International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue XI, November- 2016

# EFFICIENT NODE AUTHENTICATION USING INSENS PROTOCOL FOR MANET NETWORK

*[1]Priyanka.M, [2]P.Chandrasekar*
M.E.(Communication System),
[1]PG Scholar, Professor,
Department of Communication Systems,
RVS College Of Engineering and Technology,

**Abstract-** Mobile Ad-Hoc Networks (MANETs) have been used in wide range of applications such as disaster management, emergency and rescue operations where it is not possible to have well defined infrastructure. In MANETs, the topology is highly dynamic as nodes frequently join or leave the network, and roam in the network. Though MANETs are dynamic in nature, security services need to be provided in mobile nodes as they move from one place to another. Unlike fixed wired networks, mobile wireless adhoc networks need more security mechanisms as attackers may intrude into the network through subverted nodes. Therefore, a powerful security solution is required to identify and isolate malicious nodes in the network. In addition to protecting the network from intruders, the security solution should also protect each node in the network. The security scheme adopted by each node in MANET has to work within its own resource limitations in terms of energy supply, communication capacity, and memory and computation capability. In this Project Intrusion-Tolerant Routing protocol for Manet (INSENS) protocol &Small Minimum-Energy communication Network (SMECN) is used to focus on a Malicious control by identity the characteristics, to improve an energy and avoid Malicious. This property implies that for any pair of sensors in a graph associated with a network, there is a minimum energy-efficient path between them that is, a path that has the smallest cost in terms of energy consumption over all possible paths between this pair of sensors.

***Keywords-Sensor Networks, Network Protocols, Fault Tolerance, Security.***

***Introduction***

Mobile Ad-hoc Networks consist of a multitude of tiny sensor nodes capable for wireless communications and a few powerful base stations. The sensor nodes usually perform some monitoring task (e.g., measure various environmental parameters). The base stations collect sensor readings and forward them for further processing to a service center.

Based on how the sensor readings reach the base stations, we can distinguish synchronous And asynchronous sensor networks. In the synchronous case, the sensor readings are sent to the base stations in real-time using multi-hop wireless communications, where the sensor nodes cooperatively forward data pack-

ets on behalf of other sensor nodes towards the base stations. In the asynchronous case, the sensor readings are fetched by the base stations after some delay (e.g., once every day or week). In this case, the base stations

are often mobile, and they physically approach the sensors in order to fetch their data through a single wireless hop. Examples of synchronous sensor network applications include forest fire alarm systems and building automation systems where real-time operation is indispensable. Examples of asynchronous applications include habitat monitoring systems and agricultural applications such as vineyard monitoring where real-time operation is not an issue. As sensor nodes are often severely resource constrained, various techniques have been proposed to ensure the efficient operation of sensor networks. One of these techniques is called aggregation or in-network processing. The idea is that instead of forwarding (in case of synchronous applications) or storing (in case of asynchronous applications) raw sensor readings, data can be first processed, combined, and compressed by some distinguished sensor nodes, called aggregators.

While aggregation increases the overall efficiency of the sensor network, the aggregator nodes them elves use more resources than the regular sensor nodes. For this reason, it is desirable to change the aggregators from time to time, and thereby, to better balance the load on the sensor nodes. For this purpose, aggregator node election protocols can be used in the sensor network that allow dynamic re-assignment of the aggregator role.

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 aspects: 1) Source/

destination anonymity—it is difficult to identify the sources or the destinations of the network flows. 2) End-to-end relationship anonymity—it is difficult to identify the end to-end communication relations. To achieve anonymous MANET communications, anonymous routing protocols have been proposed.

Though a variety of anonymity enhancing techniques like onion routing [9] and mix-net [10] are utilized, these protocols mostly rely on packet encryption to hide sensitive information (e.g., nodes' identities and routing information)from the adversaries. However, passive signal detectors can still eavesdrop on the wireless channels, intercept the transmissions, and then perform traffic analysis attacks. Over the past few decades, traffic analysis models have been widely investigated for static wired networks (e.g., [9],[10], [11], [12], [13]). For example, the simplest approach to track a message is to enumerate all possible links a message could traverse, namely, the brute force approach [11].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 [14], [15], [16]and disclosure attacks [17], [18], [19], [20] are two representatives. However, all these previous approaches do not work well to analyze MANET traffic because of the following three natures of MANETs: 1) The broadcasting nature: In wired networks, a point-to-point message transmission usually has only one possible receiver. While in wireless networks, a message is broadcasted, which can have multiple possible receivers and so incurs additional uncertainty. 2) The ad hoc nature: MANETs lack network infrastructure, and each mobile node can serve as both a host and a router. Thus, it is difficult to determine the role of a mobile node to be a source, a destination, or just a relay. 3) The mobile nature: Most of existing traffic analysis models do not take into consideration the mobility of communication peers,

which make the communication relations among mobile nodes more complex. In [21], Huang devised an evidence-based statistical traffic analysis model specially for MANETs. In this model, every captured packet is treated as an 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. 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 hope 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 native 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 in accuracy in the derived probability distributions.

**2. Related Work**

Traffic analysis attacks against the static wired networks(e.g., Internet) have been well investigated. The brute forceattack proposed in [11] tries to track a message byenumerating all possible links a message could traverse. In
node flushing attacks (a.k.a blending attacks, n _ 1 attacks)[10], the attacker sends a large quantity of messages to thetargeted 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 (e.g., [12]) 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
Water marking 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 [14].

Later works such as [15] and [16] extend them to all kinds of anonymous communication systems including onion-routing[9], mix-net [10], and DC-net [22]. 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. The statistical disclosure attacks as mentioned in [17], [18], [19], and [20] are similar. 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 in [23] 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 [24], 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 anonymous routing protocols but not a general approach. Both [23] and [24] are analytical strategies which heavily rely on the deterministic network behaviors.

## 3. Proposed model – INSENS

### Our Assumption

Traffic analysis models have been widely investigated for static wired networks. 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). Many anonymity enhancing techniques have been proposed based on packet encryption to protect the communication anonymity of mobile ad hoc networks (MANETs).

Statistical traffic pattern discovery system, To disclose the hidden traffic patterns in a MANET communication system, INSENS&SMECNS 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). 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).

INSENS&SMECNS is basically an attacking system, which only needs to capture the raw traffic from the PHY/MAC layer without looking into the contents of the intercepted packets. From the captured packets, INSENS&SMECNS 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. Our empirical study demonstrates that the existing MANET systems can achieve very restricted communication anonymity under the attack of INSENS&SMECNS. The probability distributions produced by INSENS&SMECNS 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. To discover the communication patterns without decrypting the capturedpackets, we present a novel statistical traffic pattern discovery system (INSENS&SMECNS). INSENS&SMECNS works passively to perform traffic analysisbased on statistical characteristics of captured raw traffic. INSENS&SMECNS is capable of discovering the sources, the destinations, and theend-to-end communication relations. Empirical studies demonstrate that INSENS&SMECNS achieves good accuracy in disclosing the hiddentraffic patterns.

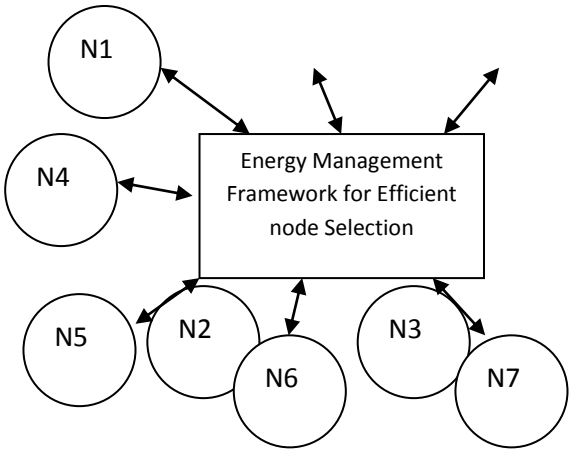


**Figure 1: Energy Management of the Wireless Sensor Network**

We further assume the communication time between the sink and sensor nodes is negligible, as compared with the sink node's travelling time. Similarly, the delay due to multi hop communications including transmission, propagation, and queuing delays is negligible with respect to the travelling time of the mobile sink in a given round. Each RP node has sufficient storage to buffer all sensed data. The mobile sink is aware of the location of each RP. All nodes are connected, and there are no isolated sensor nodes. Sensor nodes have a fixed data transmission range.

**Definition 1 (Delay of data).** The delay of data is defined as the time spent by the mobile sink moving from one sink site to the next sink site.

**Definition 2 (Network lifetime (T)).** The network lifetime (T) is defined as the elapsed time since the launch of this network till the instant that the first node dies.

**Network Model and Assumption**

The MANET has been modeled using a distributed routing protocol utilizing the diverse traffic handling by nodes through aware of their positions. Each node is supposed to be aware of its current node state and forwarding node state in order to route the data to the destination. Wireless Sensor Network does a packetization to transmit the data to a destination node through intermediate nodes.

## 3.1 SYSTEM ARCHITECTURE DESIGN

The architecture diagram clearly explains hop by hop authentication features and functionalities. The fig 4.2 describe about the system architecture for the proposed system.

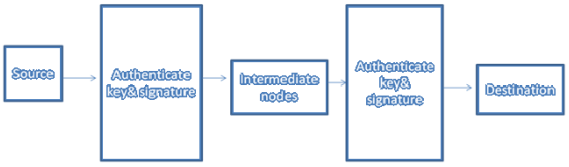


**Fig 3.1 System Architecture**

Data are communicated from one node to another node in the above process. First the source node will send the data it is passed into the automatic key generator here a secrete key will be generated automatically for the source node. After the key is generated data is passed into the network with key value in the data.

Above process is made for each and every node in the network by generating its own key until it reaches the destination.

When the data reach its destination it will check for the key of destination node, once validated data is delivered.

## 3.2 ARCHITERCTURE DIAGRAM

The architectural diagram for hop by hop message authentication.

International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue XI, November- 2016

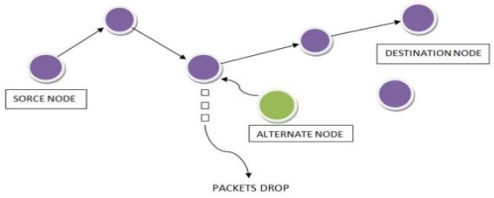


**Fig. 3.2Architecture Diagram**

When the data is transmitted from source to destination, Communication will be established in 2 ways either hop by hop or multi hop. The intermediate nodes are taken as load node. When there is energy drain in load nodes, alternative node can be replaced. This protocol is named as active protocol. Here Multicasting is also applied, so every node will easily knows the maximum energy level of other nodes.

## 4. MODULE DESCRIPTION

### 4.1 NODE FORMATION MODULE

This module is formation of nodes what all needed for sending and receiving information.
One node is assumed as sender node and another node is assumed as receiver node. And some nodes are assumed as information passing nodes.

### 4.2 DATA TRANSMISSION MODULE

The sender node sends the information to the receiver node through this module. These modules have an option for sending the file from one location to the other location. Each node has an identity using the IP address.

### 4.3 DATA RECEIVING AND VERIFICATION MODULE

This module is for receiving the information. It checks whether the information is coming from secure sender and from the correct path. After authentication, the receiver receives the information through the secure nodes.

### 4.4 EXPERIMENTAL RESULTS

The below screenshots will describe how the proposed system for identifying the adjacent nodes in the network.

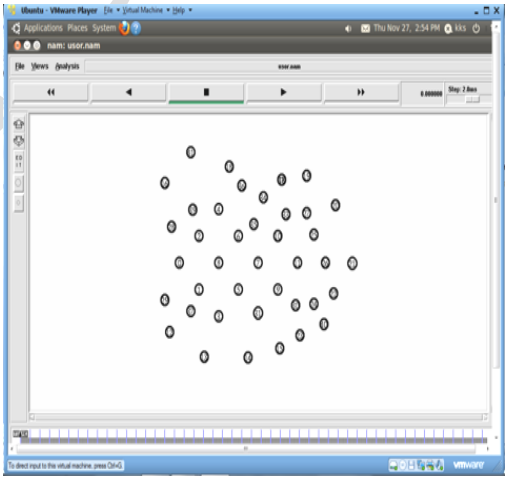

**Fig 4.1 Viewing Adjacent Nodes**

In Fig 5.1 shows the adjacent nodes which are between source and destination. Each node has a automatic key value that will be generated, when the data passed through that node.

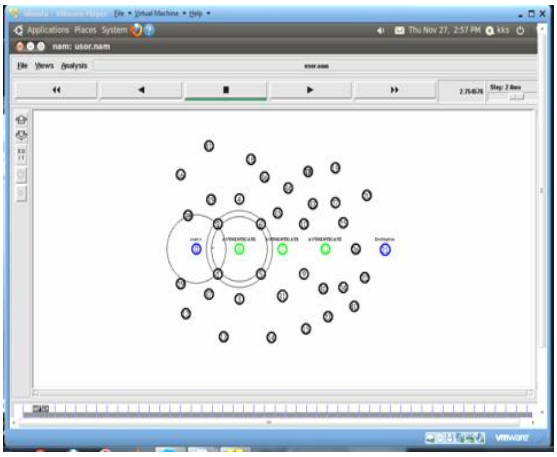

**Fig 4.2Authenticating Each Node while sending data**

In order to transfer data between nodes, one node will be selected as source node another will be destination node. Before sending data to the destination node first we have to broadcast node. By broadcasting a shortest path is identify for transferring data which is shown in the Fig 5.2 while visiting each node automatic key authentication is made on that node. While transferring data from one node to another node there is a possible for data loss, above Fig 5.3 shows the data loss in node.

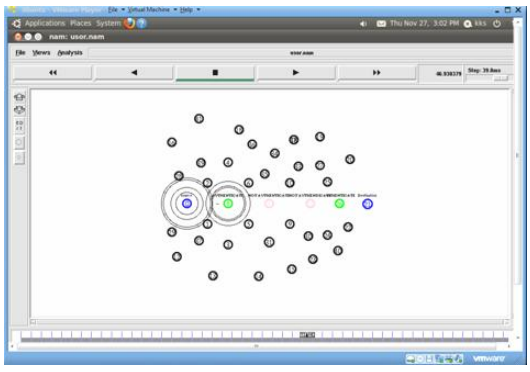

**Fig 4.3 Finding Unauthenticated Node**

Once data loss is occur it seems that the original data doesn't reach the destination. The above Fig 5.4 check for unauthenticated node in that path.

After identifying alternate node, those nodes are placed in the appropriate location. Now the source node will retransmit the data to the destination node. Finally data is reached in the destination node without data loss.

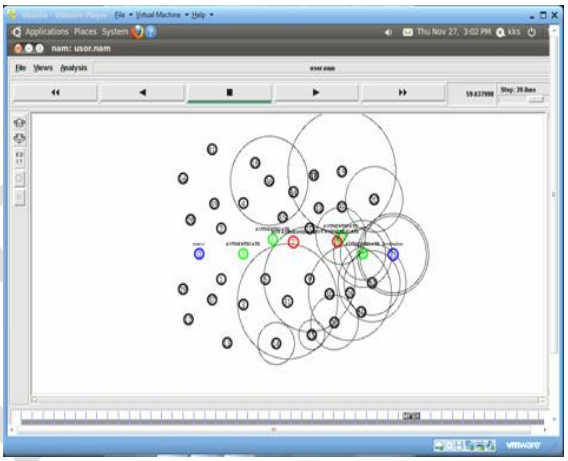

**Fig 4.4 Removing the Unauthenticated Node**

In Fig 5.55 the red color node in the path indicates the unauthenticated node. Once the nodes are identified those nodes are removed from the path. After the nodes are removed, the destination node will find the alternate node and placed in that path.

## 5. CONCLUSION

MOBILE ad hoc networks (MANETs) are originally designed for military tactic environments. MANET communications, many anonymous routing protocols such as ANODR , MASK , and OLAR have been proposed. Though a variety of anonymity enhancing techniques like onion routing and mix-net are utilized, these protocols mostly rely on packet encryption to hide sensitive information (e.g., nodes' identities and routing information)from the adversaries.

However, passive signal detectors can still eavesdrop on the wireless channels, intercept the transmissions, and then perform traffic analysis attacks. To demonstrate how to discover the communication patterns without decrypting the captured packets, we present a novel statistical traffic pattern discovery system (INSENS&SMECNS). INSENS&SMECNS works passively to perform traffic analysis based on statistical characteristics of captured raw traffic. INSENS&SMECNS is capable of discovering the sources, the destinations, and the end-to-end communication relations.

## 6. FUTURE ENHANCEMENT

The implemented work has been tested for density upto 50nodes and it can be tested for high density of nodes having bigger mix of wired nodes and ireless nodes. The high density networks shall cause the high values of reliability and having nodes with almost equal reliability value will increase the competition among the nodes. In future, this work can also be enhanced to test on the protocols. The mechanism can also be tested for other output parameters such as end to end delay, packet delivery ratio etc.

**Reference**

[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 Light weight 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 Workshops
'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 Connections 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 Un observability, pp. 10-29, 2001.

[12] W. Dai, "Two Attacks against a PipeNet-Like Protocol Once Used by the Freedom Service," http://weidai.com/freedomattacks.
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 Transactions," 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.QIN ET AL.: STARS: A STATISTICAL TRAFFIC PATTERN DISCOVERY SYSTEM FOR MANETS 191
Fig. 6. Evaluation results.

[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, "Unlink ability 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: Un conditional Sender and Recipient Un traceability," 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-aboutwi-i-location-tracking/, 2004.

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