Mobile Traffic Sensor Network versus Motion-MIX: Tracing and Protecting Mobile Wireless Nodes [*]

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

[*]Dept. of Computer Science
University of California
Los Angeles, CA 90095

[†]Dept. of Electric & Computer Eng.
University of Florida
Gainesville, FL 32611

[‡]Dept. of Computer Science
University of Alabama
Tuscaloosa, AL 35487

{jkong,gerla}@cs.ucla.edu, wu@ece.ufl.edu, hxy@cs.ua.edu

ABSTRACT

In this paper we focus on passive attacks that threaten the privacy of mobile wireless networks. We define the concept of "venue privacy attack" (VPA) to illustrate the emerging anonymity attacks to trace mobile wireless nodes. Then we propose "motion-MIX" as the countermeasure to defend against various venue privacy attacks. We study the necessary conditions to implement motion-MIXes. These conditions include identity-free routing, one-time packet content and various other concerns in the network protocol stack. Then we use a new asymptotic security model to verify motion-MIX's effectiveness against venue privacy attacks. In a scalable ad hoc network, we prove that the probability of security breach is negligible (aka. sub-polynomial) with respect to the polynomial-bounded network scale (i.e., number of node in the network). This notion is conforming to the existing security notions in computational cryptography, where the polynomial-bounded metric is key length.

Categories and Subject Descriptors

C.2.0 [**Computer-Commmunication Networks**]: General—*Security and protection*

General Terms

Security, Design

Keywords

Anonymity, Mobility, Motion-MIX, Identity-free Routing, ANODR

1. INTRODUCTION

The recent progress in embedded real-time system development has realized mobile traffic sensors, for example, embedded systems carried by palm-size Unmanned Aerial Vehicles (UAV, Figure 1). This has great impact on privacy design in mobile networks, which has very different semantics from the conventional notion for infrastructure networks like the Internet and distributed banking systems. Message privacy is the major concern in the latter systems, but mobility enabled by wireless communication has changed privacy issues in many ways. First, these fast moving traffic sensors are capable of tracing any wireless target moving at lower speed. The mobility of both the adversarial side and the guarding side introduces new privacy problems. In a mobile network, node's motion pattern, traffic pattern, standing venue and route-driven packet flows, and even the dynamic network topology, all become new interests of the mobile traffic sensors, bringing in new anonymity challenges in addition to conventional identity privacy and message privacy. Second, in wireless ad hoc networks mobile nodes must rely on their protocol stack (e.g., ad hoc routing) in communication. As the wireless medium is open to anyone within the transmission range, the baseline of the mobile traffic sensors is to exploit this opportunity to conduct various privacy attacks. Therefore, many anonymous routing schemes have recently been proposed to protect ad hoc networks [25][22][7][41][46]. However, it is not clear whether these anonymous schemes provide the needed protection, and whether a security model can formally measure the protection.

The contributions of this paper are of three dimensions. First, we study how mobile traffic sensors can trace mobile nodes to see their motion patterns and traffic patterns. We show several new privacy attacks, named as *venue privacy attacks* (VPA), that challenge the privacy defense system of an ad hoc network. The legitimate mobile nodes are facing a dilemma: "*loquo ergo sum* (I speak so I exist)". Either they do not communicate, say, do not participate in routing and forwarding process, thus disappear from the network, or they are susceptible to being traced by the mobile traffic sensors.

Second, in mobile wireless networks, we propose to use "*motion-MIX*", a mobile analogue of David Chaum's classic notion of message MIX [9], to protect the mobile nodes. A *Chaumian MIX* is a *private processor* that hides the relation between multiple incoming messages and multiple outgoing messages. Since the adversary cannot see the internal state of a Chaumian MIX, the MIX-ing goal in the private processor is achievable by shuffling the order of messages, using various cryptosystems to randomize the contents, and injecting truly random decoy messages (if less incoming messages arrive at the MIX processor within reasonable time). In this paper, a *motion-MIX* is a *private venue* that hides the relation between multiple incoming mobile nodes and multiple outgoing mobile nodes, where the term "venue" refers to the smallest area to which the adversary can locate the node via the node's wireless communication. We show the necessary conditions to implement a motion-MIX venue. In particular, since a nearby network member could be adversarial, a wireless routing or packet forwarding scheme must

[*]Part of the work is funded by ONR MINUTEMAN grant N00014-01-C-0016 and NSF NRT WHYNET grant ANI-0335302.

SASN'05, November 7, 2005, Alexandria, Virginia, USA.

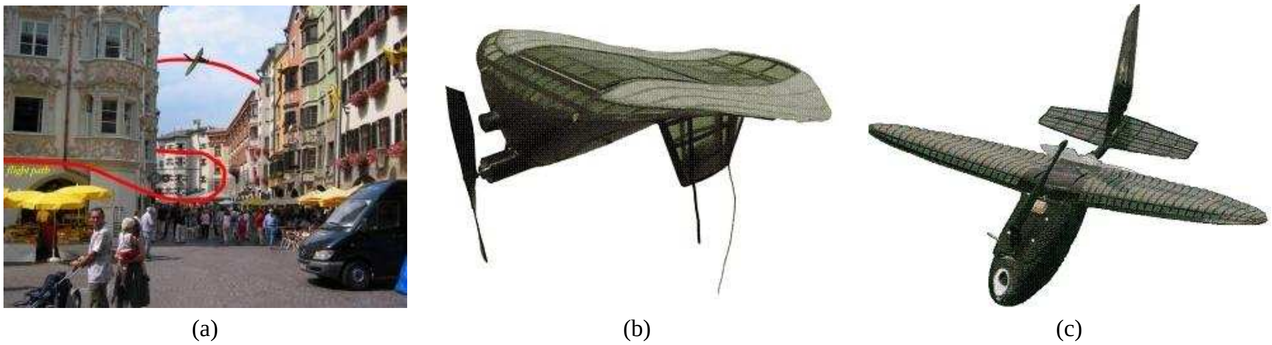

Figure 1: (a) Street patrol, (b) an MAV of 5-inch wingspan, and (c) an MAV of 24-inch wingspan.

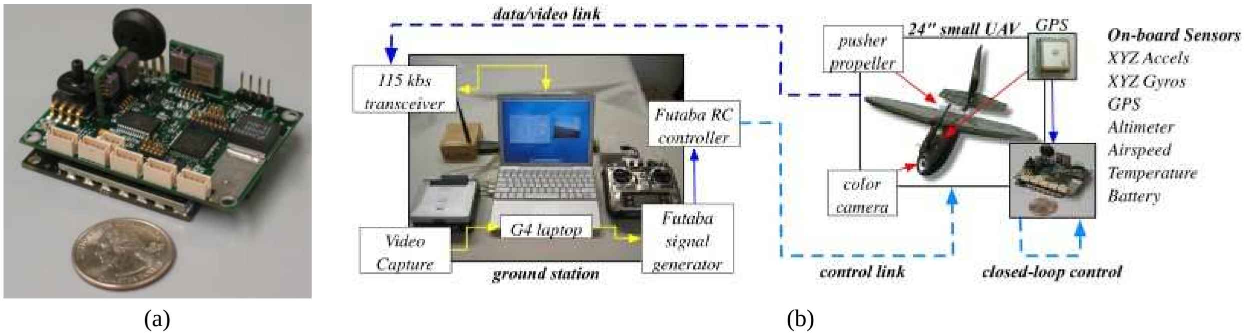

Figure 2: (a) MAV circuit board with sensors onboard, and (b) MAV testbed.

be free of any form of node identities. Moreover, in order to thwart traffic analysis, the traffic originated from the motion-MIX venue is required to be (computationally) indistinguishable from truly random traffic. Amongst several recently proposed anonymous routing schemes [25][22][7][41][46], only ANODR [25][22] satisfies these two necessary conditions.

Third, we propose "scalable network security", a new asymptotic network security model, to formally measure the anonymity protection provided in a motion-MIX venue. In our asymptotic network security model, security can be ensured by using a network metric like network scale (i.e., number of nodes in the network) to replace the role of key length in computational cryptography. We require that the probability of security breach must be negligible (aka. sub-polynomial) in regard to a polynomial-bounded network metric. Within this new network security model, a motion-MIX ensures a variant of k-anonymity [42][43] for all mobile nodes inside its venue.

The paper is organized as follows. In Section 2 we present our problem statement. It is now feasible to implement mobile traffic sensor network as the adversary, who can launch various venue privacy attacks to trace mobile nodes. Section 3 proposes the concept of "motion-MIX", differentiates the motion-MIX concept from the existing concept of "MIX-Zone" [4], and shows the necessary conditions to implement a motion-MIX. Section 4 proposes the asymptotic network security model and presents a stochastic analysis to quantify the anonymity protection provided by the motion-MIX design. In Section 5 we describe related work. Finally Section 6 concludes the paper.

2. PROBLEM STATEMENT

2.1 Mobile traffic sensor network

Recent advances in manufacturing technologies have enabled the physical realization of small, light-weight, low-power, and low-cost micro air vehicles (MAVs) [21]. These MAVs refer to a new breed of unmanned air vehicles (UAVs) or aerial robots that are significantly smaller than currently available UAVs. Typically, the dimension of MAVs is not greater than 24 inches; the smallest MAV developed as of today has a dimension of 5 inches, and development of insect-size MAVs is expected in the future. MAVs can have fixed wings or rotary wings or flapping wings like insects. These aerial robots, equipped with information sensing and transmission capabilities, extend the sphere of awareness and mobility of human beings, and allow for surveillance or exploration of environments too hazardous or remote for humans.

The MAV research group of our collaborator has established a long track record in designing, building, and test-flying autonomous vision-guided MAVs. The next-generation MAVs to be developed are expected to serve as an enabling technology for a plethora of civilian and military applications, including homeland security, reconnaissance, surveillance, tracking of terrorists/suspects, rescue and search, and highway/street patrol (see Fig. 1(a)). Figs. 1(b) and 1(c) show the MAVs developed by the research team at University of Florida. Fig. 2(a) shows the MAV circuit board with video camera, Global Positioning System (GPS) receiver, accelerometers, gyroscopes, altimeter, and airspeed sensor onboard, and Fig. 2(b) shows the MAV testbed, which has been tested through actual flight tests. The systems shown in Fig. 2 were developed by our research team.

With signal processing techniques (and other out-of-band techniques like visual perception which will not be discussed in this paper), one can use three MAVs to locate the position of a target such as a person's or a car's communication interface. Due to the small size of MAVs, the tracking of MAVs is almost unnoticed by the target being tracked.

2.2 Concepts of mobile anonymity

In existing anonymity notions proposed for fixed networks [30], anonymity protection is defined on an **anonymity set**, which is the set of all (uncompromised) network members in a distributed system or computer network. Each network member is identified by an unique ID (e.g., MAC address, IP address, or any static pseudonym). The concept of *anonymity* is defined as the state of being not identifiable within the anonymity set, and is measured by information theoretic metrics [38][14].

In fixed networks, a node's identity and its location are synonyms, that is, identifying a node's location implies the compromise of node's identity anonymity. Besides, a fixed node does not move, thus the motion pattern of the node is not a security concern.

Nevertheless, these remarks are no longer true in mobile networks. Besides identity, a mobile node's location area (i.e., a region defined by the *adversary*'s positioning capability) also demands anonymity protection [26]. For a mobile node, we define its "**venue**" as the smallest area to which the *adversary* can "pinpoint" the node only via the node's communication. Although visual information is also useful in locating a mobile node, in this paper we *only* consider wireless radio communications for the purpose of network security research. Therefore, a venue is at most the one-hop radio eavesdropping range (Figure 3). With better positioning support the adversary can reduce the one-hop circle to a smaller one quantified by the radius Δ (note that the circle can be generalized to an arbitrary geometric shape that is equal in size). We assume that Δ is *not* infinitesimal (Figure 4).

Figure 3 illustrates an adversary's eavesdropping network which is comprised of a number of eavesdropping cells. Each cell corresponds to a vertex/venue in an undirected graph $G = \langle V, E\rangle$. All possible venues form a vertex/venue set V. And neighboring relation in regard to wireless communication amongst the venues forms an edge set E. Likewise, the **venue anonymity set** is comprised of all venues, and the sender/recipient venue should not be identifiable within the new venue anonymity set given all intercepted wireless transmissions.

At each wireless traffic sensor's vertex/venue, the adversarial analyst can correlate node identities with its own exact location (obtained via its own positioning system like GPS). On one hand, the undirected graph G characterizes the capability of a collection of colluding wireless traffic analysts staying in multiple venues. On the other hand, it also characterizes the capability of a set of *mobile* traffic sensors traveling along the grid of venues to launch anonymity attacks anywhere and anytime.

2.3 Mobile anonymity attacks

In this work we consider the following passive attacks to trace mobile nodes by a set of fast mobile traffic sensors/analysts.

EXAMPLE 1. *(Motion pattern tracing attack by mobile traffic analysts) As depicted in Figure 4, after the distance and angle estimations are collected, a tri-group of adversarial nodes can use trilateration and triangulation to locate a wireless sender at the granularity of "venue". Obviously, if the adversary's mobility speed is faster than the victim, it can always follow an identifiable sender and trace its motion pattern. For instance, a simple control strategy for the tri-group of mobile sensors is to fly to the reverse direction if the receiving signal strength is diminishing. As a result, an active mobile sender is always vulnerable to the attack launched by a faster mobile adversary.* □

Additionally, in a fixed network, network topology is physically determined *a priori*. Hence there is no privacy concerns on protecting the network topology. However, in mobile wireless networks the network topology constantly changes due to mobility. If the adversary is able to acquire the fresh network topology, it then can visualize the mobile network all the time. *Privacy of network topology* becomes a new anonymity aspect in mobile networks, as demonstrated in the following examples.

EXAMPLE 2. *(Venue privacy attack: VPA) The adversary can attack the privacy of network topology by quickly scanning every venue and combining the partial results. Given any venue L depicted in Figure 3, the inside wireless traffic sensor may gather and quantify (approximate) information about local mobile nodes, for example, (VPA-a) enumerating the set of currently active nodes in L; (VPA-b) computing related metrics such as the size of the set; (VPA-c) doing traffic analysis against L, e.g., how many and what kind of connections in-and-out the venue. It is important to note that the adversary has already reached its positioning optimality according to the definition of "venue". The precise positions of different mobile nodes inside a venue are thus unknown.* □

EXAMPLE 3. *(Venue traffic analysis) It is possible to hide a node's real identity using a static pseudonym (e.g., an encrypted version of the real identity). Unfortunately, such a static pseudonym becomes another identity of the node. This pseudonymous scheme only hides what the real identity is, but not the measurements associated with the real identity. The network is at least vulnerable to the attack VPA-b and VPA-c.*

For instance, the adversary can use its own pseudonym system *to name each detected distinct node. Then its VPA-b and VPA-c attacks are unaffected even though every local node is renamed to another static pseudonym. Intuitively, given arbitrarily x (e.g., $x = 100$) locally intercepted data packets, the adversary may see the traffic pattern in regard to the 100 packets. The two extreme cases are: (1) all 100 packets were transmitted from a single node to single node, and (2) the 100 packets were transmitted from 100 distinct nodes to 100 distinct nodes. Ideally, an anonymous protocol for mobile networks must ensure that the two extreme cases and all cases in-between are equally likely to the adversary.* □

3. COUNTERMEASURE

In this section, we propose the concept of *motion-MIX* as the countermeasure. The concept of "motion-MIX" is a strict analogue of David Chaum's classic notion of message/packet "MIX" [9]. In Chaum's message MIXing, a message MIX node is a *private processor* that hides the relation between multiple incoming messages and multiple outgoing messages. In motion MIXing, a motion-MIX is a *private venue* that hides the relation between multiple incoming nodes and multiple outgoing nodes. We illustrate the difference between "motion-MIX" and a related location privacy work called "*MIX-Zones*" [4]. We also show that *identity-free routing* and *one-time packet content* are necessary conditions to realize "motion-MIX".

- In "identity-free routing", every mobile node does not reveal its own identity to other nodes. This prevents a local internal attacker from launching venue privacy attack VPA-a.
- In "one-time packet content" design, packet contents are computationally one-time. In other words, any two transmitted packets $X{\rightarrow}Y$,$X'{\rightarrow}Y'$ (i.e., packet sender's pseudonym is X or X', packet recipient's pseudonym is Y or Y') are independent in the eyes of any node who is not X, X', Y, Y', that is, it is equally likely whether $X = X'$ or $X \neq X'$, also equally likely whether $Y = Y'$ or $Y \neq Y'$. This design is needed to thwart venue privacy attack VPA-b and VPA-c.

3.1 Design assumptions

Public and finite anonymity set In this paper we always assume *public and finite anonymity sets*. This assumption is crucial in our security proofs (Theorem 4). For example, if the 32-bit IPv4 address is treated as the identity anonymity set AS_{id}, then the size of the anonymity set $|AS_{id}|$ is at most 2^{32} for the entire Internet, but

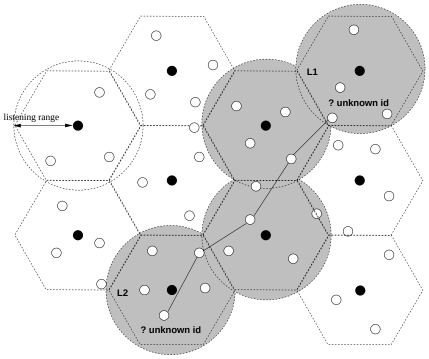

Figure 3: Underlying graph $G = \langle V, E \rangle$ (Adversarial traffic sensors are depicted as solid black nodes. A sender in venue $L1$ is communicating with a recipient in cell $L2$. Sensed active routing venues are depicted in shade)

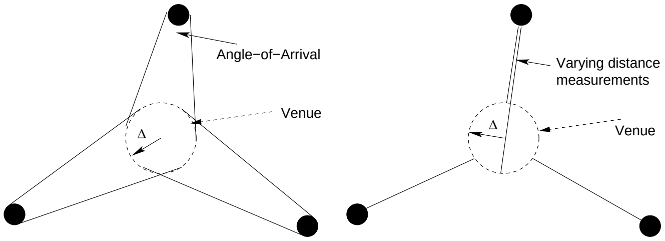

Figure 4: Imperfect wireless positioning against mobile nodes at the granularity of an area defined by radius Δ (Adversarial traffic sensors are represented by solid black nodes using directional reception or distance estimation to locate the sender of a wireless transmission)

only at most 2^8 in a wireless LAN. The *bounded* public network area is the venue anonymity set AS_{venue} that is comprised of finite amount of venues.

Internal adversary and external adversary We assume that mobile nodes can be hijacked and compromised. Once intruded, all cryptographic materials known by the victim node are revealed to the internal adversary. Nevertheless, we only assume a *honest-but-curious* adversary (i.e., it follows the protocol correctly but tries to learn as much information as possible from its execution). A dishonest adversary belongs to a different threat model and will be addressed in the future. For intact network members, the adversary is external. The external adversary is a polynomial-bounded cryptanalyst who cannot invert one-way functions or differentiate cryptographically strong pseudorandom bits from truly random bits with non-negligible probability.

Network assumption We assume a protocol stack similar to the IP protocol stack. An IOI is a wireless transmission of a link layer frame of the format:

link layer header	network layer header	transport layer header	application payload

where the transport layer header becomes part of network layer payload, and network layer header becomes part of link layer payload. In wireless ad hoc networks, it is expected that every node is a router, thus the line between the link layer and the network layer is not as clear as the one in the infrastructure networks. A link layer or network layer payload is encrypted with a per-hop key that is unique for each stop. This requires a pairwise key agreement scheme for any pair of nodes in the network. The transport layer payload is encrypted with an end-to-end session key to protect message privacy. In this paper we do not study the key agreement problem, we assume a pairwise symmetric key shared between any pair of communicating network nodes. We demand that no node identity is revealed during key agreement. Examples of anonymous key agreement are studied in ANODR [22][25] and MASK [46].

3.2 Motion-MIX

In [9], David Chaum proposed to use a network of MIX nodes to implement anonymous communication. "The purpose of a MIX is to hide the correspondences between the items in its input and those in its output." More concisely, as depicted in Figure 5 and 6, a MIX node ensures that the outgoing messages are equally likely from the incoming messages.

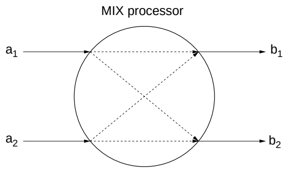

Figure 5: Chaumian MIX (a_i,b_j are messages)

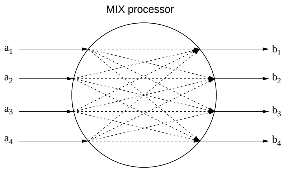

Figure 6: Chaumian MIX on batch of messages

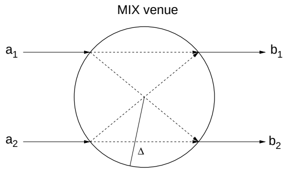

Figure 7: Motion-MIX given the venue quantifier Δ (a_i,b_j are mobile nodes)

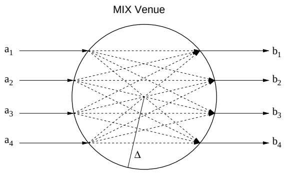

Figure 8: Motion-MIX on aggregation of mobile nodes

In mobile networks, the concept of MIX can be generalized to protect mobile (transmitting) node's motion pattern. As depicted in Figure 7 and 8, *a motion-MIX is a venue that can hide the relation between incoming mobile nodes and outgoing mobile nodes* (In the figures, the entry points and exit points of the mobile nodes a_i and b_i are merely figure-of-speech. They could be anywhere on the venue's border). The concept of "motion-MIX" is different from the existing concept of "MIX-Zone" [4] in various aspects:

- A single motion-MIX is a *strict* analogue of a single Chaumian MIX by replacing messages with mobile nodes — the adversary is incapable of seeing the internal state of a *single* (Chaumian or motion) MIX. In contrast, a MIX-Zone is *not* a strict analogue of Chaumian MIX. According to [4], a MIX-Zone only ensures that "user identity is mixed with all other users in the MIX-Zone". But it is possible that the user identities fail to mix together. In fact, the MIX-Zone literatures[4][2] seek to quantify probabilistic anonymity degradation in a *single* MIX-Zone. This is inapplicable to a single Chaumian MIX or a single motion-MIX, where perfect permutation can be implemented[1]. Motion-MIX ensures perfect identity anonymity.

On the other hand, this paper does *not* study anonymity guar-

[1] Readers who are familiar with Shannon's perfect secrecy [40] can see the similarity between Figure 6 and Shannon's depiction.

antee in a *network* of (Chaumian or Motion) MIXes. It is well-known that anonymity protection degrades in a network of Chaumian MIXes [44]. In a distributed network, only DC-net [10] can ensure perfect anonymity. The reasons are explained in [23] where DC-net is treated as an analogue of Shannon's perfect secrecy [40][2].

- A motion-MIX is defined by "venue", which is in turn defined by the adversarial side's positioning capability. On the other hand, in below we will show that the legitimate side can dynamically create a motion-MIX venue or enlarge an existing motion-MIX venue by sending decoy traffic and/or delay-tolerant communication [16] at any time. Therefore, a motion-MIX is a *dynamic* network entity that can be created and changed by both the adversarial side's behavior and the legitimate side's actions. In contrast, according to [4], MIX-Zones are *static* "geographic regions" with boundary lines. They are fixed during the network lifetime.
- A motion-MIX is proposed to protect the entire protocol stack, in particular the link layer packet forwarding and the network layer routing. It must prevent adversarial traffic sensors from seeing the link layer (MAC) address, network layer (IP) address, or any unique node identity including the application layer (user) identities. In contrast, MIX-Zone is only defined for middleware systems to protect user identities. The adversary can trace a user via the network identities/addresses of the user's mobile device.

Consequently, motion-MIX has to face the same adversary of Chaumian MIX.

Timing analysis First, timing analysis is a critical concern. In Chaumian MIX, a MIX processor should send dummy/decoy traffic to thwart the adversary's timing analysis. In the worst case, during a unit time Δt there is only one incoming message, a necessary condition to ensure k-anonymity [42] is for the MIX processor to send out $k-1$ decoy messages, which are indistinguishable from the real message. In motion-MIX, any mobile node inside a motion-MIX venue should send out decoy traffic to ensure k-anonymity where k is a pre-defined network parameter given a pre-defined time unit Δt. Otherwise, when a mobile sender must transmit all the time according to its application demand (e.g., multimedia streaming applications cannot tolerate large delay), it is thus traced by the adversary if no other node in the same motion-MIX venue is transmitting. In the worst case, during the unit time Δt there is only one node sending out one packet, a necessary condition to ensure k-anonymity is for all nodes in the motion-MIX venue to send out $k-1$ decoy packets during the same interval.

```
Algorithm D: Fully distributed decoy traffic regulation per node:
Prerequisite: Pre-defined system parameter $k$ and $\Delta t$.
Divide current unit time $\Delta t$ into $k$ slices.
FOR (each time slice $i$) DO
    IF (I have only heard $x < i$ transmissions so far
            during the current unit time interval)
        In the next time slice, transmit a decoy packet
        with probability $\frac{i-x}{i}$.
    END IF
END FOR
```

The probabilistic Algorithm D running on mobile nodes ensures that there are approximately k wireless transmissions (including decoy transmissions) in its one-hop neighborhood during the unit time interval Δt.

Moreover, in order to reduce the amount of decoy traffic, a Chaumian MIX processor can delay outgoing messages by gathering more incoming messages over a longer time interval. This idea is equally applicable to motion-MIX. In motion-MIX, any mobile node can also delay its transmissions [18][19][20] or increase its motion speed. In delay tolerant communication [16], the time interval *δt between two consecutive legitimate transmissions* is enlarged to let more mobile nodes have chance to roam into the venue.

Recall that in this paper we only study how to trace mobile nodes via wireless transmissions (visual information etc. is not assumed), and "venue" is defined as the smallest area to which the adversary can pinpoint a node via the node's transmissions.

- For a snapshot of a single transmission, the size of the smallest area Δ that the transmitter could be in is determined by the adversary's positioning capability.
- But in a mobile network, given the same area Δ, many other mobile nodes could roam into the area over time δt if we increase δt and/or the node's average motion speed v_{avg}. As depicted in Figure 9, the size of the motion-MIX venue is thus dynamically enlarged from the scale quantified by Δ to a larger scale quantified by $\Delta' \geq (\Delta + v_{avg} \cdot \delta t)$. Here the equation part is true only when all mobile nodes $(\in AS_{id})$ constantly send packets per δt. If any node sends packets at a lower rate, the inequation is true. Thus $(\Delta + v_{avg} \cdot \delta t)$ measures the worst case to break motion-MIX's protection.

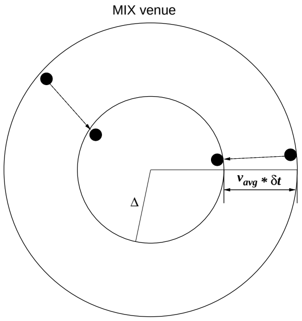

Figure 9: Dynamic motion-MIX (Δ determined by the adversary; $v_{avg} \cdot \delta t$ determined by the legitimate nodes)

Obviously, the delay tolerant approach is inapposite to time-critical applications like multimedia streaming. The speed-up approach is inapplicable to stationary sensor networks. Both the delay tolerant approach and the speed-up approach incur performance degradation in the time-critical mobile ad hoc routing, where route outage is mainly caused by node inaction and node mobility.

Content analysis Second, content analysis is another critical aspect. In Chaumian MIX, real messages processed by a MIX processor should be indistinguishable from the decoy messages (in regard to both message contents and length). And from nearby adversarial nodes' perspective, any two outgoing messages that are *not* transceived from or to the colluding adversarial nodes should also be indistinguishable (in regard to message contents and length) from each other.

As an analogue, in a motion-MIX compliant anonymous protocol, two necessary conditions must thus be satisfied:

1. A mobile node should be indistinguishable from other nodes in the same motion-MIX venue from the adversary's view. This leads to the "*identity-free routing*" design. Otherwise,

[2] If the anonymity set in DC-net is analogous to the message space in Shannon's perfect secrecy, and multi-hop packet routing/forwarding is analogous to message permutation, then DC-net is analogous to perfect secrecy [23]. As pointed out in [33], flooding is needed in such perfectly anonymous but less practical schemes. So far no analogue can be formed between a polynomial-bounded cryptanalyst and a polynomial-bounded timing-analyst. In [23] we seek to build such an analogue using hypercubes.

the (internal) adversary can launch VPA-a to distinguish a node from another by seeing the unique node identities.

2. A mobile node's traffic should be indistinguishable from another's in the same motion-MIX venue from the adversary's view. This leads to the "*one-time packet content*" design. Or the adversary can launch VPA-b and VPA-c to distinguish one node's traffic pattern from another's.

3.3 Necessary conditions

3.3.1 Identity-free routing

In "identity-free routing", every mobile node does not reveal its own identity to other nodes. This is a *necessary* condition of the success of motion-MIXing due to the internal adversary model assumed in this paper. During routing and packet forwarding process, if any mobile node reveals its identity to another node, then the node's identity anonymity is compromised because the intended receiving node could be adversarial. (1) A straight example is the foreign agent in Mobile IP [28], which is assumed to be adversarial in literatures like [1][37]. A colluding wireless access router in the mobile IP foreign domain can thus identify wireless traffic from any mobile node who reveals its network identity in the packets. (2) In wireless ad hoc networks, a node must rely on at least one of its neighbors to forward its packets. On one hand, it must forward its packets to one of its neighbors, so that the neighbor(s) can further forward the packets towards the destination. On the other hand, the node does not know whether there is an adversarial node amongst its neighbors, and if yes, which neighbor is compromised.

In wired Internet, PipeNet [12] and Onion Routing [34] employ *anonymous virtual circuit* in routing and data forwarding. Recently, ANODR [25] and MASK [46] apply the same design to wireless ad hoc networks. In these routing schemes, each forwarding node maintains a routing table with two columns of virtual circuit identifiers (VCI) in the form of '$vci_x \leftrightarrow vci_y$'. If a node receives a packet and the packet is stamped with a vci_x stored in its routing table, the node then accepts the packet, overrides the stamp with the corresponding vci_y, and sends the changed packet to next hop (the source and the destination are denoted with special VCI tags). In a nutshell, the virtual circuit based data packet forwarding scheme is practical and free of node identities.

Let's use 802.11 as an example. The original link layer frame is of the format:

dest MAC	src MAC	encrypted payload	CRC-32 checksum
48 bits	48 bits	up to 1500 bytes	32 bits

where the payload and CRC-32 checksum are encrypted with WEP/-TKiP/CCMP per hop. The link layer frame in anonymous virtual circuit reuses the same format (as we do not want to request a re-definition of IEEE standard packet formats just because of a new security demand – the re-definition is unlikely to be done in time). Only the payload part is slightly changed:

<table>
<tr><td>FF:FF:FF</td><td>FF:FF:FF</td><td>VCI || encrypted payload</td><td>CRC-32 checksum</td></tr>
<tr><td>FF:FF:FE</td><td>FF:FF:FE</td><td>up to 1500 bytes</td><td>32 bits</td></tr>
</table>

where the special MAC address FF:FF:FF:FF:FF:FE is reserved to accomplish anonymous wireless transmission (FF:FF:FF:FF:FF:FF is a special 802.11 MAC address for local broadcast). A sender can use this special address to hide its own MAC address and its one-hop receiver's MAC address [24].

Establishing virtual circuit on a multi-hop ad hoc path requires a *signaling* procedure to establish the VCI routing tables on all forwarding nodes, and the signaling procedure must be designed to be identity-free as well. In the existing anonymous virtual circuit schemes, PipeNet [12], Onion Routing [34] and MASK [46] are not identity-free in their signaling procedure, and ANODR [25] uses a global trapdoor design in its signaling process to serve the identity-free need.

Nevertheless, identity-free routing only prevents a local internal attacker from launching venue privacy attack VPA-a. As we describe below, the requirement of "one-time packet content" is needed to thwart venue privacy attack VPA-b and VPA-c.

3.3.2 One-time packet content

In "one-time packet content" design, packet contents are computationally one-time. In other words, any two transmitted packets $X \rightarrow Y$,$X' \rightarrow Y'$ (i.e., packet sender's pseudonym is X or X', packet recipient's pseudonym is Y or Y') are independent in the eyes of any node who is not X, X', Y, Y', that is, it is equally likely whether $X = X'$ or $X \neq X'$, also equally likely whether $Y = Y'$ or $Y \neq Y'$. Because two randomly generated messages are independent by definition, the one-time packet content design is feasible if the adversary cannot differentiate the two transmissions $X \rightarrow Y$,$X' \rightarrow Y'$ from two truly random transmissions.

XOR-tree [15] explores the fact that a polynomial-bounded cryptanalyst is unable to distinguish cryptographically strong pseudorandom bits from truly random bits. Similarly, this indistinguishibility approach can be applied to anonymous virtual circuit. Therefore, two communicating neighboring nodes v_a and v_b should use their agreed key material K_{ab} to generate cryptographically strong pseudorandom bits to protect their packet contents[3]. In packet forwarding and routing, this means that *every field in a link layer frame must satisfy one of the following conditions*: (1) The field is same for all frames (e.g., the redundant field FF:FF:FF:FF:FF:FE left for backward compatibility); (2) The field itself is a cryptographically strong pseudorandom bit-string; (3) The field is XOR-ed with a cryptographically strong pseudorandom bit-string; (4) In decoy frames, cryptographically strong pseudorandom bits are replaced by truly random bits.

For any third party who is not v_a and v_b, it does not know the secret seed/key and thus "sees" truly random bits. Therefore, for every uncompromised pairwise key/secret, the adversary sees that every packet transmission protected by the key/secret is indistinguishable from random traffic. This property is useful to protect the privacy of traffic pattern.

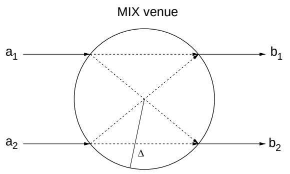

Figure 10: Traffic pattern MIXing (a_i, b_j are packet flows routing through identity-free mobile nodes inside the venue)

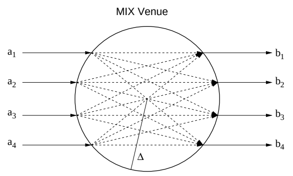

Figure 11: Traffic pattern MIXing on aggregation of packet flows

As pointed out in [33], the adversary can always trace a packet flow if the packets in the flow are not flooded in the network. Fortunately, as depicted in Figure 10 and 11, when there are multi-

[3] Anonymous per-hop key agreement between two neighboring nodes is studied in ANODR [22] and MASK [46]. Key agreement between every forwarding node and the source sender/destination recipient is studied in SDAR [7].

ple packet flows going through a motion-MIX, they are MIXed together at the venue due to the "one-time packet content" design.

3.3.3 Discussion: protocol stack issues

In the protocol stack, a transport layer packet is delivered end-to-end. It is treated as payload at the network layer. This network layer payload is encrypted with an end-to-end key, and related anonymity attacks and counter-attacks only involve the two ends. The related *end-to-end* anonymity protection includes anonymous *aliases*[37][1] and *anonymous rendezvous* [18]. This design goal is *orthogonal* to the motion-MIX design, and thus is not studied in this paper.

At the network layer, wireless packets transmitted from a motion-MIX could be of different types: control packets or data packets. For example, the IETF standard AODV [29] has following network layer packet types: RREQ, RREP, RREP-ACK, RERR and DATA, where the initial four types are control flows. In anonymous routing, a major task is to design an anonymous control flow. Amongst several recently proposed anonymous routing schemes [25][22][7] [41][46], only ANODR [25] satisfies the two necessary conditions: identity-free routing and one-time packet content. In addition, an ideal scheme [22] also requires that the following two conditions must be satisfied in regard to the packet types.

1. Any two packets, including decoy packets, of the *same packet type* must be *indistinguishable* from each other. This requires: (a) The packets of the same type must be of the same length; (b) The type field and other similar common fields of the packet type must be identical in all packets of the type; (c) For flooding packets (e.g., RREQ in AODV), the fields prepared for the other end (source/destination) are identical in one flood round, but these fields must be computationally one-time per flood; (d) All other fields are changed per hop. These fields must be computationally one-time per hop, that is, either (cryptographically strong) pseudorandom for real packets or truly random for decoy packets.
2. Any two packets of *different types* must be *independent* from the adversary's view. Control packets and data packets must not have correlation patterns that can be distinguished from truly random transmission events. For a motion-MIX, this requires the inside nodes process each type of packets independently. That is, if there are m types of packet in the network, every node must run *Algorithm D* for each packet type independently.

At the physical layer, an attacker may use more sophisticated equipment to capture different mobile nodes' radio signatures. Although the signal amplitude should not reveal anything more than a signal strength measurement, different nodes may use slightly different signal frequency due to drifted clock implementations. Typically, an error of up to 25ppm (parts per million) is tolerated in standards. For example, at 2.4GHz carrier frequency, a frequency offset of up to $\frac{2.4\times10^9\times2\times25}{10^6} = 120$kHz would be tolerated. Consequently, within a motion-MIX, a node's device should add a deliberate and random frequency offset so that two different nodes span over similar transmission frequency ranges [8].

4. NETWORK SECURITY ANALYSIS

In this section we present a new asymptotic model to quantify the security guarantee of motion-MIX in wireless ad hoc networks.

4.1 Principle of scalable network security

In modern cryptography, security is defined on the concept of "negligible", which is *asymptotically* sub-polynomial with respect to a pre-defined system parameter n. Intuitively, the parameter n is the key length.

DEFINITION 1. ***(Negligible):*** *A function $\mu : \mathbb{N} \rightarrow \mathbb{R}$ is* negligible *if for every positive integer c, and all sufficiently large n's (i.e., there exists N_c, for all $n > N_c$),*

$$\mu(n) < \frac{1}{n^c}. \qquad \square$$

When the system parameter n increases polynomially (e.g., linearly), a quantity exponentially decreasing toward 0 is negligible. For example, once a 128-bit AES encryption key is chosen, the probability of guessing the correct key is not 0, but at least $\frac{1}{2^n}$ with $n = 128$. Security can be achieved by linearly increasing the key length n. We believe that this sub-polynomial concept is also applicable to network security research. In all security analysis, we will show that the probability of security breach decreases exponentially toward 0 when the corresponding network metrics increase linearly. In this paper, the network scale (i.e., number of network members) N replaces the key length n in cryptography. N becomes the critical system parameter in network security. As a result, in cryptography, the longer the key length is, the more asymptotically secure a cryptosystem is; In our analysis, the larger the network scale is, the more asymptotically secure the network is.

4.2 Underlying mobile networking model

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

$$\begin{aligned} \rho_1 &= f_{XY}(x, y) \\ &= \lim_{\delta\rightarrow0} \frac{\mathit{Pr}[(x - \frac{\delta}{2} < X \leq x + \frac{\delta}{2}) \wedge (y - \frac{\delta}{2} < Y \leq y + \frac{\delta}{2})]}{\delta^2} \end{aligned}$$

The probability that a given node is located in a subarea $\mathcal{A}'$ of the system area $\mathcal{A}$ can be computed by integrating ρ_1 over this subarea

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

where $f_{XY}(x, y)$ can be computed by a stochastic analysis of an arbitrary mobility model. For example, as suggested in [6], we can use the analytical expression

$$\rho_1 = f_{XY}(x, y) \approx \frac{36}{a^6}\left(x^2 - \frac{a^2}{4}\right)\left(y^2 - \frac{a^2}{4}\right)$$

for random waypoint (RWP) mobility model in a square network area of size $a \times a$ defined by $-a/2 \leq x \leq a/2$ and $-a/2 \leq y \leq a/2$.

Equation (1) is universally applicable to any mobility pattern. Then ρ_1 can be obtained from related stochastic analysis [5][6][36]. Given this ρ_1, we treat it as a mobile node's arrival rate of each standing "position". Hence the random presence of mobile nodes is modeled by a *spatial Poisson point process* [11]. If there are N nodes in the network and each of them roams independently and identically distributed (i.i.d.), then $\rho_N = N \cdot \rho_1$. Let x denote the random variable of number of mobile nodes in an area, the probability that there are exactly k nodes in a specific area $\mathcal{A}'$ following a uniform distribution model is

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

More generally, in any distribution model including non-uniform models like the RWP model, the arrival rate is *location dependent*. ρ_1 is higher at some areas while lower at the other areas [5][6]. The probability that there are exactly k nodes in a specific area $\mathcal{A}'$ is

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

where $\rho_{_N}$ can be computed in simulators like NS2 and QualNet given a specific area $\mathcal{A}'$ and the finite element method. In [18], extensive simulation study on RWP model has been used to verify the correctness of the stochastic mobility model.

4.3 Security guarantee of Motion-MIX

For the ease of presentation we will assume uniform spatial distribution in a motion-MIX quantified by Δ (and the analysis can be easily extended to the non-uniform cases):

$$\mathit{Pr}[x=k] \;=\; \frac{(N\rho_1\cdot\Delta)^k}{k!}\cdot e^{-N\rho_1\cdot\Delta}$$

Besides, we adopt a probabilistic adversarial model. Amongst all N network members, there are $\gamma{\cdot}N$ uncompromised nodes and $(1-\gamma){\cdot}N$ compromised nodes. Here γ is the probabilistic *network healthy ratio*.

4.3.1 Impact of network scale N

As depicted in Figure 9, any wireless transmission is equally likely to be from any mobile transmitting nodes in the motion-MIX Δ. Besides, any mobile transmitting node, who has ever transmitted a packet δt ago and within the distance $v_{avg}{\cdot}\delta t$ of the motion-MIX, could also be in the venue now. Therefore, given an intercepted transmission at current moment, the adversary cannot decide who is the sender of the transmission amongst all nodes in the enlarged venue $\Delta'{\geq}\Delta+v_{avg}{\cdot}\delta t$.

THEOREM 1. *The security breach probability of motion-MIX, i.e., the probability that there are less than k uncompromised nodes in the venue quantified by Δ', is negligible with respect to the network scale N.*

Proof (sketch): The security breach probability is:

$$\begin{aligned} P^{fail}_{\Delta'} &= \mathit{Pr}[x<k] \;=\; \sum_{i=1}^{k-1}\mathit{Pr}[x=i] \\ &= \sum_{i=1}^{k-1}\left(\frac{(N\gamma\rho_1\cdot\Delta')^i}{i!}\cdot e^{-N\gamma\rho_1\cdot\Delta'}\right) \qquad (3) \end{aligned}$$

Given a constant k, there are k items in Equation (3), each of them has a polynomial coefficient $\frac{(N\gamma\rho_1\cdot\Delta')^i}{i!}$ but an exponentially decreasing $e^{-N\gamma\rho_1\cdot\Delta'}$. Thus $P^{fail}_{\Delta'}$ is negligible with respect to N. □

On the other hand, let's check whether the adversary can trace any specific single node v. The motion of v can be modeled as a stochastic process in a time epoch composing of a set of discrete time intervals $T=(t_1,t_2,\cdots)$. The length of each time interval is the pre-defined unit time Δt.

THEOREM 2. *The security breach probability of node tracing, i.e., the probability that the adversary can trace an actively transmitting mobile node v's motion pattern without losing the target, is negligible with respect to N and $|T|$.*

Proof (sketch): By our motion-MIX design, at least k transmissions occur per Δt if there is at least a node in a venue. The adversary's knowledge about the venue is of two cases: (1) No node in the venue during a Δt interval as there is no transmission occurred; (2) Some uncertain number of nodes are in the venue. They transmit k indistinguishable transmissions during the interval.

In any motion-MIX venue of size Δ, the adversary can successfully trace a mobile wireless node if there is no other node in the corresponding venue of size Δ' during the previous *time interval Δt (i.e., Case 1). Otherwise, it is equally likely (from the adversary's view) that the victim target stays there or keeps on moving to any neighboring venue. Therefore, the probability that the adversary can successfully trace a node v all the time is negligible with respect to N and $|T|$.*

$$P_{trace\_v} \;\leq\; \prod_{t\in T}\mathit{Pr}[x=0] = (e^{-N\gamma\rho_1\cdot\Delta'})^{|T|}.\;\;\square$$

If transmission events occur in the same set of venues, packet flow tracing is identical to node tracing. Given a packet flow that is routing through a sequence of venues $X=(x_1,x_2,\cdots)$, the size of each venue is Δ'. At each venue x_i, there are other $(k_{\Delta'_i}-1)$ uncompromised nodes inside the venue. We can prove the packet flow untraceability in a similar way of proving the node untraceability.

THEOREM 3. *The security breach probability of packet flow tracing, i.e., the probability that the adversary can trace an active packet flow on its forwarding path, is negligible with respect to N and $|X|$, where $|X|$ is the number of the corresponding forwarding venues.* □

4.3.2 k-anonymity

The previous analysis assumes that each motion-MIX ensures k-anonymity for all mobile nodes inside. The notion of k-anonymity [42] was introduced to protect privacy in the context of database systems. Recently, it was also used in anonymous communication research to quantify security guarantees [43][45]. A k-anonymous protocol ensures that the adversary is able to learn something about the sender or recipient of a particular message, but cannot narrow down its search to a set of less than k participants.

In a motion-MIX venue of size Δ', the expectation of number of nodes in the venue, $E(k_{\Delta'})$, is computable for the spatial Poisson point process: $E(k_{\Delta'}) \;=\; \sum_{i=0}^{\infty} i\cdot\mathit{Pr}[x=i] \;=\; N\gamma\rho_1\cdot\Delta'$. Let's investigate the relation between k and $E(k_{\Delta'})$.

THEOREM 4. *($min(k,E(k_{\Delta'}))$-anonymous motion-MIX) In a wireless ad hoc network, a motion-MIX is $min(k,E(k_{\Delta'}))$-anonymous in terms of AS_{id}, where $k<N$ is the predefined system parameter per Δt, and $\Delta'=(\Delta+v_{avg}\cdot\delta t)$ is the size of the least enlarged venue defined on the venue size Δ, the average node motion speed v_{avg} and the minimal delay between any two consecutive transmissions δt.*

Proof (sketch): A critical assumption in the proof is the publicity and finiteness of the anonymity sets AS_{id} and AS_{venue}. The adversary knows all the venues and all the possible identities (and certainly the network scale N). It can estimate the network characteristics such as the distribution of mobile nodes.

The public and finite network area, AS_{venue}, is partitioned into individual venues. For each venue quantified by Δ, the adversary expects there are $E(k_{\Delta'})=N\gamma\rho_1\cdot\Delta'$ possible identities capable of transmitting from the venue. By a decoy traffic regulation algorithm (e.g., Algorithm D), the capable nodes will transmit at least k packets from the venue (if multiple packet types are concerned, in Section 3.3 we already stated that different packet types are regulated separately with independent k's).

Due to the "identity-free", "one-time packet content" and physical radio deliberation requirements, any transmission is equally likely from any identity-free node inside a motion-MIX. If $k<E(k_{\Delta'})$, then $(E(k_{\Delta'})-k)$ inside nodes do not have packets to forward and do not win the chance to transmit decoy traffic. If $k>E(k_{\Delta'})$, then either some nodes inside the motion-MIX transmit more decoy traffic, or some $(k-E(k_{\Delta'}))$ previously silent nodes have roamed into the motion-MIX and just start their transmissions. □

Therefore, the analytic result suggests that an appropriate k should be set to approximately $E(k_{\Delta'})$.

5. RELATED WORK

Anonymity in fixed networks In fixed networks, the notion of anonymity is defined on node identities only. And nearly all anonymous schemes designed so far assume that the entire network topology is fixed, while many of them also assume the entire topology is known *a priori*. In DC-net [10], the network topology is suggested as a closed ring and routing is not needed. In Crowds [35] and sorting network [33], pairwise communication has uniform cost (i.e., all nodes are one logical hop away). Thus the protocol can randomly select any member to be next forwarder. This assumption is *not* applicable to mobile ad hoc networks where multihop routing is completely different from local forwarding. In MIX-net [9], a data sender solves the problem of routing by selecting a random path from the known network topology. All subsequent MIX-net designs [32][31] inherit this assumption. But static and *a priori* topology knowledge is no longer available in mobile ad hoc networks where global topology dynamically changes due to mobility, frequent route outage, and node joining/leaving. Maintaining the same global topology knowledge that is identical to fixed networks is very expensive and reveals the changing topological knowledge to node intruders. In PipeNet and Onion Routing [34], virtual circuit based routing is introduced. However, they assume that network nodes do not move and the topology is fixed after initialization. These assumptions are also inapplicable to mobile ad hoc networks. In a nutshell, these schemes treat the underlying network as a simple stationary graph. If directly used in mobile networks, the adversary can intrude one mobile node, gather fresh network topology from the node's knowledge, then use network localization schemes to pinpoint every mobile node in the network. These schemes do not address mobility and do not fit in mobile wireless networks.

Anonymity in wireless networks Existing anonymity schemes for wireless networks fall into a spectrum of classes. In "last hop" wireless networks (including cellular networks and wireless LANs), the demand of user roaming requires more promising assurance on the privacy of mobile users. The network participants considered in related research are typically the mobile user, the home server of the user, the foreign agent server local to the user, and the eavesdroppers including the other users. In [37][1], mobile users are associated with dynamic *aliases* that appear unintelligible to anyone except the home server. Then the foreign agent server accepts the user's connections upon the home server's request. Hu and Wang [18] propose to use *anonymous rendezvous*, an anonymous bulletin board, to let mobile nodes anonymously connect to their communicators. These efforts provide unlinkability protections between node identities and their credentials during *end-to-end* anonymous transactions. This design goal is above the network layer, and is orthogonal to the motion-MIX study.

In wireless sensor networks, distributed sensor nodes monitor target events, function as information sources and send sensing reports to a number of sinks (command center) over multi-hop wireless paths. The sensor nodes and sinks are typically stationary in WSN. Deng et al. [13] propose to use multi-path routes and varying traffic rates to protect recipient anonymity for the network sinks. Ozturk et al. [27] prevent a mobile adversary (e.g., a poacher) from tracing a sensor report packet flow back to a mobile target's location (e.g., a panda). The sensor nodes must report the mobile target's status to the sinks via *phantom flooding*, which is a sequential combination of random walk and controlled flooding. Both proposals seek to prevent the adversary from tracing network packet flows back to the sources or the sinks. As we described in Section 3, ongoing packet flows are mixed together in a single motion-MIX en route. Like a network of Chaumian MIXes, anonymity degrades [44][39] when the packet flows sequentially go through a network of motion-MIXes. As shown in Section 4, motion-MIX helps to stop this attack.

In mobile ad hoc networks, the *on-demand* approach has been adopted by several recent designs to support anonymous connection. In ANODR [25], the source end creates an onion in the route request (RREQ) flood packet. Each forwarder adds a self-aware layer to the onion. Eventually the destination end receives an onion that can be used to deliver a route reply (RREP) packet back to the source end, and an on-demand anonymous virtual circuit is established between the two ends. MASK [46] also uses anonymous virtual circuits in routing, but a MASK node follows an anonymous neighbor detection scheme to create one-hop virtual circuit links with its neighbors prior to on-demand route request. This reduces cryptographic processing overheads for the time-critical on-demand route discovery process. SDAR [7] is more like a MIX-net with on-demand route discovery. A neighbor detection protocol is devised to let each mobile node see its neighbors explicitly. After the on-demand route is established, data packets are delivered between the two ends using MIX-net onions. Like protecting packet flows in sensor networks, motion-MIX also helps mixing an ad hoc routing scheme's control and data packet flows in anonymous on-demand routing. But the cost could be expensive. Currently the control flows in ANODR, MASK and SDAR do not implement *Algorithm D* (mostly due to performance concerns), thus are traceable by a global timing analyst. As to data flows, SDAR is vulnerable to packet flow tracing. ANODR is not vulnerable because it pays the cost of "neighborhood traffic mixing", which is a variant of *Algorithm D*. MASK employs a delay tolerant approach, which is part of motion-MIX design.

In geographic services, both Location-Base Services [17] and Mix Zones [3] study how to use middleware service to ensure location privacy with respect to time accuracy and position accuracy. As we described in Section 3, they study user anonymity protection in static "geographic regions" with boundary lines. The regions are fixed during the network lifetime, and anonymity protection degrades in a single region. Besides, since the anonymity protection stops at the middleware layer (typically above the network IP layer), the adversary can trace a mobile node using network identities/addresses at the network layer and the link layer, or radio signatures at the physical layer. These middlewares protect upper layer user identities that are not the focus of the motion-MIX design.

6. CONCLUSION

In this paper we study how to use practical tools to trace mobile nodes' motion patterns and traffic patterns. Because routing services are essential for mobile wireless nodes, the baseline of a mobile adversary is to intercept control and data packets to launch various Venue Privacy Attacks (VPAs). Common routing and packet forwarding protocols are vulnerable to various VPAs.

In our proposal, mobile nodes can create and enlarge motion-MIXes to stop VPAs. Though the concept of motion-MIX is an analogue of the classic notion of Chaumian MIX, it is different from existing concepts like the Chaumian MIX and the geographic MIX Zones. We show that "identity-free routing", "one-time packet contents" and various protocol stack implementation concerns are necessary conditions to stop identity and traffic analysis attacks within a single motion-MIX. We propose a new asymptotic network security model to study the anonymity protection provided in a motion-MIX. In the asymptotic network security model, network scale plays the role of key length in computational cryptography. The adversary cannot break motion-MIX's anonymity protection with non-negligible probability in regard to the polynomial-bounded network scale. This new notion is conforming to the existing security notions.

7. REFERENCES

[1] G. Ateniese, A. Herzberg, H. Krawczyk, and G. Tsudik. Untraceable Mobility or How to Travel *Incognito*. *Computer Networks*, 31(8):871–884, 1999.

[2] A. R. Beresford. *Location Privacy in Ubiquitous Computing*. PhD thesis, University of Cambridge, November 2004.

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

[4] A. R. Beresford and F. Stajano. Mix Zones: User privacy in location-aware services. In *Pervasive Computing and Communication Security (PerSec)*, pages 127–131, 2004.

[5] C. Bettstetter, H. Hartenstein, and X. Perez-Costa. Stochastic Properties of the Random Waypoint Mobility Model. *ACM/Kluwer Wireless Networks, Special Issue on Modeling and Analysis of Mobile Networks*, 10(5):555–567, 2004.

[6] C. Bettstetter and C. Wagner. The Spatial Node Distribution of the Random Waypoint Mobility Model. In *German Workshop on Mobile Ad Hoc Networks (WMAN)*, pages 41–58, 2002.

[7] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks. In *29th IEEE International Conference on Local Computer Networks (LCN'04)*, pages 618–624, 2004.

[8] C. Castelluccia and P. Mutaf. Shake Them Up (A mouvement-based pairing protocol for CPU-constrained devices). In *ACM/Usenix MobiSys*, 2005.

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

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

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

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

[13] J. Deng, R. Han, and S. Mishra. Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks. In *IEEE International Conference on Dependable Systems and Networks (DSN)*, pages 594–603, 2004.

[14] C. Díaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. In R. Dingledine and P. Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002), Lecture Notes in Computer Science 2482*, pages 54–68, 2002.

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

[16] K. Fall. A Delay-Tolerant Network Architecture for Challenged Internets. In *ACM SIGCOMM*, pages 27–34, 2003.

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

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

[19] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing Wireless Location Privacy Using Silent Period. In *IEEE WCNC*, 2005.

[20] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki. Towards Modeling Wireless Location Privacy. In *Workshop on Privacy Enhancing Technologies (PET)*, 2005.

[21] P. G. Ifju, S. M. Ettinger, D. Jenkins, Y. Lian, W. Shyy, and M. Waszak. Flexible-wing-based Micro Air Vehicles. In *40th AIAA Aerospace Sciences Meeting*, 2002.

[22] J. Kong. *Anonymous and Untraceable Communications in Mobile Wireless Networks*. PhD thesis, University of California, Los Angeles, June 2004.

[23] J. Kong. Formal Notions of Anonymity for Peer-to-peer Networks. Technical Report Report 2005/132, IACR Cryptology ePrint Archive, May 2005. Also CSD-TR050014, Department of Computer Science, UCLA.

[24] J. Kong, S. Das, E. Tsai, and M. Gerla. ESCORT: A Decentralized and Localized Access Control System for Mobile Wireless Access to Secured Domains. In *ACM WiSe'03 in conjunction with MOBICOM'03*, pages 51–60, 2003.

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

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

[27] C. Ozturk, Y. Zhang, and W. Trappe. Source-Location Privacy in Energy-Constrained Sensor Network Routing. In *ACM SASN*, pages 88–93, 2004.

[28] C. Perkins and D. Johnson. Mobility Support in IPv6. In *ACM MOBICOM*, pages 27–37, 1996.

[29] C. E. Perkins, E. M. Royer, and S. Das. Ad-hoc On Demand Distance Vector (AODV) Routing. `http://www.ietf.org/rfc/rfc3561.txt`, July 2003.

[30] A. Pfitzmann and M. Köhntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In H. Federrath, editor, *DIAU'00, Lecture Notes in Computer Science 2009*, pages 1–9, 2000.

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

[32] A. Pfitzmann and M. Waidner. Networks Without User Observability: Design Options. In F. Pichler, editor, *EUROCRYPT'85, Lecture Notes in Computer Science 219*, pages 245–253, 1986.

[33] C. Rackoff and D. R. Simon. Cryptographic defense against traffic analysis. In *Symposium on the Theory of Computation (STOC)*, pages 672–681, 1993.

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

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

[36] G. Resta and P. Santi. An Analysis of the Node Spatial Distribution of the Random Waypoint Model for Ad Hoc Networks. In *ACM Workshop on Principles of Mobile Computing (POMC)*, pages 44–50, 2002.

[37] D. Samfat, R. Molva, and N. Asokan. Untraceability in Mobile Networks. In *ACM MOBICOM*, pages 26–36, 1995.

[38] A. Serjantov and G. Danezis. Towards an Information Theoretic Metric for Anonymity. In R. Dingledine and P. Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002), Lecture Notes in Computer Science 2482*, pages 41–53, 2002.

[39] A. Serjantov and R. E. Newman. On the Anonymity of Timed Pool Mixes. In *Workshop on Privacy and Anonymity Issues in Networked and Distributed Systems*, pages 427–434, 2003.

[40] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[41] R. Song, L. Korba, and G. Yee. AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2005.

[42] L. Sweeney. k-anonymity: A model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5):557–570, 2002.

[43] L. von Ahn, A. Bortz, and N. J. Hopper. k-Anonymous Message Transmission. In V. Atluri and P. Liu, editors, *10th ACM Conference on Computer and Communications Security (CCS 2003)*, pages 122–130, 2003.

[44] M. Wright, M. Adler, B. N. Levine, and C. Shields. An Analysis of the Degradation of Anonymous Protocols. In *Network and Distributed Security Symposium - NDSS '02*, 2002.

[45] S. Xu and M. Yung. k-Anonymous Secret Handshakes with Reusable Credentials. In *ACM CCS*, pages 158–159, 2004.

[46] Y. Zhang, W. Liu, and W. Lou. Anonymous Communications in Mobile Ad Hoc Networks. In *IEEE INFOCOM*, 2005.