The CSI Journal on
Computer Science and Engineering
Vol. 4, No. 2&4, 2006
Pages 25- 31
Regular Paper

Anonymous Communication in MANETs Using Pseudonymity in Chain-Based Routing

Reza Shokri[1], Maysam Yabandeh[1], Nasser Yazdani[1], Ahmad Khonsari[1,2]

[1] Department of Electrical and Computer Engineering, University of Tehran, Tehran, Iran
[2] School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran

Abstract

In this paper, we introduce a novel anonymous routing protocol form mobile ad hoc networks (MANETs), named PseudoCAR. In the proposed scheme, a random identifier is assigned as *pseudonym* to each link of a path during route discovery. Such pseudonyms are fastened privately in intermediate nodes to create a virtual chain between communicating nodes. This mechanism is called *Chain-based Routing*. Through hiding nodes' identifiers inside the chain, PseudoCAR realizes sender, receiver, and relationship *anonymity* in addition to *untraceability* in the network. In comparison to the similar protocols, the main contributions of PseudoCAR are its simplicity, flexibility and low imposed computational overhead on the network. The operation of the protocol is validated through both analytical results and simulation experiments.

Keywords: MANET, Security and Privacy, Anonymity, Pseudonymity, Chain-based Routing.

1. Introduction

Traffic analysis is one of the most subtle and unaddressed security attacks against networks. By definition 0, traffic analysis is a security attack where an adversary observes network traffic in order to infer sensitive information about the applications and/or the underlying system. Classifying as a *passive attack*, traffic analysis is invisible and difficult to detect. Particularly, passive attacks are extremely dangerous since makes adversaries able to identify critical nodes and launch directed attacks towards them. It is therefore very important to design countermeasures against such malicious traffic analysis.

Several *anonymous communication* methods, such as 0 [10], have been proposed to counter threats of passive eavesdroppers in ad hoc networks. The essence of anonymous communication is to hide nodes' identities from outside observers. As a result, adversaries could not correlate eavesdropped traffic information with actual network traffic patterns and hence, traffic analysis attack can be efficiently defeated. Several encryption/decryption operations especially in end nodes 0 and periodic cryptographic operations in relay nodes [10] are some aspects of complexity in proposed protocols.

To overcome the drawbacks of existing techniques, we propose the concept of anonymous chain-based routing for MANETs, which elegantly performs the routing task without disclosing the real identities of participating nodes. In the chain-based routing, every node involved in a chain (i.e. a sequence of correlated links which cooperatively construct the route) has two links respectively to its upstream and downstream nodes. These two links are labeled with different identifiers and are fasten together by means of a private entry in the node's routing table. Through hiding nodes' identifiers inside the chain, no node is identifiable within the network (the anonymity set) and therefore *anonymity* is realized [2].

In addition, due to link pseudonymity approach, by which

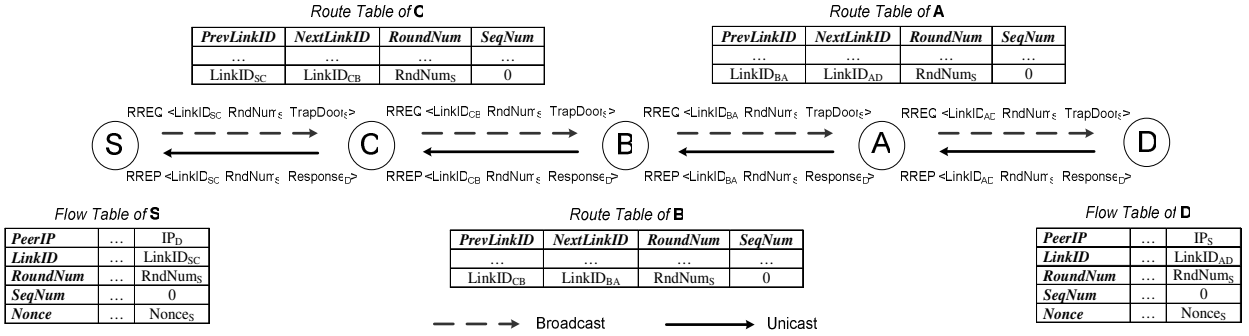


Figure 1. Message flow in PseudoCAR route discovery.

relations between links are privately kept in the nodes, our method prevents eavesdroppers from tracing packets and thus it insures *untraceability*. Finally, the protocol could be adapted to other security methods to counter *active attacks*.

The rest of the paper is organized as follows. Section 2 is devoted to study the related work. Section 3 demonstrates our assumptions and system model. PseudoCAR is explained in Section 4. Security evaluation and performance analysis are illustrated in Sections 5 and 6. Finally, Section 7 concludes the paper.

2. Related Work

In this section, we briefly revisit several anonymous routing schemes recently proposed for wireless ad hoc networks. Almost all of the methods are inspired from fixed wired network techniques [3][4]00. Unfortunately special characteristics of ad hoc networks such as absence of fixed infrastructure, mobility of nodes, energy and computation power constraints make previous approaches inapplicable to mobile ad hoc networks. Some works address the anonymity problem in terms of routing schemes. 0 explores the use of mixes [4] in MANETs. An anonymous on-demand routing protocol, named ANODR, has been proposed in 0 to conceal network identifiers of communicating nodes using onion routing. In ASR 0 and MASK [10], nodes forwarding a route request message keep the state of the messages to reforward them later. SDAR 0 is another protocol which uses encrypted route messages to achieve anonymity. ARM 0, as another method, uses random data padding in addition to an onion like technique 0 to harden the protocol in front of passive adversaries. Moreover, the effect of mobility on an anonymous routing protocol is shown in 0 illustrating the impact of anonymous algorithms on routing performance.

Low efficiency and large overhead on relay nodes in route discovery and forwarding phases are the main drawbacks of the mentioned protocols. In addition, in most of these methods the sender should be aware of the entire path. Moreover, some of the protocols put the overhead of several encoding/decoding operations on either relays or end nodes that makes them inapplicable to ad hoc networks.

3. Assumptions and Data Structures

We assume that the radio channel is symmetric. Hence, routes between nodes are bidirectional. Besides, we assume that each node has a common public/private key pair, which is assigned by a trusted off-line certificate authority when the node joins the network. The common public key is known to regular nodes. Moreover, every node is equipped with a random generator function which is initiated with different seed values in deployment phase of the network. In addition, we assume that there exist internal or external attackers that monitor nodes' behavior for the sake of preventing malicious purposes.

In the proposed method, we hide IP and MAC addresses of nodes. Instead, we use the triple <*LinkID*, *RoundNumber*, *SeqNumber*> in the MAC frame and IP packet. Every node maintains a routing table to store forwarding information and a flow table to store information about other ends of its ongoing connections. The routing and flow table attributes are <*PrevLinkID*, *NextLinkID*, *RoundNumber*, *SeqNumber*> and <*PeerIP*, *LinkID*, *RoundNumber*> respectively. We will explain these structures and their usage in detail throughout the following sections.

4. Anonymous Routing Scheme

Here, we introduce a chain-based anonymous routing protocol, named PseudoCAR, which exploits pseudonymity to provide anonymity and untraceability.

4.1. PseudoCAR Route Discovery

The message flow in route discovery of PseudoCAR is shown in Figure 1. Once a source needs to find a route towards its destination, first it generates a locally unique pseudonym by means of its random generator to initiate the chain. For the sake of preserving the locally uniqueness of new identifiers, every node maintains a pool of previously generated identifiers by both itself and its neighbors. The source then sends out a route request (RREQ) message. The RREQ message carries essential information for routing; including the link identifier, sequence number correspondent to the

initiated route discovery, as well as a *Trapdoor*. The last field gives the ability to destination node to detect itself as designated destination. The *Trapdoor* could be opened correctly only by the designated destination.

$$Trapdoor = E_{PK_{Dst}}\left(IP_{Src} \| IP_{Dst} \| Nonce \| RoundNumber\right). \quad (1)$$

As illustrated in equation (1), the *Trapdoor* field which compounded from IP addresses of source and destination nodes, the round number of route discovery (*RoundNumber*) and a random *Nonce*, is encrypted using the destination public key. Like 0 0, we consider the *RoundNumber* as a globally unique number corresponding to each round of route discovery[1]. The *Nonce* and *RoundNumber* fields together are used to prevent replay and modification attacks against the PseudoCAR.

The neighbors around the source, called *receivers*[2], will receive the RREQ. A receiver checks the existence of *RoundNumber* field in its routing table to avoid acceptation of duplicated packets. This prevents more than one occurrence of a node along the path and thus assures loop-free routes construction. After that, the receiver tries to decrypt the *Trapdoor* field of the message to find out whether it is the intended destination (by comparison between its IP address and the IP_{Dst} field of the decrypted *Trapdoor*). If not, it is just a relay node. Hence, it generates a fresh link identifier for its downstream node along the path and fastens it to corresponding upstream link identifier by means of inserting new entry in its route table (i.e. virtually creates a chain). This new entry remains inactive unless the route reply (RREP) packet later crosses the container node. Then, it replaces the embedded *LinkID* field in packet by its own and rebroadcasts the updated RREQ message. On the other hand, if the receiver detects itself as the designated destination, it first creates a new flow table entry corresponding to the received RREQ message. Then the *PeerIP* of the entry is filled by IP_{Src} of decrypted *Trapdoor* and other parts are copied directly from the message. Afterwards, the destination node creates the RREP message and launches the Route Reply phase.

Destination node creates a *Response* to authenticate itself and convinces the source that it has received RREQ message correctly. As illustrated in equation (2), *Response* field compounded from IP addresses of source and destination nodes, the *RoundNumber* (all are retrieved from the decrypted *Trapdoor* of RREQ message), and the incremented *Nonce* which will be encrypted under the source public key.

$$\text{Re}sponse = E_{PK_{Src}}\left(IP_{Src} \| IP_{Dst} \| Nonce+1 \| RoundNumber\right). \quad (2)$$

Other parts of RREP are *RoundNumber* and *LinkID* which are the same as the received RREQ message one. The RREP message is unicasted back to the source following the reverse path which is established before. It is worth pointing out that the source and destination addresses of the MAC frames are replaced with the *LinkID* and *RoundNumber* as well in order to implement anonymous MAC frame.

As the RREP travels back to the source, each intermediate node which has an inactive routing entry matched by the message (i.e. *LinkID* and *RoundNumber* of the message by *NextLinkID* and *RoundNumber* of the entry) activates the entry, replaces the *LinkID* of the message by the *PrevLinkID* of the selected entry, and finally forwards the updated message. When the source node receives the RREP message, it decrypts the *Response* field and checks the *Response*'s parts by the corresponding flow table. If the node gets convinced that the message has been sent from the designated destination, it activates the selected flow table entry and thereafter data transmission becomes possible.

4.2. Route Maintenance

Routing maintenance mechanisms used in traditional ad hoc routing algorithms [14] can be easily applied to PseudoCAR. When a route breaking is detected, an error message (RERR) will be sent back to the source by the node that has discovered the broken link. The RERR message traverses the network similar to data packets.

4.3. Anonymous Data Forwarding

The data forwarding of packets inside a chain is very similar to virtual circuit switching process. Each end node of a connection fills the *LinkID* and *RoundNumber* fields of the data packet by picking them up from the flow table. Then, the packet is sent out to the neighbor who has an activated entry corresponding to *LinkID* and *RoundNumber* fields. The corresponding entry means the entry whose *RoundNumber* is equal to the packet's one and also either its *PrevLinkID* or *NextLinkID* matched with the *LinkID* filed of the packet. To continue transmission of the packet over the chain, the intermediate node replaces the *LinkID* field of the packet by *NextLinkID* field of the matched entry if it was matched by *PrevLinkID* and vise versa. Additionally, the intermediate node updates the *SeqNumber* of the matched routing entry by the packet's one. This avoids loop in data transmission by preventing forwarding of pre-forwarded packets. The scenario is repeated until the packet reaches to the other end of the connection.

4.4. Pseudonym Collision Issues

Here, we study the effect of collision between two or more link pseudonyms. First, we demonstrate that the equality of generated pseudonyms could not affect correctness of PseudoCAR protocol. Then, it is worth mentioning that the pseudonym collision will increase the anonymity in the network as a result of decreasing the certainty of the attacker in distinguishing between two packets.

In situations where some neighbors of a sender node has generated the same link identifier for a specific *RoundNumber*, each of them presumes itself as the sender's

[1] Its globally uniqueness could be implied by using several methods such as [13].

[2] A *receiver* (*sender*) is defined as the node who receives (forwards) a message from (to) its immediate neighbors.

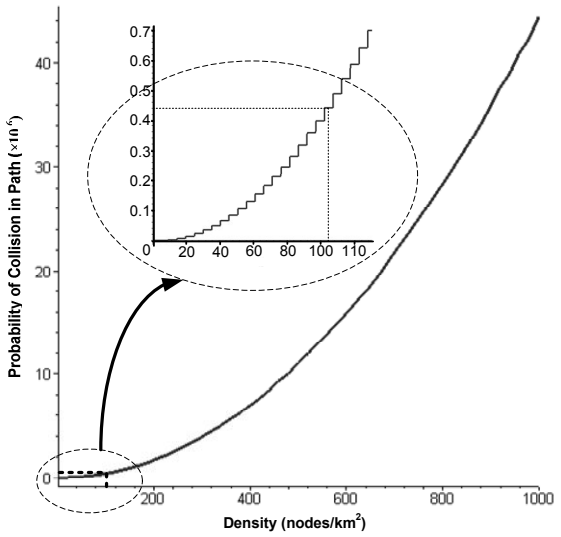


Figure 2. The maximum collision probability along a path with respect to average density of nodes. The highlighted point corresponds to D=7.8*10^{-7}, the common deployed density. (Pseudonym length: 32bit)

next hop. Thus, all of them try to respond to the RTS signal issued by the sender. When a single neighbor wins the contention, one path is selected for the flow and therefore the pseudonym collision does not influence the protocol. On the other hand, in the case that more than one node consider themselves as the winner of the contention, each one acts as a receiver and forwards the packet. Thus, one packet will flows through multiple paths redundantly and hence waste the bandwidth. We analytically show the capacity reduction is negligible in our scheme.

Suppose that the nodes are uniformly distributed throughout the field. Consider D as the average density of nodes, L as the size of pseudonym space, and r as transmission range. Therefore, the average number of neighbors, M, for an arbitrary node is as follows:

$$M = \left\lfloor D.\pi.r^2 \right\rfloor. \tag{3}$$

Clearly, the chance of collision around a sender is:

$$P_c = 1 - \frac{P(L,M)}{N^M}, \tag{4}$$

where P stands for the permutation function. Consequently, the probability of a collision occurrence along a path with length of α is as follows:

$$P_{Path-c} = 1 - \prod_{i=1}^{\alpha}(1 - P_c) = 1 - (1 - P_c)^{\alpha}. \tag{5}$$

While 10-hop is considered a reasonably big path length in related research [15], we have:

$$P_{Path-c} \le 1 - \left(\frac{p\left(L, \left\lceil D.\pi.r^2 \right\rceil\right)}{L^{\left\lceil D.\pi.r^2 \right\rceil}} \right)^{10}. \tag{6}$$

Figure 2 shows the chance of collision along a path with respect to different nodes densities. As depicted by the diagram, occurrence of collision is roughly non-probable. For example, in the case that 150 nodes uniformly deployed in a 2400×600m^2 square field, the maximum probability of collision is in order of 10^{-7} which could be easily tolerated since its impact on the network is negligible.

5. Security Analysis

We analyze our protocol in the presence of several active and passive attacks and show that PseudoCAR ensures anonymity, unlinkability and untraceability in the network.

Modification attacks compromise the integrity of routing computations. In our proposed algorithm, an attacker can modify control and data packets. If the attacker modifies RREQ messages, it will be dropped by receiving neighbors. Since every node broadcasts the RREQ messages to its neighbors, the probability that an attacker can prevent establishment of a route is extremely low. Modifying RREP, RERR, and data messages can alter the route and hence the flow of communication between source and destination. But, as the modified message will be dropped by all the receiving nodes, the altered flow is stopped as near as possible and will not affect the whole network. This will not allow an attacker to redirect the messages toward a different destination or increase the delay of communication. Another problem arises when a selfish node wants to save battery life for its own communication and endangers the correct network operation simply by not participating in the routing protocol or by not executing the packet forwarding. This problem, called *Lack of Cooperation*, is solved in PseudoCAR by means of multi-path routing. In other words a selfish node cannot alter the procedure because other nodes cooperate to introduce all other possible routes to the destination. Here, we relax the problem of *Impersonation* and *Fabrication*, since they can be addressed by an effective authentication protocol and are out of the scope of this paper.

In case of passive attacks, we analyze the power of an eavesdropper to degrade the anonymity of our protocol. Since real identifier of mobile nodes is kept confidential during running of the protocol, we have successfully realized anonymous communication. In other words, sender and receiver anonymity and their relationship anonymity have been achieved. Based on the inherent characteristics of the defined chain, in route discovery and also forwarding phase it is not clear for a node that a message comes directly from the source or just a relay node. On the other hand, after set up of the route a forwarder cannot specify which neighbor will capture the message. Also, it is not apparent even for the last relay nodes which neighbor is the destination of a connection. In other words, every node is unaware of its location in the route. Moreover, an adversarial eavesdropper learns nothing more than some seemingly random numbers from the transient messages. Subsequently, no node can trace any route or data message to discover end points of the connection and hence, untraceability is realized in PseudoCAR. It is worth noting that when all of the nodes along a path are compromised, the path is traceable and linkable.

6. Experimental Results

Here, we evaluate the performance of PseudoCAR and compares to other routing protocols through simulation experiments.

6.1. Simulation Model

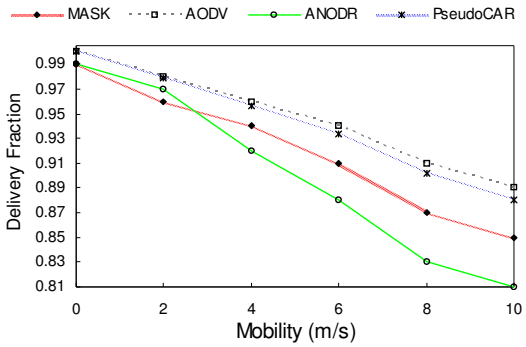
We have carried out several experiences using Network Simulator, ns-2 0. Distributed Coordination Function (DCF) of IEEE 802.11 is used as MAC layer and an unslotted Carrier Sense Multiple Access (CSMA) technique with collision avoidance (CSMA/CA) is used to transmit data packets. We have simulated an ad hoc network with 150 nodes uniformly deployed in a 2400×600 m^2 square field. The transmission range was 250m. Random Waypoint mobility model was used to simulate node's motion behavior. According to the model, a node travels to a random chosen location in a certain speed and stays for a whole before going to another random location. In our simulation, mobility speed varied from 0 to 10 m/sec, and the pause time was set to 30 seconds. Continuous bit rate (CBR) traffic sessions were used to generate network data traffic. For each session, data packets of 512 bytes were generated in a rate of 4 packets per second. Source-Destination pairs were random over the network. During running of our simulation for 10 minutes, 5 pairs of nodes were maintained to communicate. Simulations were conducted in identical network scenarios and routing configuration across all the schemes. Results were averaged over multiple runs with different seeds for the random number generators.

The processing overhead used in our simulation is based on actual measurement on a pocket PC. Table I shows the measurement presented by 0 on the performance of different cryptosystems. For public key cryptosystems, the table shows processing latency per operation, and for symmetric key cryptosystems, it shows encryption/decryption bit-rate. For MASK and ANODR, taking consideration of the crypto systems proposed by the original authors, we choose the cryptosystem specification for simulation like 0.

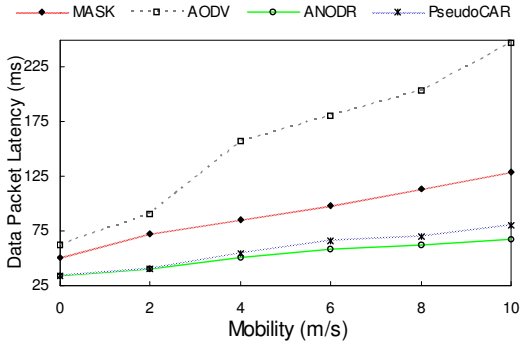
We evaluate the performance of our protocol in relation to these metrics: *packet delivery fraction* (the ratio of the data packets delivered to the destinations to those generated by the sources), *normalized routing load* (the number of routing packets transmitted per data packet delivered at the destination), and the *average data packets end-to-end delay* (the time from when the source generates the data packet to when the destination receives it. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times).

6.2. Simulation Results

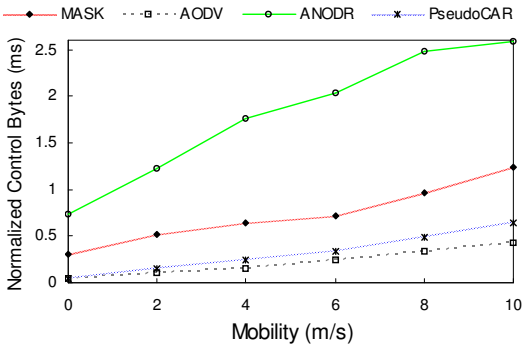
Figure 3 shows comparison of the mentioned metrics among PseudoCAR, AODV [14], and two other anonymous routing protocols ANODR 0, and MASK [10]. In almost all diagrams PseudoCAR works roughly near AODV. Considering the invariability of the nodes identifiers in AODV, it reduces the overhead of route discovery by utilizing route caches. Due to the absence of this feature in PseudoCAR, AODV outperforms our method only in high mobility speeds. Diagram (a) illustrates the effect of mobility on packet delivery fraction. Diagram (b) illustrates the data packet latency. Thanks to the very low overhead on relay nodes in PseudoCAR, the end-to-end latency of data packets is lower than MASK and ANODR. Finally, diagram (c) compares the normalized control overhead in terms of bytes.



(a) Packet Delivery vs. Mobility Rate



(b) Data Packet Latency vs. Mobility Rate



(c) Normalized Control Bytes vs. Mobility Rate

Figure 3. Comparison of simulation results between PseudoCAR and other routing protocols (AODV, ANODR, and MASK).

7. Conclusion

Security and privacy are one of the most challenging issues in wireless ad hoc networks. In this paper, we have proposed a novel anonymous routing, called pseudonym chain-based routing (PseudoCAR), to achieve anonymity in routing and data dissemination. By a careful and simple design, PseudoCAR provides anonymity of sender and receiver in any communication, as well as node unlocatability. Also, it realizes relationship anonymity and connection untraceability in spite of any internal or external eavesdroppers. Moreover, we have shown that PseudoCAR is resilient to different types of active attacks as well as passive ones. Finally, due to low computational overhead of PseudoCAR and based on the experimental results our protocol could be implemented as a cost effective anonymous routing protocol in wireless ad hoc networks.

References

[1] Y. Guan, X. Fu, D. Xuan, P. Shenoy, R. Bettati, and W. Zhao, "NetCamo: Camouflaging Network Traffic for QoS-Guaranteed Mission Critical Applications," in IEEE Transactions on System, Man, and Cybernetics, Vol. 31, No. 4, pp. 253-266, July 2001.

[2] M. Kohntopp, and A. Pfitzmann, "Anonymity, Unobservability, and Pseudonymity: A proposal for terminology," in LNCS 2000.

[3] M. Reiter, and A. D. Rubin, "Crowds: Anonymity for Web Transactions," ACM Transactions on Information and System Security, 1998.

[4] D. Chaum, "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms," Communication of the ACM, 1981.

[5] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," Journal of Cryptography, 1988.

[6] M. Reed, et. Al, "Proxies for Anonymous Routing," In 12th Annual Computer Security Application Conference, 1995.

[7] S. Jiang, N. Vaidya, and W. Zhao, "Dynamic mix method in wireless ad hoc networks," In IEEE Milcom'01, 2001.

[8] J. Kong, and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks," In MOBIHOC 2003.

[9] B. Zhu, et. Al, "Anonymous secure routing in mobile ad hoc networks," In IEEE LCN, 2004.

[10] Y. Zhang, W. Liu, and W. Lou, "Anonymous Communications in Mobile Ad Hoc Networks," In IEEE Infocom, 2005.

[11] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba., "A Novel Solution for Achieving Anonymity in Wireless Ad Hoc Networks," In the ACM Workshop on Performance Evaluation of Wireless Ad hoc, Sensor, and Ubiquitous Networks, 2004.

[12] S. Seys, and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," In International Conference on Advanced Information Networking and Applications, 2006.

[13] J. Kong, et. Al, "Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing," In IEEE Symposium on Computers and Communications (ISCC), 2005.

[14] G. Montenegro and C. Castelluccia, "Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses," in Network and Distributed System Security Symposium (NDSS), 2002.

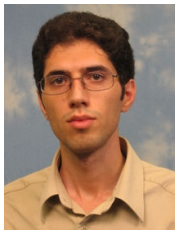
[15] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing," in IEEE WMCSA, 1999.

[16] D. B. Johnson, D. A. Maltz, Y.-C. Hu, and J. G. Jetcheva, "The dynamic source routing protocol for mobile ad hoc networks," IETF Internet draft, Apr. 15, 2003.

[17] NS-2, available at http://www.isi.edu/nsnam/ns/.

[18] V. Gupta, et. Al, "Performance Analysis of Elliptic Curve Cryptography for SSL," In ACM Workshop on Wireless Security, 2002.

[19] J. Liu, J. Kong, X. Hong, and M. Gerla , "Performance Evaluation of Anonymous Routing Protocols in MANETs," IEEE Wireless Communications and Networking Conference 2006, April 2006.

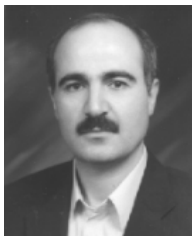


Reza Shokri received his B.Sc. and M.Sc. degrees in Computer Science and Engineering form Universities of Isfahan and Tehran, respectively in 2003 and 2007. His main research interests include network security, privacy protection and wireless networks.
E-mail: r.shokri@ece.ut.ac.ir

Maysam Yabandeh first received the B.S. degree in Computer Science and Engineering from University of Tehran, Tehran, Iran, in 2005. Then, he received his M.S degree in the same university and working as a research assistant in the Router Laboratory, University of Tehran. His main research interests include distributed computing, computer networks, operating systems, and theoretical computer science.
E-mail: m.yabandeh@ece.ut.ac.ir

Nasser Yazdani got his B.S. degree in Computer Engineering from Sharif University of Technology, Tehran, Iran. He worked in Iran Telecommunication Research Center (ITRC) as a researcher and developer for few years. To pursue his education, he entered to Case Western Reserve Univ., Cleveland, Ohio, USA, later and graduated as a Ph.D. in Computer Science and Engineering. Then, he worked in different companies and research institutes in USA. He joined the ECE Dept. of Univ. of Tehran, Tehran, Iran, as an Assistant Professor in September 2000. His research interest includes Networking, packet switching, access methods, Operating Systems and Database Systems.

E-mail: yazdani@ut.ac.ir



Ahmad Khonsari received the B.Sc. degree in electrical and computer engineering from Shahid-Beheshti University, Iran, in 1991, and M.Sc. degree in computer engineering from the Iran University of Science and Technology, Iran, in 1996 and Ph.D. degree in computer science from the University of Glasgow, UK, in 2003. He is currently an assistant professor in the Department of Electrical and Computer Engineering, University of Tehran, Iran and a researcher in School of Computer Science, Institute for Studies in Theoretical Physics and Mathematics (I.P.M.), Iran. His research interests are performance modeling/evaluation, mobile and ubiquitous computing, communication networks and distributed systems, and high performance computer architecture.

E-mail: ak@ipm.ir