International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-5, May 2015

# Providing Security for Patten Detection without Using Decryption for MANETs

**Pavithra R, Manjula K**

***Abstract*— There are many obscurity enhancing techniques have been proposed based on encrypting the packets to keep the communication obscurity of mobile ad hoc networks (MANETs). However, in this paper, we show that MANETs are still weak under passive geometric traffic scrutiny attacks. To show how to determine the communication patterns without decrypting the captured packets, we present a novel secure geometric traffic pattern detection system (SGTPDS). It is capable of finding the sources, the destinations, and the end-to-end communication relations. SGTPDS works passively to achieve analyze the traffic based on geometric characteristics of captured raw traffic. Observed studies express that SGTPDS achieves good accuracy in disclosing the unknown traffic patterns.**

***Index Terms*—unspecified communication, mobile ad hoc networks, geometric traffic analysis**

## I. INTRODUCTION

Mobile ad hoc networks (MANETs) are originally designed for military tactic environments. Communication anonymity is a critical issue in MANETs, which generally consists of the following aspects1.Source/ destination obscurity-it is hard to make out the sources or the destinations of the network flows. End-to-end relationship obscurity-it is hard to make out the end-to-end communication relations. To achieve unspecified MANET communications, many unspecified routing protocols such as ANODR [1], MASK [2], and OLAR [3] have been proposed. There are many of obscurity enhancing techniques like onion routing [9] and mix-net [10] are utilized, these protocols mostly rely on packet encryption to cover sensitive information (e.g., nodes identities and routing information) from the adversaries. However, passive signal detectors can still snoop on the wireless channels, catch the transmissions, and then perform traffic analysis attacks. The attackers aim is to find out the traffic patterns among mobile nodes. Particularly, there are the following four assumptions for attackers:

1. The adversaries are passive signal detectors, i.e., they are not actively involved in the communications. They can monitor every single packet transmitted through the network.
2. The adversary nodes are connected through an additional channel which is different from the one used by the target MANET. Therefore, the communication between adversaries will not influence the MANET communication. 3. The adversaries can locate the signal source according to certain properties (e.g., transmission power and direction) of the detected signal, by using wireless location tracking techniques such as triangulation, nearest sensor, or RF fingerprinting. Note that none of these techniques can identify the source of a signal from several nodes very close to each other. Hence, this assumption actually indicates that the targeted networks are sparse in terms of the node density. In other words, any two nodes in such a network are distant from each other so that the location tracking techniques in use are able to uniquely identify the source of a wireless signal. In the following of this paper, unless specifically denoted as signal source or source of signal, the word source indicates the source of a network flow.
4. The adversaries can mark out the movement of each mobile node, by using cameras or other types of sensors. In this case, the signals (packets) transmitted by a node can always be associated with it even when the node moves from one spot to another.

Attacker can take advantage of SGTPDS to perform traffic analysis as follows:

1. Divide the whole network into several sections geographically;
2. Install sensors along the boundaries of each section to monitor the cross-component traffic;
3. Treat each region as a super node and use SGTPDS to figure out the sources, destinations, and end-to-end communication relations; and
4. Analyze the traffic even when nodes are close to each other by treating the nearest nodes as a super node.

We call this SGTPDS as the Generalized SGTPDS(GSGTPDS ). To perform GSGTPDS, the adversaries only need to examine the nodes nearby the boundaries of the super nodes. The traffic inside each super node can be unnoticed, since it will not affect the inter-region traffic patterns. In addition, GSGTPDS does not want the signal detectors to place in particular signal source. They are only necessary to find out which super node (region) the signals are sent from. In SGTPDS, the actual receiver of a point-to-point transmission is not identifiable among all the potential receivers within the senders transmitting range. This inaccuracy can be mitigated in GSGTPDS because most potential receivers of a packet will be contained within one or a few super nodes.

Reusing the evidence-based model, in this paper, a novel geometric traffic pattern detection system is proposed (SGTPDS). aims to derive the source/destination probability distribution, i.e., the probability for each node to be a message source/destination, and the end-to-end link probability distribution, i.e., the probability for each pair of nodes to be an end-to-end communication pair. To achieve its goals, SGTPDS includes two major steps1) Construct point-to-point traffic matrices using the time-slicing technique, and then derive the end-to-end traffic matrix with a set of traffic

**Pavithra R**, Department of Computer science, Don Bosco Institute of Technology, Bangalore, India, 9538719351.
**Manjula K**, Department of Computer science, Don Bosco Institute of Technology, Bangalore, India, 9538282393.

filtering rules and 2) Apply a heuristic approach to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations.

The contribution of SGTPDS is twofold
1 SGTPDS is the first geometric traffic analysis approach that considers the salient characteristics of MANETs the broadcasting, ad hoc, and mobile nature.
2. most of the previous approaches are partial attacks in the sense that they either only try to identify the source (or destination) nodes or to find out the corresponding destination (source) nodes for given particular source (destination) nodes. SGTPDS is a complete attacking system that first identifies all source and destination nodes and then determines their relationship.

## II. RELATED WORK

Over the past few decades, traffic analysis models have been widely investigated for static wired networks. For example, the simplest approach to track a message is to enumerate all possible links a message could traverse, namely, the brute force approach. Recently, statistical traffic analysis attacks have attracted broad interests due to their passive nature, i.e., attackers only need to collect information and perform analysis quietly without changing the network behavior (such as injecting or modifying packets). The predecessor attacks and disclosure attacks are two representatives. However, all these previous approaches do not work well to analyze MANET traffic.
First, the scheme fails to address several important constrains (e.g., maximum hop-count of a packet) when deriving the end-to-end traffic from the one hop evidences. Second, it does not provide a method to identify the actual source and destination nodes (or to calculate the source/destination probability distribution). Moreover, it only uses a naive accumulative traffic ratio to infer the end-to-end communication relations (e.g., the probability for node j to be the intended destination of node i is computed as the ratio of the traffic from i to j to all traffic coming out from node i), which incurs a lot of inaccuracy in the derived probability distributions.
In[21],Huang devised an evidence based statistical traffic analysis model especially for MANETs. In this model, every captured packet is treated as evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. A sequence of point-to-point traffic matrices is created, and then they are used to derive end-to-end (multi hop) relations. This approach provides a practical attacking framework against MANETs but still leaves substantial information about the communication patterns undiscovered.

Traffic analysis attacks against the static wired networks (e.g., Internet) have been well investigated. The brute force attack proposed, it tries to track a message by enumerating all possible links a message could traverse. In node flushing attacks, the attacker sends a large quantity of messages to the targeted anonymous system (which is called a mix-net). Since most of the messages modified and reordered by the system are generated by the attacker, the attacker can track the rest a few (normal) messages. The timing attacks as proposed in [9] focus on the delay on each communication path. If the attacker can monitor the latency of each path, he can correlate the messages coming in and out of the system by analyzing their transmission latencies. The message tagging attacks require attackers to occupy at least one node that works as a router in the communication path so that they can tag some of the forwarded messages for traffic analysis. By recognizing the tags in latter transmission hops, attackers can track the traffic flow. The watermarking attacks are actually variants of the message tagging attacks. They reveal the end-to-end communication relations by purposely introducing latency to selected packets
Different from the attacks mentioned above, statistical traffic analysis intends to discover sensitive information from the statistical characteristics of the network traffic, for example, the traffic volume. The adversaries usually do not change the network behavior (such as injecting or modifying packets). The only thing they do is to quietly collect traffic information and perform statistical calculations. The predecessor attacks are first pointed out by Reiter and Rubin. Later works extend them to all kinds of unknown communication systems including onion-routing [9], mix-net [10], and DC-net. In a typical predecessor attack, the attackers act exactly as legitimate nodes in the network communications. They collectively maintain a single predecessor counter for each legitimate node in the system. When an attacker finds himself to be on an anonymous path to the targeted destination, he increments the shared counter for its predecessor node in this path. The counters are then used for the attackers to infer the possible source nodes of the given destination. Obviously, to launch such an attack, a large number of legitimate nodes must first be compromised and controlled by the attackers. This is usually not achievable in MANETs. Moreover, in a MANET protected by anonymity enhancing techniques, it is a difficult task itself to identify an actual destination node as the target due to the ad hoc nature. That is, destinations are indistinguishable from other nodes (e.g., relays) in a MANET. In fact, they usually act as relay nodes as well, forwarding traffic for others. The adversaries are not able to determine whether a particular node is a destination depending on whether the node sends out traffic. This is totally different from the situation in traditional infrastructural networks where the role of every node is determined.
A statistical disclosure attack often targets a particular given source node and intends to expose its corresponding destinations. It is assumed that the packets initiated by the source are sent to several destinations with certain probability distribution. The background (covering) traffic also has certain probability distribution (usually assumed to be uniformly distributed). After a large number of observations, the attackers are able to figure out the possible destinations of the given source. Nonetheless, the statistical disclosure attacks cannot be applied to MANETs either, because the attackers cannot easily identify the actual source nodes in MANETs. Even if a source node is identified, the attacks can only be performed when the attackers know for sure when the targeted source is originating traffic and can observe the network behavior in the absence of the source. However, the attackers are prevented from being able to do so by the ad hoc nature of MANETs, i.e., they cannot tell if the source is originating traffic or just forwarding traffic as a relay. Due to the unique characteristics of MANETs, very limited investigation has been conducted on traffic analysis in the context of MANETs. He et al. proposed a timing-based

approach to trace down the potential destinations given a known source. In this approach, assuming the transmission delays are bounded at each relay node, they estimate the flow rates of communication paths using packet matching. Then based on the estimated flow rates, a set of nodes that partition the network into two parts, one part to which the source can communicate in sufficient rate and the other to which it cannot, are identified to estimate the potential destinations. In Liu et al., designed a traffic inference algorithm (TIA) for MANETs based on the assumption that the difference between data frames, routing frames, and MAC control frames is visible to the passive adversaries, so that they can recognize the point-to-point traffic using the MAC control frames, identify the end-to end flows by tracing the routing frames, and then infer the actual traffic pattern using the data frames. The TIA achieves good accuracy in traffic inference, while the mechanism is tightly tied to particular unknown routing protocols but not a general approach.

## III. SYSTEM MODELS

In this section, the primary system models adopted by SGTPDS are presented.

Communication Model

Assume the obscurity enhancing techniques are used to protect the MANETs. However, these techniques are designed to different levels of obscurity. To focus on the statistical traffic analysis, assume, that a combination of these techniques is applied and the targeted MANET communication system is subject to the following model:

1. The PHY/MAC layer is controlled by the commonly used 802.11(a/b/g) protocol. But all MAC frames
(Packets) are encrypted so that the adversaries cannot decrypt them to look into the contents.
2. Padding is applied so that all MAC frames (packets) have the same size. Nobody can trace a packet
according to its unique size.
3. The virtual carrier sensing option is disabled. The source/destination addresses in MAC and IP headers are set to a broadcasting address (i.e., all 1) or to use identifier changing techniques. In this case, adversaries are prevented from identifying point-to point communication relations.
4. No information about the traffic patterns is disclosed from the routing layer and above.
5. Dummy traffic and dummy delay are not used due to the highly restricted resources in MANETs.

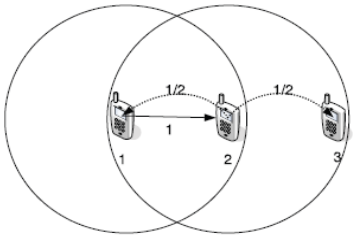


Fig 3.1 A simple wireless ad hoc network

## IV. GEOMETRIC TRANSFER PATTERN DETECTION SYSTEM

To disclose the unknown traffic patterns in a MANET communication system, SGTPDS includes two major steps. First, it uses the captured traffic to construct a sequence of point-to-point traffic matrices and then derives the end-to end traffic matrix. Second, further analyzing the end-to end traffic matrix, it calculates the probability for each node to be a source/destination (the source/destination probability distribution) and that for each pair of node to be an end-to-end communication link (the end-to-end link probability distribution). To illustrate the basic idea of SGTPDS, use a simple scenario shown in Fig. 1 as an example. In this network, there are three wireless nodes (1, 2, and 3). Node 2 is located in the transmission range of node 1, and node 3 is located in the transmission range of node 2 (but not the transmission range of node 1). Two consecutive packets are detected node 1 broadcasts a packet and then node 2 broadcasts a packet.

### 4.1 Traffic Matrices Construction

4.1.1 Point-to-Point Traffic Matrix

With the captured point-to-point (one-hop) traffic in a certain period T, first need to build point-to-point traffic matrices such that each traffic matrix only contains independent one-hop packets. Note that two packets captured at different time could be the same packet appearing at different locations, such as the two packets sent by node 1 and node 2 consecutively in Fig. 1, so they are dependent on each other. To avoid a single point-to point traffic matrix from containing two dependent packets, apply a time slicing technique. That is, take snapshots of the network, and each snapshot is triggered by a captured packet. A sequence of snapshots during a time interval te constructs a slice represented by a traffic matrix, which is an NN one-hop traffic relation matrix. The length of each time interval te is determined by two criteria:

1) A node can be either a sender or a receiver within this time interval. But it cannot be both.
2) Each traffic matrix must correctly represent the one-hop transmissions during the corresponding time interval. The time slicing has to make sure that all packets captured in any of the time intervals are independent with each other. In other words, two packets residing in different entries of the same matrix must not be the same packet transmitted through multiple hops. Note that, using the time slicing techniques can effectively handle the nodal mobility by taking snapshots of a sequence of relatively fixed network topologies. In addition to the time slicing, follow the three rules listed below

1) The number of captured packets rather than the actual size of payloads is considered as the traffic volume, since the size of payloads does not affect the traffic pattern (and assuming all MAC frames are of the same length due to the application of padding).
2) All nodes within the transmitting range of a packet have the same probability to be the actual receiver. 3) Each packet p has three associated features p.vsize, p.time and p.hop, denoting the virtual size, transmitting time, and hop count of this packet, respectively. A packets hop count is set to 1 when added to the point-to-point traffic matrix.

4.1.2 End-to-End Traffic Matrix

Given a sequence of point-to-point traffic matrices, our goal is to derive the end-to-end traffic matrix R is the accumulative

traffic volume from node i to node j, including both the point-to-point traffic captured directly and multi hop traffic deduced from the point-to-point traffic. In this paper, use the term accumulative traffic matrix and end-to-end traffic matrix interchangeably. The following Algorithm 1 (function f) takes W|1k as the inputs to derive the accumulative traffic matrix R.

**Algorithm 1.** $—f(\mathbf{W}|_{1\times K})$.

1: $\mathbf{R} = \mathbf{W}_1$
2: **for** $e = 1$ to $K - 1$ **do**
3: $\quad \mathbf{R} = g(\mathbf{R}, \mathbf{W}_{e+1}) + \mathbf{W}_{e+1}$
4: **end for**
5: **return** R

In this algorithm, each update to R (line 3) includes the multi hop traffic derivation function g and the addition of the point-to-point traffic matrix which is the evidence of possible direct (single hop) communication.

Function g takes two inputs:
1) R is an end-to-end traffic matrix derived from point-to-point matrices W1 to We, and
2)We+1is the next point-to-point traffic matrix. The output is the end-to-end traffic matrix derived from W1 to We+1.

**4.2 Traffic Pattern Discovery**

The traffic matrix R tells us the deduced end-to-end traffic volume between each pair of nodes. However, we still need to perform further investigation to discover the actual source/destination probability distribution and end-to-end link probability distribution, that is, to figure out who are the actual sources and destinations and who are communicating with whom.

4.2.1 Source/Destination Probability Distribution

Geographically adjacent nodes may have negative impacts on the accuracy of the algorithms above. For example, if node j is one of the neighbors of node i, j may frequently forward the packets originated from node i to other nodes in the network and in addition frequently forward the packets from other nodes to node i. In this case, the high probability for node j to be a source does not indicate the high probability for node i to be a destination, though the traffic volume from j to i is large. On the other hand, the high probability for node j to be a destination and the large traffic volume from i to j do not indicate the high probability for node i to be a source. We call this kind of negative impacts as the neighborhood noise. Especially, when the mobility is low, the negative impacts will be substantial since the neighborhood of a node rarely changes. To reduce the neighborhood noise, we utilize the vector space similarity assessment. The vector space similarity (or cosine similarity) of two vectors V and U is defined as follows:

$$Sim(\mathbf{V}, \mathbf{U}) = \mathbf{V} \cdot \mathbf{U}/(|\mathbf{V}\|\mathbf{U}|),$$

where V.U denotes the dot product of V, and U, |V|, and |U| denote the norm of V and U. We realize that, if two nodes have similar outgoing and incoming traffic vectors (in the end-to-end traffic matrix R), they are likely to be neighboring nodes (relays of each other), and so they should have less impact on the source/destination probability distribution of each other.
By introducing the vector space similarity (VSS) assessment, ensure that, two nodes with higher probability to be neighbors (relays of each other) have less impact on each other's source/destination probability distribution, which reasonably reduces the neighborhood noise.

4.2.2 End-to-End Link Probability Distribution

Our goal in this section is to derive a probability distribution matrix in which each represents the probability of the i -> j linkability (i.e., node i and node j are a pair of actual source and destination). Again, note that only the relative order among these entries is of interest, since we aim at discovering the most possible communication links. As described above, the probability for node i to be a destination depend on two factors the traffic from each node j to node i and node js probability to be a source. Suppose j - i is an actual source-destination pair. If we set the total traffic coming out from j to zero, the probability for i to be a destination will decrease. Similarly, if we set the incoming traffic to node i to zero, the probability for node j to be a source will also decrease. Thus, we can identify a source-destination (S-D) pair by evaluating the significance of the probability reduction due to the elimination of the traffic sent by the source or received by the destination. For instance, in the example scenario shown in Fig. 1, to identify the most possible destination of node 1, we can erase all traffic sent by node 1 from the point-to-point traffic matrices. By comparing D with D (obtained using the original point-to-point matrices), can find out the node whose destination probability drops most significantly due to elimination of the traffic sent by node 1. This node is most possible to be the destination of node 1.

**4.3 Performance**

From the previous section, it is seen that the probability distributions produced by SGTPDS are good indicators of the actual traffic patterns, i.e., actual sources, destinations, and end-to-end links. Different strategies can be used to speculate the actual traffic patterns from the probability distributions. In this section, evaluate the performance of SGTPDS based on the following two basic strategies, T1 and T2. [T1] Suppose the number of actual sources, destinations, or end-to-end links is known to be k. simply select the top k items (nodes or links) with the highest probabilities. [T2] Suppose the number k is unknown. Keep selecting the top items with the highest probabilities until both of the two criteria are satisfied
1) The sum of the probabilities of the selected items has reached u and 2) The probability of the last selected item is v times larger than the current one. u and v are two adjustable thresholds, which are set to 0.8 and 4 in the experiments, respectively.

To conclude the evaluation, the hidden traffic patterns can be revealed in good accuracy using SGTPDS, even without the number of actual sources, destinations, and end-to-end communication relations known to the traffic analyzers.

The antagonist model assumes that the adversaries can globally monitor the traffic across the entire network region.

This assumption is conventional from the network users point of view. Typically, it is complex for the attackers to perform such global traffic detection. However, even though the adversaries are not able to monitor the entire network, they can monitor several parts of the network simultaneously. For example, an attacker can deploy sensors (signal detectors) around some particular mobile nodes to track their movements and eavesdrop all of their traffic. These sensors may even move accordingly.

## V. CONCLUSION

In this paper proposes a novel SGTPDS for MANETs. SGTPDS is basically an attacking system, which only needs to incarcerate the raw traffic from the PHY/MAC layer without looking into the contents of the intercepted packets. From the captured packets, SGTPDS constructs a sequence of point-to-point traffic matrices to derive the end-to-end traffic matrix, and then uses a heuristic data processing model to reveal the hidden traffic patterns from the end-to end matrix. The empirical study demonstrates that the existing MANET systems can accomplish very restricted communication obscurity under the attack of SGTPDS.

## REFERENCES

[1] J. Kong, X. Hong, and M. Gerla, "An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 6, no. 8, pp. 888-902, Aug. 2007.

[2] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.

[3] Y. Qin and D. Huang, "OLAR: On-Demand Lightweight Anonymous Routing in MANETs," Proc. Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking (ICMU '08), pp. 72-79, 2008.

[4] M. Blaze, J. Ioannidis, A. Keromytis, T. Malkin, and A. Rubin, "WAR: Wireless Anonymous Routing," Proc. Int'l Conf. Security Protocols, pp. 218-232, 2005.

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

[6] S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," Proc. IEEE 20th Int'l Conf. Advanced Information Networking and Applications Workshops (AINA Work-shops '06), pp. 133-137, 2006.

[7] R. Shokri, M. Yabandeh, and N. Yazdani, "Anonymous Routing in MANET Using Random Identifiers," Proc. Sixth Int'l Conf. Networking (ICN '07), p. 2, 2007.

[8] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks," Proc. Third ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05), pp. 33-42, 2005.

[9] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connec-tions and Onion Routing," IEEE J. Selected Areas in Comm., vol. 16, no. 4, pp. 482-494, May 2002.

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

[11] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobserva-bility, pp. 10-29, 2001.

[12] W. Dai, "Two Attacks against a PipeNet-Like Protocol Once Used by the Freedom Service," http://weidai.com/freedom-attacks.txt, 2013.

[13] X. Wang, S. Chen, and S. Jajodia, "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems," Proc. IEEE Symp. Security and Privacy, pp. 116-130, 2007.

[14] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transac-tions," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.

[15] M. Wright, M. Adler, B. Levine, and C. Shields, "The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems," ACM Trans. Information and System Security, vol. 7, no. 4, pp. 489-522,2004.

[16] D. Figueiredo, P. Nain, and D. Towsley, "On the Analysis of the Predecessor Attack on Anonymity Systems," technical report, Computer Science, pp. 04-65, 2004.

[17] G. Danezis, "Statistical Disclosure Attacks: Traffic Confirmation in Open Environments," Proc. Security and Privacy in the Age of Uncertainty (SEC '03), vol. 122, pp. 421-426, 2003.

[18] G. Danezis and A. Serjantov, "Statistical Disclosure or Intersection Attacks on Anonymity Systems," Proc. Sixth Information Hiding Workshop (IH '04), pp. 293-308, 2004.

[19] G. Danezis, C. Diaz, and C. Troncoso, "Two-Sided Statistical Disclosure Attack," Proc. Seventh Int'l Conf. Privacy Enhancing Technologies, pp. 30-44, 2007.

[20] C. Troncoso, B. Gierlichs, B. Preneel, and I. Verbauwhede, "Perfect Matching Disclosure Attacks," Proc. Eighth Int'l Symp. Privacy Enhancing Technologies, pp. 2-23, 2008.

[21] D. Huang, "Unlinkability Measure for IEEE 802.11 Based MANETs," IEEE Trans. Wireless Comm., vol. 7, no. 3, pp. 1025-1034, Mar. 2008.

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

[23] T. He, H. Wong, and K. Lee, "Traffic Analysis in Anonymous MANETs," Proc. Military Comm. Conf. (MILCOM '08), pp. 1-7, 2008.

[24] Y. Liu, R. Zhang, J. Shi, and Y. Zhang, "Traffic Inference in Anonymous MANETs," Proc. IEEE Seventh Ann. Comm. Soc. Conf. Sensor Mesh and Ad Hoc Comm. and Networks (SECON '10), pp. 1-9, 2010.

[25] J. Wexler, "All About Wi-Fi Location Tracking," Network World, http://features.techworld.com/mobile-wireless/2374/all-about-wi-fi-location-tracking/, 2004.

[26] Scalable Network Technologies, "QualNet Simulator," http:// www.qualnetcomm.com/, 2008.