Mobility changes anonymity: new passive threats in mobile ad hoc networks

Xiaoyan Hong [*] Jiejun Kong [†]
Mario Gerla [‡]

[*]University of Alabama, Tuscaloosa
[†]UCLA
[‡]UCLA

Xiaoyan Hong, Jiejun Kong, and Mario Gerla, "Mobility changes anonymity: new passive threats in mobile ad hoc networks" (2006). Wireless Communications & Mobile Computing. 6 (3), pp. 281-293. Postprint available free at: http://repositories.cdlib.org/postprints/2041

Mobility changes anonymity: new passive threats in mobile ad hoc networks

Abstract

Privacy in mobile ad hoc networks has new semantics in addition to the conventional notions for infrastructure networks. Mobility enabled by wireless communication has significantly changed privacy issues and anonymity research in many ways. In particular, mobility requires ad hoc routing schemes to transmit messages frequently in an open wireless medium. The routing traffic facilitates adversaries in conducting various attacks threatening the network security and privacy. In this work, we focus on passive routing attacks. We present an extensive study on new anonymity threats and classify the corresponding security demands into three new categories: (1) venue anonymity; (2) privacy of ad hoc network topology; and (3) privacy of motion pattern. These new aspects are all introduced by mobility and left unaddressed in fixed infrastructure. This leads us to investigate new design principles. Our study suggests that on-demand routing, identity-free routing, and neighborhood traffic mixing are better design choices to defend against the new anonymity threats in mobile networks. The paper also demonstrates through examples

on the

visualization of the mobile anonymity attacks and on the quantification of the effectiveness of the attacks.

Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks

Xiaoyan Hong[*‡], Jiejun Kong[†], and Mario Gerla[†]

[*] Computer Science Department, University of Alabama, Tuscaloosa, AL 35487
[†] Computer Science Department, University of California, Los Angeles, CA 90095

***Abstract*— Privacy in mobile ad hoc networks has new semantics in addition to the conventional notions for infrastructure networks. Mobility enabled by wireless communication has significantly changed privacy issues and anonymity research in many ways. In particular, mobility requires ad hoc routing schemes to transmit messages frequently in an open wireless medium. The routing traffic facilitates adversaries in conducting various attacks threatening the network security and privacy. In this work, we focus on passive routing attacks. We present an extensive study on new anonymity threats and classify the corresponding security demands into three new categories: (1) *venue anonymity*, (2) *privacy of ad hoc network topology*, and (3) *privacy of motion pattern*. These new aspects are all introduced by mobility and left unaddressed in fixed infrastructure. This leads us to investigate new design principles. Our study suggests that *on-demand routing*, *identity-free routing* and *neighborhood traffic mixing* are better design choices to defend against the new anonymity threats in mobile networks. The paper also demonstrates through examples on the visualization of the mobile anonymity attacks and on the quantification of the effectiveness of the attacks.**

***Index Terms*— Mobile Anonymity, Anonymous Routing, On Demand Routing, Mobile Ad Hoc Networks, Network Security and Privacy**

I. Introduction

Mobile wireless networks, such as mobile ad hoc networks (MANETs), are capable of establishing an instant communication infrastructure for many time-critical and mission-critical applications. Nevertheless, the innate characteristics of mobile wireless networks, such as node mobility and wireless transmissions, make them very vulnerable to security threats. Among all forms of the threats, in this work, we focus on passive routing attacks that threat the privacy of mobile wireless networks. Consider for example a homeland security emergency scenario with MANET support. Mobile wireless communications are essential to coordinate the motion of law-enforcement teams in such a mission. But, in a venue chosen by the terrorist, the open-air wireless communication can be explored by a coordinated high-tech adversarial team to trace the mobile nodes and prepare the counterattacks. The needed eavesdropping devices, such as sensors and portable computing devices, are all available off-the-shelf on-line or from local electronic stores. Providing supports of identity anonymity, location privacy, and motion pattern privacy for law-enforcement teams is critical. This poses challenging constraints on secure routing and data forwarding.

In this paper, we seek to demonstrate that MANET routing protocols become a critical factor in anonymity research. We identify new privacy and anonymity requirements for mobile wireless networks by showcasing a set of passive routing attacks and defense strategies against these new threats. More specifically, we demonstrate that mobility enabled by wireless communication has changed privacy and anonymity issues in many ways compared to legacy privacy issues discussed in infrastructure network research (e.g., message privacy in the Internet, transaction anonymity in distributed banking systems).

The contribution of this paper is three-fold. We firstly define "*mobile anonymity*", namely the new anonymity aspects for mobile wireless networks. In addition to the conventional identity anonymity, the mobile anonymity has to address *venue anonymity*, *privacy of network topology*, and *privacy of motion pattern*. These new anonymity aspects have little significance in fixed infrastructure, but become critical issues in mobile networks. We then identify design principles of new countermeasures. Our study suggests that a hybrid approach of *identity-free routing* and *on-demand routing* assisted with *neighborhood traffic mixing* provides better mobile anonymity support than other approaches. Finally, we demonstrate through examples on the quantification of the effectiveness of the mobile anonymity attacks and on the visualization of them. Our study calls for attention to efficient anonymous routing schemes for mobile ad hoc networks.

The rest of the paper is organized as follows. Section II describes related work including adversary models, existing anonymous schemes, and MANET routing protocols. In Section III we illustrate the changes in the semantics of the anonymity concept when node mobility prevails MANETs. Section IV proposes design principles for countermeasures in dealing with the new challenges. Section V gives examples on quantification of the effectiveness of the attacks and on visualization of them. Finally Section VI summarizes the paper.

II. Background and related work

Original MANET routing protocols are designed for friendly and collaborative scenarios. However, many MANET applications will deploy networks in hostile environments. In

‡Correspondence: Xiaoyan Hong, Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487, USA. Email: hxy@cs.ucla.edu, Tel: (205)348-4042, Fax: (205)348-0219.

Part of the work is funded by MINUTEMAN project sponsored by Office of Naval Research under Contract N00014-01-C-0016.

this section, we describe the passive form of the attacks presented in the hostile environments and briefly review MANET routing protocols and related anonymity research.

A. Security and threat models

Wireless communications can be protected by strong cryptographic methods at application (end-to-end) or MAC layer (hop-by-hop). However, these protections are not sufficient for the privacy purpose. For examples, MAC addresses are not encrypted by the standard MAC security protections. In addition, an eavesdropper assisted with radio detection devices can always detect a radio wireless transmission near its own location. With the help of localization algorithms [29] and GPS information, the eavesdropper can use its own coordinates and naming system to name all identified network members without knowing their real identities. Moreover, the re-occurrences of some payload patterns provide plenty of opportunities for analysis on the traffic contents and time instances. In a nutshell, besides denial-of-service threats, propagation of routing messages is challenged by traffic analysis as well.

Independent of whether and how the wireless transmissions are protected, traffic analysis leads to a passive type of attacks against the ad hoc routing schemes. The goal of such attacks is very different from other related routing security problems such as route disruption and "denial-of-service" attacks. In fact, the passive enemy will avoid such aggressive schemes, in the attempt to be as "invisible" as possible, until it traces, locates, and then physically destroys the assets. The attackers try to be *protocol compliant*, so they are harder to be detected before potential devastating physical attacks are launched.

We further characterize the passive adversary in terms of an escalating capability hierarchy.

- *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. The minimum 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 imposes serious physical threats to mobile 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, thus hard to detect. It participates in collaborative network operations (e.g., ad hoc routing) to boost its attack strength against mobile anonymity, thus it threatens the entire network including all other uncompromised nodes. This implies that a countermeasure must not be vulnerable to single point of failure/compromise.
- *Mobile colluding attackers*: Adversaries having different levels of attacking ability can collaborate through separated channels to combine their knowledge and to coordinate their attacking activities. This realizes the strongest power at the adversary side.

B. Routing in mobile ad hoc networks

Most routing protocols in MANETs fell into two categories: proactive routing and reactive routing (aka., on demand routing) [6]. In proactive ad hoc routing protocols like OLSR [9], TBRPF [32] and DSDV [35], mobile nodes constantly exchange routing messages which typically include node identities and their connections to other nodes (Link State, or Distance Vector), so that every node maintains sufficient and fresh network topological (or routes) information to allow them to find any intended destinations at any time. On the other hand, reactive routing has become a major trend in MANETs. AODV [36] and DSR [23] are dominant examples. Unlike their proactive counterparts, reactive routing operation is triggered by the communication demand at sources. Typically, a reactive routing protocol has two components: *route discovery* and *route maintenance*. In route discovery phase, the source seeks to establish a route towards the destination before sending the first data packet. The source floods a route request (RREQ) message, and the destination will reply a route reply (RREP) message upon receiving a RREQ. The RREP traces the reverse path that the RREQ takes to the source, which pinpoints the on-demand route. In the route maintenance phase, nodes en route monitor the status of the forwarding path, and report to the source about link breakages. Optimizations could lead to local repairs of broken links.

Clearly, transmitted routing messages and cached routing tables, if revealed to the adversary, will leak large amount of private information about the network. When this happens, proactive protocols and on-demand protocols show different levels of damages by design. With the proactive routing, a compromised node has fresh topological knowledge about other mobile nodes during the entire network lifetime. The adversary can also translate the topological map to a physical map with the help from localization algorithms [29] and GPS. Thus, a single-point of compromise allows the adversary to trace the entire network. On the other hand, with the on-demand routing, an adversary has reduced chances in breaking mobile anonymity in the sense that only active routing entries are in cache and in transmission, and the traffic pattern is probabilistic (with respect to communication needs) and expires after a while.

Secure ad hoc routing protocols, such as SEAD [18], Ariadne [19] and ARAN [42], focus on authentication rather than anonymity. Simple encryption of routing information [2] can stop less sophisticated eavesdroppers, but not traffic analysts studied in this article. Using pairwise keys between neighbors in encryption can alleviate the damages, but can not fully thwart intruders and traffic analysts, for example, a DSR route is traceable by a single intruder en route, while an AODV route is traceable by collaborative intruders.

C. Anonymous communication schemes in Internet

Research on privacy in infrastructure networks has resulted in many schemes that deliver messages anonymously. The most popular ones are based on Crowds [40], DC-net [8] and MIX-Net [7]. In Crowds, nodes are pairwisely one (logical) hop away, such that a forwarder can send the message directly to the final recipient, or with certain probability (p_f) choose

another arbitrary node as the next forwarder. In DC-net and XOR-tree [13], nodes are arranged into a fixed topology, for instance, a closed ring or a fixed multicast tree. Since network-wide broadcasts deliver encrypted messages to all nodes, the adversary cannot identify the real recipient. In MIX-Net, examples including ISDN-MIXes [38], Web-MIXes [4], Stop-and-Go-MIXes [24] and many others [30][11], the network topology is a fixed graph of MIXes (a node is called a MIX). The sender can use an arbitrary path in the graph to send messages to its recipient. Assuming each MIX's public key can be acquired, the sender uses these public keys to encrypt its message in a layered "onion" structure, such that when the onion goes through a sequence of MIXes, each MIX en route decrypts the outmost layer using its private key and peels off the layer (which is produced by the sender for this MIX) and forwards the remaining onion downstream, until the intended recipient receives the message (i.e., the onion core). PipeNet [10] and Onion Routing [39] reduce the processing overhead by establishing bidirectional secure pipes prior to data delivery. In this case data delivery only incurs little overhead from symmetric key cryptography.

After all, these schemes are not suitable in mobile wireless networks due to at least one of the following reasons: (1) regard network topology as stationary and known; (2) make impractical cryptographic assumptions, e,g, relying on *a priori* secure pipes; (3) do not protect network topology and mobility pattern; (4) may incur excessive overhead due to expensive public key processing, which in turn incurs hundreds of millisecond delay on most portable mobile devices.

D. Anonymity study in wireless network

Existing anonymity schemes for wireless networks fall into a spectrum of design goals. In basestation-based wireless networks (Cellular or WiFi), privacy is concerned when services are requested. Gruteser and Beresford work on anonymous use of Location-Based Services [14] or pervasive computing applications [3]. In these studies, location privacy is addressed at application level, i.e., to disassociate a user's identifier from his location when location information is needed by applications in order to provide services. The location could be geographical coordinates or a service area. He et al. [15] studies location privacy for mobile users of wireless infrastructure networks when they roam to foreign cells. The home agents help to protect users' identity anonymity. Hu et al. [22] studies anonymous end-to-end transactions between mobile users and their communicators. An anonymous bulletin board provides unlinkability between node identities and their credentials. All these application-wise efforts do not address threats that exploit vulnerabilities in ad hoc routing protocols.

In wireless sensor networks, Deng [12] studies location and identity privacy of fixed base stations. *Phantom routing* [33] solves the location privacy of mobile sources in the presence of individual eavesdroppers. The network scenarios studied are stationary sensor networks and only the sinks or the sources are concerned. In mobile ad hoc networks, ANODR [26] is an anonymous protocol using on-demand routing approach to protect identity, motion and topology privacy. It uses one of the design principles identified here, namely, *identity-free* routing. The research spawned the issues we discuss here. SDAR [5] uses a neighbor detection protocol for key exchange in assisting the anonymous on-demand route discovery. Data packets are delivered using a variant of MIX-net onion. MASK [43] is another anonymous routing protocol that addresses identity anonymity problem. But opportunities exist that fresh (and partial) network topology could be revealed to the adversary.

III. Mobility changes anonymity

In this section, we describe various new anonymity threats and vulnerabilities in MANET routing protocols. On one hand, mobile nodes' locations and motion patterns, standing venues, and even the varying network topology, become new interests of the adversaries. This brings in new privacy challenges in addition to conventional identity anonymity and message privacy. On the other hand, new vulnerabilities exist in current MANET routing protocols. Mobility requires an ad hoc routing protocol to transmit messages frequently in an open wireless medium. The routing traffic, if not protected from anonymity attacks, facilitates adversaries in conducting various attacks threatening the network security and privacy. We present extensive examples to illustrate the feasibility and effectiveness of these new privacy threats, and to present the new anonymity aspects for mobile wireless networks, namely "*mobile anonymity*". The mobile anonymity includes *venue anonymity*, *privacy of network topology*, and *privacy of motion pattern*.

A. Conventional concept of anonymity

The concept of *anonymity* is defined as the state of being not identifiable within a set of subjects, namely the *anonymity set* [37]. In conventional anonymity research, the anonymity set is the set of the *identities* of possible senders/recipients. Further, anonymity is defined in terms of *unlinkability*. *Unlinkability* describes the property that a sender/receiver not to be identified from the anonymity set, and the relationship of the sender and the receiver not to be identified. In this paper, the notion of identity refers to a mobile node's routing and forwarding ID, such as an IP address or a MAC address, since our focus is on routing and data forwarding. Another aspect of anonymity is the *unobservability*, a property says that transmissions are physically indiscernible from random noises. Discussions on the *unobservability* problem is not the intension of this paper.

B. Venue anonymity

Figure 1 illustrates an adversary's network which is comprised of a number of eavesdropping cells. The dense grid of eavesdroppers presents a strong form of adversary that collaboratively gathers global knowledge of traffic. The figure helps to illustrate several possible attacks described in the section. For example, it characterizes the capability of a collection of colluding traffic analysts from multiple cells. And it also characterizes the capability of a mobile traffic analyst who can travel along the grid structure to launch anonymity attacks anywhere and anytime.

Besides the identity, a mobile node's location area demands anonymity protection. For a mobile node, we define its

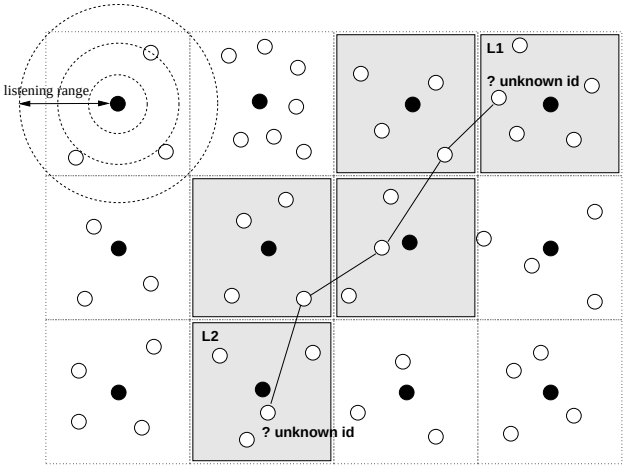

Fig. 1. A network with a number of eavesdropping cells. Traffic analysts are depicted as solid black nodes. A sender in cell $L1$ is communicating with a recipient in cell $L2$. Active routing cells are depicted in shade.

"**venue**" in terms of the *adversary*'s capability in positioning a wireless transmission, i.e., a "**venue**" is the smallest area to which the adversary can "pinpoint" the mobile node via wireless eavesdropping. In another word, a venue is a location perceived by an adversary. Therefore, a venue is at most as large as the radio receiving range of the eavesdropper (Figure 1). With a better positioning technique support, the adversary can improve the precision to a smaller area. The network is then, comprised of many venues given all intercepted wireless transmissions. Several mobile nodes could be associated with the same venue. An undirected graph $G = \langle V, E \rangle$ can describe the adversarial network. For example, in Figure 1, when a cell is a venue, it is a vertex in the graph G. Adversarial eavesdropping nodes form the vertex/venue set V. The topological links amongst the vertexes, indicating the communication capability among the adversaries, form the edge set E. The **venue anonymity set** is the set of all the venues. The **venue anonymity** is defined as the state of the sender/recipient's venue being not identifiable within the venue anonymity set. The relationship between the sender's and recipient's venues should not be linked given the venue anonymity set. Clearly, the venue anonymity concept is defined in parallel to the identify anonymity. However, to ensure venue anonymity, the identities of the transmitting nodes must not be revealed.

Both relating to location, we use *venue anonymity* to capture the subtle differences between the term *location privacy* mentioned in early literature and the problem addressed in this paper. In the context of venue, when the association between the venue and the node's identity is concerned, we can define the concept of *venue privacy*, which maps to location privacy directly (for this reason, we don't use the term *venue privacy* in the paper). As mentioned in Section II-D, location privacy has a broad spectrum in its semantics. Using the term of *venue anonymity*, we exclude the location privacy issues where nodes' identities and their locations are concerned for application needs [3] [12] [14] [15] [22]. Also, rather than the geographical positions used in geo-routing [25], [28], the concept of *venue* denotes the adversary's knowledge about legitimate wireless ad hoc routers, which can not be used by any legitimate nodes in routing. On the other hand, the venue anonymity can be compromised by the adversary through various routing attacks regarding the legitimate nodes. In this sense, with the venue anonymity, we focus on the location privacy issue studied in [26], [33], [43] where routing messages are greatly concerned. In a nutshell, the venue anonymity presents new semantics in describing location related privacy issue of mobile network where routing presents major vulnerability.

Mobility differentiates venue anonymity from identity anonymity. In static networks (e.g, the public Internet), a sender (or recipient)'s identity and its venue are synonyms due to the rich semantics carried in the identity (e.g, an IP address, or a domain name). Thus, identifying a sender's (or recipient's) venue implies the compromise of sender (or recipient) anonymity. But in mobile networks, a legitimate node is not locked in a vertex/venue of the underlying graph. Thus a node's identity is dissociated from a specific venue. However, at each traffic analyst's vertex/venue, the adversarial analyst can correlate a mobile node with its own exact location.

Example 1, 2 and 3 show that *identity anonymity* and *venue anonymity* are different concepts in mobile networks. While identity anonymity is still an issue, venue becomes a new anonymity problem which needs to be addressed separately.

Example 1: (Sender or recipient identity anonymity attack in on-demand route request flooding) In common on-demand ad hoc routing schemes like DSR and AODV, identities of the source/sender and the destination/recipient are explicitly embedded in route request (RREQ) packets. Any eavesdropper who has intercepted such a flooded packet can uniquely identify the sender's and the recipient's identities. However, he may not know the venue/vertex of the sender or the recipient. This example also verifies that neither sender nor recipient identity anonymity is protected in DSR and AODV. ∎

Example 2: (Sender or recipient identity anonymity attack in on-demand route request flooding with per-hop encryption) A seemingly-ideal cryptographic protection is to apply *per-hop* encryption using pairwise key agreement, i.e., a transmission is protected by an ideal point-to-point secure pipe between the two neighbors of a forwarding hop. The secure channel protects every packet including the packet header. This solution prevents eavesdroppers from understanding routing messages. But it does not prevent passive node intruders from identifying the sender's and the recipient's identities upon receiving a RREQ packet. Again, the intruder may not know the venue/vertex of the sender or the recipient. ∎

Example 3: (Packet flow tracing attack) Similar to anonymity attacks revealing the relationship between senders and recipients, the packet flow tracing attack can reveal the relationship between a sender's venue and its recipient's venue. Even protected by ideal encryption along a multi-hop forwarding path, timing correlation and content correlation analysis can be used to trace a packet flow. For example, by collusion or mobility, mobile traffic analysts can trace an ongoing packet flow to the sender's venue $L1$ and the recipient's venue $L2$

(Figure 1), thus break sender (or recipient) venue anonymity. But they may not be able to see the identities. ∎

C. Privacy of ad hoc network topology

Internet topology are mostly stable and can be viewed through various public tools. Routing protocols in Internet (eg.,BGP [41], OSPF [31] and RIP [16]) make no attempts to protect the privacy for network topology. However, in mobile networks, network topology constantly changes due to mobility. Once information about the network topology (or routes as partial topology information) is revealed, the adversary can launch further security breaches or locate positions of a few nodes given other out-of-band information like geographic positions and physical boundaries of the underlying mobile network. If the targeted ad hoc network has localization and positioning support, the topology privacy problem is aggravated when the localization results (locations) are revealed. Therefore, the privacy of network topology becomes a new anonymity requirement in mobile networks. Example 3 has shown a packet flow tracing attack to compromise relationship anonymity between a sender's venue and its recipient's venue. It is also an example of partial compromise of topology anonymity (the path connecting the sender and the receiver).

Example 4: (A mobile node intruder tries to locate where a specific node is) In proactive ad hoc routing protocols, mobile nodes constantly exchange routing messages to ensure that each sender knows enough network topological information for any intended recipient at any moment. Such design indeed establishes a lot of single points of compromise in the network, i.e., a single node intruder can break anonymity protection by seeing the topological map. This example shows that pre-computing routing schemes, in particular proactive routing schemes, directly conflict with anonymity protection requirements in mobile networks. With on-demand routing, a node intruder can simply function as a sender/source to establish a route towards the victim, then position and move towards the next hop close to the victim. By continuously probing and moving, the attacker can shorten the route and finally reach the victim. If more attackers collude, locating a victim is easier. Thus, an anonymous routing protocol should prevent a sender from knowing a forwarding path towards any mobile node. ∎

Example 5: (Vulnerabilities of MIX-Net in mobile networks) In MIX-Net, the sender must know the multi-hop forwarding path toward its recipient and produce an onion before the data can be sent out. If we directly port Chaumian MIX-Net into a mobile network by treating all or some mobile nodes as Chaumian MIX nodes, then any node intruder can function as a sender to trace the entire network. ∎

In infrastructure networks, a node's topological location and related physical location are determined *a priori*. Therefore, anonymity solutions proposed for infrastructure networks use neighborhood information for transmission. For example, a Chaumian MIX knows its immediate upstream and downstream MIXes, a jondo in Crowds [40] knows its next jondo or the destination recipient. If directly ported to mobile networks, these schemes are vulnerable to attacks described in Example 6.

Example 6: (Neighborhood location privacy attack) Given any cell L depicted in Figure 1, a mobile traffic analyst or an intruder may gather and quantify (approximate) information about active mobile nodes within the transmission range. For example, it can (a) enumerate active nodes in L; (b) get related quantities such as the size of the set; (c) perform traffic analysis against L, e.g., how many and what kind of connections in-and-out the cell. Currently common ad hoc routing protocols [23][36][43] do not address this attack. ∎

Mobile networks could be deployed in severe environments, where nodes with inadequate physical protection are susceptible to being captured and compromised. Any nodes in such a network must be prepared to operate in a mode that allows no gullibility. In the network, the combination of the ad hoc networking and the topological privacy concern presents a dilemma described in Example 7.

Example 7: (location privacy dilemma for MANET routing) Being a member of MANET, a node must rely on at least one of its neighbors to forward its packets. When anonymity service is concerned, a node is facing a dilemma. On one hand, a node must forward packets to one of its neighbors, so that the neighbor(s) can further forward the packets towards the destination. On the other hand, this node does not trust any of his neighbors. Given the node has no way of knowing which neighboring node is adversarial (passive attacker), the node must not reveal its identity and other identifiable information in its transmission. ∎

D. Privacy of motion pattern

Besides venues, the change of venues, or the nodes' motion patterns are very important information. For example, a network mission may require a set of legitimate nodes to move towards the same direction or a specific spot. Any inference of the motion pattern will effectively visualize the outline of the mission and may finally lead to the failure of the mission. Ensuring the privacy for mobile nodes' motion patterns is a new expression. If the network fails to ensure topological venue privacy, a mobile node's motion pattern can be inferred by a dense grid of traffic analysts, or even by a sparse set of node intruders under certain conditions [17], e.g, capable of knowing neighbors' relative positions (clockwise or counter-clockwise), and capable of overhearing or receiving route replies (RREPs) of on-demand routing.

Example 8: (Motion pattern inference attack: dense mode) The goal of this passive attack is to infer (possibly imprecise) motion patterns of mobile nodes. In Figure 1, the omnipresent colluding intruders can monitor wireless transmissions in and out a specific mobile node, they can combine the intercepted data and trace the motion pattern of the node at the granularity of cell. ∎

Example 9: (Motion pattern inference attack: sparse mode) When node intruders are sparse in the network, they may still be able to infer motion patterns from ongoing routing events, though the information gathered could

be imprecise. Here we describe a probabilistic *H(op)-clique* attack. Figure 2 depicts the situation when a node intruder X finds from the routing packets that its next hop towards the node Y switches from node $V1$ to $V2$ (both are X's neighbors). With high probability, this routing event indicates that either the target node Y (left figure) or some intermediate forwarding nodes (right figure) have moved along the direction $V_1 \rightarrow V_2$ (clockwisely). We assume that a node intruder can be furnished with basic ad hoc localization techniques (e.g., using Angle-of-Arrival, Receiver-Signal-Strength-Index, etc.). The H-clique is comprised of a single node intruder and its gullible neighbors. Through colluding, multiple H-cliques can combine their knowledge to obtain more precise information on motion pattern. Figure 3 shows that a mobile node cutting through two H-cliques is detectable by the adversary. Figure 4 shows the case of three H-cliques. Therefore, a few node intruders can effectively launch motion pattern inference attacks against the entire network. Both proactive routing schemes and on-demand schemes are vulnerable to such passive attacks. ∎

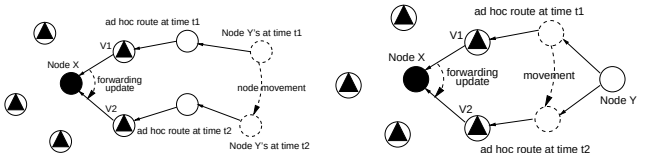

Fig. 2. Sparse mode motion pattern inference (H-clique attack). The solid black node is a protocol-compliant node intruder. The neighbors (denoted by circled triangles) are legitimate network members, but cannot detect a protocol-compliant node intruder. Left: target movement; Right: forwarding node movement.

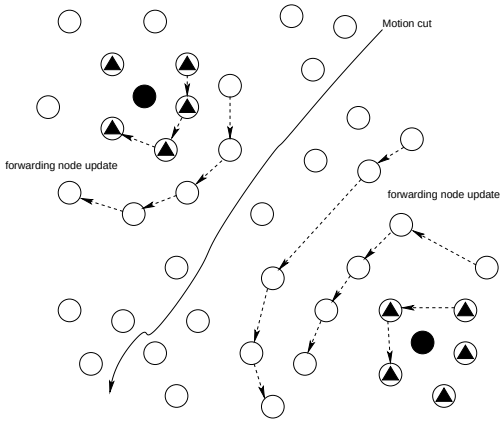

Fig. 3. H-clique attack: a motion cutting through two H-cliques is detectable from forwarding node updates

As a summary of this section, we point out that without security protections, all the listed privacy goals are violated by easy eavesdropping and traffic analysis. Further, while encryption and pseudonyms can be used for the mobile anonymity as a first defense as they have been widely used in the Internet practice, problems such as the venue anonymity still exist. If coordinations among the attackers are possible, the motion pattern privacy and topology privacy are in great danger. With intrusions, the listed privacy goals are also mostly

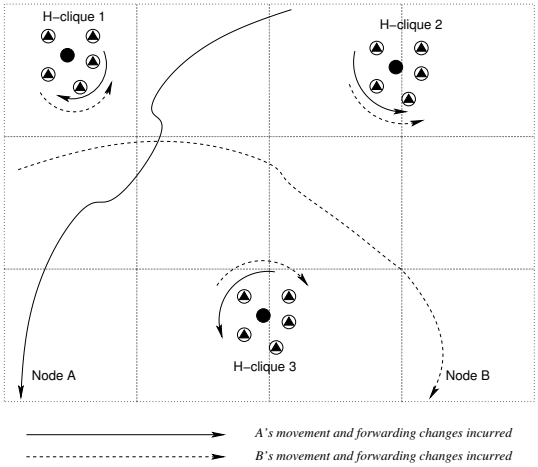

Fig. 4. Composite H-clique attack: More H-cliques can obtain more precise motion patterns

compromised. More design issues have to be addressed to ensure the mobile anonymity for routing in a mobile wireless network facing various passive adversaries.

IV. Designing countermeasures

The major challenge of designing an anonymous routing protocol for mobile networks is to deal with the venue anonymity and the associated ad hoc network privacy problems, such as the dilemma presented in Example 7. The venue anonymity requires a routing protocol to hide a node's identity and also to hide the relationship among nodes from each other (the relations may lead to leaking of enough network routes or topology by inferences), yet still to be able to build up a route and forward packets. Given the limited dimensions in routing protocol design, the following directives are useful to serve the cause.

- *On-demand routing approach as a baseline to ensure privacy of network topology*: In on-demand routing, fresh network topology knowledge is gathered only when needed. Compared to proactive routing and any other proactive features (e.g., constant neighborhood beaconing), purely on-demand routing schemes reduce the node intruders' chances in knowing fresh network topology. In addition, on-demand routing generates less routing overhead and is more energy efficient. These features are highly desirable for many MANET applications.
- *Identity-free routing for strong identity protection*: The idea of identity-free routing is to hide a node's identity from its neighboring nodes in exchanging routing messages. This also implies *identity-free forwarding* for packets. In the design, usage of any identity/pseudonym of any node is not allowed in routing. Thus when the worst case presents, the adversary only knows the presence of neighboring nodes (by wireless transmissions) but not their identities (or any replacement pseudonyms) nor the associated relationship amongst identities. This design ensures perfect identity anonymity against strong passive node intruders.

- *Wireless neighborhood traffic mixing*: Without using identities directly in any routing message, traffic should be further mixed within a neighborhood where multiple nodes move in and out of the venue. Any counting or statistical meaningful analysis is difficult to obtain over a certain period of time. Thus the traffic from or to a venue is protected against strong passive traffic analysts. The venue anonymity and the neighborhood location privacy are partly ensured.
- *Minimizing expensive public key processing in large-scale network operations (e.g., flooding)*: Public key cryptography not only incurs expensive overhead, but also offers the adversary abundant chances to deplete ad hoc nodes' limited resource. A mobile node intruder that is compliant to the underlying routing protocol can issue network wide route discovery floods to consume computing resource on all nodes.

Collectively, the directives illustrate critical design principles for building anonymous ad hoc routing protocols for mobile wireless networks. It is possible to apply these principles to design various anonymous routing protocols that achieve different levels of balances between the protocol efficiency and the degree of anonymity protection. Protocols visited in the previous section have used some of the principles. They differ in the mechanisms of establishing identity-free routes using the on-demand routing approach. But none of them are perfect in providing all the anonymity protections under the strongest attacks, e.g, MASK does not guarantee recipient identity anonymity; SDAR and MASK fail to defend the neighborhood location privacy attack (Example 6) launched by node intruders; ANODR's RREP traffic and data traffic reveal active routes when under the global colluding attack in dense format. On the other hand, however, we note that the passive adversary (e.g., Figure 1) also pays non-trivial deployment and communication cost in its anonymity attacks. Therefore, performance evaluation plays a critical role in the anonymous routing design. As neither the adversarial side nor the legitimate side can completely achieve its goal in a network using a properly designed anonymous routing protocol, the effectiveness of adversarial attacks and legitimate countermeasures is performance driven. Technical details on how the principles are used in routing protocols, e.g, how to establish a route, can be found in papers [5] [26] [43] and the performance issue is discussed in [27].

V. Threats Evaluation

This section aims at illustrating various issues discussed above through simulation. We present two sets of simulation study on the mobile anonymity attacks. First, we show how to quantify the effectiveness of the mobile anonymity attacks; we use the packet flow tracing attack as the example. We then show a visual illustration of the mobile anonymity attacks; we use the sparse mode motion inference attack (SMIA) as the example.

A. Route traceable ratio

In order to realize *identity-free routing*, we have to employ a very different approach from common on-demand routing protocols [23][34][36]. Figure 5 depicts a typical active route established by different on-demand routing protocols. In Figure 5, common on-demand routing protocols use node's identity to furnish packet forwarding, while an identity-free routing must use a *random* pseudonym shared between neighboring forwarders. This design bears resemblance to virtual circuits used in Internet QoS [1]. We use a new metric called *traceable ratio* to quantify the degree of exposure of path segments. Such exposure leads to the violation of the motion pattern privacy and the topology privacy (a route contributing partially to topology knowledge).

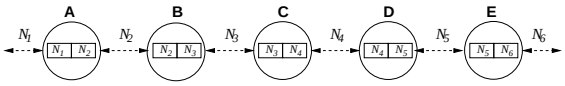

Fig. 5. Identity-free routing (using random pseudonyms $N_1, N_2, \ldots$) vs. common routing (using node identity pseudonyms $A, B, \ldots$)

In an identity-free routing, when a node X is compromised, the adversaries can link two random pseudonyms together for each route passing the node X. Thus, for each route, if F forwarding nodes are compromised and they are consecutive en route, then a route segment of $F + 1$ hops are linked together. If the compromised nodes are not consecutive en route, then the adversary is able to construct multiple route segments, but not to link the multiple compromised segments together. For example, if A is the source and E is the destination in Figure 5, and A, B, D, E are intruded, then the adversaries can form traceable segments $\overline{ABC}$ and $\overline{CDE}$, but they have to intrude C to discover that $\overline{ABC}$ and $\overline{CDE}$ belong to the same route. For the same example, if an ordinary on-demand routing is used, comprising A, B, D, E leads to revealing the entire path $\overline{ABCDE}$.

Let's quantify the damage caused by node intrusion. Suppose a route has L hops in total, where K route segments are compromised. And suppose the hop count of i-th compromised segment is F_i,$1 \leq i \leq K$, we define the *traceable ratio* R of the route as

$$R = \frac{\sum_{i=1}^{K}(F_i \cdot W_i)}{L} = \frac{\sum_{i=1}^{K}(F_i \cdot \frac{F_i}{L})}{L}$$

where W_i is a weight factor. The weight W_i can be of form $(\frac{F_i}{L})^r$ where $r \geq 0$, so that the traceable ratio of a route is 100% when all forwarding nodes en route are intruded, or 0 when no forwarding node en route is intruded. Without loss of generality, we select $W_i = \frac{F_i}{L}$. In addition, the longer a compromised segment is, the larger the traceable ratio R is. This means that the victim being traced is under greater danger if the mobile intruders can get as far as possible to approach the victim. Using the same example in Figure 5, we have $L = 4$, the traceable ratio $R = \frac{2 \cdot \frac{2}{4} + 2 \cdot \frac{2}{4}}{4} = \frac{1}{2}$ when A, B, D, E are intruded, or $R = \frac{3 \cdot \frac{3}{4} + 1 \cdot \frac{1}{4}}{4} = \frac{5}{8}$ when A, B, C, E are intruded.

In our simulation, we compare the traceable ratio between DSR and the identity-free routing for identical scenarios. Figure 6 shows the traceable ratios over different path lengths. Longer paths are more likely to include intruded forwarding nodes. The figure shows that identity-free routing is not sensitive to the path length because the knowledge exposed to

intruders is localized only in the intruded node. The traceable ratio of the identity-free routing remains at the percentage of the intruded nodes. In contrast, the traceable ratios of DSR increase quickly (note that DSR does not scale to long hops, thus data collected for the path length as long as 7 or more is not sufficient for statistically meaningful display).

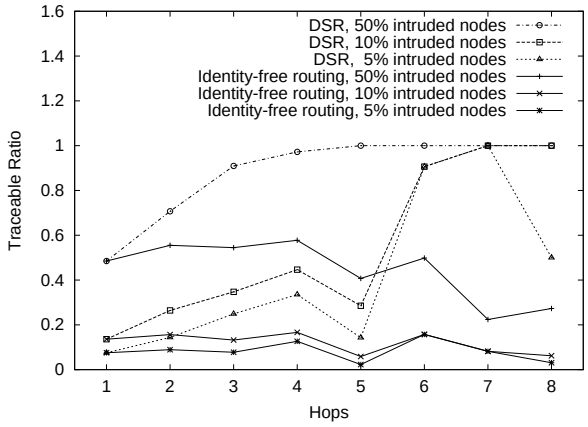

Fig. 6. Traceable ratio evaluation

B. Illustration: sparse mode motion inference attack

We simulate a scenario where a target node moves straightly across a network from the left side to the right. Figure 7 is a snapshot of the simulation. While moving, the target node periodically communicates with other nodes (two in the figure) using the routes established by the AODV routing protocol. In the figure, a routing path between the target and the destination is depicted by the linked solid lines. When the target moves, different paths are taken and the figure shows that the intermediate forwarding nodes have changed for several times due to the target mobility. In the meantime, node intruders (two in the figure, shown also their radio ranges) are presented in the network. They use the aforementioned radio techniques to obtain the relative positions of its neighbors. In addition, a node intruder is capable of launching wormhole attacks [20] and rushing attacks [21] to place itself on the ad hoc routes with high probability. By analyzing the intercepted RREQs and the corresponding RREP packets, e.g., taking the source, destination and broadcast-id tuple from the RREQs and matching them with the later received/intercepted RREP, the attackers can detect that the next hop has switched from one neighbor to another for this target node. When encryption is not implemented to protect the routing messages, this H-clique attack is easier in the sense that no intrusion is needed.

In Figure 7, the "$adversary1$" suggests a clockwise motion to its north-west, the "$adversary2$", hearing the path migration from node Q1 to node Q2, figures out that the target is moving counterclockwise to its south-west. Combining these two pieces of information, the adversaries successfully discover that there is a motion cutting through between them. Through the case, we demonstrated that with a certain number of adversaries (which are capable of communicating with each other), in a bounded time, the motion pattern inference is possible.

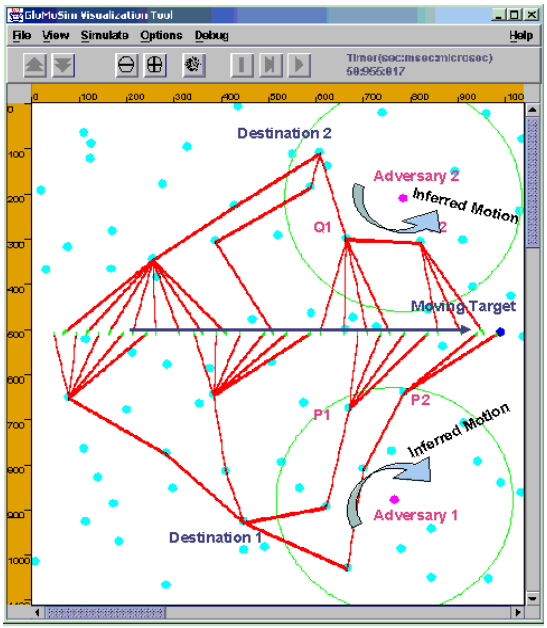

Fig. 7. Illustration through simulation: 2 H-clique attacks (Depicted nodes and ad hoc routes are from GloMoSim animation).

VI. Summary

In this paper we have presented an extensive study on anonymity threats against mobile ad hoc networks. In addition to anonymity required in an infrastructure network, a mobile ad hoc network should prevent its mobile members from being traced by passive adversary. The network needs new mobile anonymity protections like (1) venue anonymity in addition to conventional identity anonymity, (2) privacy of ad hoc network topology, and (3) privacy of a node's motion pattern. We have presented practical examples to illustrate the feasibility and effectiveness of many attacks that threat the new privacy requirements. These new threats are all introduced by mobility and are little meaningful in fixed infrastructure, thus are left unaddressed. We suggest that in the new context, on-demand and identity-free routing with neighborhood traffic mixing are better design choices that lead to defense against the new anonymity threats in mobile networks. Simulations show examples on quantifying and visualizing the effectiveness of the attacks.

Acknowledgment

The authors would like to thank the anonymous reviewers for their invaluable comments.

References

[1] ATM Forum. Asynchronous Transfer Mode. `http://www.atmforum.org`, 2002.

[2] S. Basagni, K. Herrin, E. Rosti, and D. Bruschi. Secure Pebblenets. In *MobiHoc*, pages 156–163, 2001.

[3] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2(1):46–55, 2003.

[4] O. Berthold, H. Federrath, and M. Köhntopp. Project Anonymity and Unobservability in the Internet. In *Computers Freedom and Privacy Conference 2000 (CFP 2000), Workshop on Freedom and Privacy by Design*, 2000.

[5] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks. In *The 29th IEEE International Conference on Local Computer Networks (LCN04)*, 2004.

[6] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In *ACM MOBICOM*, pages 85–97, 1998.

[7] D. L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[8] D. L. Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[9] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol(OLSR). Internet RFC 3626, `http://www.ietf.org/rfc/rfc3626.txt`, March 2005.

[10] W. Dai. PipeNet 1.1. `http://www.eskimo.com/~weidai/pipenet.txt`, 2004.

[11] G. Danezis, R. Dingledine, and N. Mathewson. Mixminion: Design of a Type III Anonymous Remailer Protocol. In *IEEE Symposium on Security and Privacy*, 2003.

[12] J. Deng, R. Han, and S. Mishra. Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks. In *IEEE International Conference on Dependable Systems and Networks (DSN)*, 2004.

[13] S. Dolev and R. Ostrovsky. XOR-trees for Efficient Anonymous Multicast and Reception. *ACM Transactions on Information and System Security (TISSEC)*, 3(2):63–84, 2000.

[14] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *MobiSys03*, 2003.

[15] Q. He, D. Wu, and P. Khosla. Quest for Personal Control over Mobile Location Privacy. *IEEE Communications Magazine*, 42(5):130–136, 2004.

[16] C. Hedrick. Routing Information Protocol. `http://www.ietf.org/rfc/rfc1058.txt`, 1988.

[17] X. Hong, J. Kong, and M. Gerla. A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks. In *IEEE MILCOM*, 2003.

[18] Y.-C. Hu, D. B. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In *Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02)*, 2002.

[19] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks. In *ACM MOBICOM*, pages 12–23, 2002.

[20] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *IEEE INFOCOM*, 2003.

[21] Y.-C. Hu, A. Perrig, and D. B. Johnson. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In *ACM WiSe'03 in conjunction with MOBICOM'03*, pages 30–40, 2003.

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

[23] D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In T. Imielinski and H. Korth, editors, *Mobile Computing*, volume 353, pages 153–181. Kluwer Academic Publishers, 1996.

[24] D. Kesdogan, J. Egner, and R. Buschkes. Stop-and-go MIXes Providing Probabilistic Security in an Open System. *Second International Workshop on Information Hiding (IH'98), Lecture Notes in Computer Science 1525*, pages 83–98, 1998.

[25] Y.-B. Ko and N. Vaidya. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In *ACM MOBICOM*, pages 66–75, 1998.

[26] J. Kong and X. Hong. ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks. In *ACM MOBIHOC'03*, pages 291–302, 2003.

[27] J. Kong, X. Hong, M. Sanadidi, and M. Gerla. Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing. In *The Tenth IEEE Symposium on Computers and Communications (ISCC)*, 2005.

[28] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris. A Scalable Location Service for Geographic Ad HOc Routing. In *ACM MOBICOM*, pages 120–130, 2000.

[29] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak. Exposure in Wireless Ad Hoc Sensor Networks. In *ACM Procs. of 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01)*, 2001.

[30] U. Möller, L. Cottrell, P. Palfrader, and L. Sassaman. Mixmaster Protocol — Version 2. `http://www.abditum.com/mixmaster-spec.txt`, July 2003.

[31] J. Moy. OSPF Version 2. `http://www.ietf.org/rfc/rfc1131.txt`, 2005.

[32] R. Ogier, F. Templin, and M. Lewis. Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). Internet RFC 3684,`http://www.ietf.org/rfc/rfc3684.txt`, March 2005.

[33] C. Ozturk, Y. Zhang, and W. Trappe. Source-location privacy in energy-constrained sensor network routing. In *the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2004.

[34] V. D. Park and M. S. Corson. A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks. In *IEEE INFOCOM*, pages 1405–1413, 1997.

[35] C. E. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *ACM SIGCOMM*, pages 234–244, 1994.

[36] C. E. Perkins and E. M. Royer. Ad-Hoc On-Demand Distance Vector Routing. In *IEEE WMCSA'99*, pages 90–100, 1999.

[37] A. Pfitzmann and M. Köhntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In H. Federrath, editor, *Designing Privacy Enhancing Technologies; Workshop on Design Issues in Anonymity and Unobservability (DIAU'00)*, June 2000.

[38] A. Pfitzmann, B. Pfitzmann, and M. Waidner. ISDNMixes: Untraceable Communication with Very Small Bandwidth Overhead. In *GI/ITG Conference: Communication in Distributed Systems*, pages 451–463, 1991.

[39] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communications*, 16(4), 1998.

[40] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for Web Transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[41] Y. Rekhter and T. Li. A Border Gateway Protocol 4 (BGP-4). `http://www.ietf.org/rfc/rfc1771.txt`, 2005.

[42] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Royer. A Secure Routing Protocol for Ad Hoc Networks. In *10th International Conference on Network Protocols (IEEE ICNP'02)*, 2002.

[43] Y. Zhang, W. Liu, and W. Lou. Anonymous communications in mobile ad hoc networks. In *IEEE INFOCOM'05*, 2005.

Xiaoyan Hong is an Assistant Professor in the Department of Computer Science at the University of Alabama. She received the B.S. and M.E. degrees in Computer Science from Zhejiang University in China, and the Ph.D. degree in Computer Science from University of California at Los Angeles in 2003. Her research interests include network protocol design, performance evaluation and implementation for wireless networks, especially for mobile ad hoc networks and energy concerned sensor networks. Her current research focuses on routing, mobility, secure routing and anonymity issues in wireless networks.

Jiejun Kong is a post-doctoral researcher in Computer Science Department, University of California at Los Angeles (UCLA). He is interested in developing efficient, scalable, and secure network protocols for wireless networks. His research topics include secure and anonymous routing, authentication, access control, distributed data harvesting, and network security modeling in mobile wireless networks, in particular those with challenging network constraints and with 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 NSF iMASH project, ONR MINUTEMAN/STTR project, and NSF WHYNET project.

Mario Gerla was born in Milan, Italy. He received a graduate degree in engineering from the Politecnico di Milano, in 1966, and the M.S. and Ph.D. degrees in engineering from 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 an IEEE fellow.