Privacy-Preserving Location-Based On-Demand Routing in MANETs

Karim El Defrawy, *Member,* and Gene Tsudik, *Senior Member*

***Abstract*—Mobile Ad-Hoc Networks (MANETs) are particularly useful and well-suited for critical scenarios, including military, law enforcement as well as emergency rescue and disaster recovery. When operating in hostile or suspicious settings, MANETs require communication security and privacy, especially, in underlying routing protocols. Unlike most networks, where communication is based on long-term identities (addresses), we argue that the location-centric communication paradigm is better-suited for privacy in suspicious MANETs. To this end, we construct an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries. We analyze the security, privacy and performance of PRISM and compare it to alternative techniques. Results show that PRISM is more efficient and offers better privacy than prior work.**

***Index Terms*—Privacy, communication system security, communication system routing, on-demand routing protocol, mobile communication, location-based communication, military communication.**

I. Introduction

MOBILE Ad-Hoc Networks (MANETs) play an increasingly important role in many environments and applications, especially, in critical settings that lack fixed network infrastructure, such as: emergency rescue, humanitarian aid, as well as military and law enforcement [1]. Since most MANETs are multi-hop in nature, agile and resilient routing is a crucial function with requirements appreciably distinct from those in fixed networks. At the same time, many MANET deployment scenarios involve operation in *hostile* environments, meaning that attacks are either expected or, at least, possible. Moreover, threats can originate from both outside and inside the network. While most prior work in secure MANET routing focused on security issues, less attention has been devoted to privacy. Note that, in this context, privacy does not mean confidentiality of communication (i.e., data) among MANET nodes. The latter is a fundamental part of secure MANET operation; it is easily attained by encryption, assuming that appropriate key management solutions are used to set up or distribute cryptographic keys. What we mean by *privacy* is resistance to tracking. We believe that this narrow interpretation of privacy is well-justified. Since mobility is the only distinctive MANET feature, the sequence of movements by a given MANET node can represent sensitive private information. This is clearly not always the case, i.e., some MANETs do not require privacy of this type. Whereas, any setting where tracking of MANET nodes is undesirable or dangerous would benefit greatly from hiding node movements and movement patterns.

Manuscript received 15 November 2010; revised 1 May 2011.

The authors are with the Computer Science Department, University of California, Irvine, Bren Hall, 3rd Floor, Irvine, CA 92697-3435 (e-mail: eldefrawy@gmail.com, keldefra@uci.edu, gts@ics.uci.edu).

Digital Object Identifier 10.1109/JSAC.2011.1112xx.

Application Examples: As mentioned above, military and law-enforcement MANETs are compelling examples of settings where privacy, in addition to security, is very important [2]. Zooming in on the military example, one can imagine a battlefield MANET composed of different types of nodes, e.g., infantry soldiers, vehicles, aircrafts as well as other types of personnel and equipment. If the adversary can track nodes' movements, it can easily deduce node types. For example, one that moves 50 miles within 10 minutes is most likely, an aircraft. Whereas, one moving only 5 miles within the same interval is probably a vehicle. Another example in the same setting is an adversary aiming to track specific nodes. If the adversary knows that a certain node corresponds to a commander, it could wait until this node moves within reach of sniper fire, with obvious consequences.

With the focus on privacy, our central goal is to design tracking-resistant techniques for MANETs. As discussed below, such techniques can not offer a privacy panacea, since they depend on certain environmental factors, such as sufficient network size and pervasive mobility. If nodes do not move, tracking-resistance is clearly impossible. This is because an adversary observing successive snapshots of the topology can easily see that certain nodes remain at the exact same positions. Furthermore, tracking-resistance requires us to re-examine the very basics of MANET communication, e.g., how nodes refer to each other and why they communicate in the first place.

Contributions: This paper makes two contributions. First, it shows how to obtain privacy-friendly on-demand location-centric MANET routing. By "privacy-friendly" we mean *resistant to node tracking by both outsider and insider adversaries*. Moreover, this is achieved without sacrificing security. Second, it demonstrates – via simulation – that the proposed PRISM protocol offers better privacy and better efficiency than prior results.

Organization: The rest of this paper is organized as follows. We first discuss certain key features of the envisaged MANET setting and justify certain choices in our design in Section II. We present our assumptions and adversary model in Section III. We then describe the details of PRISM and analyze its security and privacy in Sections IV. PRISM's efficiency is compared through simulation to prior work in Section V and an overview of related work is presented in Section VI. We summarize our conclusions in Section VII.

II. Design Elements and Choices

A. Goals

Our work has three main goals:
(1) *Privacy:* maximize tracking-resistance of individual nodes, by outsider and insider adversaries.
(2) *Security:* provide protection against active and passive outsider and insider attacks.
(3) *Efficiency:* attain the above two goals with reasonably efficient solutions.

B. Long-Term Identities and Communication Paradigm

The need for comprehensive addressing is fundamental in most networks. Some form of a unique address (or name) is usually a pre-requisite for one node to communicate with another. However, we argue that in a privacy-conscious MANET setting, using long-term or persistent identifiers can be harmful. The first threat comes from outsiders: tracking nodes based on their identifiers is possible by eavesdropping on routing information exchanged. This can be easily remedied by having all MANET nodes share a network-wide key and encrypting all routing information. The second threat comes from malicious insiders, i.e., MANET nodes that aim to track their peers. This threat is much harder to address, since a typical (even secure) MANET routing protocol is designed to provide routing information based on a destination address.

Our privacy goal dictates that long-term identities can only be used in conjunction with flooding (which is inefficient). Whereas, random short-term (one-time) identities are not meaningful as the sole basis for communication. This leads us to consider a fundamental question:
Is communication identity-centric or location-centric?
The term *identity-centric* means that one node decides to communicate with another based on the long-term identity, regardless of the latter's location, current MANET topology or other ephemeral factors. Location-centric communication means that communication decisions are made largely on the basis of current topology or some other related criteria, e.g., nodes' physical coordinates. We observe that many critical MANET scenarios are not inherently identity-centric. For example, in a disaster relief setting, current node location might be much more important than node identity. There might be scenarios that require both location and long-term identity for nodes to make communication decisions. In the rest of this paper, we restrict the scope of our work to MANETs where communication decisions are location-centric. There is an inherent trade-off between privacy and session duration in location-centric mobile communication. If addressing is strictly location-based, high node mobility limits effective communication to short-lived sessions. To support longer data sessions end nodes can establish a short-lived session and use it to agree on a secret session-specific identifier. This identifier can then be advertised when nodes move to a new location, so that they recognize each other. The long term session is now supported by addressing messages to this identifier. The disadvantage of such an approach is that it gives insider adversaries the ability to track other nodes over longer periods of time by mapping such a session identifier to locations. Protection against active insider is discussed in detail in Section V-B1.

Another important privacy issue is topology exposure: *to what degree should the routing protocol advertise current topology?*[1] Generally, since less information means better privacy, we can conclude that the best approach is to use a reactive (on-demand) routing protocol that hides MANET topology. AODV is a good example – it reveals only the hop-count for a given destination.

If the current MANET topology is unknown and there are no long-term node identities, how do nodes communicate? One possibility is to use a *hit-and-miss* approach, which we adopt in this paper. In it, a node picks a geographical location (coordinates), draws a certain perimeter around it (e.g., by specifying a radius or points of a polygon) uses the resulting area as the destination address. The message (route request) addressed in such a way propagates through the network (via flooding, as in AODV) and either fails to find any nodes in the specified area or reaches one or more. Destination node(s) then reply (if they want to) using state along the reverse route, with intermediate nodes using information cached during route request processing. This simple location-based technique is effective as it guarantees that, as long as the network is connected, all destinations within the specified area are reached. However, it complicates operation since the specified area might be empty. In this case, the source needs to either expand the perimeter or try a different area altogether.

III. Environment Features

This section describes details of the envisaged MANET environment, including network assumptions, adversarial model and security infrastructure.

A. Network Assumptions

- A node has no public identity. There might be a private long-term identity (or address) for each node but this information is assumed to remain private between each node and a trusted off-line authority (see section III-C).
- All communication is hit-and-miss and location-centric: a source node selects a destination location (area) and attempts to communicate to a destination node (or nodes) at that location. If the specified location is empty, the source node times out. Most communication sessions are short-lived. (See Section V-B1).
- The MANET environment is suspicious, meaning that even genuine nodes can not be trusted. (See Section III-B).
- Each node has a means of determining its location with reasonable accuracy, e.g., a GPS device.
- Nodes are loosely time synchronized; (this feature is "free" with GPS).
- Nodes are capable of generating good-quality random numbers and performing basic public key operations (e.g., encryption and signatures).

[1]In this context, "advertise" applies to genuine MANET nodes, i.e., we assume that outsiders are unable to obtain topology information.

B. Adversary Model

We now discuss several types of anticipated adversaries.[2]

1) Passive and Active Outsiders: The goal of such outsiders is to violate privacy, security or both. A *passive outsider* eavesdrops on all communication and aims to compromise privacy, i.e., track nodes. An *active outsider* can inject, modify and replay messages in addition to tracking nodes. Its goals can include: disruption of routing, node impersonation and creation of phantom nodes via Sybil attacks. Both do not possess the cryptographic keys used to secure the MANET.

2) Passive (Honest-but-Curious) Insiders: A *passive* insider receives messages exchanged within the MANET and outwardly behaves correctly by following all rules and protocols. In other words, it sends no fraudulent messages, does not attempt to impersonate other nodes and does not delete or modify other nodes' traffic. Behaving otherwise would attract attention and could result in eventual detection and exposure [3]. However, a passive insider is not assumed to be *silent*, i.e., its communication patterns are not different from those of non-malicious nodes. A passive insider can also attempt to track other nodes' movements by linking different location announcement messages or using trajectory information [4].

3) Active Insiders: Active insiders are the most powerful adversary type. An active insider can modify, inject and replay messages, in addition to tracking nodes. In more traditional MANET settings, the identity of each node is known and the power of the active insider is constrained, since its activity can be detected. However, since privacy is one of our main goals, nodes may have no persistent identities. Therefore, an active insider can easily modify or inject seemingly genuine routing messages, thus masquerading as other nodes. We consider two kinds of active insider attacks:

- *Sybil attack:* adversary creates one or more phantom nodes by generating fake routing control messages ostensibly from these nodes' locations. Such routing messages contain valid authentication information (e.g., signatures), however, other nodes cannot link them to the same malicious node.
- *Location fraud*: adversary lies about its own location. This can be very harmful in situations where node communication is location-centric. For example, a malicious insider claiming a certain fake location can result in attracting (or repelling) traffic.

The adversary is not restricted to one or the other attack type, i.e., it is free to combine them.

C. Security Infrastructure

We make several assumptions about the MANET security infrastructure. First, we assume an **off-line** Trusted Third Party (TTP). This TTP performs the functions of a Certification Authority (CA). It sets up the MANET, manages its membership and performs other tasks, such as forensic auditing of security logs and after-the-fact tracing of misbehavior by rogue MANET nodes (insiders). Second, we assume that, prior to each deployment, each MANET node has been registered with the TTP and has been issued appropriate credentials, such as a public key (or a group signature) certificate. If a new node needs to be added to the MANET after deployment, it has to first interact with the TTP to obtain its credentials. TTP responsibilities also include the distribution and management of a MANET-wide secret key used for all traffic encryption. This is needed to protect against passive outsiders who might eavesdrop on intra-MANET communication. We stress that the TTP is the only party aware of each node's long-term identity. One disadvantage of our off-line TTP model is that members (nodes) can only be evicted between deployments. Consequently, our security model takes into account active insider attacks; this way, we defend against a misbehaving node that might operate within the MANET until the end of current deployment.

[2]Physical-layer attacks based on time difference of arrival (TDoA) of messages is outside the scope of this paper. Such attacks are difficult in practice since they require the adversary to be within one hop.

TABLE I
NOTATION USED.

$RREQ$	Route Request
$RREP$	Route Reply
DST-AREA	Destination area (or location)
PK_X, SK_X	Public, private key of X
TS_X	Time-stamp of X
$GSIG_X$	Group signature generated by X
DST_{Loc}	Exact location of a destination node
$H(m)$	Hash of m (e.g., SHA-256)
$E_K(m)$	Encryption of m with key K

IV. PRISM PROTOCOL

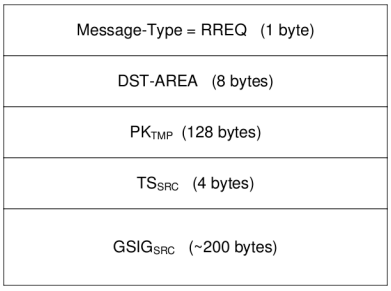
This section describes the Privacy-friendly Routing in Suspicious MANETs protocol (PRISM). PRISM is an anonymous location-centric on-demand routing protocol based on three main building blocks: (1) the well-known AODV routing protocol, (2) any secure group signature scheme (or one time public key certificates), and (3) location information. Location information, as mentioned in Section III-A, is assumed to be available to each node, e.g., via GPS. Table I summarizes the notation used in describing PRISM.

A. Why AODV?

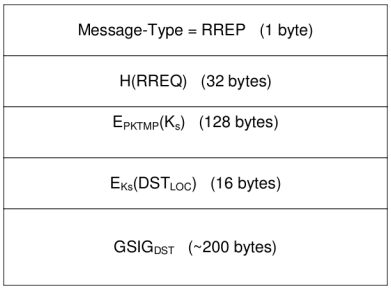
AODV [5] presents an attractive foundation for PRISM, for several reasons. AODV is on-demand (reactive) and thus does not *propagate* topology information, in contrast with proactive protocols, such as OLSR [6]. AODV is distance-vector; it does not return source routes (which reveal partial topology), unlike source-routing-based protocols, such as DSR [7]. AODV is robust since it uses flooding for route discovery; thus, it does not require mobility to be synchronized. We do not describe AODV in detail, since, as an established routing protocol, it is well-known and has been extensively studied [5].

B. Why Group Signatures?

Group signatures [8], described in Appendix A, are an appealing building block for anonymous MANET routing protocols, mainly because they satisfy the conditional privacy property. Group signatures can be viewed as traditional public key signatures with additional privacy features. In a group signature scheme, any member of a large and dynamic group



(a) PRISM RREQ Message



(b) PRISM RREP Message

Fig. 1. PRISM RREQ and RREP Message Format

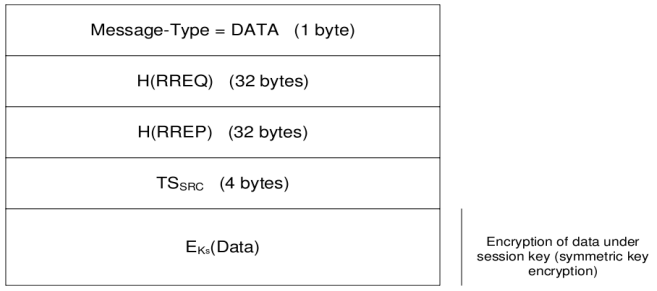


Fig. 2. PRISM Data Message Format

can sign a message, thereby producing a *group signature*. A group signature can be verified by anyone who has a copy of a constant-length group public key. A valid group signature implies that the signer is a *bona fide* group member. But, given two valid group signatures, it is computationally infeasible to decide whether they are generated by the same (or different) group members. Furthermore, if a dispute later arises over a group signature, a special entity called a Group Manager (GM) can force open a group signature and identify the actual signer. This important feature is referred to as *Escrowed Anonymity*. Referring to the Appendix, it is easy to imagine a group signature scheme deployed in a MANET setting, where each node corresponds to a group member and the off-line TTP (see Section III-C) corresponds to a Group Manager (GM).

C. Protocol Features

PRISM is designed with the following features in mind: the source authenticates the destination and vice versa. Intermediate nodes do not learn current location of the source or the *exact* current location of the destination(s). Intermediate nodes are not authenticated. After route discovery, all communication between source and destination is encrypted and authenticated using a one-time (session-specific) secret key. The TTP (group manager) can later learn claimed locations of all nodes that engage in direct communication, i.e., serve as either sources or destinations. The privacy achieved by PRISM is not restricted to a specific mobility pattern (more details and analysis under different mobility model in Section V-B).

D. Protocol Operation

The basic operation of PRISM is similar to AODV. PRISM allows a source to specify a destination area and simultaneously discover multiple destination nodes in it. However, to keep the description simple, we assume that only one node exists within each destination area.

(1) The source broadcasts a route request (RREQ) which contains the destination location, in the form of coordinates and a radius – DST-AREA. RREQ also contains a temporary public key PK_{TMP}, a time-stamp TS_{SRC} and a group signature, $GSIG_{SRC}$ computed over all previous fields. The RREQ message format is shown in Figure 1(a). The process of how the source decides to communicate and the process involved is shown in Figure 3. Note that the source starts by searching in an area with a smaller radius and if no reply is received within a specific time window, it increases the radius of the area and sends another RREQ. A received RREP is considered erroneous if the time-stamp included is incorrect, or the exact location of the replying node is not within the destination area or the verification of the group signature included in the RREP fails. In any of these cases the RREP is logged as a failing one and the source waits to receive another RREP for this RREQ.

(2) Upon receiving a RREQ, each node first checks if TS_{SRC} is valid. If not, the RREQ is dropped. Next, the node checks whether it has previously processed the same RREQ. This is done by computing a hash of the new RREQ ($H(RREQ)$) and looking it up in the local cache where all recently handled RREQ hashes are stored. Then, the node checks whether it is within DST-AREA: (A) If not, the intermediate node caches $H(RREQ)$ and re-broadcasts the RREQ. Note that no RREQ fields are changed. (B) If the node is within the destination area, it verifies $GSIG_{SRC}$. If invalid, the RREQ is discarded. Otherwise, it stores the entire RREQ (including $GSIG_{SRC}$). This is needed for forensic analysis, in order to identify and track misbehavior. The destination then composes a route reply (RREP) which contains: (1) $H(RREQ)$, (2) a new random session key K_S and (3) the exact destination location. Both (2) and (3) are encrypted under PK_{TMP} obtained from the RREQ. The RREP also includes the group signature – $GSIG_{DST}$ of all fields. Finally, the destination broadcasts RREP. The previous sequence of operation is shown in the receiver process in PRISM in Figure 4. Note that, unlike some other anonymous routing protocols, PRISM does not require nodes in DST-AREA to re-broadcast RREQ or to delay sending RREP in order to hide their presence. Any insider "overhearing" an RREP already knows that the destination is within the area specified in the corresponding RREQ. In other words, an eavesdropping insider can infer from a RREP that a node exists in DST-AREA, however, it can not learn which node. PRISM does not hide the presence of a node within a certain destination

area or the fact that some node responds to a certain RREQ. It hides which node responded and prevents tracking of such nodes.

(3) Upon receiving a RREP, each node checks whether it has cached the corresponding $H(RREQ)$. If not, the RREP is dropped since this node was not on the forward route. If $H(RREQ)$ is already cached, the node checks if the same RREP has been processed. If so, the RREP is dropped. The intermediate node now creates a new entry in its active routes table and re-broadcasts the RREP. Each active table entry contains: $H(RREQ)$, $H(RREP)$ and the time-stamp of entry creation.

(4) When the RREP is received, the source first checks for the correctness of the time-stamp and the exact location of the replying node then verifies the group signature. If invalid, the RREP is discarded and logged as a failure. Next, the source decrypts the session key and location supplied by the destination. This key is subsequently used for message encryption and/or authentication. Next, the source stores the entire RREP for forensic purposes. This completes the route set-up process (also shown in Figure 3).

Once the route is established, each source-destination data message specifies the tuple of RREQ and RREP hashes, $< H(RREQ), H(RREP) >$, as a unique route identifier. In the opposite direction, the reverse tuple ($< H(RREP), H(RREQ) >$) is used as a route identifier. The data is encrypted with the session key that was included in the RREP from the destination. Figure 2 shows the format of data messages with appropriate field sizes. If the route breaks, a route error (RERR) message similar to that in AODV is generated.

For backward compatibility, PRISM messages can be easily sent over IPv6. We can define a new extension header to carry PRISM route identifiers (i.e., $< H(RREP), H(RREQ) >$) and use it to encapsulate data packets. RREQ and RREP encapsulated inside an IPv6 header can be broadcasted (or geocasted) based on DST-AREA. Since DST-AREA is only 4 bytes, in can fit into the IPv6 address, or it could be a part of PRISM extension header in RREQ.

V. Security Analysis and Simulations

We first present PRISM's security analysis then its simulation results.

A. Security Analysis

We now consider how PRISM prevents different types of attacks according to the adversary model.

1) Passive Outsiders: PRISM is immune to passive outsiders, since simple link encryption using a common MANET-wide key prevents eavesdropping. As mentioned in Section III-C, we assume that the TTP sets this up before deployment.

2) Passive Insiders: Passive insiders are more worrysome than passive outsiders. The former can observe RREQ-s and corresponding RREP-s, which reveals several things: (1) The time-stamp of the RREQ source TS_{SRC} informs the insider about the distance away from the source, even though the direction is unknown. However, this is easily prevented by using coarsely-granular timestamps, i.e., TS_{SRC} can be expressed in seconds. (2) DST-AREA in RREQ is *visible* and thus betrays the source's interest. There seems to be no practical way to address this issue, since the content of DST-AREA is precisely what enables routing in PRISM. (3) Mere existence of an RREP tells the insider that at least one node is in the DST-AREA specified in the RREQ. Multiple RREP-s provide even more information. This leaks parts of current topology to passive intermediate nodes. However, recall that the destination's precise location is encrypted and is visible only to the source. At the same time, a passive insider cannot link two RREQ-s from the same source. This is due to the basic property of group signatures that makes it infeasible to decide whether two valid group signatures are generated by the same signer. Moreover, each RREQ includes a unique PK_{TMP} and, once established, each route uses a distinct K_S for traffic encryption and authentication.

3) Active Outsiders: Since all traffic within the MANET is protected by a group-wide secret key, an active outsider is unable to modify, replay or introduce messages. Specifically, replays are prevented since each RREQ is timestamped and each RREP must correspond to a previous RREQ. Spurious RREQ-s are simply discarded. Consequently, the attacker can obtain the group-wide secret key only by compromising a genuine node, which transforms it into an *active insider*.

4) Active Insiders: PRISM without any extensions is not secure against active insider attacks. An active insider can lie about its location and reply to RREQs even though it is not within DST-AREA. This misbehavior might remain undetected, either in real time or later. However, it does not create any loss of privacy. Active insiders can also launch a Man-in-the-Middle (MiTM) attack where an insider node receiving a RREQ will remove the session key in it and add its own. The attacker will produce a new group signature and forward the modified RREQ (the same will be carried out in the reverse path with the RREP). The attacking insider will then be able to eavesdrop on the data exchanged between the two communicating nodes and will translate from one encryption key to the other. MiTM attack cannot be detected in real time, it can be inferred off-line by analyzing PRISM logs. Note that, in a MiTM attack, the group signature in the same RREQ will change at the node mounting the attack.

One way to mitigate active insiders is via one-time certificates. In this case, an off-line Certification Authority (CA) issues each node a number of public key certificates with the following fields: (1) a unique public key for a plain (non-group) signature scheme (e.g., RSA or DSA [9]), (2) a time-stamp indicating the future time-slot when this certificate can be used and (3) a signature by the CA on the certificate. As long as all public keys are independent, linking multiple RREQ-s originating with the same source is infeasible. Insider attacks are thus thwarted, since each node only knows its own sequence of one-time certificates and corresponding private keys. Specifically, Sybil attacks are prevented by tying each certificate to a fixed time-slot and only allowing the use of one certificate per node, per time-slot. The only insider attack not addressed here is location-fraud. Main disadvantages of one-

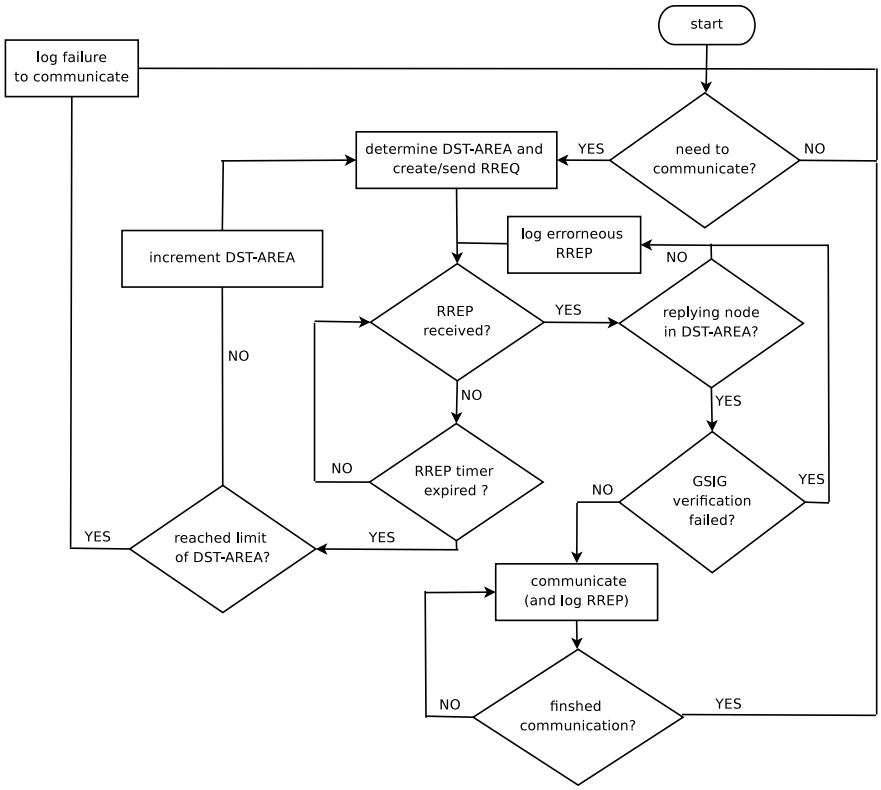


Fig. 3. PRISM Sender Process

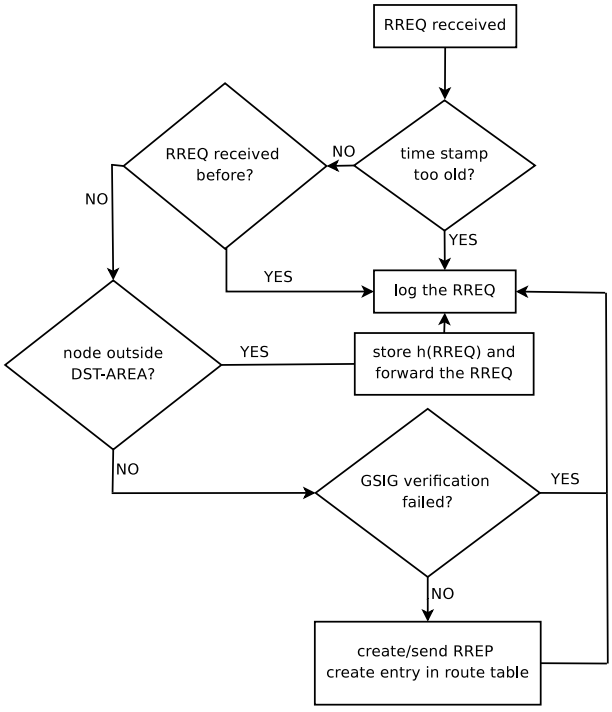


Fig. 4. PRISM Receiver Process

TABLE II
PRISM SIMULATION PARAMETERS

Parameter	Value
Simulation Area	$1000m$ x $1000m$
Simulation Time	10000 sec
Repetitions	100 runs of each simulation scenario
Number of Nodes	Varied from 20 to 100
Dst Area Radius	50m
Mobility Models	– Random Walk Mobility Model (RWMM) – Reference Point Group Mobility Model (RPGMM) with 5 groups and 20 nodes per group – Time-variant User Mobility Model (TVUMM) with 4 communities

time certificates are: (1) the need to pre-determine maximum duration of MANET deployment and (2) additional storage and transmission bandwidth due to certificates.

An alternative is to implement group signatures within tamper-resistant hardware. For example, [10] shows an example of group signature functionality on smartcards. If such an implementation can be coupled with a tamper-resistant GPS device, active insider attacks in PRISM can be virtually eliminated, since an insider would be unable to lie about its current location or to mount a Sybil attack.

A real threat to privacy stemming from malicious insiders is to continuously probe the topology by generating a multitude of RREQ-s, in an effort to monitor node movements and topology fluctuations. In PRISM, such attacks can not be detected in real time since group signatures are unlinkable. We use simulations to assess the effect of such attacks. Off-line, the TTP (Group Manager) can open all group signatures logged by each node and determine the exact long-term identity of each node which generated every RREQ or RREP.

B. Simulation Results

We simulate PRISM and compare it with a location-based link-state protocol, e.g., ALARM [11]. We did not compare

PRISM with other anonymous reactive protocols because they are identity-centric. A direct comparison between a location-centric and identity-centric protocol through simulation is not applicable. ALARM, on the other hand, is the only other anonymous location-centric MANET routing protocol to the best of our knowledge. The goal of the simulations is two-fold: (1) to determine the routing control traffic load and required storage in PRISM, and (2) to determine how much of the network topology is leaked by PRISM.

We simulate a MANET with nodes moving according to the used mobility models in an area of $1000m$ x $1000m$ for 10000 sec (166 min). Simulations are performed using the SimPy [12] discrete-event simulation framework. The NumPy [13] and SciPy [13] packages are used to calculate statistics and confidence intervals. We use the following mobility models in our simulation: (a) one entity-based: (1) random walk mobility model (RWMM) [14], and (b) two group-based: (2) reference point group mobility model (RPGMM) [15] and (3) time-variant user mobility model (TVUMM) [16]. Simulation parameters are summarized in Table II.

1) Effect of Node Mobility on Route Availability and End-to-End Sessions : A thorough study [17] of effects of mobility on MANET routing protocols shows that, in a MANET of 40 nodes in a 1000m-×-1000m area, moving according to the RPGMM model (consisting of one big group), average link lifetime is around 900sec for speeds less than 30m/sec. For a setting with 4 groups of 10 nodes each, link lifetime drops significantly, but still exceeds 240sec for speeds up to 50m/sec. Link lifetime is around 60sec under the Freeway and Manhattan mobility models [17]. The same study analyzed path lifetime and showed that similar durations are observed for path availability (i.e., 100-s of seconds for RPGMM and 10-s of seconds for RWMM, Manhattan and Freeway). [17] also reports that path availability for RPGMM (single and multiple groups), RWMM, Freeway and Manhattan was found to be 100%, 92%, 97%, 99% and 95%, respectively. If PRISM is deployed in settings similar to those analyzed in [17], end-to-end data sessions and location-based identifiers can be expected to last 100-s of seconds. Otherwise, PRISM's utility would be limited to short-lived sessions.

2) Traffic Load Generated by PRISM: Figure 5 shows the average number of RREP received (both to own RREQ and those to forward) by a node in a setting as described above. Each node periodically (every 5 sec to match OLSR[6] and ALARM's periods) sends a RREQ to a random destination area. RREPs will be generated if nodes exist in that area. We see from the figure that for all mobility models, the number of RREP is always at least an order of magnitude less (sometimes even two) than the number of link-state announcements that would be required if a link-state based protocol, e.g., ALARM, was used. Note that we do not show the number of RREQ sent. This number is fixed and depends on the sending rate which we determine in our simulation. In this simulation each node generates a new RREQ every 5 sec. The result is that in total PRISM will, at most, generate around 120% of the number of routing control messages of a link-state based protocol. In such a heavy traffic scenario, where *all nodes* continuously search for new destinations to communicate with, PRISM will generate slightly more traffic overhead but will be better at hiding the topology as we will show next. If only a fraction of nodes (30-50%) generate RREQs, PRISM would incur significantly less control traffic than a link-sate protocol.[3]

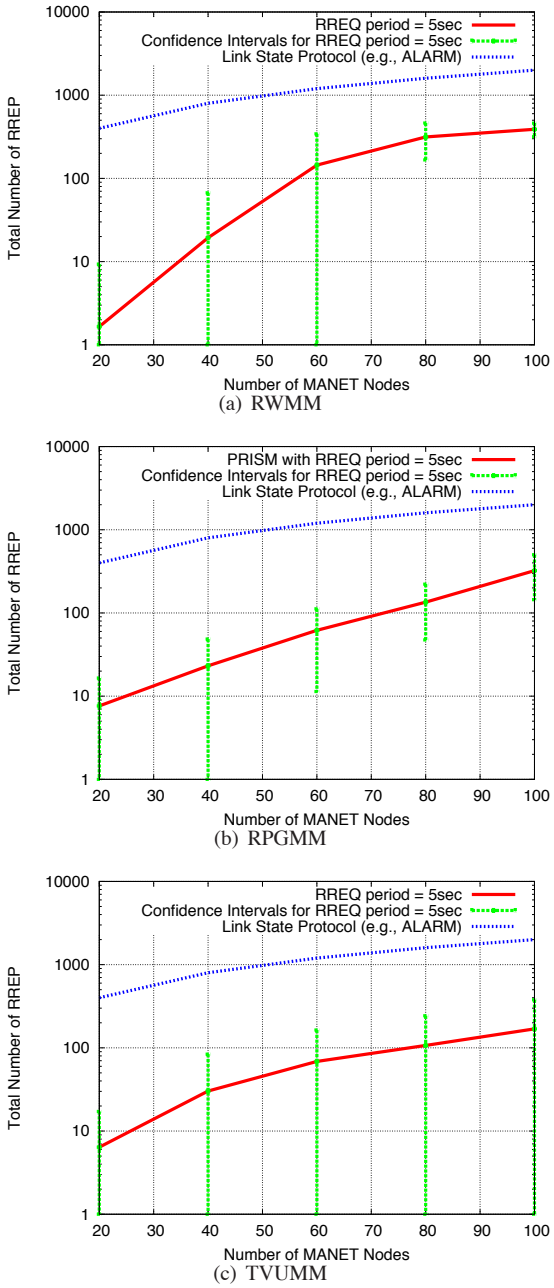


Fig. 5. Routing Control Traffic (Number of RREPs) in PRISM for Different Mobility Models

Nodes are divided into five groups in simulations of RPGMM in Figure 5. We use the following values for TVUMM: 4 communities, defined as an area covered by a circle with 100m radius and center selected at random. NMP is 200sec and CMP is 400sec. The probability of switching from local to roaming epoch is $p_r = 0.4$, and, from roaming to local – $p_l = 0.7$. Local epoch is set to 200sec and roaming – 100sec.

An interesting observation is that in RPGMM and TVUMM

[3]In fact, it would incur one order of magnitude less traffic. Actual results are not shown due to space limitations.

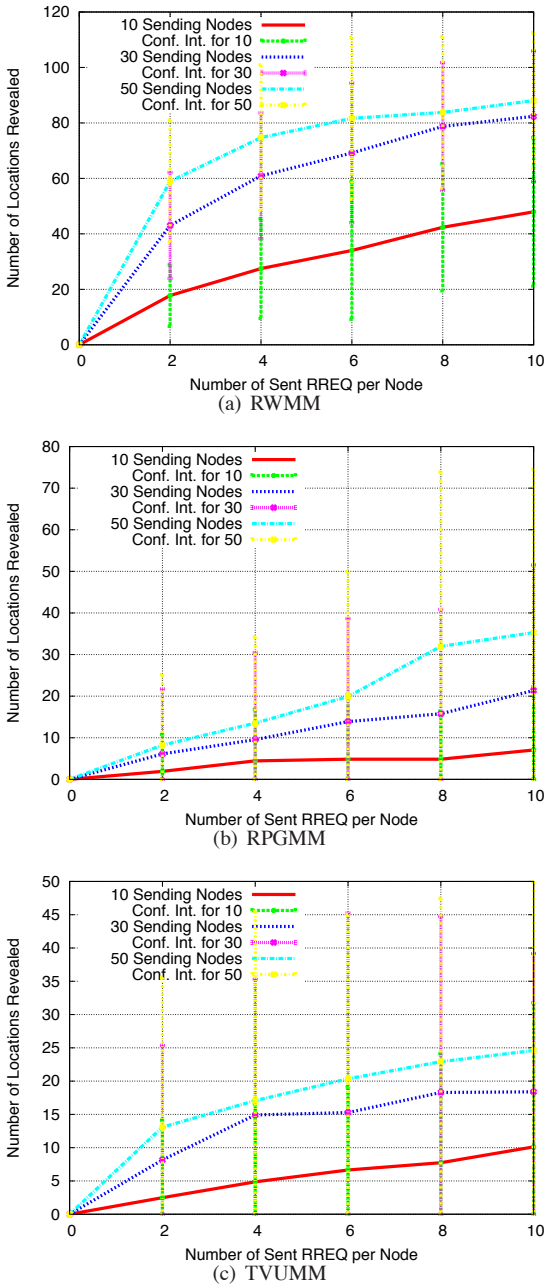


Fig. 6. Network Topology Leakage in PRISM

for low number of nodes (less than 40) the number of RREP is higher than that under RWMM. This is because in RPGMM and TVUMM nodes are more likely to be closer together in the area so a RREQ that hits is more likely to get several RREP. Note that considering the confidence intervals of the results of different mobility models, RPGMM and TVUMM have wider intervals for larger networks while RWMM has smaller intervals. This is due to the uniform distribution of nodes in the area under RWMM.

3) Storage of Logs Required by PRISM: Each node logs all unique RREQ and RREP messages that it hears. Logs are later used for analysis and, as discussed in Section V-A, can be used to detect Sybil or Man-in-the-Middle attacks. To estimate log storage requirements, we consider the simulation settings above (results in Figure 5). In a 100-node MANET simulated for 10,000 sec with each node sending an RREQ every 5 sec, there are 2000 RREQ-s and each node receives fewer than 300 RREP-s. RREQ and RREP are 341 and 377 bytes, respectively. Each node needs about 795 Kbytes of log storage. For longer deployments, e.g., 10 days, 690 Mbytes would be required. Considering that today's handheld devices and laptops normally have many Gigabytes of storage, PRISM logs can be easily accommodated.

4) Topology Leakage in PRISM: We compare the fraction of network topology that is revealed in PRISM to that in a link-state protocol, e.g., ALARM [11]. In link-state protocols, nodes periodically flood the entire network topology. Since a passive insider obtains successive snapshots of the entire topology, it can violate node privacy by attempting to map nodes between adjacent snapshots. Whereas, in PRISM, nodes do not periodically announce their locations. A node receiving an RREQ for a destination area where it resides, can choose not to respond if it has already responded to another RREQ within a certain window of time. The longer the window, the higher the degree of node privacy, i.e., tracking-resistance. Different pockets of network topology are continuously revealed at irregular intervals. It would be very hard for a passive insider adversary to assemble them in snapshots.

To assess the degree of topology leakage to a passive insider we simulate a scenario varying the number of nodes (out of 100) that generate RREQ-s. At the beginning of the simulation, each node generates a certain number of RREQ-s (depicted on the x-axis) to random destination areas. Nodes send these RREQs, or forward those of others, while moving according to the mobility model. The y-axis shows the number of destination locations that are revealed as a result. The results in Figure 6 show that more of the topology is exposed on average when nodes move according to RWMM. We see that in all cases when 10% or less of the nodes send at most 10 RREQ, less than 50% of the topology will be revealed (and less than 10% in RPGMM and TVUMM). When the fraction of nodes generating RREQs increases to half of the nodes, up to 80% of the topology will be revealed in the RWMM case, but less than 40% and 25% in RPGMM and TVUMM respectively.

VI. Related Work

The most relevant body of MANET research tackles secure anonymous reactive MANET routing, e.g., SPAAR [18], AO2P [19], ASR [20], MASK [21], ANODR [22], D-ANODR [23], ARM [24], ASRP [25] and ODAR [26]. A survey comparing ANODR, ASR and discussing general anonymity and security issues in MANET routing protocols can be found in [27]. Of the anonymous reactive protocols, SPAAR [18] and AO2P [19] require on-line location servers. ASR [20] and ARM [24] assume that each authorized source-destination pair pre-shares a unique secret key. AnonDSR [28], ASRP [25], EARP [29] and ARMR [30] assume that each source-destination pair shares some secret information, which could be the public key of the destination or a secret key. ANODR [22] assumes that the source shares some secret with the destination for the construction of a trapdoor, for example the destination's TESLA [31] secret key. SDAR [32] assumes that the source knows the public key of the destination, obtained

from a certification authority (CA), and ODAR [26] requires an on-line public key distribution server. MASK [21] and D-ANODR [23] contain the final destination in the clear in each RREQ message. AMRSS [33] and ARMR [30] utilize multiple paths for routing. AMRSS [33] assumes that the entire network shares a pair of public private keys and that the destination ID will be encrypted under the public key. AMRSS also includes the entire path encrypted under the network key in each data message. In addition, all aforementioned protocols assume that nodes know long-term identities of all other nodes, i.e., the communication paradigm is identity-centric.

PRISM is fundamentally different from all prior anonymous on-demand MANET routing protocols on two accounts: (1) PRISM uses a location-centric, instead of an identity-centric, communication paradigm. Therefore, it does not assume any knowledge of long-term node identifiers or public keys. (2) PRISM requires neither pre-distributed pairwise shared secrets nor on-line servers of any kind. As an on-demand protocol, PRISM is also very different from the protocol in [11] (ALARM), even though the latter uses group signatures and is also location-centric. ALARM is a link-state protocol and exposes the entire topology to all insiders.

VII. Conclusion

This paper presents the PRISM protocol which supports anonymous reactive routing in suspicious location-based MANETs. It relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. It works with any group signature scheme and any location-based forwarding mechanism. We evaluate its routing overhead and show that it can outperform anonymous link-state based approaches under certain traffic patterns. We also evaluate PRISM's tracking-resistance by comparing its degree of topology exposure to link-state based approaches. PRISM reveals less of the topology and is thus more privacy-friendly.

References

[1] B. Hartzog and T. Brown, "Wimax- potential commercial off-the-shelf solution for tactical mobile mesh communications," *Milcom*, 2006.

[2] "RFC1677-Tactical Radio Frequency Communication Requirements for IPn," http://www.faqs.org/rfcs/rfc1677.html.

[3] L. Kissner and D. Song, "Privacy-preserving set operations," *CRYPTO*, 2005.

[4] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 2, pp. 1187–1192 Vol. 2, March 2005.

[5] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90–100.

[6] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," 2001, pp. 62–68. [Online]. Available: http://dx.doi.org/10.1109/INMIC.2001.995315

[7] D. B. Johnson, D. A. Maltz, and J. Broch, "Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in *In Ad Hoc Networking*. Addison-Wesley, 2001, pp. 139–172.

[8] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. CCS 2004*. ACM Press, 2004, pp. 168–177.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[10] S. Canard and M. Girault, "Implementing group signature schemes with smart cards," in *CARDIS'02: Proc. 5th conference on Smart Card Research and Advanced Application Conference*. Berkeley, CA, USA: USENIX Association, 2002, pp. 1–1.

[11] K. El Defrawy and G. Tsudik, "Alarm: Anonymous location-aided routing in suspicious manets," *IEEE ICNP 2007*, pp. 304–313, Oct. 2007.

[12] "Simpy simulator," http://simpy.sourceforge.net/.

[13] "NumPy and SciPy packages," http://numpy.scipy.org/.

[14] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, pp. 483–502, 2002.

[15] X. Hong, M. Gerla, G. Pei, and C. Chinag, "A group mobility model for ad hoc wireless networks," *ACM/IEEE MSWiM*, 1999.

[16] W. jen Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling time-variant user mobility in wireless mobile networks," May 2007, pp. 758–766.

[17] N. S. Fan Bai and A. Helmy, "Important: A framework to systematically analyze the impact of mobility on performance of routing protocols for adhoc networks," in *INFOCOM*, 2003.

[18] S. Carter and A. Yasinsac, "Secure position aided ad hoc routing," *Proc. IASTED International Conference on Communications and Computer Networks (CCN02)*, pp. 329–334, 2002.

[19] X. Wu and B. Bhargava, "Ao2p: ad hoc on-demand position-based private routing protocol," *IEEE Trans. Mobile Computing*, vol. 4, no. 4, pp. 335–348, July-Aug. 2005.

[20] B. Zhu, Z. Wan, M. Kankanhalli, F. Bao, and R. Deng, "Anonymous secure routing in mobile ad-hoc networks," *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, pp. 102–108, Nov. 2004.

[21] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Mask: anonymous on-demand routing in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2376–2385, September 2006.

[22] J. Kong and X. Hong, "Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in *ACM MobiHoc '03*. New York, NY, USA: ACM, 2003, pp. 291–302.

[23] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," *Securecomm and Workshops, 2006*, pp. 1–10, 28 2006-Sept. 1 2006.

[24] S. Seys and B. Preneel, "Arm: anonymous routing protocol for mobile ad hoc networks," *Int. J. Wire. Mob. Comput.*, vol. 3, no. 3, pp. 145–155, 2009.

[25] Y. Cheng and D. Agrawal, "Distributed anonymous secure routing protocol in wireless mobile ad hoc networks," *OPNETWORK*, 2005.

[26] D. Sy, R. Chen, and L. Bao, "Odar: On-demand anonymous routing in ad hoc networks," *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on*, pp. 267–276, Oct. 2006.

[27] E. Kumari and A. Kannammal, "Privacy and security on anonymous routing protocols in manet," in *Computer and Electrical Engineering, 2009. ICCEE '09. Second International Conference on*, vol. 2, 28-30 2009, pp. 431–435.

[28] R. Song, L. Korba, and G. Yee, "Anondsr: efficient anonymous dynamic source routing for mobile ad-hoc networks," in *SASN '05*. New York, NY, USA: ACM, 2005, pp. 33–42.

[29] H. L. J. M. Xiaoqing Li and W. Zhang, "An efficient anonymous routing protocol for mobile ad hoc networks," in *IAS*, 2009, pp. 287–290.

[30] Y. Dong, T. W. Chim, V. O. K. Li, S. M. Yiu, and C. K. Hui, "Armr: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1536–1550, 2009.

[31] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, p. 2002, 2002.

[32] A. Boukerche and K. E.-K. et al., "An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks," *Elsevier Computer Communications*, 2005.

[33] S. Chen and M. Wu, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks," in *Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on*, vol. 1, 13-14 2010, pp. 582–585.

Karim El Defrawy obtained a Ph.D. in Networked Systems from the Bren School of Information and Computer Science (ICS) at the University of California in Irvine (UCI) in 2010. He holds an M.Sc. in Networked Systems from UCI (2008), an M.Sc. and B.Sc. in Electrical Engineering from Cairo University in Egypt (2006 and 2003). His research interests include: security and privacy in wireless networks, in peer-to-peer networks, mitigating large-scale attacks on the Internet and applied cryptography.

Gene Tsudik is a "Lois and Peter Griffin" Professor of Computer Science at the University of California, Irvine (UCI). He obtained his PhD in Computer Science from USC in 1991 for research on firewalls and Internet access control. Before coming to UCI in 2000, he was a Project Leader at IBM Zurich Research Laboratory (1991-1996) and USC Information Science Institute (1996-2000). Over the years, his research interests included: routing, firewalls, authentication, mobile networks, secure e-commerce, anonymity ad privacy, group communication, digital signatures, key management, mobile ad hoc networks, as well as database privacy and secure storage. He currently serves as Director of Secure Computing and Networking Center (SCONCE) and Vice-Chair of the Computer Science Department. In 2007, he was on sabbatical at the University of Rome as a Fulbright Senior Scholar. Since 2009, he is the Editor-in-Chief of ACM Transactions on Information and Systems Security (TISSEC).