International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

# DISCOVERY OF TRAFFIC PATTERN IN MANETS

**K.GAYATHRI[1], S.SIVAGAMI[2]**

[1]Student, M.E-CSE (with spln in networks), Dept of IT, Dhanalakshmi Srinivasan Engg College, India

[2]Associate professor, M.Tech, Dept of IT, Dhanalakshmi Srinivasan Engg College, India

Article Received: 11/04/2015 | Article Revised on:19/04/2015 | Article Accepted on:23/04/2015


**ABSTRACT**

Wireless networks are defined as that the network nodes which are connected by wireless data connections. The devices are connected via wireless link to communicate in Manets. This communication can be done without decrypting the captured packet. This works passively to perform traffic analysis based on the captured raw packets. Measuring the packet delivery ratio and energy decreased performance of end-to-end nodes is the one of the most convoluted issues in wireless networks. This paper proposes a heuristic approach with dynamic route flows. This approach improves performance of packet delivery ratio, energy drop and delay performance for dynamic wireless. Furthermore this mechanism achieves better concert in terms of end-to-end delay and packet delivery ratio.

**Key Words**—End-to-end delay, Mobile ad-hoc network ,passive attack



## I. INTRODUCTION

Manets is nothing but Mobile Ad hoc Networks, it is majorly used in Military applications. Found that it is difficult to communicate because cannot identify the sender and receiver and peer to peer relations. Can able to communicate in Manets through ANODR[1], MASK[2] & OLAR[3] (see more in [4], [5], [6], [7], and [8])protocols. Onion routing[9] and Mix net[10] are the two protocols to protect the important data's from the hijackers, but however they are getting through wireless channels without changing the original message or information. For past few decades traffic analysis models have been analyzed in static wired networks. An active adversary can arbitrarily modify the computations and messages (adding and deleting) whereas a passive adversary can only listen. For example, an external active adversary can remove and add messages from the wire(s) he controls and a passive internal adversary can easily correlate messages coming in a compromised node with messages going out (but can't modify them). This activity is similar to brute force approach that could traverse a message [11]. All the approaches does not work well to analyze the traffic because of nature of Mantes: 1) The broadcasting nature: In wired network has only one possible receiver i.e. point to point packet transmission and in the wireless transmission packet can be broadcasted so it's have multiple possible receivers so its uncertainty 2) The ad-hoc nature: This network does not have fixed infrastructure and each mobile node can be serve as host and route 3) The mobile nature: To make the communication relation among mobile

nodes more complex. A purpose of traffic analysis is to reveal who is talking to whom. The anonymous connections described here are designed to be resistant to traffic analysis i.e. to make it difficult for observers to learn identifying information from the connection (e.g., by reading packet headers, tracking encrypted payloads, etc.). Any identifying information must be passed as data through the anonymous connections. Our implementation of anonymous connections, onion routing, provides protection against eavesdropping as a side effect. Onion routing provides bidirectional and near real-time communication similar to TCP/IP sockets connections.

The new anonymity threat poses challenging constraints on routing and data forwarding. The purpose of this paper is to study the characteristics of passive anonymity attacks against routing schemes in a mobile ad hoc environment. The goal of such attacks is very different from other related routing security problems such as resistance to route disruption or prevention of "denial-of-service" attacks. Evidence-based statistical traffic analysis model can be used in MANETs. In this model, every packet is treated as evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. They can create a point to point transmission and then created end to end (multi-hop) transmission. This can be used for attacking framework against MANETs but the communication patterns are undiscovered. 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 sequence of point-to-point traffic matrices are created, and then they 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.

This project is to perform passive attack and identify the source node and destination node in MANETs.

In the 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, discovery of traffic pattern 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 .Discovery of traffic pattern is an attacking system which identifies all the source nodes and destination nodes and also determines relationship between them.

The organization of the paper as follows. In section II, the system model is defined. In section III the proposed system is explained with heuristic approach. Section IV describes the performance analysis using simulation and results.

**II. SYSTEM MODEL**

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

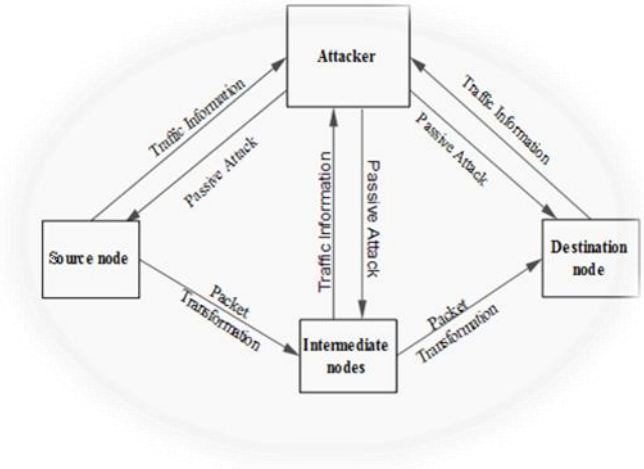


Fig 1: Architecture Diagram for Discovery of traffic pattern

2.1 Communication Model

The anonymous communication techniques as proposed in [1-4] that is 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.

2.2 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.

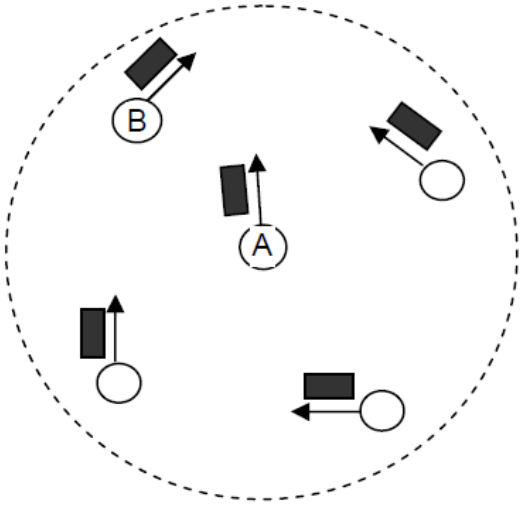


Fig 2: An anonymous broadcast network

In an anonymous broadcast network, each attack may take a bit different form, in that the attacker searches for correlation between apparently independent transmissions by different nodes (see Fig. 2) For example, Node A transmits a frame at time t, and node B, one of its neighbors, transmits at time t+€. This may suggest that node B is the receiver of node A's frame and is forwarding the frame to its next hop. However, for this timing attack to succeed, the following conditions must be satisfied:

1. The queue is empty when node _receives the frame, and

2. All other neighbors of node have no frames to transmit.

If any of the above conditions is not satisfied, then the probability of a successful attack would be reduced, due to a larger delay between two transmissions of the same frame. This suggests that each node having a non-empty queue, i.e., always in saturation mode, has benefits to security.

**III .ATTACKING MANETS USING HEURISTIC APPROACH**

The communication between the nodes takes place via TCP-IP sockets and the data is transmitted between the nodes in mobile Ad-hoc networks. 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 much 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. Here, the performance analysis is presented which consists of two components namely demonstration and evaluation.

3.1 DEMONSTRATION

First demonstrate the working of heuristics approach i.e., how we can detect the source node, destination node and the other nodes involved in the communication. Then evaluate the performance of the system. Demonstration For the purpose of demonstration created five nodes namely node1, node2, node3, node4, node5 and the Attacker node. The communication takes place between the nodes via the instances of routing path. Here used oracle VM virtual box for the above purpose.

3.2 EVALUATION

From the previous works, that the traffic patterns discovered by heuristics approach 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. 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 patterns can be discovered in good accuracy, 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.

**IV. SIMULATION AND RESULTS**

The trade-off between packet delivery and delay is analyzed using network simulator. Network simulator is constantly maintained and updated by its large user base and a small group of developers at ISI. In this system the performance analysis is done by using the system of heuristic approach in wireless network. The performance of the routing protocol is analyzed by considering three parameters as follows: Delay, Throughput and packet delivery ratio.

*4.1* Network Environment Setup and Configuration

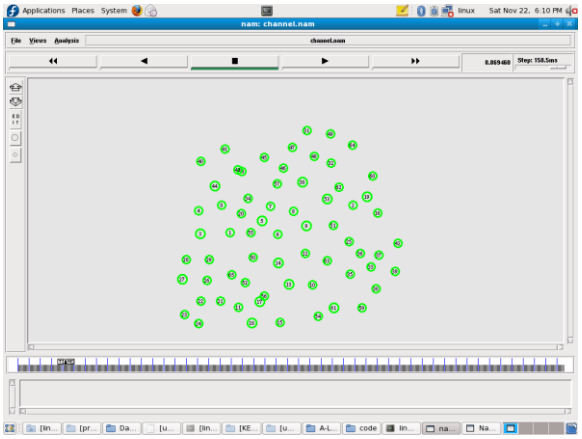

Fig 3 Simulation environment

The network animator is a powerful tool for teaching networking concepts. The IP protocols typically visualized the animations of the system performance. The parameters are used to discuss the closed form solution of packet delivery and end to end delay in wireless networks. The simulation results are displayed with graph analysis using network animator.

*4.2 Delay performance*

The End-To-End Delay is the time of generation of a packet by the source up to the destination reception. This the time that a packet takes to go across the network.

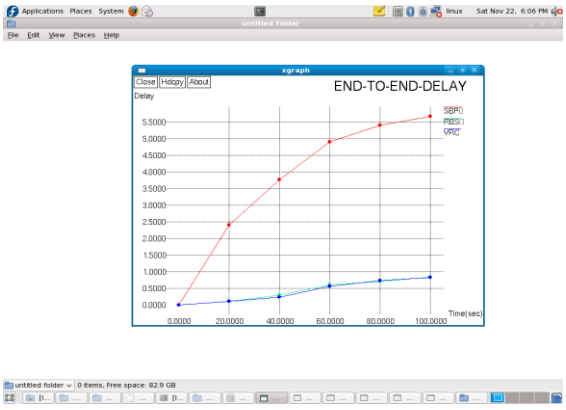


Fig. 4 End- to end delay graph result

4.3 Throughput performance

Throughput is defined as the ratio of the total data reaches a receiver from the sender. The time taken by the receiver to receive the last message is called as throughput.

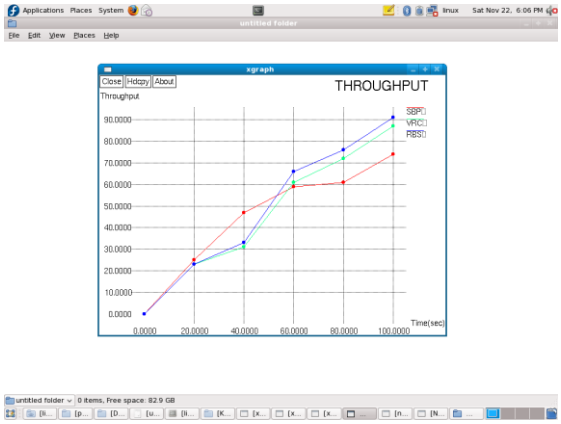


Fig. 5 Throughput analysis

*4.4 Packet delivery ratio*

The ratio of the number of delivered data packets to the destination.

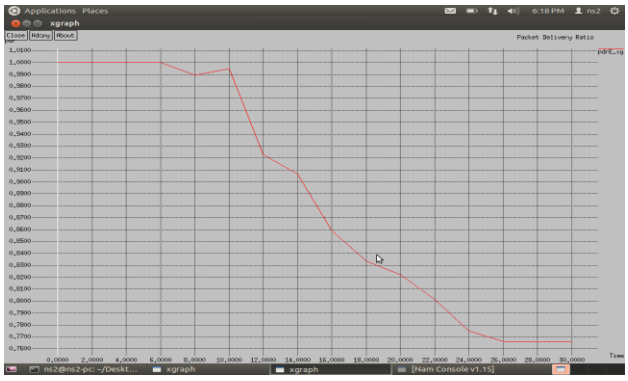


Fig. 6 Packet delivery ratio

This illustrates the level of delivered data to the destination.

**V. CONCLUSION AND FUTURE WORK**

In this paper traffic pattern discovery 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 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, and then 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 well as the exact location of the source and the destination devices.

**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 Workshops '06), pp. 133137, 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 Unobservability, 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.