Secure Anonymous Routing in Clustered Multihop Wireless Ad Hoc Networks

Lijun Qian and Ning Song
Department of Electrical Engineering
Prairie View A&M University
Prairie View, Texas 77446
Email: LiQian, NSong@pvamu.edu

Xiangfang Li
WINLAB
Rutgers University
Piscataway, NJ 08854
Email: xfli@winlab.rutgers.edu

***Abstract*— Providing security and anonymity to users are critical in wireless ad hoc networks. In this paper, a secure anonymous routing scheme is proposed for clustered wireless ad hoc networks. In the proposed scheme, intra-cluster routing uses the common broadcast channel in wireless networks to provide anonymity, while inter-cluster routing uses a sequence of temporary public keys as the trapdoor information. Symmetric cipher is employed in most part of the proposed scheme to reduce computational complexity and maximize network efficiency. Public key is only used to distribute symmetric keys. Both privacy analysis (including sender anonymity, receiver anonymity and sender-receiver anonymity) and attack analysis show the effectiveness of the proposed scheme against a wide range of strong adversarial attacks.**

I. Introduction

There has been great interest in wireless ad hoc networks recently since they have tremendous military and commercial potential. In order to deploy wireless ad hoc networks to cover a large area and to support a large amount of users, scalability of such networks is one of the main concerns. Clustering is a very effective technique to achieve scalability and distributed control for such networks. In this paper, it is assumed that a clustered architecture is established in the wireless ad hoc network and there is a cluster head (CH) and multiple gateways (GWs) within each cluster.

Security is of paramount importance in wireless ad hoc networks. Routing security is one of the main concerns because routing is needed for both intra-cluster and inter-cluster communications, and the adversary may perform various attacks on the routing traffic. In addition, passive attacks based on eavesdropping and traffic analysis are easy in wireless ad hoc networks and they will provide opportunities for effective active attacks when critical network elements are located. Thus providing anonymity to users (including users' locations, data, etc.) is also very important, especially in a hostile environment, such as in a battlefield. For example, it is critical to protect the cluster heads by making them indistinguishable from other nodes in the network, thus keeping them anonymous to the enemy.

Secure anonymous routing is one of the primary countermeasures to various attacks on the routing traffic. It is very challenging to provide both security and anonymity in wireless ad hoc networks, because of the infrastructure-less nature of the networks, limited network resources and numerous possible attacks. In this paper, we restrict our interests in secure anonymous routing in clustered multi-hop wireless ad hoc networks. Specifically, a novel Secure Anonymous Routing scheme in Clustered multi-hop wireless ad hoc networks (SARC) is proposed to provide both security and anonymity, and prevent various attacks on the routing traffic.

The paper is organized as follows. Background of security in clustered ad hoc networks and anonymous communications are given in Section II. Secure anonymous routing for intra-cluster and inter-cluster are proposed in Section III and Section IV, respectively. Secure and anonymous data transmissions are discussed in Section V. Section VI provides anonymous analysis and attack analysis. Implementation details and overhead analysis are given in Section VII. Section VIII contains the concluding remarks.

II. Related works

Anonymous communication protocols have been studied intensively in wired networks. The concept of mix was proposed in [7], and was employed in various anonymous communications proposals for the Internet, such as P^5 [8]. A similar but different concept, crowd, was introduced in [11] for Internet web transactions. However, these methods can not be directly applied in wireless ad hoc networks due to the lack of fixed infrastructure.

Secure anonymous routing for wireless ad hoc networks attracts a lot of attentions lately. In [1], a protocol was proposed to allow trustworthy intermediate nodes to participate in the path construction protocol without jeopardizing the anonymity of the communicating nodes. The basic idea is that each node will classify its neighbors into different security levels, and a common key is shared between them for each level. Only nodes at certain level can receive and transfer data during routing. ANODR [3], an anonymous on-demand routing protocol for mobile ad hoc networks, is based on "broadcast with trapdoor information", in which a cryptographic onion [10] is used for route pseudonym establishment. Since in ANODR each node in the route only knows the next node with a fake identity, it can prevent strong adversaries from tracing a packet flow back to its source or destination and ensure that adversaries cannot discover the real identities of local transmitters. In Routing Response of ANODR, the node ID is transmitted to next node. Although it is a pseudonym, the attacker can launch a Denial-of-Service (DoS) attack based on that ID. ASR (Anonymous Secure Routing) [2]

solves this problem by a scheme in which node one sends a temporary public key to node two in Routing Request, and in Routing Response node two transmits its pseudonym encrypted by the key to node one. Besides location privacy and route anonymity, ASR also supports limited hop count and destination verification by intermediate node so as to provide more security properties. A more recent work [4] proposed an anonymous on-demand routing protocol, termed MASK, based on a new cryptographic concept called pairing. An anonymous neighborhood authentication protocol is used and MASK fulfills the routing and packet forwarding tasks without disclosing the identities of participating nodes under a rather strong adversarial model. Although the above works addressed secure anonymous routing for wireless ad hoc networks, none of them considered clustered architecture.

Security in clustered wireless ad hoc networks was considered in several recent studies. The authors in [5] proposed a security architecture based on public key schemes and distributed certification. The cluster heads perform admistrative functions and hold shares of a network key for node authentication using proactive digital signatures. A similar design is proposed in [6] for cluster-based Near-Term Digital Radio (NTDR) ad hoc networks. A security infrastructure is provided for secure intra-cluster and inter-cluster communications. However, anonymity is not considered in these studies.

In this paper, a Secure Anonymous Routing scheme in Clustered multi-hop wireless ad hoc networks (SARC) is proposed to provide both security and anonymity. It is assumed that the nodes are grouped into a number of overlapping or disjoint clusters in a distributed manner. A cluster head (CH) is elected for each cluster to maintain cluster membership information and perform other administrative functions. There are also multiple gateways (GWs) within each cluster. We further assume that key distribution has done and each node has one or more public-private key pairs, which might be pre-installed or generated by itself, or using a scheme such as the one proposed in [5].

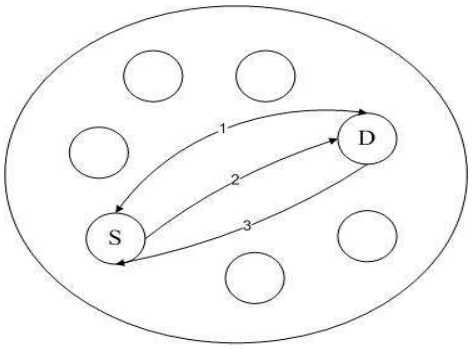
III. Intra-cluster Secure Anonymous Routing

Single-hop communication is assumed within each cluster, i.e., every node can directly communicate with any other node in the same cluster. Furthermore, links between nodes are assumed bi-directional since most routing protocols and wireless Medium Access Control (MAC) protocols (such as the MAC protocol in 802.11) require symmetric links.

In intra-cluster secure anonymous routing, each node (including cluster head and gateway) behaves exactly the same. Intra-cluster anonymous routing includes three steps: Key Broadcasting, Intra cluster routing request (Intra-RREQ), and Intra cluster routing response (Intra-RRSP) (see Fig. 1).

In the step of key broadcasting, each node will randomly generate a pseudo name, and broadcast the pseudo name and the corresponding public key (expressed by KU) with the format

[H(CN, TS), pseudonym, KU]



1. Key Broadcasting
2. Intra-RREQ
3. Intra-RRSP

Fig. 1. intra-cluster routing

Here we use the hash value of the cluster name (CN) and a time-stamp (TS) rather than the cluster name itself. The strong collision resistance of the hash function and the use of time-stamp guarantee the uniqueness of the hash value H(CN, TS), thus prevent replay attacks. All the nodes in a cluster need to build a table to map public key and node name (pseudo name) of any cluster member, see for example, Table I. Because one-hop communication is assumed within each cluster, all other cluster member can receive the broadcast and keep the message in its local mapping table. In order to improve anonymity, nodes will periodically update their public keys and pseudo names.

Name	Key	Timestamp
A	Key1	time1
B	Key2	time2
..	..	..

TABLE I
NAME-PUBKEY MAPPING TABLE

Because of the high computational complexity of the public key schemes, it is only used to identify the designated receiver and help to deliver a symmetric session key. In other words, if node S wants to communicate with node D, they need to negotiate a symmetric session key first. Node S simply broadcasts a routing request (RREQ) packet that is encrypted by node D's public key. Although all nodes of that cluster will receive the RREQ, only node D has the corresponding private key and thus can decrypt it. Therefore, it guarantees receiver anonymity. Node D will send a routing response (RRSP) and encrypt it with node S's public key, which will guarantee sender anonymity. Furthermore, the pseudonyms of the source and destination nodes will guarantee sender-receiver anonymity. After node S decrypts the RRSP, node S and node D will have a shared session key for secure data transmissions. In order to thwart packet analysis attacks, each packet need to have the same packet size (by added padding).

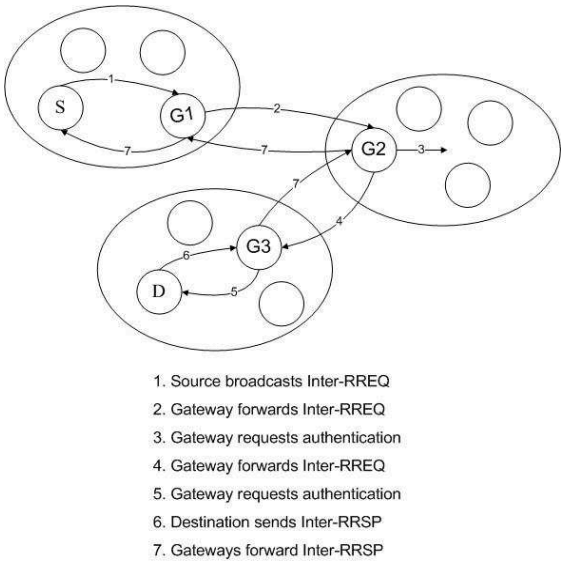


Fig. 2. inter-cluster routing

The format of the Intra-RREQ is

[H(CN, TS), $KU_D(K_s)$, K_s(RREQ $|Req_ID|$PN$_S$), padding]

and the format of the Intra-RRSP is

[H(CN, TS), $KU_S(K'_s)$, K'_s(RRSP $|Req_ID|$K$_{ses}$), padding].

Where PN_S is the pseudonym of S; KU_D and KU_S are the public keys of node D and node S, respectively; K_s and K'_s are temporary symmetic keys; K_{ses} is the symmetric session key for data transmissions. Req_ID is an identifier for the request and is also used to defend against replay attacks.

Note that each request and response only broadcast once in intra-cluster secure anonymous routing and do not propagate. Hence, high bandwidth efficiency can be achieved. Furthermore, since each node (including cluster head and gateway) behaves exactly the same, no special function need to be performed by the cluster head and gateway in the intra-cluster routing process, critical network elements can be hidden from the attackers.

IV. Inter-cluster Secure Anonymous Routing

In the proposed inter-cluster anonymous routing, we extend the method in [2] to clustered wireless ad hoc networks. The tradeoff between bandwidth efficiency and the level of anonymity achieved is taken into consideration.

It is assumed that all links between nodes are bi-directional and there exists a security association between any source and destination node pairs. The shared keys may be distributed by a Key Distribution Center (KDC) or manually.

The procedures of inter-cluster anonymous routing are shown in Fig. 2.

A. Source broadcasts inter-cluster routing request

Source node S generates an inter-cluster routing request (Inter-RREQ), and broadcasts Inter-RREQ in its cluster. Here we require that only gateway nodes will take part in inter-cluster routing. Other cluster members will simply ignore this request to avoid packet propagating (thus avoid wasting bandwidth). The format of this request is

[RREQ, Req_ID, $K_{sd}(K_{ses})$, K_{ses}(Req_ID), PK0]

where

- Req_ID: identifier of the request
- K_{sd}: the shared key between node S and node D
- K_{ses}: a session key (used to verify response later)
- PK0: a temporary public key of node S

K_{sd} is used for authentication between source node S and destination node D. K_{ses} is used by intermediate nodes to verify whether it is the destination, because only destination node D has K_{sd} to get K_{ses} and is able to verify that it is indeed the destination by decrypting the 4th field in Inter-RREQ and comparing it with Req_ID. PK0 is kept by its next hop node (gateway) to encrypt routing response. Since only node S has the corresponding private key and the public key is temporary, it can guarantee both security and anonymity in this step.

B. Gateway forwards Inter-RREQ

The Inter-RREQ will be forwarded by gateways to neighboring clusters. Before forwarding Inter-RREQ, the gateway firstly keeps the public key of the sender and replaces it with the public key of the current gateway. For example, in step 2 of Fig. 2, G1 will keep PK0, and replace it with PK1 (a temporary public key of G1). The Inter-RREQ changes to

[RREQ, Req_ID, $K_{sd}(K_{ses})$, K_{ses}(Req_ID), PK1]

Similarly, in step 4, the Inter-RREQ changes to

[RREQ, Req_ID, $K_{sd}(K_{ses})$, K_{ses}(Req_ID), PK2]

where PK2 is a temporary public key of G2.

When a local gateway receives a fresh Inter-RREQ, it will forward the Inter-RREQ to gateways in neighboring clusters. When a foreign gateway receives a fresh Inter-RREQ, it will first broadcast an authentication request in its local cluster to check whether the destination is in there. For example, the packet format in step 3 is

[AREQ, H(CN, TS), Req_ID, $K_{sd}(K_{ses})$, K_{ses}(Req_ID), PK2]

Here AREQ represents authentication request, and H(CN, TS) is used to identify cluster. Because it is an intra-cluster request, nodes in other clusters will ignore it.

The gateway may wait until a node replies and stop forwarding Inter-RREQ, or a timer expires and then forward Inter-RREQ to gateways in neighboring clusters. However, there are two concerns with the above design. Firstly, this may incur excessive delay in inter-cluster routing. Secondly, anonymity may be sacrificed if the gateway stop forwarding the Inter-RREQ. At the least an attacker can figure out the cluster of the destination node although not the exact location of the destination. Hence, in order to avoid the above problems, in

our design the gateway will not wait for responses and will forward the Inter-RREQ immediately after step 3 in Fig. 2. Of course, additional bandwidth is needed since each gateway will re-broadcast the Inter-RREQ exactly once.

C. Destination sends inter-cluster routing response

When a cluster member receives an authentication request, it checks whether it is the destination by trying to decrypt the session key K_{ses} and verifying Req_ID. If succeeded, it will generate an inter-cluster routing response (Inter-RRSP), step 6 in Fig. 2. It uses a pseudonym T4, and encrypts it by sender's public key (PK3) such that intermediate gateways and the source can authenticate the destination. It also includes the encrypted session key K_{ses} and Req_ID by T4. The packet format of Inter-RRSP is

[RRSP, PK3(T4) , T4(K_{ses} $|Req\_ID$)]

D. Gateway forwards Inter-RRSP

When an intermediate gateway receives a routing response, it decrypts the pseudonym Tx by using its corresponding private key. Then it uses the obtained Tx to decrypt the session key K_{ses} and verify destination, because the original session key K_{ses} and the corresponding Req_ID in the routing request has been saved by intermediate gateways. If the verification is succeeded, the intermediate gateway will perform the same operation as that of the destination, i.e., it will generate a new pseudonym and encrypt it by last sender's public key. Then it will encrypt K_{ses} and Req_ID with the new pseudonym. For example, in step 7, the packet format is

[RRSP, PK2(T3) , T3(K_{ses} $|Req\_ID$)]

Therefore, after the Inter-RRSP reaches the source, an inter-cluster route is formed as S:T1:T2:T3:T4(D).

V. Data Transmission

Intra-cluster data transmissions can be achieved by source node broadcasting data encrypted with the negotiated session key K_{ses} from intra-cluster route discovery. The packet format is

[DATA, H(K_{ses}), K_{ses}(data)]

where DATA is the packet type. Each node within the same cluster will first check whether it is the destination by verifying the hash value of its session keys. Because only the destination need to decrypt the data, computational complexity is low for all other nodes.

Inter-cluster data transmissions rely on the sequence of symmetric keys generated during Inter-RRSP. After inter-cluster routing is done, each node i on the path will keep a mapping [T_i, T_{i+1}]. T_i is the symmetric key generated by itself and transmitted upstream (to node $i-1$) as a part of the routing response. T_{i+1} is the symmetric key received in the routing response from downstream node $i+1$. During inter-cluster data transmissions, the hash value of T_{i+1} is used to identify the downstream node. The packet format is

[DATA, H(T_i), T_{sd}(data)]

where data is encrypted by the share key between source and destionation if data security is required. Since we use hash value to identify the next hop, the attacker can not track the data flow. Thus sender-receiver anonymity can be maintained.

VI. Anonymous Analysis and Attack Analysis

A. Anonymous Analysis

In the proposed intra-cluster anonymous secure routing, the adversary may observe Intra-RREQs and Intra-RRSPs, but would be unable to tell the identities of the sender and the receiver and the relations between different Intra-RREQs and Intra-RRSPs because a common broadcast channel is employed.

The proposed inter-cluster anonymous secure routing implements two different packet formats at a gateway for forwarding Inter-RREQ and authentication within its local cluster. Thus an adversary may distinguish gateway nodes from other nodes. However, since each gateway re-broadcasts exactly twice for each Inter-RREQ (one for forwarding Inter-RREQ and the other for local authentication), it is not possible for the adversary to locate the cluster of the destination node.

Note that gateways may use the same packet format for forwarding Inter-RREQ and authentication within its local cluster. However, this approach violates the semantics of clusters. For example, every node will have to examine every routing packets (local or not) which results in much higher overhead.

Furthermore, the proposed scheme ensures unlocatability of nodes because nodes do not reveal their real identity to other nodes, and their pseudonyms are changed dynamically. Therefore, an attacker can trace a node identifier to a certain cluster at the most. Moreover, since source and destination identifiers are never disclosed during route discovery, the relationship anonymity between the source and destination is guaranteed.

B. Attack Analysis

The active attacks such as the denial-of-service (DoS) attacks are usually easy to detect because the caused abnormal traffic pattern under many circumstances. Intrusion detection systems can act as counter-measures against such active attacks. Hence, active attacks are not addressed by this work. However, from a simple analysis it is clear that secure routing in clustered ad hoc networks is much more resistant to attacks than routing in pure ad hoc networks. The main reason is the existence of an on-line authority (i.e., cluster heads) capable of controlling traffic and monitoring node behavior.

On the contrary, passive attacks such as eavesdropping and traffic analysis are difficult to detect. However, once locating certain critical nodes through overheard routing information, passive adversaries can perform active attacks on the critical network element. Therefore, passive adversaries are more dangerous than active adversaries because they are difficult to detect. Such passive attacks are the main concern of this paper.

In anonymous communications, two main passive attacks are packet analysis attack and traffic analysis attack. In packet

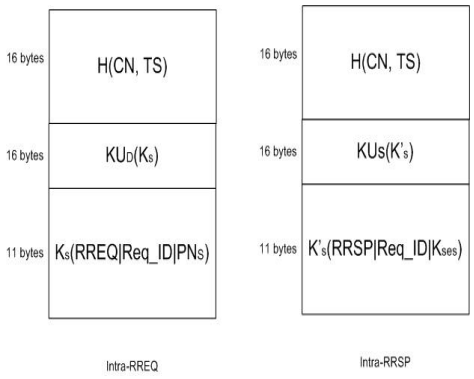


Fig. 3. Intra-cluster routing: packet fields

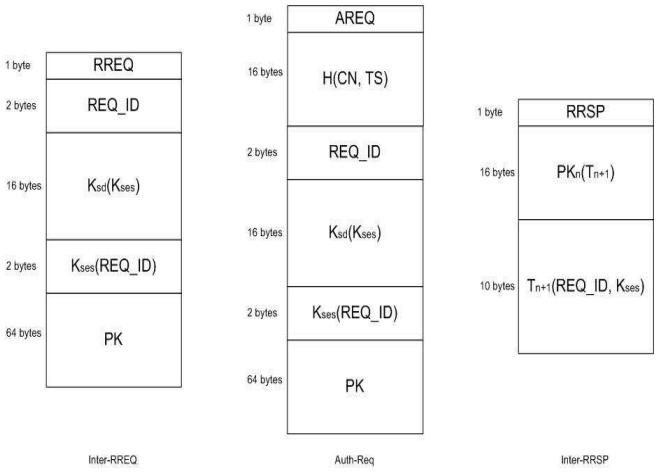


Fig. 4. Inter-cluster routing: packet fields

analysis attack, the attacker(s) try to deduce routing information by analyzing the packet length, type, etc. In traffic analysis attack, the attacker(s) try to deduce routing information by analyzing the amount of traffic flow among nodes and correlating eavesdropped traffic information to actual network traffic patterns.

In cluster-based wireless ad hoc networks, cluster head plays an important role as the central controller and the trusted authority in a cluster. Thus one of the main tasks of anonymous secure routing is to hide cluster head from attackers. In the proposed anonymous secure routing scheme, cluster head acts exactly the same as the other nodes throughout the routing procedures in both intra-cluster and inter-cluster anonymous routing, which makes it indistinguishable from the other nodes in the network. Consequently, the cluster heads are safe from both packet analysis attacks and traffic analysis attacks.

Note that the attackers may be able to identify gateways from other nodes. However, since each cluster typically has more than one gateway nodes, it is not as critical as the cluster head. Furthermore, it is feasible to allow some nodes perform gateway functions from time to time. This will shuffle the routing traffic and make traffic analysis attack more difficult to succeed.

In the proposed scheme, the integrity of the routing packets are guaranteed although routing packets are not encrypted (in order to keep the overhead low). The attacker will not be able to alter any field in the routing packets without being detected.

VII. Implementation and Overhead Analysis

One routing design for clustered wireless ad hoc networks is the Cluster Based Routing Protocol (CBRP) [12]. CBRP does not contain any security features. In this study, CBRP is used as a baseline for overhead comparison analysis.

Suppose that 3DES and RSA-512 are employed as the symmetric and public key algorithms, and MD5 is adopted as the hash algorithm. The detailed packet fields of intra-cluster routing and inter-cluster routing are shown in Fig. 3 and Fig. 4, respectively. In intra-cluster routing, public key is only used to deliver a symmetric key, thus the computational complexity is low. The overhead is also low due to the use of hash function.

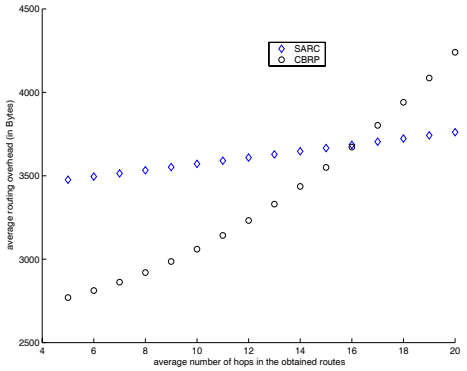


Fig. 5. Routing overhead of SARC and CBRP for Inter-cluster routing

In inter-cluster routing, the size of Inter-RREQ packet is 85 bytes. The packet size for authentication request from gateway to cluster member is 101 bytes. The packet size for Inter-RRSP is 27 bytes. Since in SARC the routing packets' sizes are fixed, while in CBRP the routing packets' sizes grow because it is source routing, the overhead between them becomes close as the obtained routes becomes longer (more hop counts). A simulation is performed to demonstrate this effect and the result is shown in Fig. 5. It is assumed that there are 20 clusters in the network and each node in each cluster want to communicate with any other node in a different cluster. The result shown is the average overhead over all obtained routes. It is observed that the overhead of SARC is 26.3% higher than that of CBRP when the average number of hops in the obtained routes is 4 (source and destination are in neighboring clusters). This drops to only 16.7% when the average number of hops in the obtained routes increases to 10. When the average number of hops in the obtained routes is more than 16, SARC has lower overhead than CBRP. These observations are in agreement with our expectation.

VIII. Conclusions

In this paper, a secure anonymous routing scheme termed SARC is proposed for clustered wireless ad hoc networks. Anonymous and attack analysis show the effectiveness of the proposed scheme. The overhead of both intra-cluster and inter-cluster anonymous routing is low. In addition, the computational complexity of data forwarding is also low due to the use of symmetric ciphers rather than public key schemes.

Acknowledgment

This research work is supported in part by the U.S. Army Research Laboratory under Cooperative Agreement No. W911NF-04-2-0054. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U. S. Government.

References

[1] A. Boukerche, K. El-Khatib, L. Xu, 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 (LCN'04)*, pp. 618-624, Tampa, Florida, USA, November 16 - 18, 2004.

[2] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks", *The 29th Annual IEEE Conference on Local Computer Networks (LCN) 2004*, Tampa, Florida, U.S.A., 2004.

[3] Jiejun Kong, Xiaoyan Hong, and Mario Gerla, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks", *In Proceedings of ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc 2003)* , Annapolis, MD, June 2003.

[4] Yanchao Zhang, Wei Liu, and Wenjing Lou, "Anonymous communications in mobile ad hoc networks", *IEEE INFOCOM 2005*, Miami, FL, March 2005.

[5] M. Bechler, H.J. Hof, D. Kraft, F. Pahlke and L. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks", *IEEE INFOCOM 2004*, Hong Kong, March 2004.

[6] V. Varadharajan, R. Shankaran and M. Hitchens, "Security for cluster based ad hoc networks", *Computer Communications*, Vol.27, pp.488-501, 2004.

[7] David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, vol.24, no.2, 1981.

[8] Rob Sherwood, Bobby Bhattacharjee, and Aravind Srinivasan, "P5: A Protocol for Scalable Anonymous Communication", *In the Proceedings of the 2002 IEEE Symposium on Security and Privacy* , May 2002.

[9] Nathalie Weiler, "Secure Anonymous Group Infrastructure for Common and Future Internet Applications", *In 17th Annual Computer Security Applications Conference (ACSAC'01)*, pp. 401-410, December 10 - 14, 2001.

[10] M. Reed, P. Syverson, D. Goldschlag, "Anonymous Connections and Onion Routing", *IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection*, 1998.

[11] Michael K. Reiter, Aviel D. Rubin, "Crowds: anonymity for Web transactions", *ACM Transactions on Information and System Security (TISSEC)*, Vol. 1, Issue 1, pp.66 - 92, 1998.

[12] M. Jiang, J. Li, and Y.C. Tay, "Cluster Based Routing Protocol (CBRP) Function Specifications", *IETF Draft draft-ietf-manet-cbrp-spec-00.txt*, Aug. 1999.