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

MD5: Anonymous Location-Aided Routing in Suspicious Secure MANETs

Manjuladevi.V[1], Jennie Bharathi.R[2]

M.E, Department of ECE, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India[1]

Assistant Professor, Department of ECE, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India[2]

ABSTRACT: Mobile Ad Hoc Networks use anonymous routing protocols to hide node identities and routes from outside observers in order to provide anonymity protection. However, in existing Anonymous Location-based Efficient Routing Protocol (ALERT) dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. ALERT cannot provide full anonymity protection to data sources, destinations, and routes. ALERT could not provide much more anonymity and efficiency. In ALERT, GPSR routing protocols been used. GPSR routing protocol is used for data transmission between source and destination. During data transmission using GPSR, it takes much time to reach the data to destination from the source. So in GPSR routing, there have no time constraint. We propose an protocol which uses advanced cryptographic technique in order to improve security. Anonymous Location-Aided Routing in Suspicious Secure MANETs provides both security and privacy features. This includes node authentication, anonymity, data integration and untraceability (tracking-resistance). It also offers protection against active and passive insider attacks. Here, we also propose for more security during data transmission and other things by using MD5 hashing Technique.

KEYWORDS: Security, Anonymity, GPSR, ALERT, MD5, Hierarchical Routing.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a type of wireless network, and is a self-configuring network of mobile devices connected by any number of wireless links. Rapid growth of mobile users will be the need of the next generation wireless communication systems. A mobile ad-hoc network is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Network scenarios which include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. Rapid topology change due to un predictable mobility of nodes. This arises the need of incorporating the routing functionality into nodes. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks.

The design of network protocols for these networks is a complex issue. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to eliminate any of these effects. Moreover, in a military environment, preservation of security, reliability, intentional jamming, and recovery from failure are significant concerns.

Military networks are designed to maintain a low probability of intercept and/or a low probability of detection and high security. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network. MANET is very useful for many time-critical and mission-critical applications-military and civilian operations.

The shared wireless medium of MANET facilitates passive, adversarial eavesdropping on data communications whereby adversaries can launch various devastating attacks on the target network. On-Demand (or reactive) routing protocols are prevalent in MANETS in which a node attempts to discover a route to some destination only when it has a packet to send to that destination. So far, researchers have generally studied the routing problem in a non-adversarial network setting, assuming a trusted environment.

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

To protect wireless communication, many security protocol suites have been designed and deployed. But, they do not give significance to anonymity protection and leave mobile nodes to be traceable by wireless traffic analysts. First, need to identify the new anonymity requirements for mobile wireless networks.

Existing anonymity research has to make new underlying assumptions when it considers the case of mobile nodes. Thus, those meant for fixed networks do not support mobile environment. Therefore, design principles of new counter measures have to be studied. A hybrid approach of identity-free routing and on-demand routing can meet the requisites of a wireless network. There are various other anonymous routing protocols being used to attain anonymity. Anonymous routing is becoming relevant in the present scenario of networks as there is an increased use of wireless networks. Anonymity is provided for sender, receiver, and route and with location.

II. ANONYMITY

Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. Anonymity is an important issue in electronic payments and electronic voting, electronic auctions, email and web browsing. The distinction between data anonymity and connection anonymity is as follows: data anonymity is filtering any identifying information out of the data that is exchanged in a particular application; connection anonymity is hiding the identities of source and destination during the actual data transfer and also it hides the routes. In terms of unlinkablity anonymity can be classified into Sender anonymity,a particular message is not linkable to any sender and that to a particular sender, no message is linkable. Receiver anonymity ,a particular message cannot be linked to any recipient and that to a particular recipient, no message is linkable and relationship anonymity is the sender and the recipient cannot be identified as communicating with each other, even though each of them can be identified as participating in some communication. Mutual anonymity, a particular message is not linkable to both sender and receiver.

III. NECESSITY OF ANONYMITY IN MANET

Concept of anonymity has recently attracted attention in mobile wireless security research. Proactive routing and global knowledge-based routing schemes are the ones used in infrastructure networks to provide anonymity protection. These are not applicable in the case of mobile ad hoc networks. Rapid mobility in of nodes makes topology prediction a tough process. Anonymity is required in order to give privacy to users and some covert missions may require anonymous communication. In hostile environments, end-hosts may need hidden their communications to against being captured. The adversary can launch traffic analysis against interceptable routing information in routing messages and data packets. This should be prevented to make sure that active attacks do not take place. Route anonymity and location privacy are the two addressed issues to be handled by the anonymous routing protocol.

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. "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. 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 nodes have information about the real identities and locations of intermediate nodes en route. Also, in order to dissociate the relationship between source and destination (i.e., relationship un observability, it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

IV. EXISTING SYSTEMS

The 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. Many approaches cannot provide all of the aforementioned anonymity protections. ALARM[2] cannot protect the location anonymity of source and destination, SDDR cannot provide route anonymity, and ZAP only focuses on destination anonymity. ALERT[1] is not bullet proof to all active attacks. 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

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

quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations. In order to provide low cost and compromised anonymity protection the protocol is designed.

V. DESIGN CHOICES AND GOALS

Routing Protocol Choices

MANET routing protocols can be classified in to two types: reactive protocols and proactive protocols The latter can be further broken down into link-state and distance-vector (including path-vector) protocols. Reactive protocols typically use route discovery to identify a route to a given destination. The notion of discovering the destination is premised upon the source knowing the persistent identity or address of the destination. Distance vector (DV) protocols inherently offer relatively weak levels of security. In order to improve security advanced cryptographic algorithm is used

Goals

The following assumptions are necessary in Anonymous Location-Aided Routing in Suspicious Secure MANETs:

Location: Universal availability of location information of the mobile node .Each node is equipped with a device that provides accurate positioning information, e.g., GPS.
Mobility: mobility of nodes can be maintained not too rapid or too low mobility moderate mobility is maintained.
Time: All nodes maintain loosely synchronized clocks. This is easily obtainable with GPS.

Anonymous Location-Aided Routing in Suspicious Secure MANETs has the following goals:

Privacy: There are no public node identities or addresses. Each node is anonymous and its occurrences at different locations (movement patterns) cannot be linked; we elaborate on this later.
Security: The network must be resistant to passive and active attacks stemming from both outsiders and malicious (e.g., compromised) insiders.
Performance: Security and privacy goals must be achieved without undue sacrifices in performance (i.e., without requiring excessive computations and or high delay).

VI. PROPOSED SYSTEMS

Network Model:

Network models with various node movement patterns such as random way point model and group mobility model. MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. The powerful nodes are pretend to be legitimate nodes and inject packets to the network. Those powerful nodes are according to the analytical results from their eavesdropped packets.

Dynamic Pseudonym and Location Service:

Each and every node has separate location in the MANET. Each node has a location server. We can choose source and destination node in the network. All nodes should have mobility process in the network. The nodes are having unique MAC address and time stamp. Before finding location we are implementing has function of MD5 Algorithm. The source node wants to be sending the data to destination. Before this process find the neighbor location nodes to forward the data from source to destination. We can increase the computation complexity by using randomization for the time stamps. In this MANET, All nodes have public and private key. The public key is used to enable two nodes to securely establish a symmetric key K_s for secure communication. The destination location enables a node to determine the next hop in geographic routing. Specifically, trusted normal nodes or dedicated service provider nodes are used to provide location service. The existence of the location servers are opposed to the ad hoc property of MANETs, and it is not necessary to use location servers in a MANET without security consideration.

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

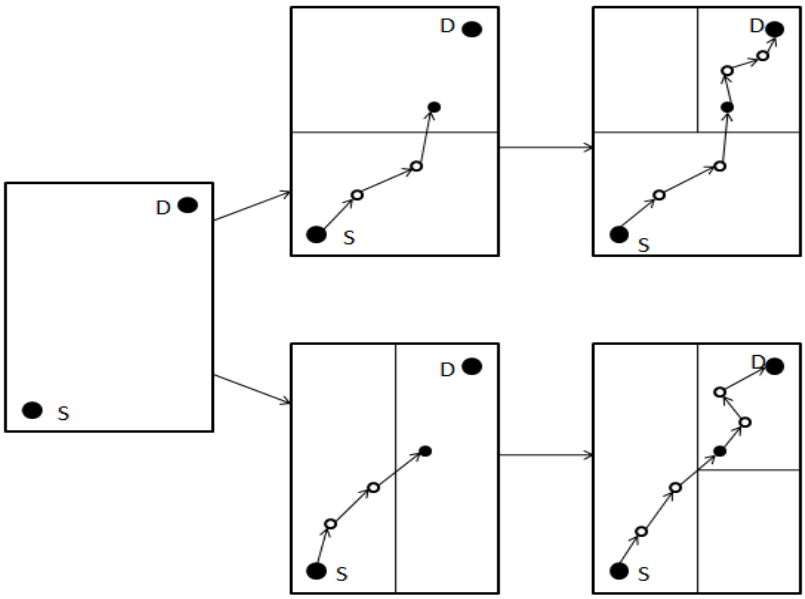

Figure 1. Example of zone partition in MANET

Anonymous Location-Aided Routing algorithm:

An Anonymous Location-Based Efficient Routing algorithm has been used to find the anonymity from the MANETs. Anonymity node may be drop the data during data transmission from the source to destination. So we cannot receive all data. This is the major problem of communication between nodes.

Anonymous Location-Aided Routing in Suspicious Secure MANETs features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. In this MANETs, the nodes are partitioned based on hierarchical location service into hierarchical zone and vertical zone.

Find the possible path to deliver the data from source node to destination node. The possible paths could find based on location service. The location server has all nodes location information. We should find optimal path and forward the data to destination. When find the location, we should check the capable of the relay nodes to forward the data. After trust the node only we can forward the data. And relay nodes should place on every partition zone. It uses GPSR[12] packet forwarding to forward packet to next destination.

Packet Format of Anonymous Location-Aided Routing in Suspicious Secure MANETs:

For successful communication between SandD, Sand each packet forwarder embeds the following information into the transmitted packet.

- The zone position of ZD, i.e., the Hth partitioned zone.
- The encrypted zone position of the Hth partitioned zone of S using D's public key, which is the destination for data response.
- The current randomly selected TD for routing.
- A bit (i.e., 0/1), which is flipped by each RF, indicating the partition direction (horizontal or vertical) of the next RF.
- Group signature

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

An attacker needs very high computation power to be able to launch attacks such as dictionary attack decrypt it in order to discover the source of a session with a specific destination. In order to hide the packet content from adversaries, Anonymous Location-Aided Routing in Suspicious Secure MANETs employs cryptography. Here MD5 hashing algorithm is used. The work experimentally proved that generally symmetric key cryptography costs hundreds of times less overhead than public key cryptography while achieving the same degree of security protection. Thus, instead of using public key cryptography, Anonymous Location-Aided Routing in Suspicious Secure MANETs uses symmetric key encryption for transmitted data.

Anonymity Protection and Strategies against Attacks:

Anonymous Location-Aided Routing in Suspicious Secure MANETs offers identity and location anonymity of the source and destination, as well as route anonymity. Anonymous Location-Aided Routing in Suspicious Secure MANETs makes the route between an S-D pair difficult to discover by randomly and dynamically selecting the relay nodes[1]. The data forwarding from source to destination node by using GPSR routing protocol. Using this protocol we can protect the data from the anonymity. 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. The route anonymity due to random relay node selection in Anonymous Location-Aided Routing in Suspicious Secure MANETs prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In Anonymous Location-Aided Routing in Suspicious Secure MANETs, 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 Anonymous Location-Aided Routing in Suspicious Secure MANETs 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. Here advanced cryptographic algorithm is used to improve security and speed of processing is improved.

Message Digest 5

The hash is used to produce a message digest is a unique reduced representation of the complete message. The hash algorithms are one-way encryption algorithms, so it is impossible to recover the original message from the digest. MD5 is a hash function block. That is to say that cutting the chopping block messages of fixed size and is working on a block at a time. If the message size chopping is not a multiple of block size, it will be completed (this is the padding operation) until a complete block. We chose MD5 because it works on blocks of 512bit (64 bytes) and produces a digest of 128 bits.

VII. PERFORMANCE ANALYSIS

In this section, we provide experimental analysis of the Anonymous Location-Aided Routing in Suspicious Secure MANETs, which exhibit consistency with our analytical results. Anonymous Location-Aided Routing algorithm in providing anonymity with low cost of overhead. The simulation area will be 1000x1000 units. In each of these simulations, the sensor nodes were distributed uniformly over the space. The total simulation time will be 200 seconds, in that the simulation begins at 35seconds and ends at 199 seconds.

We now present the graphical presentation of the results. Figure 1 shown below is end to end delay is the time taken for a packet to be transmitted across the network from source to destination. The end to end delay include the transmission delay, propagation delay and the processing delay From the graph it can be observed that there is a decrease in the delay for the proposed protocol. The use of location aided routing helps to direct the traffic towards the source and thus reduce the delay in the network.

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 1. Average Delay

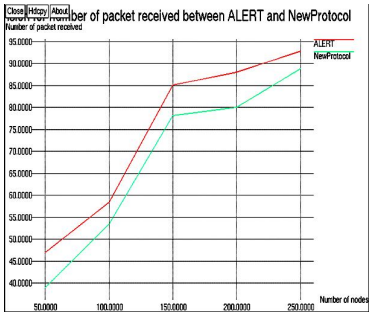

Figure 2. Packet delivery ratio

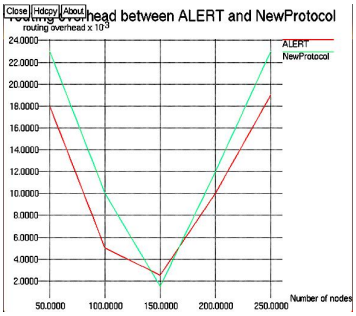

Figure 3. Routing overhead

Packet delivery ratio is the ratio between numbers of packet received to number of packet send. Packet delivery ratio includes the number of packet received and number of packet send. Figure 2, can be observed that there is a decrease in the delivery for the proposed protocol due to hash collisions. To maintain the efficiency of the routing protocol need to improve the packet delivery ratio of the routing.

Normalised routing overhead is the ratio between a control overhead and number of packet received across the network from source to destination. From Figure 3, it can be observed that there is a increase in the control overhead for the proposed protocol. The use of location aided routing helps to direct the traffic towards the source and thus increase the control overhead in the network.

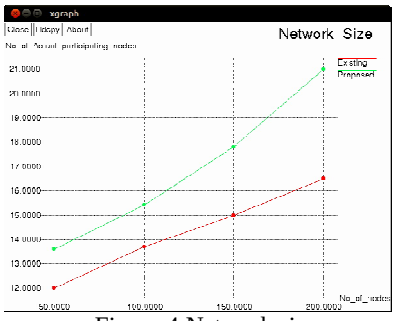

Figure 4.Network size

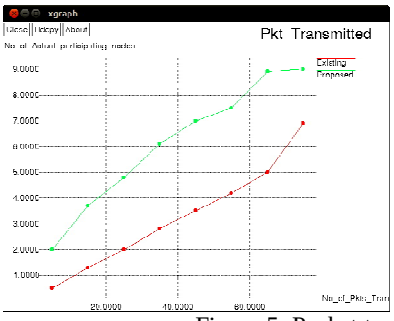

Figure 5. Packet transmitted

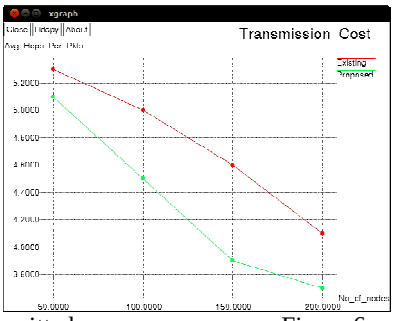

Figure 6. Transmission cost

Figure 4, shows that number of actual participation nodes increases with the increase size of the network. when number of nodes increases which leads to increase the number of relay nodes in network which may increase the participation of more nodes in the network. Figure 5, explains that packet transmission ratio in the network. graph drawn between the Number of packet transmitted to the Number of actual participation in the network. Number of packet transmitted is increased with the increased number of actual participation nodes. Transmission cost determined by the Number of nodes to the average hops per packet. Transmission cost decreased when increase the number of nodes in the network Proposed protocol is cost efficient then the existing protocol.

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

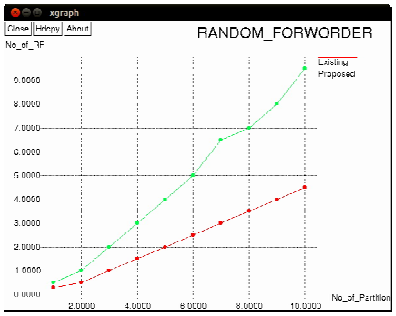

Figure 7. Number of Random forwarder

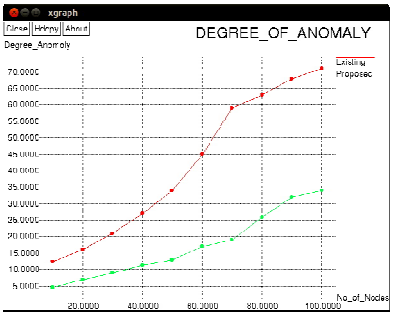

Figure 8. Degree of Anomaly

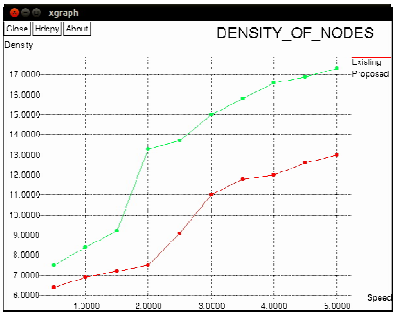

Figure 9. Density of nodes

Hierarchial partion of the network zone into horizontal and vertical zones, all horizontal zones are taken as the level1 and vertical zones are taken as level2. Random forwarders forward the message from the source to the destination,When number of partition increases which increases the number of random forwarders in the network.when number of partition increases number of random forwarder also increases. Figure 8, deals about the degree of anomaly when number of nodes increases degree of anomaly also increases.

VIII. CONCLUSION

Anonymous Location-Aided Routing in Suspicious Secure MANETs is designed to give anonymity in sender, receiver and routes. In this protocol MD5 cryptographic algorithm is used which is much faster then SHA1 and digest itself is very small and it can be easily encrypted. It is very easy and fast (and therefore cheap) to check some data for validity. It is difficult to crack MD5 algorithm. It can prevent some active attacks such as Sybil attacks but it is not bullet proof to all active attacks. This protocol suffers from hash collision. It is susceptible to brute force attacks.

A number of items remain for future work inorder to improve security advanced cryptographic algorithms going to be used and need to check this protocol by performing different active attacks in it.

REFERENCES

1. L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, pp. 304–313 June 2013.
2. K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," *IEEE Trans. Mobile Comput.*, vol. 10, no. 9, pp. 1345–1358, 2011.
3. Z. Zhang, W. Liu, and Y. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," *IEEE Trans. Wireless Commun.*, vol. 5, pp. 2376-2385, Sept. 2006.
4. S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks," in *20th International Conference on Advanced Information Networking and Applications (AINA)*, Vienna, AU, pp. 133-137, 2006.
5. D. Sy, R. Chen, and L. Bao, "ODAR: On-Demand Anonymous Routing in Ad Hoc Networks," University of California, Irvine, pp. 1-10, 2006.
6. J. Liu, X. Hong, J. Kong, Q. Zheng, N. Hu, and P. Bradford, "A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks," in *Military Communications Conference (MILCOM)*, pp. 1-7, 2006.
7. R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-hoc Networks," in *3rd ACM Workshop on Security of Ad hoc and Sensor Networks* Alexandria VA, USA, pp. 33-42, 2005.
8. X. Wu and E. Bertino, "Achieving K-anonymity in Mobile Ad Hoc Networks," in *1st IEEE ICNP Workshop on Secure Network Protocols (NPSec)*, pp. 37-42, 2005.
9. X. Wu and B. Bhargava, "AO2P: Ad hoc On-demand Position-based Private Routing Protocol," in *IEEE Trans. Mobile Computing*. vol. 4,pp. 335-348, 2005.
10. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in *29th Annual IEEE International Conference on Local Computer Networks*, pp. 618-624, 2004.
11. J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks," in *4th ACM International Symposium on Mobile Ad-hoc Networking & Computing (MobiHoc)*, Annapolis MD, USA, pp. 291-302, 2003.
12. B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in *6th Annual International Conference on Mobile Computing and Networking (Mobicom)*, Boston, MA, pp. 243- 254, 2000.