An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad-Hoc Networks

Jiejun Kong, Xiaoyan Hong, and Mario Gerla, *Fellow*, *IEEE*

Abstract—Introducing node mobility into the network also introduces new anonymity threats. This important change of the concept of anonymity has recently attracted attentions in mobile wireless security research. This paper presents *identity-free routing* and *on-demand routing* as two design principles of anonymous routing in mobile ad hoc networks. We devise ANODR (ANonymous On-Demand Routing) as the needed anonymous routing scheme that is compliant with the design principles. Our security analysis and simulation study verify the effectiveness and efficiency of ANODR.

Index Terms—Anonymity, identity-free routing, negligibility, ad hoc network, network complexity theory.

1 Introduction

A mobile ad hoc network (MANET) can establish an instant communication structure for many time-critical and mission-critical applications. Nevertheless, the intrinsic characteristics of MANET, such as node mobility and open wireless transmissions, make it very vulnerable to security threats. Even though many security protocol suites have been proposed to protect wireless communications [23], [41], they nevertheless did not consider anonymity protection and left identity information intercepted by nearby eavesdroppers. Consider, for example, a battlefield scenario with ad hoc, multihop wireless communications support. Suppose a covert mission is launched, which includes swarms of reconnaissance, surveillance, and attack task forces. The ad hoc network must provide routes between command posts and swarms as well as routes between swarms. Anonymity protections for the task forces are critical, else the entire mission may be compromised. However, the adversary could deploy reconnaissance and surveillance forces, for instance, embedded systems carried by Unmanned Aerial Vehicles (UAV) or Miniature Aerial Vehicles (MAV), in the battlefield and maintain communications among them. They could form their own network to infer the location, movement, number of participants, and even the goals of our covert missions. This has a great impact on privacy design in mobile networks, which has very different semantics from the conventional notion for infrastructure networks like the Internet and distributed banking systems. Message privacy is the major concern in the latter systems, but mobility enabled by wireless communication has changed privacy issues in many ways. First, the adversarial reconnaissance UAV/MAV nodes are capable of tracing pedestrian soldier's wireless interfaces moving at lower speeds. The mobility of both the adversarial side and the guarding side introduces new privacy problems. In a mobile network, a node's motion pattern, traffic pattern, standing venue, route-driven packet flows, and even the dynamic network topology all become new interests of the adversarial reconnaissance team, bringing in new anonymity challenges in addition to conventional identity privacy and message privacy. Second, in wireless ad hoc networks, mobile nodes must rely on their protocol stack (e.g., ad hoc routing) in communication. As the wireless medium is open to anyone within the transmission range, the baseline of the adversarial reconnaissance team is to exploit mobile ad hoc routing schemes to conduct various privacy attacks.

The new anonymity threat poses challenging constraints on routing and data forwarding. The purpose of this paper is to study the characteristics of passive anonymity attacks against routing schemes in a *mobile ad hoc* environment. The goal of such attacks is very different from other related routing security problems such as resistance to route disruption or prevention of "denial-of-service" attacks. In fact, in our case, the passive enemy will avoid such aggressive schemes in an attempt to be as "invisible" as possible until it traces, locates, and then physically destroys legitimate assets. In particular, for mobile ad hoc routing security, it is necessary to realize defense against anonymity threats to prevent the adversary from launching passive attacks, such as tracing where a mobile node is, inferring the motion pattern of the mobile node, and visualizing a multihop path between a pair of nodes.

The contributions of our study are listed below:

- We show that anonymity defense proposed in infrastructure networks does not address the new anonymity attacks threatening mobile nodes. The

- *J. Kong is with Scalable Network Technologies, Inc., 6701 Center Drive West, Suite 520, Los Angeles, CA 90045. E-mail: jkong@scalable-networks.com.*
- *X. Hong is with the Department of Computer Science, University of Alabama, Tuscaloosa, AL 35487. E-mail: hxy@cs.ua.edu.*
- *M. Gerla are with the Department of Computer Science, University of California, Los Angeles, CA 90095. E-mail: gerla@cs.ucla.edu.*

Manuscript received 20 May 2005; revised 28 Feb. 2006; accepted 17 Oct. 2006; published online 7 Feb. 2007.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-0145-0505.
Digital Object Identifier no. 10.1109/TMC.2007.1021.

global-knowledge-based routing and proactive routing approaches are widely used in infrastructure networks to provide anonymity protection, but they are inefficient or even impractical in mobile ad hoc networks. Moreover, since mobile nodes can be traced by various new methods that were previously infeasible in infrastructure networks, now they need more anonymity protections to prevent the passive adversary from knowing their private motion patterns and other network metrics. This calls for the on-demand routing approach, which does *not* send out unneeded routing advertisements to reveal mobile nodes' private network metrics.

- We propose a new anonymous routing protocol ANODR (ANonymous On-Demand Routing) as the countermeasure. ANODR is a *purely on-demand* routing scheme that just sets up anonymous routes as needed in real time. This limits the chance of eavesdropping and traffic analyzing to a time-critical on-demand window. In a mobile environment, the adversary is left with few options—it must launch the attack in the time-critical window or its information about the guarded mobile nodes is out-of-date. Another distinction of ANODR is that it is the first *identity-free* ad hoc routing scheme, which is contrary to all existing ad hoc routing schemes based on node identities (e.g., IP and MAC addresses). Instead of using node identities, ANODR relies on one-time cryptographic trapdoors in routing. Without node identities, the adversary has no means to break a mobile node's identity anonymity except via a node intrusion. This poses a great physical challenge to the adversary.

The rest of the paper is organized as follows: Section 2 explains related work, including anonymous schemes used in infrastructure networks and several recently proposed anonymous routing schemes used in mobile ad hoc networks. In Section 3, we describe the first on-demand and identity-free anonymous protocol ANODR. The security protection provided by ANODR is analyzed in Section 4. In Section 5, we evaluate ANODR's routing performance. Finally, Section 6 summarizes the paper.

2 Anonymous Routing Revisited

In this section, we briefly review anonymous routing approaches that do *not* follow the on-demand design approach first. We then revisit several recently proposed on-demand anonymous routing schemes.

2.1 Anonymous Routing Not Based on the On-Demand Approach

Before ANODR [29], SDAR [10], AnonDSR [45], and MASK [48], the global routing approach and the proactive routing approach are the dominant choices in anonymous routing design.

In the global-knowledge-based routing approach, the network topology is fixed and prestored on each node. This includes the following designs: 1) In Chaum's DC-net [12], the network topology is suggested as a fixed and closed ring. 2) In Chaum's MIX-net [11], each message sender prestores the entire network topology and then selects a random path from the known network topology in message routing. All subsequent MIX-net designs [36], [25], [27], [6] inherit this assumption. 3) In Crowds [39] and the sorting network [37], all nodes are one logical hop away, pairwise communications exist with uniform cost. Anonymous messages are forwarded to the next node, which is selected in a random manner. If this node is unavailable due to mobility or a system crash, then another selection must be made following the same probabilistic method. In other words, every Crowds node (named as "jondo" in [39]) or sorting network node is a member of an *overlay* network. Although, at the network IP layer, every node-to-node (or jondo-to-jondo) route is comprised of multiple IP routers, at the anonymized overlay layer, such a node-to-node route is a single-hop logical link. This overlay anonymous network assumes either a global routing design or a proactive routing design at the IP network layer. In contrast, static and global topology knowledge is no longer available in mobile ad hoc networks where the network topology constantly changes due to mobility, frequent route outage, and node joining/leaving. Maintaining the same global topology knowledge that is identical to fixed networks is very expensive and reveals the changing topological knowledge to node intruders.

In the proactive routing approach, every node proactively and periodically exchanges routing messages with other nodes. Similar to the global routing approach, every node maintains fresh topology knowledge by paying routing communication overheads. In mobile ad hoc networks, various optimized proactive routing schemes, such as OLSR [1] and TBRPF [34], have been proposed to reduce the incurred routing communication overheads. However, like their wired counterparts, the proactive ad hoc routing schemes let every message sender maintain fresh topology knowledge about the network (even though the incurred communication overhead is less than their wired counterparts). Based on the proactively collected fresh routing knowledge, it is then possible to route anonymous messages to the next stop, which in turn routes the messages toward the final destination. This includes the following designs:

1. All MIX-nets leverage proactive routing protocols at the IP layer to acquire network topology knowledge, which is then used at the anonymized overlay MIX layer to route messages.
2. Like MIX-nets, an overlay of Crowds [39] or sorting network [37] leverages proactive routing information as well.
3. In infrastructure networks, PipeNet [14], Onion Routing [38], and Mist [2] employ an *anonymous virtual circuit* in data forwarding. After a connection establishment procedure, a sequence of routing tables are created on the forwarding nodes to deliver data packets. Each route table holds two columns of virtual circuit identifiers (VCI) in the form of "$vci_x \leftrightarrow vci_y$." If a node receives a packet and the packet is stamped with a vci_x stored in its routing table, the node then accepts the packet, overrides the stamp with the corresponding vci_y, and sends the changed packet to next stop. Mist assumes a fixed

routing hierarchy. Both PipeNet and Onion Routing assume that the underlying proactive routing scheme has already provided the needed routing service. Besides, every node in the anonymous network knows its immediate previous stop (upstream node) and immediate next stop (downstream node).

4. In MIX route [26], a backbone network is formed to cover a mobile network. Every backbone node is a MIX, which uses proactive routing protocols to maintain a fresh network topology of the backbone MIX-net.

In a nutshell, these global-knowledge-based routing and proactive routing schemes treat the underlying network as either a stationary graph or fresh snapshots that can be treated as stationary graphs per proactive period. A shortcoming of applying these approaches in mobile networks comes from node intrusions. If adequate physical protection *cannot* be guaranteed for *every* mobile node, intrusion is inevitable within a long time window. The adversary can compromise one mobile node, gather fresh network topology from the node's knowledge, then use network localization schemes (e.g., distance vector-based APS [33]) to pinpoint every mobile node in the network.

Therefore, although various anonymous mechanisms, such as anonymous virtual circuit [14], MIX-net onion, and backbone-style MIX-net [26] remain effective in ad hoc networks, the global routing topology caching and proactive routing topology acquisition approaches are gradually replaced by the *on-demand* routing approach, which is initiated by ANODR [29]. Now, we describe several recently proposed on-demand anonymous routing schemes that are different from ANODR. We explain the major features of each scheme and its major difference from ANODR.

2.2 SDAR and AnonDSR

SDAR [10] and AnonDSR [45] are anonymous routing protocols with a combination of on-demand route discovery [29] and MIX-net onion data delivery [11], [36], [27], [6].

Trust Management. SDAR node uses a *proactive* and *explicit* neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. It periodically sends out a HELLO message holding the certified public key of the node and, at the same time, collects other nodes' public keys. By observing the behavior of one-hop neighboring nodes or using other approaches, a node classifies its one-hop neighbors into different trust levels. Keys corresponding to these levels are negotiated among same-level nodes. They are later used to enforce trust-based secure communication. For the AnonDSR protocol, a security parameter establishment (SPE) flooding is used before the anonymous routing. SPE establishes a shared key (and key index) between the source and the destination, which is then used to set up a trapdoor between the two ends.

Route discovery. SDAR and AnonDSR employ *on-demand* route discovery procedures to establish ad hoc routes. Similar to ANODR, an SDAR source node S puts a global trapdoor in its RREQ flood packet. The SDAR global trapdoor is a public key encryption of a message that can only be decrypted by the destination. A symmetric key is piggybacked into the global trapdoor to fulfill end-to-end key agreement. Nevertheless, unlike ANODR, which uses an identity-free global trapdoor, SDAR uses the destination D's ID in the global trapdoor. AnonDSR also uses a global trapdoor. However, as it has used an SPE flooding to let the source node share a symmetric key with the destination, the global trapdoor in RREQ is encrypted using symmetric cryptography. Like SDAR, AnonDSR also uses destination's clear ID in its global trapdoor.

SDAR's RREQ flooding is not based on onion. The source node S puts its one-time public key TPK in the RREQ flood packet. S also piggybacks the corresponding one-time private key TSK in the global trapdoor. Each RREQ forwarder records TPK, chooses a random symmetric key K, and uses TPK to encrypt this per-stop K. This encrypted block is appended to the current RREQ packet. Finally, the destination D opens the global trapdoor and knows TSK, then uses TSK to decrypt every TPK-encrypted block and, thus, shares a symmetric key with every forwarder of the received RREQ packet. This process is just like transferring a locked $SuggestionBox$. Both source and destination can open the box. While the intermediate nodes can inject information into this suggestion box, they cannot open it. After the destination opens the $SuggestionBox$, it gets all the information added by intermediate nodes and accomplishes key agreements with these nodes.

AnonDSR uses onion in RREQ. However, unlike the uniform-size ANODR onion described in later sections, an AnonDSR onion consists of two parts. The first part is the secret key selected at each hop encrypted by the one-time public key handed from the source node, and the other part is the previous onion received from RREQ upstream node with a nonce encrypted all together using that secret key.

Similar to MIX-net, for both of SDAR and AnonDSR, the destination D has the l (symmetric) keys to form an RREP packet in the form of MIX-net onion, where l is the number of hops from the source to the destination. The destination D puts all symmetric key Ks in the innermost core so that only the source S can decrypt the onion core and share D's symmetric key with every RREP forwarder.

In contrast with other on-demand protocols, for SDAR and AnonDSR, the overhead of public key coding for the destination node to perform is proportional to the hop count en route from the source to the destination. This is because, at each hop, public key encryption is used for packing pairwise session keys. Furthermore, decoding using public keys is expensive. It is obvious that, when the number of hops is large for a source-destination pair, it takes a huge overhead for the destination to extract the intermediate nodes' session keys.

Once the source S receives the coming-back RREP, both the source S and the destination D have made a symmetric key agreement with every intermediate forwarder. Like the way RREP packet is delivered, S and D use MIX-net onion to deliver data payload to each other.

2.3 Mask

Similar to SDAR, MASK [48] relies on a *proactive* neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. However, the MASK's neighbor

TABLE 1
Protocol Comparison

	ANODR	SDAR	AnonDSR	MASK
Purely on-demand?	Purely on-demand	Proactive neighbor detect.	Purely on-demand	Proactive neighbor detect.
PKC in RREQ flood	First contact	All the time	All the time	No
Data delivery	Virtual circuit	MIX-net onion	MIX-net onion	Virtual circuit
Neighbor exposure	No	Exposed	No	No
Recipient anonymity	Crypto-protected for destination	Crypto-protected for destination	Crypto-protected for destination	Broken by any RREQ receiver

detection protocol is identity-free. Each MASK node only knows the physical presence of neighboring ad hoc nodes. This is achieved by a pairing-based anonymous handshake [5] between any pair of neighboring nodes. MASK uses a three-stage handshake for key exchanges among a node and its new neighboring nodes. After the handshake, each pair of nodes shares a chain of secret key and locally unique LinkID pair which corresponds to the pseudonyms used during handshake. In general, every MASK node periodically sends out a HELLO message holding the pairing cryptographic materials. The MASK HELLO messages are not necessarily too long, since it could only consist of an 8-byte pseudonym and a 4-byte nonce.

Route discovery. Like ANODR, MASK employs an on-demand signaling procedure to establish a virtual circuit for later data delivery. The source node S assembles an RREQ flood packet which is similar to AODV in format. Unlike ANODR and SDAR, MASK does *not* use a global trapdoor. In the MASK's RREQ packet, S *explicitly* puts in the destination node D's network ID. This saves the processing overhead to open the global trapdoor, thus sparing the need of end-to-end key agreement and results in a more efficient RREQ procedure. However, the security trade-off is that recipient anonymity is compromised by every RREQ receiver [35].

Besides the removal of the global trapdoor, MASK is more efficient because the proactive neighbor detection protocol has already established every anonymous link needed by the virtual circuit. During the RREQ phase, every RREQ forwarder remembers which outgoing pseudonym is used to forward the RREQ packet from an incoming LinkID. During the RREP phase, a node looks up its pseudonym corresponding to the incoming LinkID included in RREP packet, finds out the incoming LinkID received during RREQ corresponding to that pseudonym, and inserts this two LinkID pair into its route table. When the source receives RREP, the anonymous virtual circuit is established.

2.4 Comparison

Table 1 compares several design choices that may have a significant impact on routing protocol performance and on security/performance trade-offs.

We compare these aspects due to five reasons. The first three aspects have significant performance impacts on mobile ad hoc routing: 1) Proactive neighbor detection incurs periodic communication and computational overhead on every mobile node. 2) Because public key cryptography requires longer keys and more CPU cycles, using expensive public key cryptography (encryption/decryption) with expensive RREQ flood incurs intensive communication and computational overheads per flood. 3) In terms of data delivery performance, virtual circuit-based schemes are more efficient than MIX-net's onion-based schemes—the latter one incurs l real-time encryption delay on the source node and then a single real-time decryption delay on every data packet forwarding node. The next two aspects affect anonymity protection: 4) In MIX-net, a one-hop neighborhood is exposed to an internal (and possibly external) adversary. This is not a security problem in fixed networks, but in mobile networks, this reveals the changing local network topology to the mobile wireless adversary, which can quickly scan the entire network at once and obtain an estimation of the entire network topology. 5) Ensuring recipient anonymity (of the destination's network ID) is a critical security concern. Otherwise, every RREQ receiver can see how busy a destination node is. This traffic analysis can be used by the adversary to define the priority in node tracing attacks.

3 ANODR Design

In this section, we describe the ANODR protocol. ANODR relies on purely *on-demand* routing and *identity-free* routing. The purely on-demand approach is more "covert" in nature in that it does not send out wireless advertisements in advance—it just sets up routes as needed. The identity-free approach ensures identity anonymity for all mobile wireless routers.

3.1 Passive Threat Model

Anonymity threats are from the attackers that are passive in nature. The attackers are protocol compliant, so they are harder to detect before potentially devastating physical attacks are launched. ANODR further characterizes the passive adversary in terms of an escalating capability hierarchy.

TABLE 2
The Notations Used in this Paper

PK_A	Node A's public key	K_A	An encryption key only known by node A
SK_A	Node A's private key corresponding to PK_A	K_{AB}	An encryption key shared by node A and B
$\{M\}_{PK_A}$	Encryption/verification of message M with key PK_A	$f_{K_A}(M)$	Encryption/decryption of message M with symmetric key K_A using a symmetric encryption function f
$[M]_{SK_A}$	Decryption/signing of message M with key SK_A	N_A, N_A^i	Nonce or nonces chosen by node A
src	"source!", a special bit-string tag denoting the source	$dest$	"destination!", a special bit-string tag denoting the destination

- *Mobile eavesdropper and traffic analyst*. Such an adversary can at least perform eavesdropping and collect as much information as possible from intercepted traffic. It is mobile and equipped with GPS to know its exact location. It is a *global* adversary as we assume that it can scan the entire network area in short delay round by round. The baseline traffic it can intercept is the routing traffic from the legitimate side. An eavesdropper with enough resource is capable of analyzing intercepted traffic on-the-scene. This ability gives the traffic analyst quick turnaround action time about the event it detects and reduces the chance of evasion for those victim nodes.
- *Mobile node intruder*. If adequate physical protection cannot be guaranteed for every mobile node, node compromise is inevitable within a long time window. A successful passive node intruder is protocol-compliant and thus hard to detect. It participates in collaborative network operations (e.g., ad hoc routing) to boost its passive attack strength; thus, it threatens the entire network, including all other uncompromised nodes. This implies that a countermeasure must not be vulnerable to a single point of failure/compromise.
- *Mobile colluding attackers*. Adversaries having different levels of attacking ability can collaborate through a separated channel to combine their knowledge and to coordinate their attacking activities. A subset of guarded network members (measured by intrusion percentage/probability) can be compromised. This realizes the strongest power on the adversary side.

3.2 Network and Network Security Assumption

We assume wireless links are symmetric; that is, if a node X is in transmission range of some node Y, then Y is in transmission range of X. A mobile node's physical interface is capable of using omni-directional radio to transmit packets. Within its transmission range, a network node can send a unicast packet to a specific node or a broadcast packet to all local nodes. A node may hide its identity pseudonym using an anonymous broadcast address. In 802.11, a distinguished predefined multicast address of all 1s can be used as source MAC address or destination MAC address to realize anonymity for local senders and receivers. In addition, by anonymous acknowledgment and retransmission, a local sender and a local receiver can implement locally reliable unicast. If the count of retransmission exceeds a predefined threshold, the sender considers the connection on the hop lost.

In ANODR, each node is capable of doing encryption and decryption in semantically secure [20] symmetric key and public key cryptosystems. We assume that an end-to-end network security suite has already protected the IP packet payload. The baseline information used by the passive adversary is the unprotected routing information, such as IP header, link layer header, and, in regard to multihop routing, any unchanged packet characteristics like unique packet length and unchanged packet field (even if the field is encrypted in a semantically secure system).

For the sake of end-to-end security, the source/sender knows the certified public key of any intended destination/recipient. 1) This implies that every network node must acquire a signed credential from an offline authority Ψ prior to network operations. The credential can be verified by the netwisely well-known PK_Ψ. The credential is in the form of "$[id, pk_{id}, validtime]_{SK_\Psi}$," where id uniquely identifies a node, pk_{id} is the certified public key of the id, and $validtime$ limits the valid period of the credential. In ANODR, instead of using the unprotected plain id, the source remembers the credential and avoids using id in communication. 2) The certified public key of the destination is the global trapdoor key used in the *first* identity-free route discovery process. To ensure end-to-end key agreement, a symmetric key is exchanged in the first route discovery. Then, the source would use the symmetric key in later route discovery processes toward the same destination.

The notations used in this paper are shown in Table 2.

3.3 Identity-Free On-Demand Routing Using One-Time Trapdoors

Contrary to conventional schemes which use node identities in packet forwarding and routing, ANODR relies on one-time cryptographic trapdoors.

Anonymous route discovery. Anonymous route discovery is a critical procedure that establishes an on-demand route. A communication source initiates the route discovery procedure by assembling an RREQ packet and locally broadcasting it. An RREQ packet is of the format with one-time contents:

$$\langle RREQ, seq\#, global\_trap, onion \rangle.$$

- $seq\#$ is a 128-bit computationally unique sequence number in the entire network. Each source randomly selects a value for this field. Due to the "birthday paradox" [32], the probability of choosing colliding values on different sources is approximately $2^{-128/2} = 2^{-64}$, a negligible quantity.

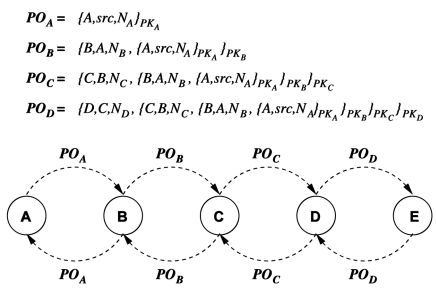


Fig. 1. Chaum's Public-key Onion (PO) between source sender A and destination recipient E.

- *global_trap* is a global trapdoor. Only the destination can decrypt the global trapdoor and know its role by seeing a well-known string tag/message (e.g., "destination!" with a one-time random nonce appended). The details of global trapdoor design are elaborated later in this section.
- The other is a 128-bit "onion" of per-hop encryptions. The source puts a random nonce as the onion "core." If each RREQ forwarder adds a layer of encryption during the RREQ phase, then only the node itself can peel off this layer during the RREP phase. The onion is formed during RREQ propagation and will be used to set up an anonymous virtual circuit when the RREPs come back.

First, let us present a scheme simply combining on-demand routing and Chaumian MIX-Net's onion processing. The onion is formed as a public key protected onion (PO). The corresponding "On-demand MIX-Net" protocol is described below:

1. *RREQ phase*. RREQ packets with previously seen sequence numbers are discarded. Otherwise, as depicted in Fig. 1, each RREQ forwarding node X prepends the incoming hop to the PO structure, encrypts the result with its own public key PK_X, and then broadcasts the RREQ locally.
2. *RREP phase*. When the destination receives an RREQ packet, the embedded PO structure is a valid onion to establish an anonymous route toward the source. The destination[1] assembles an RREP packet of the format

$$\langle RREP, N, onion \rangle,$$

holding the same cryptographic onion in the received RREQ packet, and then locally broadcasts it. N is the 128-bit random route pseudonym selected by the destination. It is computationally unique in the neighborhood due to the "birthday paradox" [32].

Any receiving node X decrypts the onion using its own private key SK_X. If its own pseudonym X does not match the first field of the decrypted result, it then discards the packet. Otherwise, the node is on the anonymous route. It selects its own random nonce N', stores the correspondence between $N \rightleftharpoons N'$ in its forwarding table, peels off one layer of the onion, replaces N with N', and then locally broadcasts the modified RREP packet. The same actions will be repeated until the source receives the onion it originally sent out. As depicted in Fig. 2, the nonce chosen by the RREP upstream node is shared on the hop. This nonce will play the role of virtual circuit identifier (VCI) [4] in anonymous data delivery.

1. The destination should do RREQ forwarding as if nothing has happened.

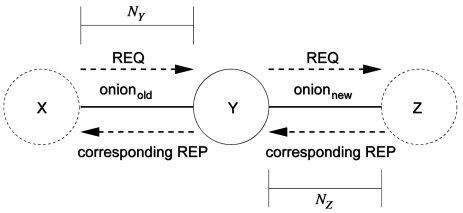


Fig. 2. ANODR route discovery at each RREP forwarder.

Unfortunately, "On-demand MIX-Net" is *not* an identity-free scheme. In addition, "On-demand MIX-Net" incurs expensive public key encryption overhead in the network-wide RREQ floods. This is not suitable in mobile ad hoc networks where many ad hoc network members may use low-end mobile devices. In contrast, except the first route discovery, ANODR is identity-free and incurs no public key encryption overhead in RREQ floods (though ANODR always incurs public key processing overhead in RREP unicasts by using one-time public keys on RREP forwarding nodes).

1. When intermediate forwarding node X sees an RREQ packet, it encrypts the incoming onion with a random symmetric key K_X. This produces the outgoing onion. The node remembers the correspondence between these two onions and broadcasts the RREQ locally. After the RREQ forwarding operation, the node tries to open the global trapdoor to check whether it is the destination.
2. The onion will be bounced back by the destination like a boomerang (Fig. 3). Given an RREP unicast packet transmitted by omnidirectional radio, only the RREQ upstream node (i.e., currently the RREP downstream node) that produced the current onion now embedded in the transmitting RREP packet will forward the RREP unicast. This chosen node strips

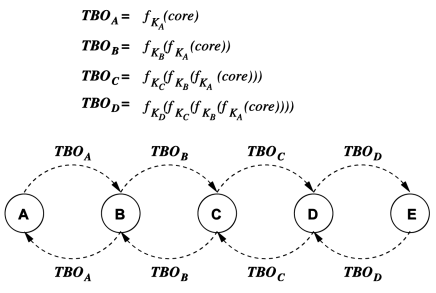


Fig. 3. Trapdoored Boomerang Onion (TBO) between source sender A and destination recipient E.

off a layer of the boomerang onion and forwards the modified RREP packet toward the source.

Actual ANODR route discovery design. In addition to the above description, ANODR implements 1) symmetric key agreement between two consecutive RREP forwarders and 2) enforces destination-initiated RREP procedure. Thus, the previous packet format definitions were incomplete ones for the ease of presentation. The actual ANODR route discovery packet formats with one-time contents are

$$\langle RREQ, seq\#, global\_trap, onion, pk\_1time\rangle$$
$$\text{and } \langle RREP, \{K_{seed}\}_{pk\_1time}, f_{K_{seed}}(proof_{dest}, onion)\rangle.$$

- K_{seed} is the same as the 128-bit random route pseudonym N (i.e., VCI), except now it becomes a secret key shared between two consecutive RREP forwarders. The need for the secret hop key between two neighboring RREP nodes is justified later, in the paragraph "Anonymous data forwarding."
- In its idle time, a node X generates reasonably many one-time public/private key pairs (pk_1time_X, sk_1time_X). A one-time public key is used per RREQ flood. Let us use Fig. 2 as an example. In RREQ forwarding, node Y remembers not only each incoming onion, but also the one-time public key pk_1time_X associated with the onion, and then node Y replaces the old pk_1time_X with its own one-time pk_1time_Y. Similarly, node Z performs the same operation, and so on. Later, in RREP forwarding, a random K_{seed} (or N) is selected by the RREP upstream node and encrypted by the one-time pk_1time of the RREQ upstream node (now the RREP downstream node) that will decrypt it and accomplishes the symmetric key agreement. The remaining RREP contents (including $onion$) are encrypted by the symmetric key.
- The global trapdoor $global\_trap$ holds secret information for the intended destination and a public commitment for the same destination. Using Fig. 3 as an example, the global trapdoor for the first time RREQ is

$$\langle RREQ, global\_trap = \underline{\{dest, K_{reveal}, K_{AE}\}_{PK_E}, f_{K_{reveal}}(dest)}, onion, pk\_1time\rangle.$$

Or, in all later RREQs, as K_{AE} is the end-to-end key agreed between the source and the destination,

$$\langle RREQ, global\_trap = \underline{f_{K_{AE}}(dest, K_{reveal}), f_{K_{reveal}}(dest)}, onion, pk\_1time\rangle.$$

$proof_{dest}$ is the RREP proof (or receipt) from the destination.

$$\langle RREP, \{K_{seed}\}_{pk\_1time}, f_{K_{seed}}(proof_{dest} = \underline{K'_{reveal}}, onion)\rangle.$$

This design seeks to prevent an adversarial network node to send back fake RREPs to disrupt ANODR. Among all network members, only destination E can see the special string tag $dest$ and conclude that it is the intended destination. The value K_{reveal} is a commitment value. During RREQ phase, it is a secret committed to the destination (by the source). During the RREP phase, it is revealed to fulfill the commitment. The destination E must present this commitment value $K'_{reveal} = K_{reveal}$ to prove that it has successfully opened the global trapdoor. Any forwarding node can verify the anonymous proof of global trapdoor opening by checking $f_{K_{reveal}}(dest) \stackrel{?}{=} f_{K'_{reveal}}(dest)$. Nodes other than the destination E cannot fulfill the correct K_{reveal} unless they can break the global trapdoor. RREPs with incorrect K'_{reveal} are unconditionally dropped.

Anonymous route maintenance. Following the soft state design, the routing table entries are recycled upon timeout T_{win} similar to the same parameter used in DSR and AODV. Moreover, when one or more hop is broken due to mobility or node failures, nodes cannot forward a packet via the broken hops. The one-hop sender can detect such anomalies when the retransmission count exceeds a predefined threshold. Upon anomaly detection, the node looks up the corresponding entry in its forwarding table, finds the other VCI N' which is associated with the VCI N of the broken hop, and assembles an anonymous route error report packet of the format $\langle RERR, N'\rangle$. The node then recycles the table entry and transmits the RERR packet using omni-directional radio. A receiving node of the RERR packet looks up N' in its VCI mapping table. If the lookup returns a match, then the node is on the broken route and should follow the same procedure to notify its neighbors.

Anonymous data forwarding. For each end-to-end connection, an anonymous virtual circuit is established between the source-destination pair. Intuitively, the route pseudonym N shared on a hop is used as the virtual circuit identifier (VCI) in data packets:

$$\langle DATA, route\_pseudonym, payload\rangle.$$

After the source or the current forwarder transmits the packet using its omni-directional radio, all other local receiving nodes must look up the route pseudonym in their "incoming VCI $\rightleftharpoons$ outgoing VCI" mapping tables. A node discards the packet if the route pseudonym in the packet does not match any incoming VCI in its table. Otherwise, it changes the packet's route pseudonym field to the matched outgoing VCI, then acts as the current forwarder and transmits the modified packet using omni-directional radio. The procedure is then repeated until the data packet arrives at the destination.

This is only an intuition of anonymous data forwarding for the ease of presentation. To thwart the *packet flow tracing attack* which can compromise relationship anonymity between sender and recipient venues, ANODR implements three mechanisms:

- *Randomized route pseudonym*. Even at the same hop, the route pseudonym N is updated per data packet. The data packet format is actually

$$\langle DATA, route\_pseudonym, index, payload\rangle.$$

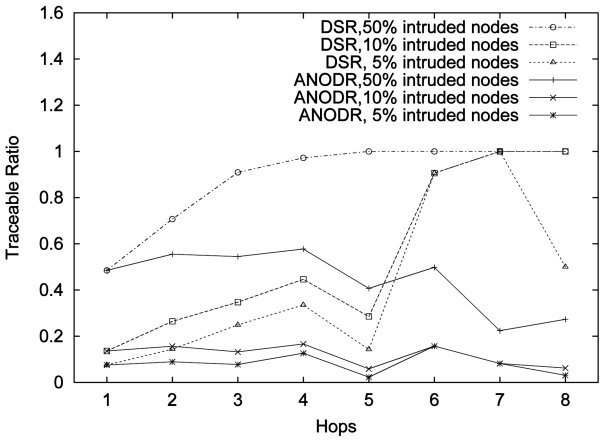


Fig. 4. Delivery fraction.

1) At each hop of an end-to-end connection, the shared VCI K_{seed} is used as the secret seed to generate cryptographically strong pseudorandom sequences. The ith data packet of the connection is marked with the ith 128-bit bit-string generated from the common K_{seed} (rather than marked by the secret K_{seed} itself). The VCIs stored in routing tables are updated in the same manner. The pseudorandom bit-strings cannot be distinguished from truly random bits by any polynomial-time algorithms. This is because provably secure pseudorandom bits [9] can be constructed using hardcore predicates [19] of a one-way function. Additionally, fast but empirically secure pseudorandom sequence generators are also available for performance gain (e.g., X9.17 [3]). All such pseudorandom sequence generators use a keyed one-way function $f_{key}(seed)$, so let us denote the ith 128-bit bit-string as $f^{(i)}_{K_{seed}}(K_{seed})$. 2) The $index$ field is added due to wireless packet loss and packet shuffling. If the channel is reliable, consecutive packets can be trivially marked with consecutive pseudorandom bit-strings. However, the wireless channel is unreliable and packet loss is possible. ANODR assumes that the chance for the channel to consecutively drop more than 2^8 packets is negligible, thus the size of the $index$ field is defined as 8 bits (certainly, the bit-field can be extended to 12 or 16 bits for more severe packet loss scenarios). At the sender side, the $index$ is increased by 1 for each distinct data packet in order and wrapped around per 2^8 packets. The sender can shuffle the order of packet transmissions as well. If the most recent $index$ received by the receiver is a and the $index$ of the current incoming packet is b, then the receiver can synchronize the pseudorandom sequence by skipping the gap $f^{(b)}_{K_{seed}}(K_{seed}) = f^{(b-a)}_{K_{seed}}(f^{(a)}_{K_{seed}}(K_{seed}))$. This way, the packet flow of the same connection will be marked by "one-time" route pseudonyms changed over time and over hops all the way from the source to the destination.

- *Payload shuffle*. To thwart content correlation where the adversary can simply monitor data payloads to trace a specific packet payload (if his collaborators are on the forwarding path or his mobility speed can catch up with the packet forwarding process), the $(index, payload)$ fields must be reencrypted and decrypted at every hop using the hop key K_{seed}. To prevent the adversary from tracing packet flow upon measuring packet length, it is reasonable to enforce a uniform packet size such that all packets are padded to be the same size and length information becomes useless to the adversary. In ANODR, uniform payload size is implementation-defined. That is, the decision is to be made in deployments.
- *Neighborhood traffic mixing*. To stop timing analysis, each node X needs to do *neighborhood traffic mixing*, a method similar to the timed pool MIX proposed in various MIX-Net designs [36], [27], [6]. Let us assume that node X autonomously chooses and adjusts t_X as its playout time window size and r_X as its playout buffer size. During the t_X period, if node X has received r data packets with distinct pseudonyms (of possibly different connections), then it generates $r_d = max(0, r_X - r)$ decoy packets. ANODR's mixing is on-demand/reactive as it does not generate decoy packets $(r_d = 0)$ if $r = 0$ or $r_X \leq r$. The route pseudonyms used in the decoy packets should be truly random and do not collide with the current pseudorandom VCIs in the node's routing table. At the end of time window t_X, node X randomly reorders all packets in the playout buffer and sends them out in a batch. Neighborhood traffic mixing is a more general design than the random latency design used by [15] and [48], which is the special case of neighborhood mixing with r_X set to 0.

3.4 Discussions

Reliable forwarding and anonymous ACK. In RREP/RERR/DATA unicasts, an anonymous transmission can be delivered in a more reliable way in spite of wireless channel errors, namely, anonymous ACK. Recall that the one-hop receiver of an RREP/RERR/DATA unicast packet already knows the K_{seed} if it does correctly receive the packet to be ACKed. This means it knows the current route pseudonym N; thus, the anonymous ACK packet is simply in the form $\langle ACK, route\_pseudonym \rangle$.

Upon timeout (similar to 802.11 unicast), the sender must try to retransmit the un-ACKed unicast packet until it receives the anonymous ACK. Like 802.11's unicasts, if the retransmission count exceeds a predefined threshold, then the sender considers the hop connection is broken. If this happens during anonymous data forwarding, route maintenance will be initiated to recycle routing table entries.

Optional neighborhood traffic mixing on control packets. To resist timing analysis, ANODR's data flow is protected by neighborhood traffic mixing, but the adversary can do timing analysis on control flows as well.

ANODR's RREQ is a flooding process which does not reveal specific packet flows, but an adversary capable of monitoring the entire network area can identify the source sender's venue. It can also identify the destination recipient's venue by monitoring the first RREP triggered by an RREQ flood. The revelation of sender venue and

recipient venue calls for mixing on RREQ and RREP traffic. In other words, it seems that we should enforce the uniform timing policy to let each mobile node send out decoy RREQ (where the global trapdoor is truly random and cannot be decrypted by any network node) and decoy RREP (where the replied RREP unicast will eventually become a networkwide flood of RREP unicasts) per time window (if during the window no real RREQ and RREP is transmitted). Unfortunately, even though we can optionally enforce this security policy, we believe that this design is *not* suitable in mobile ad hoc networks where frequent networkwide floods will rapidly drain network resources. If the adversary is capable of monitoring the entire network area, sender venue anonymity and recipient venue anonymity are not protected in ANODR. Similarly, this global adversary can also trace the RREP forwarding process and compromise relationship anonymity between sender venue and recipient venue. Fortunately, the global adversary also pays tremendous cost and it must exploit its chance in the short route discovery period.

4 Security Analysis

4.1 Foundations of Security

The first formal model of security, in particular of cryptography, was an information theoretic model introduced by Shannon in [44], where $H(M)$, the entropy of the truly random plaintext set M, equals $H(M|E)$, the conditional entropy of the plaintext set M given the interceptable ciphertext set E. In other words, the uncertainty entropy is unchanged by crypto-operations, so a truly random random variable (a.k.a. coin-flips, coin-tosses in cryptographic notions) stays as truly random after applying an information theoretically secure operation like the one-time pad. Shannon showed that it is impossible to break such a perfect system. Unfortunately, the information-theoretic notion is impractical: If we measure security strength in terms of the key length n, in the perfect system, the key length must be greater than or equal to the plaintext length; both key space size and plaintext space size are of an exponential order $O(2^n)$.

Since late 1970s, modern cryptography [18] abandoned this information theoretic notion and assumed instead that the adversary is a probabilistic algorithm running in polynomial time. The ideal goal is still to achieve *indistinguishability* from truly-randomness. 1) As described above, the perfect system exactly achieves the ideal goal by using security resources measured in exponential order of the key length n. 2) Modern cryptography seeks to achieve the same goal with acceptable difference between what can be implemented and the ideal truly-randomness. Unlike the perfect system, all crypto algorithms only use *polynomial-order* resource to produce pseudorandomness that is indistinguishable from truly-randomness *by any polynomial-time adversary*, where all the polynomials are defined on the input key length n.

The acceptable difference between truly-randomness and cryptographic pseudo-RANDOMNESS must be "*negligible,*" which is asymptotically less than the reciprocal of any polynomial of the input x (where, in cryptography, x is the key length n). For this reason, "negligible" is also known as "subpolynomial."

Definition 1 (Negligible). *A function $\mu : \mathbb{N} \rightarrow \mathbb{R}$ is negligible if, for every positive integer c and all sufficiently large xs (i.e., there exists N_c, for all $x > N_c$), $\mu(x) < \frac{1}{x^c}$.*

4.2 Perfectly Secure Routing Identities

Due to identity-free routing, the adversary *cannot* identify any mobile node's *routing identity* (e.g., IP address, MAC address). In a more formal notion, the uncertainty entropy about an uncompromised sender/receiver's identity equals the truly random guess. The security loss in regard to entropy of routing identities is zero.

4.3 Negligibility-Based Network Security

Recently, information-theoretic models for anonymity were independently proposed in [43] and [16]. As demonstrated in [28], these information-theoretic models can be translated into an equivalent form of Shannon's perfect secrecy. In this paper, we seek to pursue a further goal—we believe that the notion of negligibility is also a foundation of network security research, as shown in our complexity-theoretic model $\mathcal{GVG} - \mathcal{RP}$ [30]. This time, the polynomial input x is *not* a computational metric like the key length n, but a network metric, such as N, the number of participating nodes in the network protocol. We will show that *the probability of security breach is negligible (e.g., decreasing exponentially toward 0) when the number of mobile network members N increases linearly/polynomially.*

In the negligibility-based network security discussion, we focus on passive threats in regard to routing and packet forwarding. This is because ANODR is a secure routing protocol that provides protection for network layer routing and link layer forwarding. Threats regarding other issues like radio signature and application layer vulnerabilities are beyond the scope of ANODR design. In the future, ANODR should be used with other security schemes at other protocol stack layers to provide an all-in-one solution.

4.4 Negligibility-Based Security Guarantee of ANODR

Motion pattern tracing. In a mobile network of $N = 1$ nodes, a (global) passive adversary can trace the node's motion pattern as long as the node's transmissions to the infrastructure are interceptable. When $N > 1$, if common ad hoc routing schemes like AODV and DSR are used, the passive adversary can easily distinguish different senders/receivers using the routing identities, including those embedded in data packet headers and control packets. The growth of network scale has no impact on network security.

However, this is *not* true in the identity-free ANODR. For a mobile node, we define its "*venue*" as the smallest area to which the *adversary* can pinpoint the node only via the node's radio communication and any available positioning scheme. Such a venue area is clearly not infinitesimal. It is at most the one-hop radio eavesdropping range. With better positioning support, the adversary can reduce the one-hop circle to a smaller one quantified by the radius Δ (note that the circle can be generalized to an arbitrary geometric shape that is equal in size). In practice, a venue is at the granularity of a significant fraction of the

radio transmission circle [21]. Nevertheless, by the definition of "venue," the adversary *cannot* differentiate two or more *identity-free* nodes in a venue $\pi\Delta^2$: A packet is equally likely to be from one node or another standing in the venue region. We call this phenomenon "*localized greedy coordination*," which means that a network security service is accomplished in a local finite region as long as there is at least one uncompromised node (other than the node being attacked) in the region. In identity-free routing, for k uncompromised nodes in any venue, k-anonymity [46] is ensured in the venue.

Mobile network modeling. For a network deployed in a bounded system area, let the random variable $\Omega = (X, Y)$ denote the Cartesian location of a mobile node in the network area at an arbitrary time instant t. The spatial distribution of a node is expressed in terms of the probability density function[2]

$$\rho = f_{XY}(x, y) = \lim_{\delta \to 0} \frac{\boldsymbol{Pr}[(x - \frac{\delta}{2} < X \leq x + \frac{\delta}{2}) \wedge (y - \frac{\delta}{2} < Y \leq y + \frac{\delta}{2})]}{\delta^2}.$$

The probability that a given node is located in a subarea $\mathcal{A}'$ of the system area $\mathcal{A}$ can be computed by integrating ρ over this subarea

$$\boldsymbol{Pr}[\text{node in } \mathcal{A}'] = \boldsymbol{Pr}[(X, Y) \in \mathcal{A}'] = \iint_{\mathcal{A}'} f_{XY}(x, y) d\mathcal{A}, \quad (1)$$

where $f_{XY}(x, y)$ can be computed by a stochastic analysis of an arbitrary mobility model. For example, as suggested in [8], we can use the analytical expression $\rho = f_{XY}(x, y) \approx \frac{36}{a^6}(x^2 - \frac{a^2}{4})(y^2 - \frac{a^2}{4})$ for random waypoint (RWP) mobility model in a square network area of size $a \times a$ defined by $-a/2 \leq x \leq a/2$ and $-a/2 \leq y \leq a/2$.

Equation (1) is universally applicable to any mobility pattern. Then, ρ can be obtained from related stochastic analysis [7], [8], [40]. Given this ρ, we treat it as a mobile node's arrival rate of each standing "position." Hence, the random presence of mobile nodes is modeled by a *spatial Poisson point process* [13]. If there are N nodes in the network, $\rho_N = \sum_{i=1}^{N} \rho_i$, where ρ_i is ith node's pdf, and if every node roams independently and identically distributed (i.i.d.), then $\rho_N = N \cdot \rho$. Let x denote the random variable of number of mobile nodes in an area, the probability that there are exactly k nodes in a specific area $\mathcal{A}'$ following a uniform distribution model is

$$\boldsymbol{Pr}[x = k] = \frac{(\rho_N \mathcal{A}')^k}{k!} \cdot e^{-\rho_N \mathcal{A}'}. \quad (2)$$

More generally, in any distribution model including nonuniform models like the RWP model, the arrival rate is *location dependent*. ρ is higher at some areas while lower at the other areas [7], [8]. The probability that there are exactly k nodes in a specific area $\mathcal{A}'$ is

$$\boldsymbol{Pr}[x = k] = \iint_{\mathcal{A}'} \left(\frac{\rho_N^k}{k!} \cdot e^{-\rho_N} \right) d\mathcal{A},$$

where the integral can be computed in simulators like NS2 and QualNet given a specific area $\mathcal{A}'$ and the finite element method. The probability that a venue is empty is

$$P_{empty} = \boldsymbol{Pr}[x = 0] = \iint_{\pi\Delta^2} e^{-N\rho} \, d\mathcal{A} = O(e^{-N\rho}).$$

The last equation holds because exponential quantity e^x is a fixed point in differential calculus and integral calculus. An exponential quantity stays as an exponential one through integrals as long as the pdf ρ is continuous in the integral area. This concludes that P_{empty} exponentially approaches 0 as the number of nodes N increases linearly.

Negligible success for adversarial motion pattern tracing. Now, the motion pattern of a mobile node v can be modeled as a stochastic process across a set of venues $(x_1, x_2, \cdots, x_i, \cdots)$ in the network lifetime. In the ith venue x_i, node v meets *other* k_i uncompromised nodes.

Case 1. Let us first assume that only v moves, all other nodes are stationary, and they do ANODR's neighborhood traffic mixing all the time.

1. If $k_i > 0$ and $k_{i+1} > 0$, the adversary *cannot* see the motion from the outgoing venue x_i to the incoming venue x_{i+1} due to no change in transmission pattern. This is because, since node v's transmissions bear no identity of v, they are equally as likely as other nodes.
2. If $k_i = 0$ and $k_{i+1} > 0$, the adversary can see that node v moves from the outgoing venue x_i to a neighboring venue, but cannot identify the incoming venue x_{i+1} except by a random guess.
3. If $k_i > 0$ and $k_{i+1} = 0$, the adversary can see that node v moves into the incoming venue x_{i+1} from a neighboring venue, but cannot identify the outgoing venue x_i except by a random guess.
4. If $k_i = k_{i+1} = 0$, the adversary can see that node v moves from the outgoing venue x_i to the incoming venue x_{i+1}.

Case 2. If all nodes are moving, Case 1.1 is unchanged. Cases 1.2, 1.3, and 1.4 are the best-case scenarios for the adversary because, given the empty venue x ($x = x_i$ and/or $x = x_{i+1}$), any node in any neighboring venue of x may step into venue x. This converts Case 1.2 or 1.3 into Case 1.1 and converts Case 1.4 into Case 1.2 or 1.3 or even 1.1. Compared to Case 1, the anonymity threat is alleviated in Case 2.

Therefore, the adversary requires one or more empty venues to trace the identity-free node v. The probability is less than or equal to the previously computed P_{empty}. More specifically, the probability to trace node v along a sequence of m empty venues is

$$P_{trace\_motion} = (P_{empty})^m = O(e^{-N\rho m}).$$

This is a negligible quantity with respect to the network scale N.

2. For the ease of presentation, here the pdf is defined on 2D spatial dimensions. Bettstetter et al. [8] have computed such pdf for various mobility models on 2D spatial dimensions, and Hu and Wang [24] have verified the correctness of the computation via empirical simulations. In the real world, the pdf is defined on 4D temporal-spatial dimensions. Research results are expected to be done. Afterward, the double integrals in the following formulas must be replaced with quadruple integrals.

TABLE 3
Processing Overhead of Various Cryptosystems (on an Intel StrongARM 200-MHz CPU-Based Pocket PC Running Linux)

PK_A	Node A's public key	K_A	An encryption key only known by node A
SK_A	Node A's private key corresponding to PK_A	K_{AB}	An encryption key shared by node A and B
$\{M\}_{PK_A}$	Encryption/verification of message M with key PK_A	$f_{K_A}(M)$	Encryption/decryption of message M with symmetric key K_A using a symmetric encryption function f
$[M]_{SK_A}$	Decryption/signing of message M with key SK_A	N_A, N_A^i	Nonce or nonces chosen by node A
src	"source!", a special bit-string tag denoting the source	$dest$	"destination!", a special bit-string tag denoting the destination

5 Evaluation Methodology

In this section, we use simulation to evaluate and compare the aforementioned anonymous ad hoc routing protocols. Our evaluation concerns the influence from both the processing time needed to perform the crypto operations and the increased sizes of routing control packets on network performance.

5.1 Implementation Details

The implementation of ANODR, ASR, MASK, and SDAR are based on AODV and AnonDSR is based on DSR. Route optimizations used by the original AODV and DSR do not apply in anonymous routing, so they are not enabled in the implementations. In addition, we have made a few more justifications in order to make the results comparable and fair among all the protocols.

First of all, in our implementation and evaluation, assumptions made by each protocol are preserved. Overhead incurred in preconfigure phase or bootstrap phase is not counted in the evaluation. Second, for ANODR, an improved version [31] using Key Predistribution Schemes (KPS) (in RREP unicasts) is also implemented and evaluated in our simulation study. It is denoted as ANODR-KPS and uses the probabilistic KPS scheme proposed by Du et al. [17]. Third, for the AnonDSR protocol, the security parameter establishment (SPE) protocol is considered as a precondition and the overhead is not calculated. This is equivalent to assumptions made by other protocols on preexisting source-destination security agreements (ANODR, ASR, and SDAR) or leave the destination ID as plain text (MASK). Further, periodical broadcast among neighbors in protocols MASK and SDAR are modified from HELLO messages in AODV. For MASK, besides periodical HELLO (first stage in its three-stage neighborhood key exchanges), two more broadcast packets are added to complete the remaining two stages of the handshake among a newcomer and its neighbors. Taking into consideration that one can use adaptive frequencies to reduce the overhead from the periodical updates and to improve performance (compared to the results generated from our implementations), in our evaluation, we separate the evaluation of the periodic overhead from the evaluation on the main on-demand route discovery principles.

Moreover, assumptions implied by crypto-systems in use are also preserved, e.g., using a public key scheme, the network needs an offline authority to grant every network member a credential signed by the authority's signing key, so that any node can verify a presented credential with the authority's well-known public key; using a KPS scheme, the network needs an offline authority to load every node with personal key materials. In ANODR-KPS, the probability of achieving a successful key agreement at each hop is 98 percent. In other words, per hop key agreement fails with 2 percent at every RREP hop. A new route discovery procedure will be invoked eventually by the source. Finally, in our implementation, cryptographical operations over data packet transmission are not calculated since all the protocols use symmetric key systems.

5.2 Crypto-Processing Performance Measurement

The processing overhead used in our simulation is based on actual measurements on a low-end device. Table 3 shows the measurements performed by Gupta et al. [22] on the performance of different cryptosystems. For public key cryptosystems, the table shows processing latency per operation. For symmetric key cryptosystems, it shows the encryption/decryption bit-rate.

Clearly, different cryptosystems introduce different processing and link overhead; thus, they have different impacts on anonymous routing performance. Taking into consideration the cryptosystems proposed by the original authors, we choose the cryptosystem in favor of performance for practical reasons. For public key cryptographic operations in the simulation, AnonDSR uses RSA and the rest of the protocols use ECIES with a 163-bit key. For the symmetric cryptography, we use AES/Rijndael with a 128-bit key and block. The coding bandwidth is about 29.2 Mbps. As an example, in ANODR, computational delay is approximately 0.02 ms for each onion construction during each RREQ and RREP forwarding and another public key processing time $24.5 + 46.5 = 71$ ms for RREP packets. In general, a longer delay is required for asymmetric key encryption/decryption compared with the symmetric cryptography. The KPS-based ANODR trades link overhead for processing time, i.e., ANODR-KPS uses 1,344 bits and 1,288 bits key agreement material for RREQ and RREP packets, respectively. Each of them requires only 1 ms extra time in processing packets.

5.3 Evaluation Metrics

We evaluate the performance of these protocols in terms of the overall network performance (delivery metric) and the influence from processing delay (delay metric) and packet size (overhead metric). We use the following metrics: *packet delivery fraction*, *average end-to-end data packet delay*, and *normalized routing load* in *bytes* of total control packets per data packet delivered.

The simulation is performed in QualNet [42], a packet level simulator for wireless and wired networks developed by Scalable Network Technologies Inc. The distributed coordination function (DCF) of IEEE 802.11 is used as the MAC layer in our experiments. The radio uses the *two-ray*

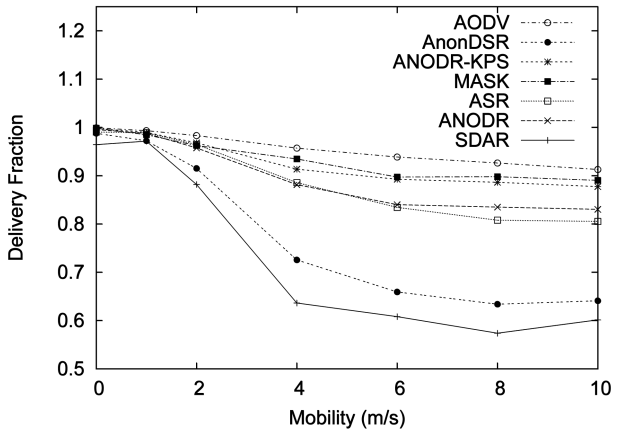


Fig. 5. Delivery fraction.

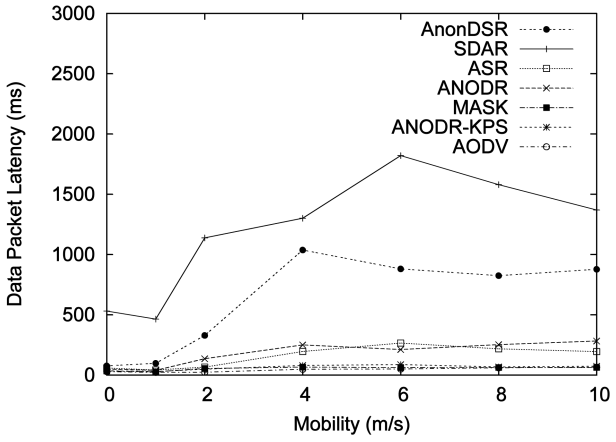


Fig. 6. Data packet latency (ms).

ground reflection propagation model. The channel capacity is 2 Mbps. The network field is $2,400\ \mathrm{m} \times 600\ \mathrm{m}$ with 150 nodes initially uniformly distributed. The transmission range is 250 m. The *Random Way Point* (RWP) model is used to simulate node mobility. In our simulation, the mobility is controlled in such a way that the minimum and maximum speeds are always the same (to fix a recently discovered problem [47]). CBR sessions are used to generate network data traffic. For each session, data packets of 512 bytes are generated in a rate of four packets per second. The source-destination pairs are chosen randomly from all the nodes. During the simulation time, a constant, continuously renewed load of short-lived pairs is maintained.

To focus on influence from anonymous design and cryptographic operation, we do not introduce attacks in the simulation. We present two sets of simulations. One set is to show routing performance variation under different mobility conditions, where mobility is increased from 0 to 10 m/sec in different runs. The pause time is fixed to 30 seconds. Five CBR pairs are constantly maintained. In the other series of simulation, showing the impact of performance due to different traffic load, we fix the mobility at 2 m/sec and vary the number of concurrent short-lived CBR communications from five to 25. Each of these series of simulation are conducted in identical network scenarios (mobility, communication traffic, and node density) and routing configurations across all schemes (except the one to be varied) in comparison.

5.4 Performance Results

In this section, we give simulation results for different network scenarios, namely, increasing mobility and increasing traffic load.

Impact from mobility. Fig. 5 shows the comparison of the packet delivery ratio. The original AODV protocol indicates the best performance possible on this metric as expected since the environment has no attackers. MASK and ANODR-KPS have similar performance with the original AODV as they both use efficient symmetric cryptography only when exchanging routing packets, effectively accelerating the route discovery process and making the established routes more durable. ANODR and ASR experience moderate delivery ratio degression. Both of them use public key cryptography in RREP. The AnonDSR and SDAR show significant degradation delivery ratios. The reason is that the two protocols need hop-related public key encryption/decryption at the destination nodes. In a mobile environment, excessive delay in the route discovery process makes it harder to establish and maintain routes. All the curves show a more or less steady descendant when mobility increases. This is natural as increasing mobility will cause more packet losses.

Fig. 6 illustrates the data packet latency. Because of the public key cryptographical overhead, SDAR and AnonDSR show significantly longer end-to-end latency. ANODR and ASR have similar average data packet latency. ANODR-KPS and MASK have the lowest and nearly the same data packet delay with original AODV, thanks to the efficient symmetric encryption algorithms and hash functions used. When there is little mobility, all protocols display small data packet latency because once a route is established, a stable network allows a longer average route lifetime. When mobility increases, data packet latency increases accordingly.

Fig. 7 compares the normalized control overhead in terms of bytes. ANODR-KPS, AnonDSR, and SDAR generate the most normalized control bytes, while ASR and

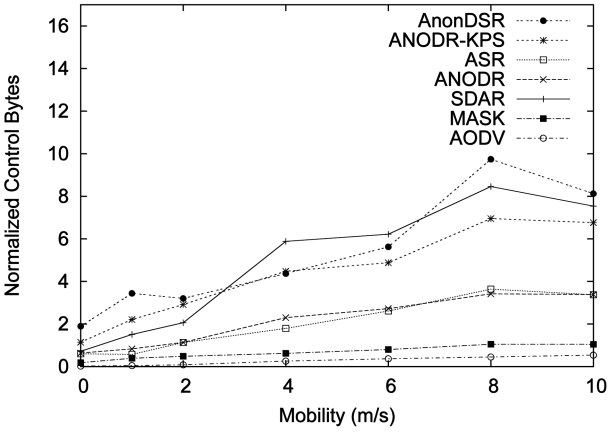


Fig. 7. Normalized control bytes.

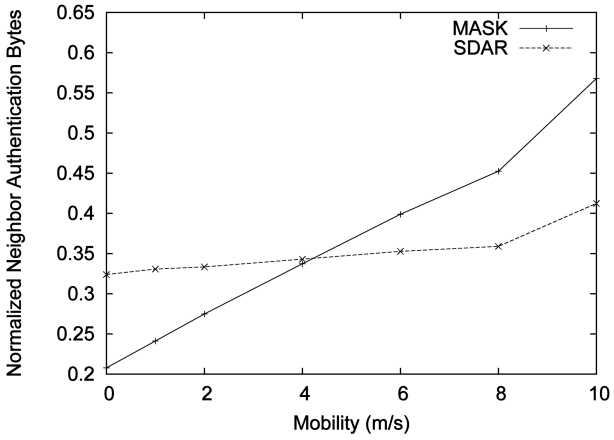


Fig. 8. Normalized neighbor authentication bytes.

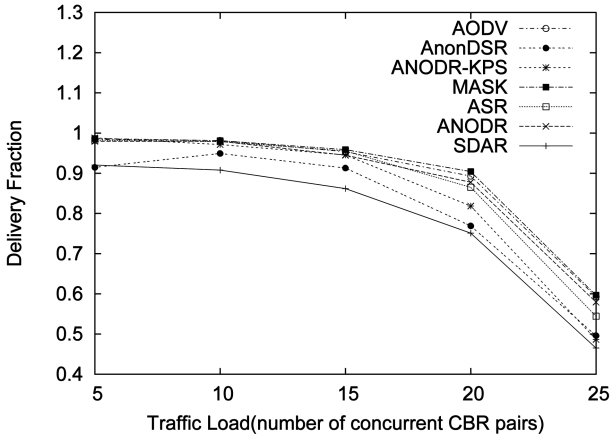


Fig. 9. Delivery fraction.

ANODR generate the least. The result is expected because SDAR and AnonDSR both have large RREQ and RREP packet sizes for carrying keys. ANODR-KPS also includes key negotiation material in RREQ and RREP messages, making them significantly larger than original ANODR control packets. In addition, AnonDSR and SDAR have low numbers of successfully delivered packets. Finally, MASK has closer values with AODV because in route discovery MASK relies on existing pairwise keys. The background key exchange overhead is not counted here (Fig. 8).

Fig. 8 reports the overhead of the proactive key establishment of MASK and SDAR. It shows the normalized *bytes* of neighbor authentication packets under different mobility conditions. SDAR uses periodical hello messages containing public keys for community management, which are not affected by mobility, but as the number of packets delivered decreases as mobility increases, Fig. 8 shows an increasing trend of SDAR when mobility increases. MASK's three-stage handshake is triggered by new neighbors; thus, it is more affected by mobility. This behavior results in higher packet overhead of MASK compared to SDAR, and faster increasing trends when mobility increases as more handshakes are needed. Other results from our simulation (not included in the paper) show that the number of packets increases. Especially, when the network is static, MASK and SDAR have almost the same number of control packets. The figure also shows an interesting crossing phenomenon. This is because the size of SDAR's HELLO message, which carries a public key, is much larger than that of MASK, which typically only needs to carry an 8-byte pseudonym. Thus, when mobility is low, SDAR incurs more normalized neighbor authentication bytes. As the mobility increases, a node tends to encounter more other nodes and handshake with more newly met neighbors. Thus, at one point, the normalized neighbor authentication bytes of MASK will exceed that of SDAR, as the overhead of MASK increases much faster.

Impact from traffic load. The network traffic load is increased by increasing the number of communication pairs. Fig. 9 compares the delivery ratio performance under different traffic load. It displays an unanimous degradation trend of delivery fraction for all protocols. This is typically because of the increasing congestions and communication collisions when traffic load increases.

Fig. 10 shows the impact of traffic load on end-to-end data packet latency. Not surprisingly, the data latency is extended as the traffic load increases. This is caused by longer queuing delay in contenting the wireless medium, and higher needs for route rediscovery. Protocols with longer computation delay always suffer more under heavy traffic load.

Fig. 11 shows the normalized control overhead in terms of bytes. More control overheads are generated when traffic becomes heavier. Again, the performance deteriorates in a regular fashion according to the computational overhead each protocol requires respectively.

Performance summary. In conclusion, our main findings are: 1) Control packet size, if controlled within a reasonable size, has less impact on performance, e.g., Fig. 5 and Fig. 9 show almost the same delivery ratio of MASK and ANODR-KPS. But ANODR-KPS has much higher control bytes as shown in Fig. 7 and Fig. 11. 2) Processing delay has great impact on delivery ratio in a mobile environment, e.g., ANODR-KPS and SDAR have similar combined packet size, while, as Fig. 5 and Fig. 9 show, their delivery ratios have a large difference.

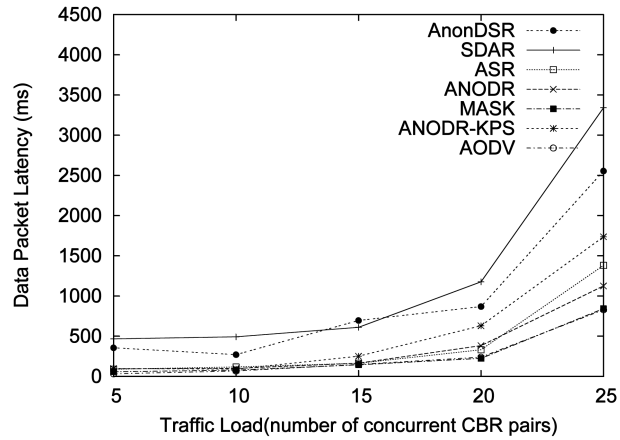


Fig. 10. Data packet latency (ms).

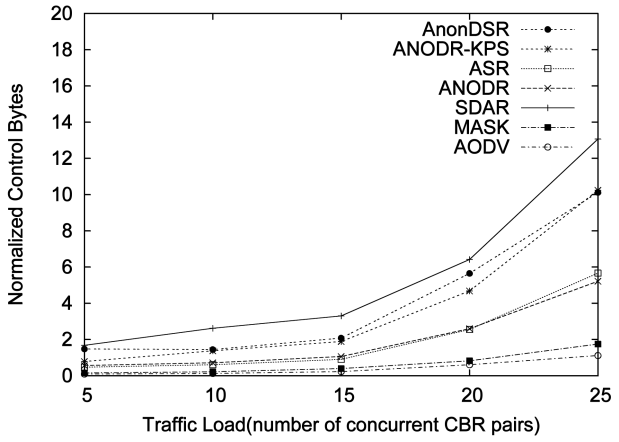


Fig. 11. Normalized control bytes.

On the other hand, the simulation results demonstrate the existence of trade-offs between routing performance and security protection. Because the ad hoc route discovery (RREQ/RREP) procedure is *time critical* in a mobile network, excessive crypto-processing latency would result in stale routes and hence devastated routing performance. Our results show that, while ANODR and ASR could be suitable for low-end nodes and medium mobility, AnonDSR and SDAR are better to be used by high-end nodes that can run public key cryptography efficiently. In order to design a practical anonymous ad hoc routing scheme, we must find out the optimal balance point that can both avoid expensive cryptographic processing and provide needed security protection at the same time.

6 Summary

In this paper, we have studied unique anonymity threats in mobile ad hoc environments. We present *identity-free routing* and *on-demand routing* as two design principles of anonymous routing in mobile ad hoc networks. ANODR is an anonymous routing scheme that is compliant with the design principles. Like formal cryptanalysis used in modern cryptography, we propose to use negligibility-based analysis to quantify network security schemes. Our analysis shows that ANODR's identity-free approach is able to satisfy the negligibility requirement after a probabilistic model quantifies the spatial probabilistic distribution function (spatial PDF) of each mobile node's physical presence in the network area. We run extensive simulations to evaluate the routing performance of ANODR and several other anonymous routing protocols. Our simulation study shows that routing performance changes significantly when different cryptosystems are used to implement the same function (e.g., link key agreement). We call for the implementation of secure and efficient anonymous routing in mobile ad hoc networks.

References

[1] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol," IETF Internet draft, work in progress, 2000.

[2] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. Mickunas, and S. Yi, "Routing through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments," *Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '02),* pp. 65-74, 2002.

[3] *American National Standard X9.17: Financial Institution Key Management (Wholesale),* Am. Nat'l Standards Inst., 1985.

[4] ATM Forum, "Asynchronous Transfer Mode," http://www.atmforum.org/, year?

[5] D. Balfanz, G. Durfee, N. Shankar, D.K. Smetters, J. Staddon, and H.-C. Wong, "Secret Handshakes from Pairing-Based Key Agreements," *Proc. IEEE Symp. Security and Privacy,* pp. 180-196, 2003.

[6] O. Berthold, H. Federrath, and S. Köpsell, "Web MIXes: A System for Anonymous and Unobservable Internet Access," H. Federrath, ed., *Proc. Workshop Design Issues in Anonymity and Unobservability (DIAU '00),* pp. 115-129, 2000.

[7] C. Bettstetter, H. Hartenstein, and X. Perez-Costa, "Stochastic Properties of the Random Waypoint Mobility Model," *ACM/Kluwer Wireless Networks,* special issue on modeling and analysis of mobile networks, vol. 10, no. 5, pp. 555-567, 2004.

[8] C. Bettstetter and C. Wagner, "The Spatial Node Distribution of the Random Waypoint Mobility Model," *Proc. German Workshop Mobile Ad Hoc Networks (WMAN '02),* pp. 41-58, 2002.

[9] M. Blum and S. Micali, "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits," *Proc. Symp. Foundations of Computer Science (FOCS '82),* pp. 112-117, 1982.

[10] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks," *Proc. 29th IEEE Int'l Conf. Local Computer Networks (LCN '04),* pp. 618-624, 2004.

[11] D.L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Comm. ACM,* vol. 24, no. 2, pp. 84-88, 1981.

[12] D.L. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *J. Cryptology,* vol. 1, no. 1, pp. 65-75, 1988.

[13] N. Cressie, *Statistics for Spatial Data.* John Wiley and Sons, 1993.

[14] W. Dai, "PipeNet 1.1," http://www.eskimo.com/~weidai/pipenet.txt, 1996.

[15] J. Deng, R. Han, and S. Mishra, "Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Dependable Systems and Networks (DSN '04),* pp. 594-603, 2004.

[16] C. Díaz, S. Seys, J. Claessens, and B. Preneel, "Towards Measuring Anonymity," *Proc. Privacy Enhancing Technologies Workshop (PET '02),* pp. 54-68, 2002.

[17] W. Du, J. Deng, Y.S. Han, and P.K. Varshney, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," *Proc. ACM Conf. Computer and Comm. Security (CCS '03),* pp. 42-51, 2003.

[18] O. Goldreich, *Foundations of Cryptography: Basic Tools,* vol. 1. Cambridge Univ. Press, 2001.

[19] O. Goldreich and L.A. Levin, "A Hard-Core Predicate for all One-Way Functions," *Proc. Symp. Theory of Computation (STOC '89),* pp. 25-32, 1989.

[20] S. Goldwasser and S. Micali, "Probabilistic Encryption," *J. Computer and System Sciences,* vol. 28, no. 2, pp. 270-299, 1984.

[21] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," *Proc. First Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '03),* 2003.

[22] V. Gupta, S. Gupta, and D. Stebila, "Performance Analysis of Elliptic Curve Cryptography for SSL," *Proc. First ACM Workshop Wireless Security (WiSe '02),* pp. 87-94, 2002.

[23] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks," *Proc. MobiCom,* pp. 12-23, 2002.

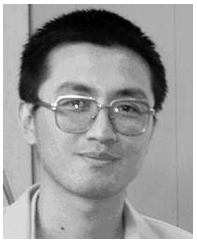
[24] Y.-C. Hu and H.J. Wang, "A Framework for Location Privacy in Wireless Networks," *Proc. ACM SIGCOMM Asia Workshop,* 2005.

[25] A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitzmann, and M. Waidner, "Real-Time MIXes: A Bandwidth-Efficient Anonymity Protocol," *IEEE J. Selected Areas Comm.,* vol. 16, no. 4, 1998.

[26] S. Jiang, N. Vaidya, and W. Zhao, "A MIX Route Algorithm for Mix-net in Wireless Ad Hoc Networks," *Proc. IEEE Int'l Conf. Mobile Ad-Hoc and Sensor Systems (MASS '04),* 2004.

[27] D. Kesdogan, J. Egner, and R. Buschkes, "Stop-and-Go MIXes Providing Probabilistic Security in an Open System," *Proc. Second Int'l Workshop Information Hiding (IH '98),* pp. 83-98, 1998.

[28] J. Kong, "Formal Notions of Anonymity for Peer-to-Peer Networks," Technical Report 2005/132, IACR Cryptology ePrint Archive, May 2005.
[29] J. Kong and X. Hong, "ANODR: ANonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks," *Proc. MobiHoc,* pp. 291-302, 2003.
[30] J. Kong, X. Hong, and M. Gerla, "Modeling Ad-Hoc Rushing Attack in a Negligibility-Based Security Framework," *Proc. ACM Workshop Wireless Security (WiSe '06),* pp. 55-64, 2006.
[31] J. Kong, X. Hong, M. Sanadidi, and M. Gerla, "Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing," *Proc. IEEE Symp. Computers and Comm. (ISCC '05),* 2005.
[32] A.J. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography.* CRC Press, 1996.
[33] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS)," *Proc. IEEE Global Telecomm. Conf. (GLOBECOM '01),* 2001.
[34] R. Ogier, M. Lewis, and F. Templin, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," IETF Internet draft, work in progress, Mar. 2003.
[35] A. Pfitzmann and M. Köhntopp, "Anonymity, Unobservability, and Pseudonymity—A Proposal for Terminology," H. Federrath, eds., *Proc. Workshop Design Issues in Anonymity and Unobservability (DIAU '00),* pp. 1-9, 2000.
[36] A. Pfitzmann, B. Pfitzmann, and M. Waidner, "ISDNMixes: Untraceable Communication with Very Small Bandwidth Overhead," *Proc. GI/ITG Conf.: Comm. Distributed Systems,* pp. 451-463, 1991.
[37] C. Rackoff and D.R. Simon, "Cryptographic Defense Against Traffic Analysis," *Proc. Symp. Theory of Computation (STOC '93),* pp. 672-681, 1993.
[38] M.G. Reed, P.F. Syverson, and D.M. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE J. Selected Areas in Comm.,* vol. 16, no. 4, 1998.
[39] M.K. Reiter and A.D. Rubin, "Crowds: Anonymity for Web Transactions," *ACM Trans. Information and System Security,* vol. 1, no. 1, pp. 66-92, 1998.
[40] G. Resta and P. Santi, "An Analysis of the Node Spatial Distribution of the Random Waypoint Model for Ad Hoc Networks," *Proc. ACM Workshop Principles of Mobile Computing (POMC '02),* pp. 44-50, 2002.
[41] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E. Royer, "A Secure Routing Protocol for Ad Hoc Networks," *Proc. IEEE Int'l Conf. Network Protocols (ICNP '02),* 2002.
[42] QualNet, "Scalable Network Protocols (SNT),"http://www. qualnet.com/, year?
[43] A. Serjantov and G. Danezis, "Towards an Information Theoretic Metric for Anonymity," *Proc. Privacy Enhancing Technologies Workshop (PET '02),* R. Dingledine and P. Syverson, eds., pp. 41-53, 2002.
[44] C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical J.,* vol. 28, no. 4, pp. 656-715, 1949.
[45] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks," *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05),* 2005.
[46] L. Sweeney, "*k*-Anonymity: A Model for Protecting Privacy," *Int'l J. Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 10, no. 5, pp. 557-570, 2002.
[47] J. Yoon, M. Liu, and B. Noble, "Sound Mobility Models," *Proc. MobiCom,* pp. 205-216, 2003.
[48] Y. Zhang, W. Liu, and W. Lou, "Anonymous Communications in Mobile Ad Hoc Networks," *Proc. INFOCOM,* 2005.



Jiejun Kong is a postdoctoral researcher in the Computer Science Department, University of California at Los Angeles. He is interested in developing efficient, scalable, and secure network protocols for wireless networks. His research topics include secure and anony-mous routing, authentication, access control, distributed data harvesting, and network security modeling in mobile wireless networks, in particular, those with challenging network constraints and high security demands, such as mobile ad hoc networks and underwater sensor networks. He has contributed to the design, implementation, and testing of network protocols within the US National Science Foundation (NSF) iMASH, ONR MINUTEMAN/STTR, and NSF WHYNET projects. He is currently working at Scalable Network Technologies, Inc.

Xiaoyan Hong received the BS and ME degrees in computer science from Zhejiang University in China and the PhD degree in computer science from the University of California at Los Angeles in 2003. She is currently an assistant professor in the Department of Computer Science at the University of Alabama. Her research interests include network protocol design, performance evaluation, and implementation for multihop, mobile, and wireless networks and wireless sensor networks. Her current research focuses on routing, monitoring, mobility, privacy, and security issues.

Mario Gerla received a graduate degree in engineering from the Politecnico di Milano in 1966 and the MS and PhD degrees in engineering from the University of California at Los Angeles (UCLA) in 1970 and 1973, respectively. He joined the faculty of the UCLA Computer Science Department in 1977. His research interests cover the performance evaluation, design, and control of distributed computer communication systems, high speed computer networks, wireless LANs (Bluetooth), ad hoc wireless networks, and next generation Internet. He is a fellow of the IEEE.