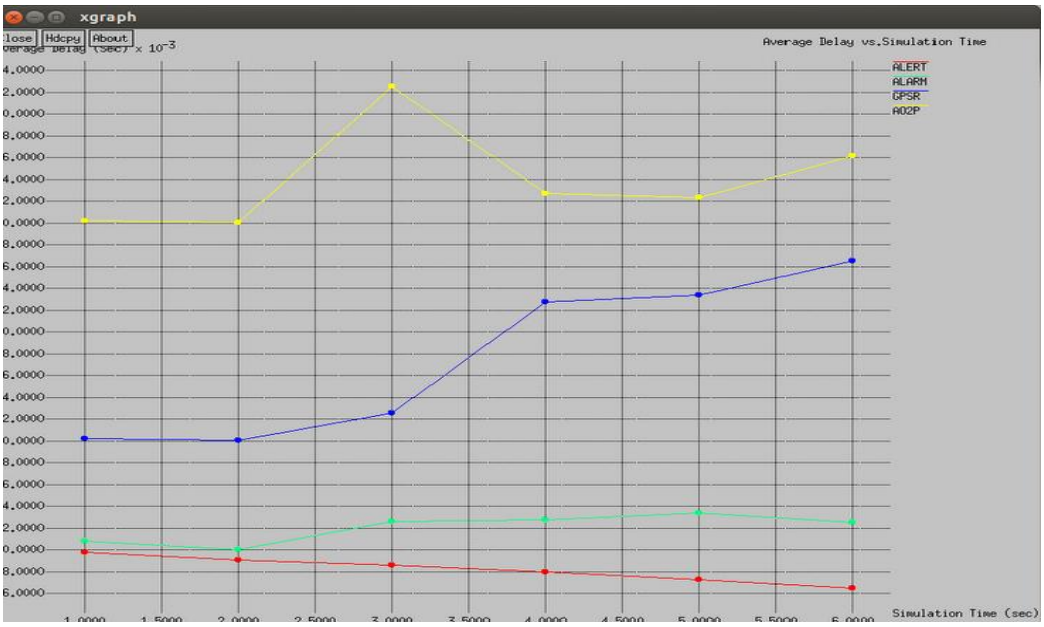

Fig 5: Latency in packet transmission comparison

5.3 Transmission Cost

The number of hops per packet is higher in ALERT than ALARM and AO2P. *T*otal routing hop counts divided by the number of packets sent gives the number of hops per packet. Routing path length of ALERT is higher than the shortest path of AO2P and ALARM. It is because of the random node selection of ALERT. Since compared to ALARM and AO2P, ALERT has relatively more hop per packet. This slightly increases the routing cost. Presence of more node density in ALERT gives better route anonymity than AO2P and ALARM. Increase in the routing cost of ALERT is avoidable when considering the route anonymity than the other protocols. Analysis of the hop by hop encryption based AO2P method and the redundant traffic based ALARM method, gives that ALERT having lower computing cost.

AO2P and ALARM is with equal number of hops per packet. ALARM with id dissemination hops for providing anonymity has higher number of hops per packet than others, and is doubled than that of ALERT. ALARM with id dissemination hops required periodical dissemination of node. This increases the cost dramatically in ALARM than others.

In summary, ALERT achieves enhanced route anonymity than ALARM and AO2P. ALERT has more number of actual participating nodes and its random relay node selection boost the anonymity. Transmission cost and latency in packet transmission are lower in ALERT compared with the other two. ALERT contributes better data delivery rate than ALARM and AO2P.

5.4 Packet delivery Rate

Fraction of successfully delivered packets to a destination is called the delivery rate. When the node moving speed increases without the destination updates, the delivery rates are reduced. In view of mobility of destination, the delivery rates are reduced in all the protocols. ALERT has higher delivery rates compared to AO2P and ALARM, as a result of final local broadcast process. ***Figure 6*** shows the packet delivery rate comparison.

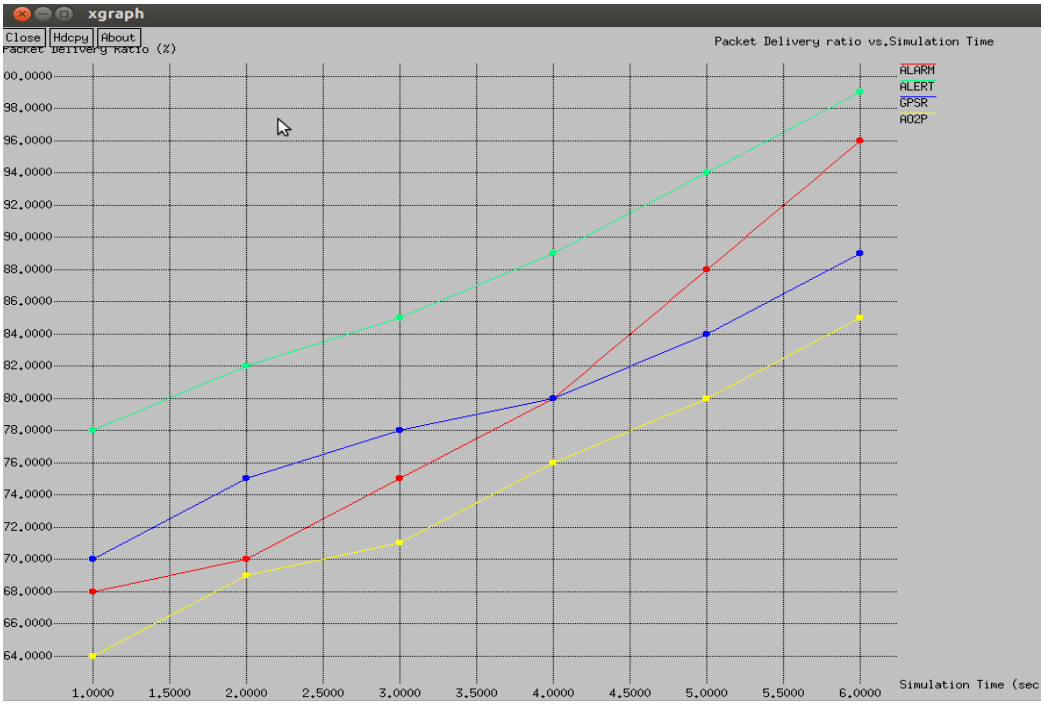

Fig 6: Packet delivery rate comparison

Table 1. Summary of anonymous routing protocols comparison

Protocol	Proactive / Reactive	Routing Mechanism	Topology/ Geographic	Single/ Multiple route	Identity anonymity	Location anonymity	Route anonymity
AO2P	Reactive	Hope by hope encryption	Geographic	Single	Source, Destination	Source, Destination	No
ALARM	Proactive	Redundant traffic	Topology	Multiple	Source, Destination	Source	No
ALERT	Reactive	Randomize	Geographic	Multiple	Source, Destination	Source, Destination	Yes

6. CONCLUSION

MANET is a dynamic, infrastructurless and decentralizes network. Due to these characters anonymous routing protocols are required to provide a very high level of security in MANET. Different techniques are used in anonymous protocols to achieve the goal of anonymity. Well known, efficient and latest anonymous routing protocols used in MANET such as AO2P, ALARM and ALERT are examined in this paper.

ALERT provides route anonymity, identity, and location anonymity of source and destination more than AO2P and ALARM. Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing and high node density to provide high anonymity. ALERT have low transmission cost and latency in packet transmission than the other two protocols. Improved data delivery rate enhances the performance of ALERT.

The limitations of other protocols comparing with the ALERT are, existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs.

Currently complete anonymous protection of MANETs is not achieved. So making changes in the existing protocols will create a new anonymous protocol meeting all the requirements of an anonymous protocol.

7. REFERENCES

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

[2] J. Kong, X. Hong, M. Y. Sanadidi, and M. Gerla, "Mobility Changes Anonymity: Mobile Ad Hoc

Networks Need Efficient Anonymous Routing," in ISCC, 2005, pp. 57–62.

[3] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous Ondemand Routing in Mobile Ad Hoc Networks," IEEE Transactions on Wireless Communications, no. 9, 2006.

[4] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," SECURECOMM, vol. 6, 2006.

[5] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Secure Dynamic Distributed Routing Algorithm for Ad Hoc Wireless Networks," ICPP Workshops, 2003, pp. 359–366.

[6] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks," IEEE LCN '04, 2004.

[7] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," LCN '04, 2004.

[8] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-hoc Networks," SASN '05, 2005, pp. 33–42.

[9] J. Kong and X. Hong, "ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," MobiHoc '03, 2003.

[10] S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks," AINA '06, 2006.

[11] Jiejun Kong, Xiaoyan Hong, "An Anonymous On Demand Routing Protocol with Untraceable Routes for Mobile Ad-hoc Networks", UCLA computer science department technical report 030020.

[12] Karim El Defrawy and Gene Tsudik," ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE Transactions on Wireless Communications.

[13] Haiying Shen and Lianyu Zhao," ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions on Wireless Communications.

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

[15] 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.

[16] X.X. Wu and B. Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Transactions on Mobile Computing, vol. 4, no. 4, pp. 335-348, July 2005.

[17] Gene Tsudik and Karim El Defrawy," ALARM: Anonymous Location-Aided Routing in Suspiciou ANETs", IEEE Transactions on Mobile Computing, Volume: 10, Issue: 9,September 2011

[18] Haiying Shen and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions on Mobile Computing, Vol. 12, NO. 6, June 2013.