MTPD: MANET TRAFFIC PATTERN DISCOVERY – A HEURISTIC APPROACH

[1]Arunkumar R, [2]Bharateshhegde, [3]Ganeshprasad, [4]Manoj C Jagatap, [5]Vishwas S

[1,2,3,4,5]*Department of CS&E, KVG College of Engineering, Sullia, D.K.(India)*

ABSTRACT

Anonymous Communication is the main issue in case of MANETs. It is difficult to find the source and destination of the communication link and the other nodes involved in it. Many techniques are proposed to enhance the anonymous communication in case of the mobile ad hoc networks (MANETs). However, MANETs are vulnerable under certain circumstances like passive attacks and traffic analysis attacks. Here we describe the traffic analysis problem, expose some of the methods and attacks that could infer MANETs are still weak under the passive attacks. To show how to discover the communication patterns without decrypting the captured packets, we present the paper MANET Traffic Pattern Discovery, a heuristic approach (MTPD). In order to discover the packet patterns MTPD works passively and does the traffic analysis based on the statistical characteristics of the captured raw traffic. Here we can determine the source node, destination node and the end-to-end communication path in case of mobile ad hoc networks.

Keywords-*Anonymous Communication, Mobile ad hoc network, Passive attack, Statistical traffic analysis.*

I. INTRODUCTION

MANET (Mobile ad hoc network) is an infrastructure less, wireless and self-configuring network of mobile devices. These are mainly used in defence field. Anonymous Communication is the main issue in case of MANETs. It is difficult to find the source or destination of the communication link and the other intermediate nodes involved in it. And also finding the information or data flow through the network. To be able to have the anonymous communication in the MANETs many protocols are used in case of ad hoc routing such as MASK [1], OLAR [2], ANDOR [3] etc. Along with the above protocols many techniques are used to improve the anonymity of the communication in case of MANETs like onion routing [4] which includes the multiple layers of encryption of data. It hides the routing information and identity of nodes from the unauthorized nodes. We assume the anonymity enhancing techniques are used to protect the MANETs.

However we can still detect the routing information via the passive attacks. Since 1990s traffic analysis have been used for the wired networks in order to track the data. For example brute force approach [5] to track the message in case of wired networks have gain much more importance. Now a day, statistical traffic analysis attacks have become popular due to the passive nature. Here the attackers need not change the data or information or the network nature, he/she can just collect the packets and do the traffic analysis. The predecessor attacks [6] and disclosure attacks [7] are two examples of traffic analysis attack. But these attacks cannot well efficiently analyze the traffic because of the following characteristics of the MANETs. They are; i) the broadcasting nature - where the packets are transmitted and received by many nodes hence it is difficult to identify the exact destination, ii) the ad hoc nature –the ad hoc networks are infrastructure less and each node can act as both the sender and receiver. Hence it is difficult to find the nature of the node to be the source or destination or not, iii) the mobile nature – here the nodes are movable and hence the communication between the mobile nodes are very complex to analyze.

The author proposed evidence based statistical traffic analysis model especially for MANETs in [8]. Here, every packet that is captured is treated as evidence supporting a point-to-point transmission between the source node and destination node. A sequenceof point-to-point traffic matrices are created, and thenthey are used to derive end-to-end relations between the communication paths in the network. This work provides a best practical attacking strategy against MANETs but leaves some sensible information about the communication traffic undetermined. This approach does not give a proper method to discover the actual source node and destination node in the communication path.

In this paper we introduce the concept of heuristic approach. This approach is used to discover the hidden traffic pattern in MANETs. Aim of this project is to perform passive attack and identify the source node and destination node in MANETs. “MTPD: MANET Traffic Pattern Discovery, a heuristic approach” works passively to perform traffic analysis based on statistical characteristics of captured raw traffic. From this approach we can identify the actual source node and destination nodes, and then correlate the source nodes with their corresponding destinations. To the best of our knowledge, MTPD is the statistical traffic analysis approach that takes the salient characteristics of MANETs; the broadcasting property, ad hoc property and mobile property. In all the previous approaches only the partial attacks are used, where they cannot identify both the source node and destination node at the same time for any given source or destination nodes. MTPD is an attacking system which identifies all the source nodes and destination nodes and also determines relationship between them.

In the earlier approaches, traffic analysis models have been widely exploited for static wired networks. For example, the simplest approach to track a message is to capture them one by one all possible paths a message could traverse, namely the brute force method as proposed in [5]. But because of the passive nature of 0these statistical traffic analysis attacks are very popular. Here the attackers only need to collect information and perform statistical traffic analysis silently without modifying the network characteristics.

The rest of the paper is organized as follows: Section2 describes the related work. Section 3 presents thefundamental system models and assumptions. In section 4, the implementation of MTPD is described in detail. Section 5 presents the program run, performance analysis and results. In section 6, we conclude this paper by discussing the possible future enhancements.

II. RELATED WORK

The Traffic analysis attack related to the wired network (say internet) is well studied. The brute force approach [5], to track the message in case of wired networks is very popular as it enumerates the message links that could be traversed. In case of node flushing attacks proposed in [10], the anonymous communication can be traced by the large amount of data that is injected by the attacker. The timing attack as in [9], is mainly based on the delay of the communication links between the nodes. If the attacker can find the delay in the transmission of packets on the node he can guess the data that is transmitted to and from the node by analyzing the transmission delay. The message tagging attacks proposed in [11], where the attacker attacks any one of the nodes that acts as the router in the communication path and tagging any message for the purpose of analysis. Later the attacker recognizes the tagged message in any of the intermediate nodes then he can detect the traffic flow.

The statistical traffic analysis attacks are different from the above mentioned attacks and aims to derive the network information from its statistical characteristics. Here in the passive attacks the attacker does not change the traffic behavior either by changing or inserting the data packets. He just collects the packets and does the statistical analysis. In predecessor attack [6] and onion routing [4], the attacker exactly acts as the valid node in the communication network and interacts with the other nodes. He maintains the counter with the other nodes and it is used to track the information about the traffic when the attacker is involved in the anonymous communication. But in order to do such attacks the nodes must be properly controlled by the attacker, which is not at all possible in case of mobile ad hoc networks. This is because of the ad hoc property of MANETs where the every nodes of the network are indistinguishable whether it is the source node or the destination node. Hence the attacker fails to identify the proper designation of the nods. Its behavior is completely different from that of the wired networks.

The disclosure attack described in [7], here the attacker first attacks to the source node which is already known and then discovers the destination node. The possibility is that the source node sends the packets to the multiple destination nodes hence the probability of the destination node is distributed across the network. The actual destination of the source node can be identified after the prolonged observations. This is possible only in wired networks because discovering the source node is too difficult in case of MANETs. Even if the attacker attacks the source node, the attack would be successful only if it is sure that the attacked node is the actual source node. The reason for the failure could be the mobile and ad hoc nature of the MANETs. Because of the previously mentioned three characteristics, the mobile ad hoc networks are stable against all these attacks.

As proposed in [12], the time based approach to find the actual destination of the network whose source node is known. Here the flow rates of the communication paths are discovered using packet matching by assuming that the transmission delays are associated with every intermediate node. On the basis of the calculated flow rate the network is divided into two parts, one in which the flow rate is high and the other where the flow rate is low. The area where the flow rate is high is the one where the destination node exists. In this way the destination node is found in case of networks. Liu et.al.designed and proposed a Traffic Inference Algorithm(TIA) [13] for MANETs. Here they assumed that the difference between data frames, routing frames and MAC frames is precisely visible to the passive attackers, which allows the attackers to discover the point to point traffic using MAC control frames, there by allows to find the end to end traffic using routing frames and finally discover the actual data or traffic pattern utilizing data frames. Traffic analysis in anonymous MANETs [14] and Traffic inference in anonymous MANETs [15] are two good approaches which is based on deterministic network behaviors.

III. PROPOSED SYSTEM

This section provides a brief idea about the communication between the nodes and the attacking system.

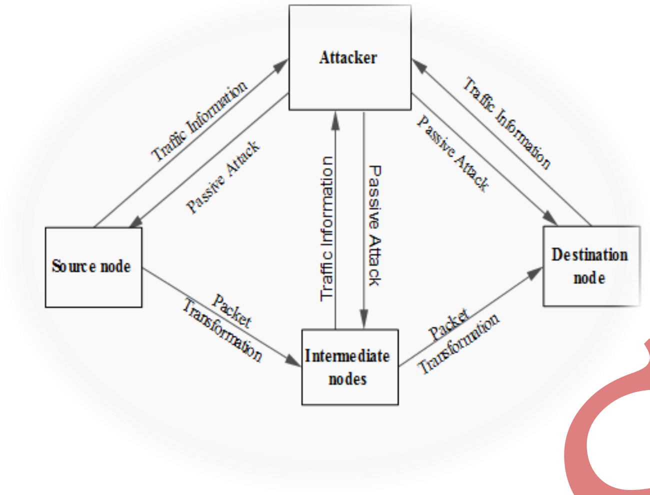


Fig 1: Architecture Diagram of MTPD

3.1 Communication Model

We consider the anonymous communication techniques as proposed in [1-4] that are available to protect the mobile ad hoc networks. But these systems are designed based on the required levels of security for MANTEs. However to focus on the statistical traffic analysis, based on the ideologies proposed in [6-8] we assume the communication system is subjected to the following model:

(i) The physical/MAC layer is connected and controlled by 802.11 protocols (network standard). All the MAC packets are protected by encryption so that the attackers cannot look into the packets.

(ii) Padding is done to all the packets to make the equal sized packets so that the attackers cannot track them according to the size.

(iii) The source or destination addresses in MAC and IP headers are all set to 1 (broadcasting address), so to prevent the attackers from discovering the point to point communication path.

(iv) The information about the routing and traffic patterns is disclosed.

(v) Extra packets and extra information are not added to the network because the MANTEs have the limited resources.

3.2 Attack Model

The main aim of the attacker is to detect the traffic patterns in the nodes. But MANETs are much secured due to three characteristics; (i) The broadcasting property, (ii) The mobility property (iii) The ad hoc property. Because of the above characteristics of MANETs all the previous approaches failed to analyze MANET traffic. But the MTPD is capable of analyzing the traffic as it uses statistical traffic analysis approach. Here the attacker first joins the existing network and does the passive attack. There are three possibilities as shown in the figure 1;

- First possibility is that the attacker may directly attack the source node and capture the packets and hence find the traffic information.
- Second chance is that he may attack one of the intermediate nodes and capture the packets and hence find the traffic information.

- At the last he may attack to the destination and capture the packets in order to get the traffic information.

IV. IMPLEMENTATION OF MTPD

This section presents the detailed implementation of the proposed system with the implementation of the communication model and the attack model.

.

4.1 Communication

In order to illustrate the communication between the nodes and the basic working idea of MTPD we consider the simple scenario as shown in the Fig. 1 as an example.

The figure 2 shows the simple mobile ad hoc network. There are three mobile nodes (A, B, C), node B is in the transmission range of node A and node C is in the transmission range of node B but not located in that of node A. Suppose if node A needs to send the data or packets to the node C, it is broadcasted via node B. If any of the nodes is not in the transmission range of any nodes then transmission between those nodes is not possible.

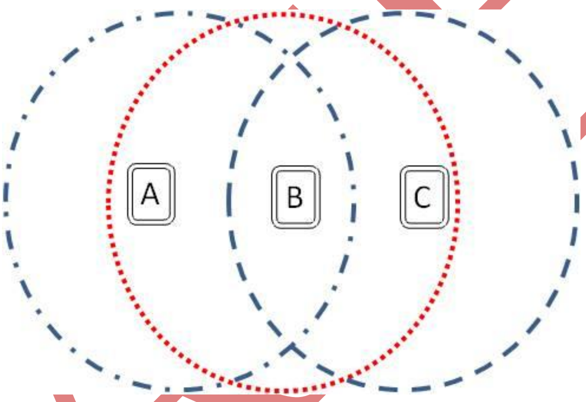


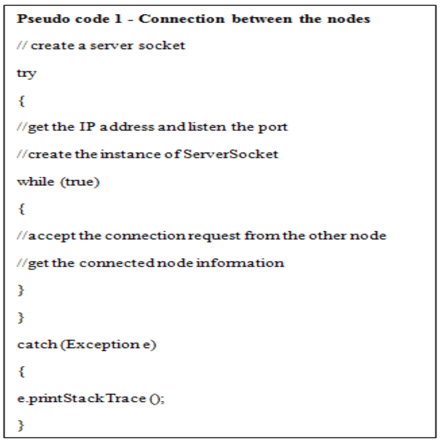
Fig. 2: A simple wireless mobile ad hoc network

In the network there may be N nodes if we need to communicate between the node 1 and node N then there must be a link between them or else the nodes must be within the transmission range of the network. In our project we have used a socket which uses TCP (Transmission Control Protocol) for the initialization of connection and the reliable communication between the nodes. TCP is used over the IP (Internet Protocol) which is called as TCP/IP. In order to establish a TCP connection a server and client are required. Firstly, a server is set up to listen at a given port. The server waits and does nothing until a client attempts to connect that port. If everything is fine, the connection is successful and both the server and client have an instance of the Socket class. From each instance of this class, an input stream and an output stream can be obtained, and all communication between the nodes is done via these streams. When the server gets a request from the client the server accepts the connection request. The data is sent from one node to other node when required. In order to accept the data from the other node, the instance of the ServerSocket is created. Here also the input stream and output stream are obtained and used to handle the communication.

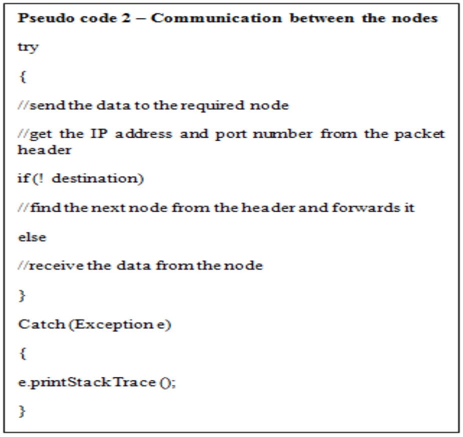
The Fig. 3 shows the pseudo code for the connection between the nodes and the Fig. 4 shows the pseudo code for the communication between the nodes of the mobile ad hoc network as described in the communication model.

4.2 Attacking the MANETs

The communication between the nodes takes place via TCP-IP sockets and the data is transmitted between the nodes using the instances of Socket and ServerSocket class.



```
Pseudo code 1 - Connection between the nodes
// create a server socket
try
{
//get the IP address and listen the port
//create the instance of ServerSocket
while (true)
{
//accept the connection request from the other node
//get the connected node information
}
}
catch (Exception e)
{
e.printStackTrace ();
}
```



```
Pseudo code 2 – Communication between the nodes
try
{
//send the data to the required node
//get the IP address and port number from the packet header
if (! destination)
//find the next node from the header and forwards it
else
//receive the data from the node
}
Catch (Exception e)
{
e.printStackTrace ();
}
```

Fig. 3: Pseudo code for the connections **Fig. 4: Pseudo code for the communication**

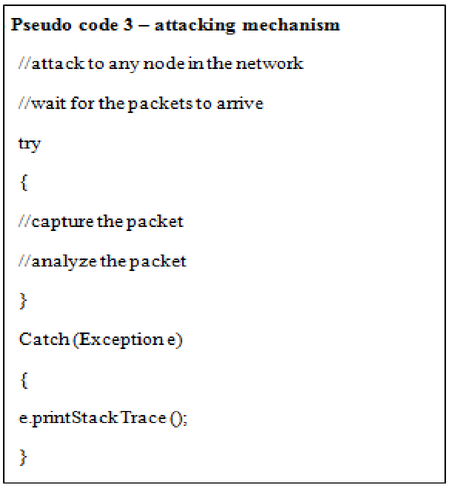
The data is transmitted in the form of packets, which is of 48 bits. Each packet consists of header and the payload. The data is delivered to the proper destination node with the help of the packet header. When any node receives the packet from the other nodes, it checks the header of the packet which consists of many information like the source, destination and the size of the data to be transmitted. Here we attack to the Physical layer (used for the physical connection between the nodes) or MAC layer (sub layer of the data link layer) of the network and capture the packets. Once the packet is captured, the header is used by the attacker to find the IP address of the source node, destination node and the other nodes involved in the communication.

V. PERFORMANCE ANALYSIS AND DISCUSSION

Here, the performance analysis is presented which consists of two components namely demonstration and evaluation. First we demonstrate the working of MTPD i.e., how we can detect the source node, destination node and the other nodes involved in the communication. Then we evaluate the performance of the system.

5.1 Demonstration

For the purpose ofdemonstration we created five nodes namely node1, node2, node3, node4, node5 and the Attacker node. The communication takes place between the nodes via the instances of Socket and ServerSocket class as specified in the section 4.1. We used Java NetBeans IDE for the above purpose. The attacker node works passively as mentioned in section 4.2.



```
Pseudo code 3 – attacking mechanism
//attack to any node in the network
//wait for the packets to arrive
try
{
//capture the packet
//analyze the packet
}
Catch (Exception e)
{
e.printStackTrace ();
}
```

Fig. 5: Pseudo code for the attacking mechanism

The fig. 5 shows the pseudo code for the attacking mechanism as described in the attacking model.

The attacker node first joins the existing mobile ad-hoc network consisting of different nodes. The data transmission may take place between any nodes. The attacker is not aware of the communication i.e., the attacker don’t have any information about the source node, destination node and the other nodes which may be involved in the communication. The attacker attacks to any one of the nodes of the network and works passively to discover the traffic pattern and information. Here we collect the information like the IP address of the source node, destination node and also we could determine the intermediate nodes involved in the data transmission.

5.2Evaluation

From the previous works, we see that the traffic patterns discovered by MTPD are good indicatorsof the actual traffic patterns, i.e. actual sources,destinations and end-to-end links. Different strategiescan be used to speculate the actual traffic patterns. Suppose if the attacker knows the exact source node or the destination node then the attacker could directly attack that node and capture the packets. Or if the attacker attacks one of the intermediate nodes then it is easy to analyze the traffic pattern. But it is not the case, here the attacker neither know the source node or the destination node nor the other nodes involved in the communication because of the three main natures of the MANETs like the ad hoc nature, mobile nature and the broadcast nature.

Hence it is difficult to attack and collect the traffic and packet information. To conclude the evaluation, the hidden traffic patternscan be discovered in good accuracy using MTPD, even without the actual sources,destinations and end-to-end communication relations known to the attacker.

By using the following graphs we can evaluate the performance of our attacking system. Here the attacking probability varies node to node while the communication pattern remains constant to every node.

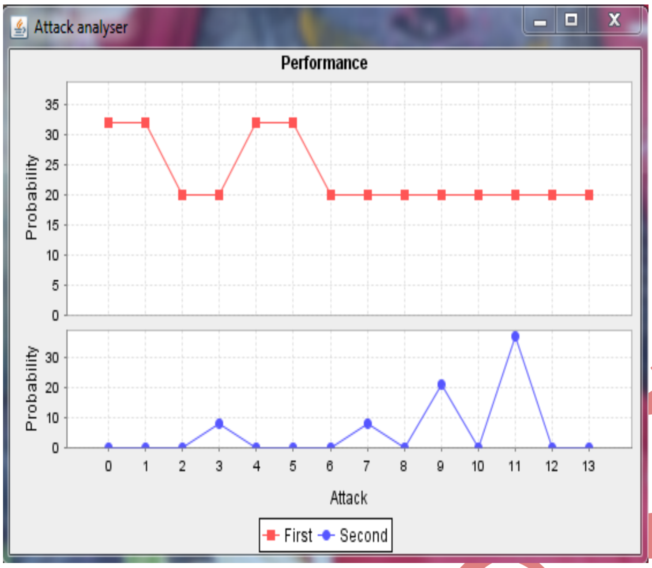


Fig.6 Graph when attacked to node 1

In Fig.6 the graph shows the attacking probability when the attacker attack to node 1. The data is sent from node 5 to node 1. The Fig.7 shows the attacking probability when the attacker attacks to the node 1. Here the data is sent from node 4 to node 1. The Fig.8 shows the attacking probability when the attacker attacks to the node 5. The data is sent from node 1 to node 5.

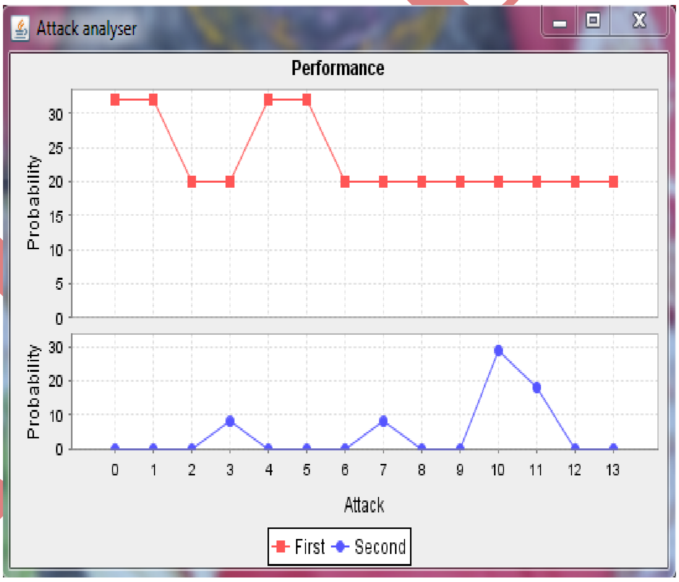


Fig. 7 Graph when attacked to node 1

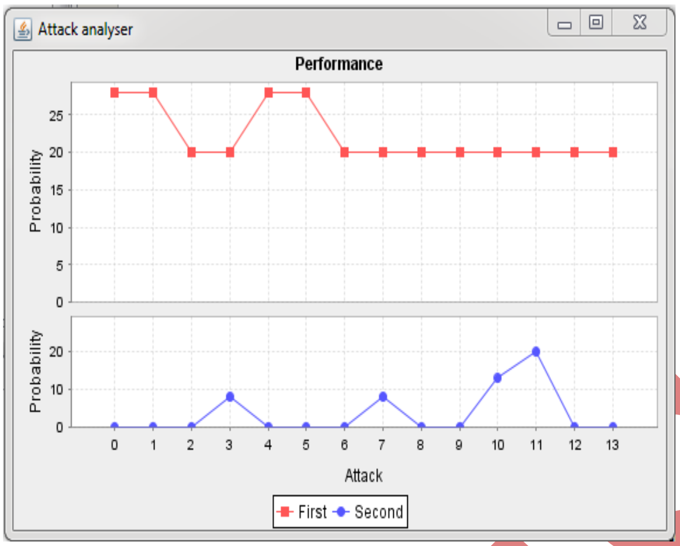


Fig.8 Graph when attacked to node 5

VI. CONCLUSIONS AND FUTURE ENHANCEMENT

In this paper, we propose an idea of attacking mobile ad hoc networks. MTPD is basically an attacking system for MANETs which works passively for identifying the traffic patterns. It captures the packets from the MAC layer or the physical layer of the network and need not look into the contents of the captured traffic. Here we use the heuristic approach for analyzing the captured packets and to discover the hidden traffic patterns.

Using the determined IP address of the source and destination nodes we can discover the physical location of the mobile devices. It could be upgraded for military uses for the defense purpose by traffic monitoring. Use of the sensors in the routers, will improve the attack as we can find the exact location of the source and the destination devices.

REFERENCES

[1] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “MASK: Anonymous on-demand routing in mobile ad hoc networks,” IEEE transactionson wireless communications, vol. 5, no. 9, pp. 2376–2385, 2006.

[2] Y. Qin and D. Huang, “OLAR: On-demand Lightweight Anonymous Routing in MANETs,” in Proceedings of the 4thInternational Conference on Mobile Computing and UbiquitousNetworking (ICMU), 2008, pp. 72–79.

[3] J. Kong, X. Hong, and M. Gerla, “An identity-free and on demand routing scheme against anonymity threats in mobile ad hoc networks,” IEEE Transactions on Mobile Computing, vol. 6, no. 8, pp. 888–902, 2007.

[4] M. Reed, P. Syverson, and D. Goldschlag, “Anonymous connections and onion routing,” Selected Areas in Communications, IEEE Journal on, vol. 16, no. 4, pp. 482–494, 2002.

[5] J. Raymond, “Traffic analysis: Protocols, attacks, design issues, and open problems,” Lecture Notes in Computer Science, pp. 10–29, 2001.

[6] M. Reiter and A. Rubin, "Crowds: Anonymity for web transactions,"ACM transactions on information and system security, vol. 1, no. 1, pp. 66–92, 1998.

[7] G. Danezis, "Statistical disclosure attacks: Traffic confirmation in open environments," in Proceedings of Security and Privacy in the Age of Uncertainty, (SEC 2003), 2003, pp. 421–426.

[8] D. Huang, "Unlinkability Measure for IEEE 802.11 based MANETs," IEEE Transactions on Wireless Communications, no. 2, pp. 1025–1034, Feburary 2008.

[9] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," Selected Areas in Communications, IEEE Journal on, vol. 16, no. 4, pp. 482–494, 2002.

[10] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communications of the ACM, vol. 24, pp. 84–88, 1981.

[11] W. Dai, "Two attacks against a PipeNet-like protocol once used by the Freedom service," http://weidai.com/freedom-attacks. txt.

[12] T. He, H. Wong, and K. Lee, "Traffic analysis in anonymousmanets," in Military Communications Conference, 2008.MILCOM 2008.IEEE. IEEE, 2008, pp. 1–7.

[13] Y. Liu, R. Zhang, J. Shi, and Y. Zhang, "Traffic inference in anonymous manets," in Sensor Mesh and Ad Hoc Communicationsand Networks (SECON), 2010 7th Annual IEEE CommunicationsSociety Conference on. IEEE, 2010, pp. 1–9.

[14] T. He, H. Wong, and K. Lee, "Traffic analysis in anonymous manets," in Military Communications Conference, 2008.MILCOM2008.IEEE. IEEE, 2008, pp. 1–7.

[15] Yang Qin, Dijiang Huang, *Senior Member, IEEE,* and Bing Li"STARS: A Statistical Traffic Pattern DiscoverySystem for MANETs", 2013.