International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 2, pp: (450-453), Month: April - June 2015, Available at: www.researchpublish.com

Disclosing Hidden Traffic Pattern Using Stars for MANET's

Keerti Gouri[1], Dr. Ravindra E[2]

[1]Student (M-Tech), [2]HOD, [1,2] ECE Dept, Gurunanakdev Engineering College, Bidar, Karnataka, India.

Abstract: **Many nameless augmentation methods have been intended pertaining to packet encryption to defend communication secrecy of mobile ad-hoc networks. Where as in this paper, MANET's are quiet unsafe covered by passive statistical traffic finding attacks. To explain how to come across the communication patterns without decrypting the captured packets, a new method that is statistical traffic pattern discovery systems for MANET's(STARS) is introduced. STARS works quietly to carryout traffic analysis in reference to statistical features of captured raw traffic. A STAR is capable of finding sources, the destinations, and end-to-end communication relations. Experimental studies demonstrate that STARS achieves good accuracy in disclosing the hidden traffic patterns.**

Keywords: **Anonymous communication, mobile ad hoc networks, statistical traffic analysis.**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are originally designed for military tactic environments. Communication secrecy is a serious issue in MANETs, which usually consists of the following aspects: 1) Source/ destination secrecy—it is complicated to classify the sources or the destinations of the network flows. 2) End-to-end relationship secrecy—it is complicated to identify end to end communication relation. To accomplish anonymous MANET communications, several anonymous routing protocols such as ANODR[1] , MASK[2] , and OLAR[3] have been anticipated. even if a variety of anonymity enhancing techniques like onion routing [9]and mix-net[10] are utilized, these protocols mostly rely on packet encryption to conceal sensitive information (e.g., nodes' identities and routing information) from the adversaries. Although, 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 broadly investigated for fixed wired networks. For example, the simplest approach to track a message is to specify all possible links a message could traverse, namely, the brute force approach. Recently, statistical traffic analysis attacks have gripped broad interests due to their passive nature, i.e., attackers only require to collect information and carry out analysis quietly without altering 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 examine 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. Whereas in wireless networks, a message is broadcasted, which can have several possible receivers and so incurs extra insecurity. 2) The ad hoc nature: MANETs lack network infrastructure, and every mobile node can serve as both a host and a router. Therefore, it is difficult to find out the role of a mobile node to be a source, a destination, or just a relay. 3) The mobile nature: Most of presented traffic analysis models do not take into consideration the mobility of communication peers, which make the communication relations peers, which make the communication relations among mobile nodes more complex.

A. Related Work:

Traffic analysis attacks adjacent to the static wired networks (e.g., Internet) have been well defined. The brute force attack [11] tries to track a message by finding all possible links a message could traverse. In node merger attacks, the hacker sends a vast quantity of messages to the embattled inscrutable system called as mix-net. Since many of the messages customized by the scheme are produced by the hacker, the hacker can track the rest a few messages. The timing attacks[9] focus on the delay on each communication path. If the hacker can see the latency of each path, he can compare the messages coming in and out of the system by calculating their transmission latencies. The message tagging attacks require hackers to occupy at least one node that works as a router in the communication path so that they can also tag some of the forwarded messages for traffic analysis .Different from the attacks which mentioned above, statistical traffic analysis intend to find sensitive information from the statistical characteristics of the network traffic, for example, the traffic volume. The source usually does not change the network behavior (such as modifying packets). The only thing they do is to quietly collect traffic information and perform statistical calculations. The ancestor attacks are first pointed out by Reiter and Rubin. Later works extend them to all kinds of inscrutability communication systems including onion routing[9] , mix-net, and DCnet[10]. In a typical predecessor attack, the hackers act exactly as legitimate nodes in the network communications. They preserve a single predecessor counter for every valid node in the system. When an hacker finds himself to be on an mystery path to the destination, he increments the shared counter for its predecessor node in this path. The counters are then used for the attackers to deduce the promising source nodes of the given destination. clearly, to launch such an attack, a large number of justifiable nodes must first be compromised and controlled by the attackers. This is typically not achievable in MANETs. Furthermore, in a MANET protected by secrecy enhancing techniques, it is a complicated job 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 typically 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.

B. Problem Statement:

Many inscrutability enhancing techniques have been proposed based on packet encryption to defend the communication secrecy of mobile ad hoc networks (MANETs). These protocols mostly rely on packet encryption to conceal sensitive information (e.g., nodes' identities and routing information) from the adversaries. However, inactive signal detectors can still eavesdrop on the wireless channels, interrupt the transmissions, and then carry out traffic analysis attacks. Here each captured packet is treated as evidence supporting a point-to-point (one-hop) transmission among the sender and the receiver. A series of point-to-point traffic matrices is created, and then they are used to develop end-to- end (multihop) relations. This approach provides a sensible attacking framework adjacent to MANETs but still leaves significant information about the communication patterns undiscovered.

C. Problem Solution:

A novel statistical traffic pattern discovery system (STARS). STARS 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, STARS includes two major steps: 1) 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 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 STARS is twofold: 1) To the best of our knowledge, STARS is the first statistical traffic analysis approach that considers the salient characteristics of MANETs: the broadcasting, ad hoc, and mobile nature; and 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.

D. Performance Metrices and Simulation Setup:

We evaluate the performance according to the following metrics:

1. Average End-to-end Delay: It is the total time taken by the nodes to transmit the data to the destination.

2. Throughput: It is the ratio of number of received packets to the sent packets.

3. Packet delivery ratio: It is calculated by dividing the number of packets received by the destination through the number of packets originated by source.

TABLE I. SIMULATION SETUP

Simulation parameters	Simulation values
Channel type	Wireless channel
Propagation model	Two-ray ground
Network interface type	Phy/wireless phy
Interface queue type	Queue/drop tail/priqueue
Transmission range	250 m
Network dimension	1182x601
Queue capacity(in packets)	50
MAC protocol	IEEE 802.11
Simulation time	20 sec
Antenna type	Omni-antenna

II. RESULTS & PERFORMANCE ANALYSIS

Throughput v/s number of nodes

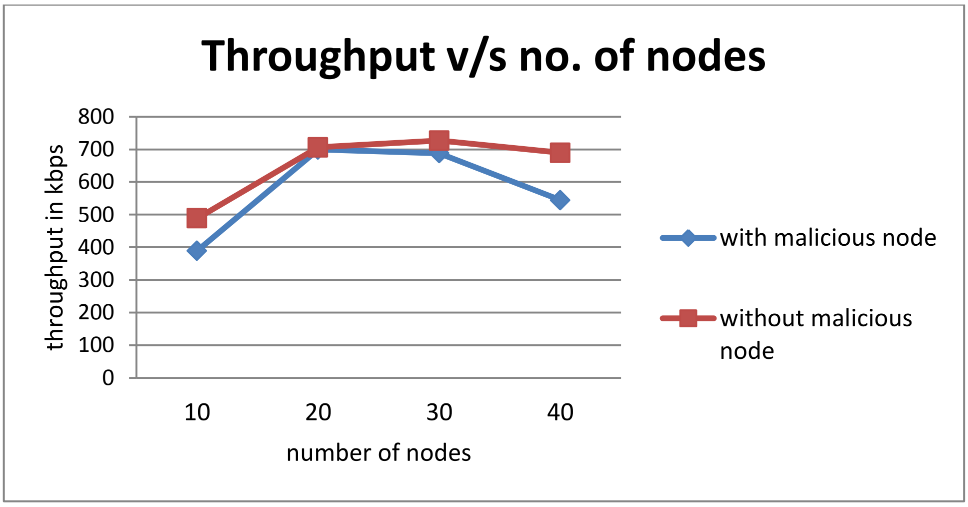

Fig.1.Throughput v/s no. of nodes

In above figure we can observe that STAR has high throughput in case of without malicious node compared to with malicious node.

End-to-End Delay v/s Number of Nodes

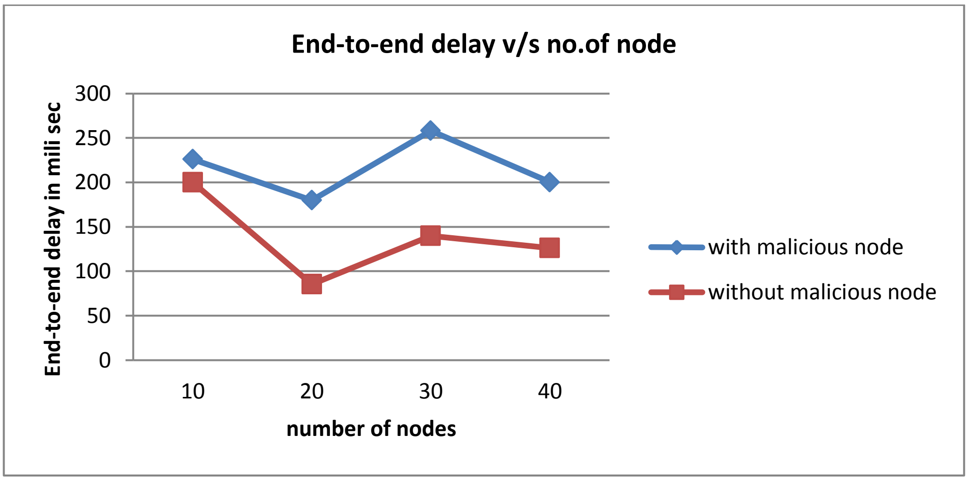

Fig.2. End –to –end delay v/s no. of nodes

In above graph we can observe that the end-to-end delay decreases in case of without malicious node compared to with malicious node..

PDR v/s Number of Nodes

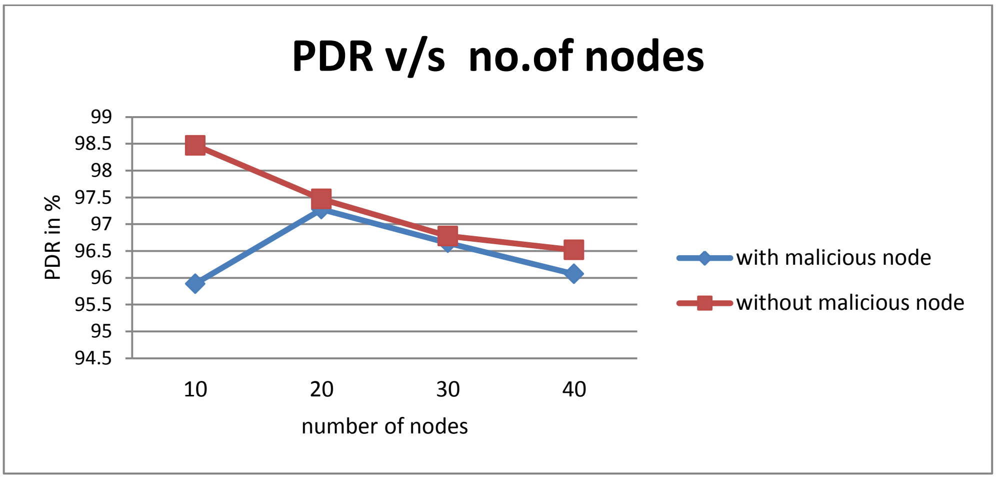

Fig.3. PDR v/s no. of node

From the above graphs we can observe that the PDR of STAR is better in case of without malicious node compared to with malicious nodes.

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

III. CONCLUSION

Here we propose a novel STARS for MANETs. STARS are 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. The hidden traffic patterns can be discovered in good accuracy using STARS, even without the number of actual sources, destinations, and end-to-end communication relations known to the traffic analyzers. Our simulation results shows that the existing MANET systems can achieve very restricted communication anonymity under the attack of STARS.

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 ComputerNetworks (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.