ALARM: Anonymous Location-Aided Routing in Suspicious MANETs

Karim El Defrawy and Gene Tsudik
School of Information and Computer Science
University of California, Irvine
keldefra,gts@uci.edu

***Abstract*— In many traditional mobile network scenarios, nodes establish communication on the basis of persistent public identities. However, in some hostile and suspicious MANET settings, node identities must not be exposed and node movements must be untraceable. Instead, nodes need to communicate on the basis of nothing more than their current locations. In this paper, we address some interesting issues arising in such MANETs by designing an anonymous routing framework (ALARM). It uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and untraceability (tracking-resistance). It also offers resistance to certain insider attacks.**

I. Introduction

In the last 10-15 years, research in various aspects of mobile ad-hoc networks (MANETS) has been very active, motivated mainly by allegedly important and numerous applications in law enforcement, military and emergency response scenarios. More recently, location information has become increasingly available through small and inexpensive GPS receivers. There is also an emerging trend to incorporate location-sensing into personal handheld devices [1]. Combining ad hoc networking with location information facilitates some appealing new applications, such as location-based advertising and focused dissemination of critical information.

If node location information is sufficiently granular, a physical map of a MANET can be constructed and node locations, instead of node identities, can be used in place of network addresses. In fact, in some application settings, such as law enforcement and search-and-rescue, node identities might not be nearly as important as node locations. In addition, if the operating environment is *hostile*, node identities must not be revealed. We use the term "hostile" to mean that communication is being monitored by adversarial entities which are not part of the MANET. Going a step further, if we assume that the MANET nodes do not even trust each other, perhaps because of possible node compromise (i.e., the environment is "suspicious"), the need to hide node identities becomes more pressing. Moreover, in a suspicious MANET environment, it is natural to require that node movements be obscured, such that tracking a given node (even without knowing its identity) is impossible or, at least, very difficult. While we do not claim that such suspicious and hostile MANET environments are (or will be) common, they do occur in military and law enforcement domains.

In this paper [1] we consider what it takes to provide secure communication in hostile and suspicious MANETs. To this end, we construct a framework for Anonymous Location-Aided Routing in MANETs (ALARM) which demonstrates the feasibility of obtaining, at the same time, both strong privacy and strong security properties. By privacy properties we mean node anonymity and resistance to tracking. Whereas, security properties include node/origin authentication and location integrity. Though it might seem that our security and privacy properties contradict each other, we show that some advanced – yet practical – cryptographic techniques can be used to reconcile them.

The rest of the paper is organized as follows: We first start by motivating the need for such a routing scheme in section II; we then describe the related work in section III. We describe the details of the framework in section IV and analyze its security in section V. We present simulation results in section VI and conclude the paper with a discussion of remaining issues and future work in sections VII and VIII.

II. Location as both Address and Identity

We envision a MANET setting with salient features and requirements as follows:

> [LOCATION] Universal availability of location information: each MANET node is equipped with a device capable of obtaining positioning information, e.g., GPS.

[1]This research was supported in part by an award from the US Army Research Office (ARO) under contract W911NF0410280. The second author was also supported in part by the Fulbright Foundation.

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

[MOBILITY] Sufficiently high mobility: a certain minimum fraction (or number) of MANET nodes moves periodically such that tracking a given node (which moved) from one topology snapshot to the next is contingent upon distinguishing it among all nodes that have moved in the interim.

[PRIVACY] No public node identities or addresses: each MANET node is anonymous, i.e., its occurrences at different locations cannot be linked (we elaborate on this below).

[SECURITY] Resistance to passive and active attacks stemming from both outsiders and malicious (e.g., compromised) insider nodes.

The main distinguishing feature of the envisaged MANET environment is the communication paradigm based not on permanent or semi-permanent identities, addresses or pseudonyms, but on instantaneous node location. In other words, a node A decides to communicate to another node B, depending only on where B is at the present time.

More generally, we anticipate that the MANET type considered in this paper would be encountered in a law enforcement, disaster recovery or military environment. Such critical settings have some characteristics in common. First, node location is very important – knowledge of the physical (as opposed to logical or relative) topology makes it possible to avoid wasteful communication and to focus on areas (nodes) that are positioned within, or at, a specific area. (Thus, the emphasis is not on the long-term node identity but rather on current node location.) Second, critical environments are susceptible to security and privacy attacks. Attacks on security aim to distribute false routing information or impede propagation of genuine routing information. Whereas, attacks on privacy aim to track nodes as they move.

As we discuss below, some geographical routing protocols have been proposed in the literature. Likewise, a number of secure and/or anonymous routing techniques have been constructed. However, none of them – and no straight-forward combination thereof – can effectively address both privacy and security requirements. We argue that existing routing (even secure or anonymous routing) approaches are unsuitable for the MANET type we are focusing on in this paper.

MANET routing protocols can be roughly partitioned into two groups: reactive (or on-demand) and proactive. The latter can be further broken down into link state and distance vector (including path vector) protocols.

We first consider reactive routing protocols such as AODV [20] and DSR [19]. In a typical reactive protocol the route discovery phase usually starts with a request by the source node to find a route to a certain destination node. Since the topology is unknown, the request is flooded throughout the network. Anyone (e.g., a passive adversary) observing a route request would infer that communication will be established between the source and the destination specified in the request. Also, the entire notion of discovering the destination node is premised on the source *knowing* the persistent identity or address of the destination. This premise is totally invalid in our MANET scenario since the destination is selected based on its location. This brings us to a contradiction: since the destination is selected based on its current location, how can a route be discovered before its location is known to the source?

One naïve approach is to perform route discovery opportunistically, i.e., the source can specify the destination location and hope that some node is indeed there. This would result in a waste of resources for route discoveries that end up being unsuccessful. All in all, since our MANET scenario involves no persistent node identifiers and since nodes are referred to by their current location, a reactive routing protocol is not suitable. Geo-casting routing protocols, such as [2], are similarly opportunistic since they attempt to deliver messages to a certain geo-cast region without any certainty of any nodes being within that region.

We can also try adapting a distance vector (DV) protocol [21] to our MANET setting. Recall that, in a DV protocol, every node maintains a table where each entry corresponds to a given destination, the cost (e.g., in hops) of, and the next hop for, getting there. This is fundamentally unsuitable for our purposes, for two reasons. First, since nodes have no persistent identities, there is no basis upon which to create DV table entries. Of course, we could base table entries upon each node's current location, but that would require that for the table to be pruned periodically since some nodes will always change their locations for each update interval. Second, the security would be quite weak: a single compromised MANET node could easily create fraudulent phantom node-location entries and propagate to the entire MANET thus "poisoning" everyone's DV tables. (Plus, DV protocols suffer from slow convergence which can be problematic in highly-mobile MANETs). The second issue can be addressed, in principle, by using a path vector protocol (e.g., BGP [38]) along with some security enhancements such as BGP-SEC [39] where each Source-Destination path component is signed. However, the expense of verifying $O(n * r)$ signatures (where n is the number of nodes an r is the network diameter) would be prohibitively expensive.

Another alternative is a link state (LS) routing protocol such as OLSR [40]. However, if the frequency of node movement is higher than the frequency of

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

communication, an LS protocol consumes much more bandwidth and power (due to frequent LS updates) than an opportunistic reactive protocol. If the opposite is true (i.e., communication frequency is higher than movement frequency), an LS protocol might be viable. An additional advantage of the link state approach is that, unlike its reactive counterpart, it obviates the need for route discovery and is thus faster. This makes it appropriate for real-time applications that impose strict delay constraints. On the other hand, LS protocols have the disadvantage of poor scalability due to excessive broadcasting – n LS updates flooded throughout the network for each update period. However, since our goal is to accommodate relatively modest-sized MANETs – on the order of tens or several hundred nodes – the poor scalability of the LS approach is not a major issue. Furthermore, link state allows us to achieve strong security since origin authentication and integrity of LS updates can be easily supported. There are a number of well-known proposals, e.g., [35] and [36], [37]. The main challenge arises from the need to reconcile security and privacy (anonymity and untraceability) features which we address below.

Based on the above discussion, we consider the link state approach to be the most amenable to supporting location-based routing with privacy and security features as described in Section I.

III. Related Work

Routing in MANETS has attracted a lot of attention from the networking and security research community. There are numerous proposals for secure on-demand routing, such as SRDP [3], Ariadne [4], SEAD [5], endairA [6] and [7]. They focus mainly on securing route discovery and route maintenance against node impersonation, as well as modification and fabrication of routing information. A comprehensive survey of secure on demand ad-hoc routing techniques can be found in [8] and [9]. We note that they do not consider node privacy and anonymity.

Other research results have yielded anonymous on-demand routing protocols, such as SPAAR [10], ASR [11], MASK [12], ANODR [13], D-ANODR [14], ARM [15] and ODAR [16]. These protocols use pseudonyms for node identification and addressing but none of them utilizes location information for routing. Location-based routing protocols mainly focus on improving the performance of the routing protocol and minimizing overhead by utilizing location information to deliver routing control messages in MANETs without flooding the whole network. Some notable techniques include [2], [17] and [18]. To the best of our knowledge, there have been no proposals for location-based proactive routing protocols that preserve node anonymity and privacy.

IV. The ALARM Framework

In this section we discuss the proposed ALARM framework. First, we state some assumptions. Then, we provide an overview of group signatures and describe in detail how to use group signatures – coupled with location information – to design an anonymous location-based routing scheme.

A. Assumptions

In addition to the requirements in section II, ALARM involves the following assumptions:

[LOCATION] as stated in Section II, each MANET node can securely and reliably obtain its present position, most likely via GPS.

[TIME] all MANET nodes maintain loosely synchronized clocks. This is easily obtainable with GPS.

[RANGE] all nodes have uniform transmission range. Once a node knows the current MANET map, it can easily determine node connectivity (i.e., transform a map into a graph).[2]

[MOBILITY] at least K nodes move at roughly the same time, i.e., within a certain fixed time period.

B. Group Signatures

Group signatures can be viewed as traditional public key signatures with additional privacy features. In a group signature scheme, any member of a potentially large and dynamic group 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. However, given two valid group signatures it is computationally infeasible to decide whether they are generated by the same (or different) group members. However, if a dispute arises over a group signature, a special entity called a Group Manager can force open a group signature and identify the actual signer. This important feature is referred to as *Escrowed Anonymity*.

Based on the above, it seems that group signatures are a perfect fit for our envisaged MANET setting. A mobile node can periodically sign its current location (link state) information without any fear of being tracked, since multiple group signatures are not linkable. At the same

[2] If transmission range is not uniform, each node should include its transmission range in its location announcement message. This would only add an extra field to the location announcement message and would not affect other details of the framework.

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

time, anyone can verify a group signature and thus be assured that the signer is a legitimate MANET node.

Group signatures were first introduced by Chaum and Van Hejst [22] and a number of schemes (e.g., [23], [24], [26]) varying in assumptions, complexity and features have been proposed since. A group signature scheme has the following basic participants:

- Group Manager (GM): entity responsible for administering the group: initializing the group and handling member joins and leaves (revocations). It is also responsible for de-anonymizing a signature in case of a dispute. Sometimes the task of adding new members is given to a separate entity called a Membership Manager. Similarly, revocation duties are sometimes delegated to a separate Revocation Manager. In this paper, for simplicity's sake, we use a unified GM for all of these tasks.
- Group Members: users/entities that represent the current set of authorized signers. In our case, a signer/member is a legitimate MANET node. Each member must have a unique private key that allows it to sign on behalf of the group. (The group public key is common to the whole group).
- Outsiders: any other user/entity external to the group. Outsiders are assumed to possess the group public key and are thus able to verify group signatures.

Each group member must have a secret long-term identity which is tied to the group and to the member's unique private key. However, only the GM knows the relationship between the group members and their long-term identities.

A group signature scheme consists of the following components:

- SETUP: A probabilistic polynomial-time algorithm, run by the GM, that outputs a cryptographic specification for the group, including the group manager's public and private keys.
- JOIN: A protocol between the GM and a new user that results in the user becoming a group member. The output of this protocol includes some private output for the user – her secret membership key.
- SIGN: An algorithm, executed by any group member, that, on input of: a message, a group public key and a member's private input, outputs a group signature.
- VERIFY: An algorithm, run by anyone, which, on input of: a message, a group public key and a group signature, outputs a binary flag indicating the validity of the said group signature.
- OPEN: An algorithm, run by the GM, that on input of: a message, a group signature, a group public key and a group manager's secret key, verifies whether the group signature is valid and returns the signer's group identity and some proof that allows anyone to verify the group identity of the actual signer. It may also return no answer which assumes to mean that the group manager is the signer.
- REVOKE: An algorithm, performed by the GM, to remove (revoke) a user from the group. It results in a new group public key and/or a set of auxiliary information aimed at either signers or verifiers.

Some recently proposed group signature schemes require less than 10 exponentiations to sign [25]. Though still appreciably more expensive than regular signatures, group signatures are rapidly becoming practical. We also point out that, in MANETs, unlike in sensor networks, computation is not a particularly scarce commodity; thus, the cost of 10 exponentiations per group signature is quite reasonable.

C. ALARM: Anonymous Location-Aided Routing

We require an off-line group manager (GM) that initializes the underlying group signature scheme and enrolls all legitimate MANET nodes as group members. (This is done well before MANET deployment.) In case of a dispute, the GM is responsible for opening the contested group signature and determining the signer. Depending on the specific group signature scheme, the GM may also have to handle future joins for new members as well as revocation of existing members. However, we claim that in most envisaged MANET scenarios, membership is likely to be fixed, i.e., all joins can be done in bulk, a priori. Also, revocation might not be feasible since it would require propagating – in real-time – updated revocation information to all legitimate MANET nodes. (However, if dynamic membership is necessary, our scheme is capable of supporting it, with minor additional assumptions.)

The basic operation of ALARM is as follows:

- Time is divided into time slots of duration T. At the beginning of every slot, each node broadcasts a message containing: its location (GPS coordinates), time-stamp, temporary public key and a group signature computed over these fields. We call this a **Location Announcement Message (LAM)**. Each LAM is flooded throughout the MANET. Figure 1 shows the LAM format used to construct the network topology snapshot in Figure 2.
- In the period between successive LAM-s, a node can be reached using a pseudonym which is set to the group signature in its last LAM. (Assuming, of course, that the signature is valid.) Each node that receives a LAM, first verifies the group signature.

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

If the signature is valid, the node broadcasts the message to its neighbors unless it has previously received the same message. Having collected all current LAM-s, each node can easily construct a geographical map and a connectivity graph of the MANET.

- If a node needs to communicate to a certain location, it first checks to see if there is a node at (or near) that location. If so, it sends a message to the destination pseudonym (determined by the group signature in the last LAM corresponding to that location). The message is encrypted with the public key included in the same LAM. We do not restrict our scheme to a particular cryptographic mechanism. One obvious choice is to use Diffie-Hellman (DH) [41] whereby each LAM includes an ephemeral (period-specific) DH half-key. The sender then simply generates its own DH half-key, computes a shared key and uses it to encrypt the message. (Clearly, the sender's half-key must be included in the clear part of the message). An alternative is to use RSA or ElGamal.

Using group signatures offers a number of benefits. First, each node can check if the received LAM is originated by a legitimate MANET node. Second, no two nodes will have the same pseudonym even if they are at the same location (since group signatures cannot collide). Third, pseudonyms are unlinkable since it is infeasible to determine whether two or more signatures are produced by the same signer. The use of time-stamps prevents replay attacks.

An additional feature that can be added to some group signature schemes is called *self-distinction*. It allows nodes to detect if a malicious insider (a MANET node) launches a so-called Sybil attack [33] by assuming several pseudonyms and pretending to be at several locations at the same time. At the first glance, the self-distinction feature seems to contradict with what group signature schemes try to achieve, i.e., anonymity and unlinkability. However, self-distinction implies that each node can only assume *one* anonymous identity within the group for a given time-slot. Thus, the privacy of each node *across multiple time-slots* is preserved, even with self-distinction. Tsudik and Xu [34] demonstrate a construction that has this additional functionality based on a specific group signature scheme. Another example appears in [42].

The intuition behind these constructions is that each node generating a group signature needs to prove that it is distinct from others. This is achieved by having nodes agree on a common parameter (e.g., a common random number). This parameter is varied in each round of signing (in each time-slot, in our case). If a node uses

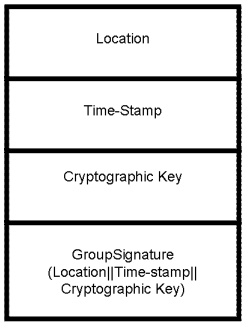

Fig. 1. LAM Format

the same parameter to sign twice within the same round, the two group signatures will be forced to have matching components which would indicate that the signer is the same. The challenge with adopting such a scheme in ALARM is how to generate this common parameter. A straightforward but inefficient mechanism would be to use a group key agreement protocol at the beginning of every time-slot. A more efficient method is to use a group key agreement protocol once, in order to agree on a common parameter. (Alternatively, the GM can generate and distribute this starting value). The concatenation of the parameter and the time-slot identifier is then hashed at the beginning of each time slot. Each hash generates a new pseudo-random value which is then used in generating a group signature.

V. Threat Model and Security Analysis

We consider two kinds of attackers: a passive insider (honest-but-curious) and an active outsider. A passive insider can only launch passive attacks, by eavesdropping on messages exchanged in the MANET. An active outsider can eavesdrop on the communication between nodes. She can also launch active attacks by injecting arbitrary messages into the network or by recording, modifying and replaying the messages sent by other nodes. We do not consider jamming and denial-of-service (DoS) attacks. Such attacks are impossible to combat at the network layer, which is the focus of this paper.

A. Passive (Honest-but-Curious) Insider

A passive insider can hear all messages exchanged within the MANET. She can determine their authenticity by verifying the group signatures. She can use this to determine the size (number of nodes) and the topology of the MANET. However, she can not identify which nodes generated what LAM-s, because it is computationally infeasible to link a group signature with a particular

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

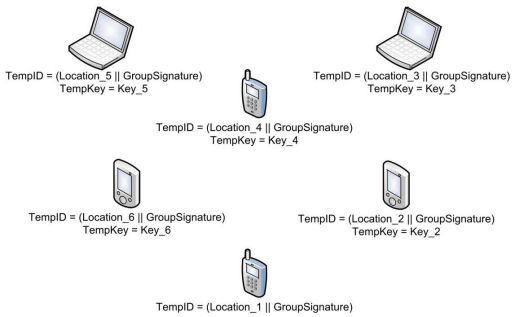

Fig. 2. Network topology constructed by LAM-s

node. A passive insider who has access to other means of collecting information (e.g., by visual means) can determine that a certain node is still at the same location. This is possible if she observes two pseudonyms in subsequent time slots mapping to the same location, and if she can visually determine that the node did not move. We are not concerned with such attacks, since they require physical counter-measures.

A passive insider can attempt to track node's movements by using trajectory information [28]. This attack can be mounted knowing the network topology, the approximate speed and trajectory of movement of a node. An attacker knowing this information can determine the moving pattern of a certain node. If the node's movement is not along straight lines and its direction is randomized, (or if K nodes move closely together and/or intersect in their paths within a certain area) then such an attack will fail. We use simulations to determine the degree of privacy afforded by ALARM when such attacks occur.

B. Active Outsider

An active outsider who only eavesdrops on LAM-s can not derive any more information than a passive insider. In fact, she might be even weaker if all LAM-s are encrypted, e.g., using some MANET-wide group key. An outsider eavesdropping on the physical layer transmission can determine if there are nodes at certain locations. Physical layer mechanisms such as CDMA could be used to hide such transmissions from unintended receivers. An active outsider can record packets and replay them. This attack is ineffective since time-stamps are included in the LAM-s. A node will not accept a LAM unless it contains the correct time-stamp of the current time slot. An active outsider can not inject new messages or adjust the location or any other field in any message, since doing so would require producing a group signature for that message.

VI. Simulation Results

ALARM preserves the privacy of nodes by preventing both insider and outsider adversaries from tracking their movement across different snapshots of the topology. To illustrate ALARM's effectiveness, we define a privacy metric referred to as *average node privacy* **(ANP)**. This metric represents the fraction of the total number of nodes (in the second snapshot) that a node could be equally likely mapped to, assuming knowledge of two subsequent topology snapshots. This is similar to the K-anonymity concept where a node's privacy is preserved by making it indistinguishable from a set of K other nodes. To calculate ANP we use the following formula between two different snapshots of the topology:

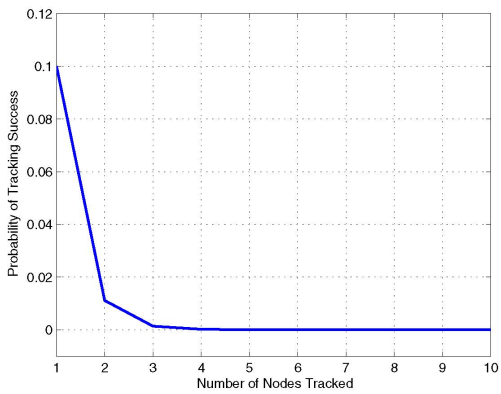

Fig. 3. Probability of successfully tracking nodes in a MANET with 10 nodes moving randomly

$$ANP = \sum_{i=o}^{i=K} (K - K_i^{'})/K^2$$

where K = Total number of nodes in the MANET, and $K_i^{'}$ = Number of nodes in the second snapshot to which node i can not be mapped to.[3]

$K_i^{'}$ depends on the underlying mobility pattern (i.e. direction and speed of movement), time between successive topology snapshots (i.e. time between two LAM-s) and size of the area within which the nodes move. For two successive snapshots of the topology, $K_i^{'}$ will include nodes outside a circle defined by x as its radius and the location of node i in the first snapshot as the center. In this case, x is the the longest possible traveling distance in the area of movement (e.g. the diagonal in the case of a square.)

ANP is highest when any node can be equally likely mapped to any of the K nodes in the second snapshot of the topology. In this case, ANP will be 1. When each node can only be mapped to one node, then we say that nodes are completely traceable and that the privacy has been violated. In this case an adversary can look at

[3]The K^2 in the denominator normalizes the metric so that it has a maximum value of 1.

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

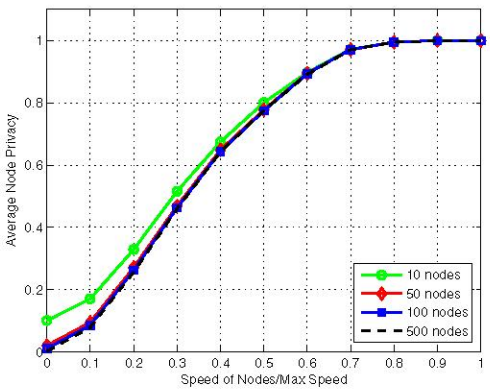

Fig. 4. The effect of the speed of nodes on ANP in a $1000m^2$ area and a max speed = $\sqrt{2*1000^2}$ m/interval between LAM-s (random walk mobility model)

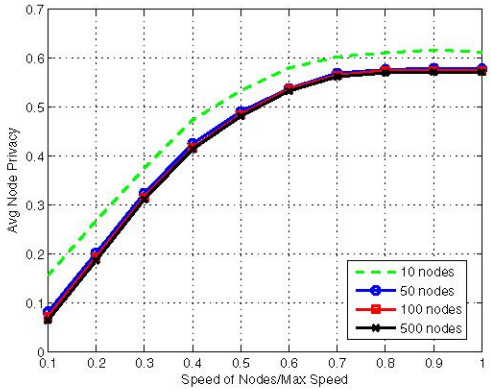

Fig. 5. Effect of node speed on ANP in $1000m^2$ area and max speed = $\sqrt{2*1000^2}$ m/interval between LAM-s (random way point mobility model)

two subsequent snapshots of the network topology and deterministically map nodes from the first snapshots to nodes in the second snapshot . The range for ANP is thus: $[\frac{1}{K}, 1]$.

If nodes move randomly inside an area (L^2), which is defined by a square of side length L, then ideally the time between snapshots should be long enough so that the slowest node can travel a distance equal to ($\sqrt{2*L^2} \approx 1.4*L$). In this case a node at a location L_1 in the first snapshot is equally likely to be at any other location L_2 in the second snapshot. An adversary that sees these two snapshots and tries to track a certain node's movement will at most be able to determine the mapping between the first snapshot and the second correctly with probability $(1/K)$ (because she is guessing randomly). If the adversary wants to track more nodes the probability of success decreases rapidly. If the adversary wants to track all (K) nodes, the probability of success will be $\frac{1}{K!}$. In general the probability of tracking i-nodes out of the (K) nodes is: $\frac{(K-i)!}{K!}$. The probability of successfully tracking several nodes by random guessing is shown in Figure 3.

Figure 4 shows the ANP under the **random walk mobility** model [32] in an area defined by a square of width ($1000m^2$). In this model, all nodes move with the same speed but choose their direction to reach as a random destination point inside the area. Once a node reaches its destination, it picks a new random destination and starts moving toward it. The number of nodes is varied between 10 and 500. The speed of the nodes is also varied between 0.1 and 1 of the maximum speed. The maximum speed is defined as $\sqrt{2*1000^2}$ and the unit is meter per time duration between two snapshots of the network (two LAM-s). The value of *(t)* can be either a system parameter, or can depend on the speed that the nodes are capable of moving with. If nodes are vehicles, then *(t)* should be in the order of tens of seconds. If nodes are pedestrians, then *(t)* should be in the order of minutes. From Figure 4 we see that ANP exceeds 0.8 until speed drops below 0.5 of the maximum. A value of 0.8 for ANP means that a node could equally likely be mapped to 80 % of all nodes. If the number of nodes is large then this number provides an acceptable level of privacy.

Figure 5 shows the effect of reduced node speed on ANP when nodes move according to the random way-point model [32]. In this model, all nodes move with the same speed, and upon reaching a destination, a node pauses with probability 0.5 and continues to another randomly selected destination with probability 0.5. If a node pauses, it remains stationary for two inter-LAM intervals, i.e., $2*t$. The adversary examining two subsequent topology snapshots can exclude stationary nodes, i.e., those who remain at exactly the same location in both snapshots. The end-result is the reduced ANP. As can be seen from the figure, maximum achievable ANP in this mobility model is 0.6, i.e., a node can be mapped into 60% of all nodes.

Figure 6 shows simulation results using the reference point group mobility (RPGM) [43] model. In this model, nodes are divided into groups, based on some criteria. Each group has a logical center which defines the behavior of movement for the entire group ,i.e. speed, acceleration and direction. Each group member is placed randomly in the vicinity of its reference point, relative to the group center. This ensures that the relative positions of nodes inside the group change with time. In this simulation the group center randomly selects destinations inside the simulated area and pursues them. All nodes inside one group follow the group center's movement

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

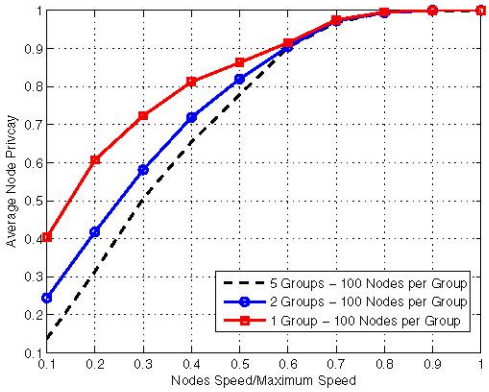

Fig. 6. Effect of node speed on ANP in $1000m^2$ area and max speed = $\sqrt{2 * 1000^2}$ m/interval between LAM-s (reference point group mobility model)

and add a random displacement to their reference point inside the group.

The result of the simulation shows that the minimum value of ANP, i.e., when the nodes move with low speed is higher than that for the case where all nodes move independently. This is because the mobility pattern guarantees that at least the nodes within the same group will be in the vicinity of each other. When the speed increases to 0.5 of the maximum, ANP is similar to the case where nodes move independently at random.

There are other mobility models common in the ad-hoc networking literature [32]. Among these, several entity mobility models exist which are essentially variations of the random walk or random way-point models. ALARM will work under any of these mobility models as long as node movement is unpredictable, e.g., caused by random events in the surrounding environment. This is often the case in military, law enforcement and rescue settings. ALARM will perform poorly, as most other location privacy schemes, in settings where an entire group of nodes moves together with relative positions of nodes remaining the same. ALARM is not designed for such settings, since limited or predictable mobility negates privacy no matter what routing protocol is used.

VII. Discussion

As described above, ALARM facilitates the dissemination of topology information by flooding LAM-s. Once each node has the whole topology view, it decides whether it wants to send a message to a certain location. Message routing is independent of the MANET topology construction. A node can explicitly embed the locations of nodes that the message should pass through (i.e., location-based source routing). Any other location aided routing algorithm, such as [29], [30] and [31], could also be used. If the MANET size increases and flooding causes significant overhead, a hierarchy could be used to limit the scope of flooding. This idea has already been utilized for geocasting in GeoGRID [29]. In GeoGRID the network is partitioned into logical grids, with a single elected node acting as a gateway for that partition. Only gateways forward packets to other gateways which limits the scope of flooding. Inside the region for which a gateway is responsible, flooding is used.

ALARM takes advantage of group signatures to preserve node anonymity while allowing authentication of location updates. There are many group signature schemes in the literature that differ widely in their security properties and efficiency features. ALARM is not restricted to any particular group signature scheme. Any secure group signature scheme can be used as long as attacks are limited to those by active outsiders and passive insiders.

However, if resistance against active malicious insiders (launching Sybil attacks) is desired, then the underlying group signature scheme must be amenable to providing the self-distinction feature discussed earlier. Thus, only certain group signature schemes can be used. Schemes that facilitate the addition of the self-distinction feature include [42] and [34].

Recent advances in group signature research have resulted in efficient schemes which have constant-size signatures and public keys. There have been proposals to implement group signatures using tamper resistant hardware. The authors in [27] show how to implement group signatures on smart cards. Implementing group signatures using smart cards provides coalition-resistance and provides easy means of revoking group members [27]. Coupling such modules with a tamper-resistant GPS device, each MANET node can easily perform what we require in ALARM. If each node is equipped with a tamper-resistant GPS module (which also includes group signature generation tools), no insider will be able to lie about its current location. Incidentally, this will prevent active insiders attempting to mount Sybil attacks by trying to appear in several places at once. Also, with tamper-resistant hardware, *any* group signature scheme can be used, i.e., we no longer need self-distinction since a node would be unable to generate more than one LAM (more than one group signature) within a given time-slot. Note that although group signature generation must take place within tamper-resistant hardware, group signature verification can be done outside. We point out that similar tamper-resistant hardware is already employed by military and law enforcement entities.

VIII. Conclusion and Future Work

In this paper, we have constructed the ALARM framework which supports anonymous location-based routing

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

in certain types of suspicious MANETS. ALARM relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations. The framework works with any group signature scheme and any location-based forwarding protocol can be used to route data between nodes. We have shown through simulation that node privacy under this framework is preserved even if a portion of the nodes are stationary, or if the speed of movement is not very high. Future work includes developing an analytical model which captures the loss in node privacy due to the dynamics of the speed and the mobility patterns of nodes inside the MANET.

REFERENCES

[1] Nokia, "Nokia 6110 Navigator," *http://europe.nokia.com/A4344146*.

[2] C. Maihofer, "A Survey of Geocast Routing Protocols," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 2, pp. 32-42, 2004.

[3] J. Kim and G. Tsudik, "SRDP: Securing Route Discovery in DSR," *The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2005)*, 2005.

[4] Y.-C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, 2002.

[5] Y.-C. Hu, D. B. Johnson and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," *Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02)*, 2002.

[6] G. Acs, L. Buttyn and I. Vajda,"Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, November 2006.

[7] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," *Proceedings of the 3rd ACM workshop on Wireless security (WiSE '02)*, 2002.

[8] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security And Privacy Magazine*, vol. 2; no. 3, pp. 28-39, 2004.

[9] P. Argyroudis and D. OMahony,"Secure Routing for Mobile Ad-Hoc Networks,"*To appear in IEEE Communications Surveys and Tutorials*.

[10] S. Carter and A. Yasinsac, "Secure Position Aided Ad Hoc Routing," *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, pp. 329-334, Nov. 4-6, 2002.

[11] B. Zhu, Z. Wan, M. Kankanhalli, F. Bao, and R. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN 2004)*, 2004.

[12] Y. Zhang, W. Liu, W. Lou and Y. Fang, "MASK: anonymous on-demand routing in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol.5, no.9, pp.2376-2385, 2006.

[13] J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks," *Proceedings of ACM MOBIHOC03*, pp. 291302, 2003.

[14] L. Yang, M. Jakobsson and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad hoc Networks," *SECURECOMM '06*, 2006.

[15] S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks," *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06)*, 2006.

[16] D. Sy, R. Chen and L. Bao, "ODAR: On-Demand Anonymous Routing in Ad Hoc Networks," *In Proceedings of The Third IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, 2006.

[17] M. Mauve, J. Widmer, and H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks," *IEEE Network Magazine*, 15(6):30–39, November 2001.

[18] F. Arajo and L. Rodrigues, "Survey on Position-Based Routing," *University of Lisbon Technical Report*, http://www.minema.di.fc.ul.pt/papers.html, Jan. 2006,.

[19] Johnson, Maltz and Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," *Internet Draft*, 2003.

[20] C. Perkins and E. Royer, "Ad hoc On-Demand Distance Vector Routing," *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999.

[21] J. Kurose and K. Ross, "Computer Networks: A Top Down Approach Featuring the Internet," *Pearson Addison Wesley*.

[22] D. Chaum and E. Van Hejst, "Group Signatures," *Advances in Cryptology EUROCRYPT '91*, D.W. Davies (Ed.), Springer-Verlag, pp. 257-265 .

[23] D. Boneh, X. Boyen and H. Shacham, "Short Group Signatures," *In proceedings of Crypto '04*, LNCS 3152, pp. 41-55, 2004.

[24] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," *In Advances in Cryptology - Crypto 2004*, Springer Verlag, 2004.

[25] J. Furukawa and H. Imai, "An Efficient Group Signature Scheme from Bilinear Maps," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Volume E89-A , Issue 5, Pages: 1328-1338, May 2005.

[26] X. Ding, G. Tsudik and S. Xu,"Leak-Free Group Signatures with Immediate Revocation," *24th IEEE International Conference on Distributed Computing Systems (ICDCS'04)*, pp. 608-615, 2004.

[27] S. Canard and M. Girault, "Implementing Group Signature Schemes With Smart Cards," *In the joint IFIP/USENIX International Conference on Smart Card Research and Advanced Applications (CARDIS'02)*, 2002.

[28] L. Huang and H. Yamaneet, "Enhancing wireless location privacy using silent period," *5th Workshop on Privacy Enhancing Technologies*, 2005.

[29] W.-H. Liao, Y.-C. Tseng, K.-L. Lo, and J.-P. Sheu, "GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID," *Journal of Internet Technology*, vol. 1, no. 2, pp. 23-32, 2000.

[30] I. Stojmenovic, A. Ruhil and D. Lobiyal, "Voronoi diagram and convex hull based geocasting and routing in wireless networks," *Proceedings of Eighth IEEE International Symposium on Computers and Communication (ISCC 2003)*, vol. 1, pp. 51-56, 2003.

[31] Y.-B. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad-Hoc Networks," *IEEE/ACM Wireless Networks*, Volume 6 , Issue 4, Pages: 307-321, July 2000.

[32] T. Camp, J. Boleng and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing*, vol. 2, pp. 483-502, 2002.

[33] J. R. Douceur, "The Sybil Attack," *First International Workshop on Peer-to-Peer Systems (IPTPS 02)*, 2002.

[34] G. Tsudik and S. Xu, "A Flexible Framework for Secret Handshakes," *ACM Conference on Principles of Distributed Computing (PODC'05)*, August 2005.

[35] R. Perlman, "Network Layer Protocols with Byzantine Robustness," *Ph.D. Dissertation*, MIT LCS TR-429, October 1988.

[36] S. Murphy and M. Badger, "Digital Signature Protection of the OSPF Routing Protocol," *ISOC Symposium on Network and Distributed Systems Security*, 1996.

[37] S. Murphy, M. Badger and B. Wellington, "OSPF with Digital Signatures," *INTERNET RFC 2154*, June 1997.

[38] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)," *INTERNET RFC 1771*, March 1995.

[39] K. Butler, T. Farley, P. McDaniel and J. Rexford, "A Survey of BGP Security Issues and Solutions," *Technical Report TD-5UGJ33, AT&T Labs - Research*, Florham Park, NJ, 2004.

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.

[40] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," *INTERNET RFC 3626*, October 2003.
[41] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Volume 22, Issue 6, Pages 644-654, 1976.
[42] G. Ateniese and G. Tsudik, "Some Open Issues and New Directions in Group Signatures," *Proceedings of the Third International Conference on Financial Cryptography*, 1999.
[43] X. Hong, M. Gerla, G. Pei and Ch.-Ch. Chinag, "A Group Mobility Model for Ad Hoc Wireless Networks," *ACM/IEEE MSWiM*, 1999.

Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on November 13, 2008 at 16:41 from IEEE Xplore. Restrictions apply.