International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 1, January-February 2015 **ISSN 2278-6856**

Study of Statistical Traffic Pattern Discovery System for Anonymous MANET Communications

Nitin Malaviya[1] , Mayura Sasane[2], Dharmesh Dhangar[3]

[1]PG Scholar, Computer Science & Engineering,
Parul Institute of Technology,Vadodara,India.

[2]Assistant Professor, Computer Science & Engineering,
Parul Institute of Technology,Vadodara,India.

[2]Assistant Professor, Computer Science & Engineering,
Parul Institute of Engineering & Technology,Vadodara,India.

Abstract

Many anonymity enhancing techniques have been proposed based on packet encryption to protect the communication anonymity of mobile ad hoc networks (MANETs). However, in this paper, we show that MANETs are still vulnerable under passive statistical 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 (STARS). STARS works passively to perform traffic analysis based on statistical characteristics of captured raw traffic. STARS is capable of discovering the sources, the destinations, and the end-to-end communication relations. Empirical studies demonstrate that STARS achieves good accuracy in disclosing the hidden traffic patterns.

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

1.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 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, many anonymous routing pro-tocols such as ANODR [1], MASK [2], and OLAR [3] (see more in [4], [5], [6], and [7]) have been proposed. 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.For example, the simplest approach to track a message is to enumerate all possible links a message could traverse, namely, the brute force approach [8]. 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).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 act 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 con-sideration the mobility of communication peers, which make the communication relations among mobile nodes more complex.

1. SURVEY ON STATISTICAL TRAFFIC PATTERN DISCOVERY SYSTEM FOR ANONYMOUS MANET COMMUNICATIONS

Reusing the evidence-based model, in this paper, we propose 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 tech- nique, 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. STARS is a complete attacking system that first identifies all source and destination nodes

and then determines their relationship.

STARS: A Statistical Traffic Pattern Discovery System for Anonymous MANET Communications [15]

Authors: Yang Qin and Dijiang Huang Arizona State University

In this paper, we propose a Statistical Traffic pattern discovery System (STARS) based on Eigen analysis which can greatly improve the accuracy to derive traffic patterns in MANETs. STARS intend to find out the sources and destinations of captured packets and to discover the end-to-end communication relations. The proposed approach is purely passive. It does not require analyzers to be actively involved in MANET transmissions and to possess encryption keys to decrypt traffic. We present theoretical models as well as extensive simulations to demonstrate our solutions.

Advantages:

- System provides better result compared to real MANET traffic patterns.
- Improve the accuracy of the end-to-end traffic matrix.

Disadvantages:

- We need to test the system with different mobility models rather than just Using Random Way-point model
- Test the system with different traffic model instead of using CBR traffic.

MTPD: MANET TRAFFIC PATTERN DISCOVERY –A HEURISTIC APPROACH [12]

Author: ArunkumarR,Bharateshhegde, Ganeshprasad, Manoj C Jagatap, Vishwas S

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 is use 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 describes 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 and the end-to-end communication path in case of mobile ad hoc networks. In this paper we introduce the concept of heuristic approach. This approach is used to discover the hidden traffic pattern in MANETs. Goal of this project is to perform passive attack and find out 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 characteristic of captured raw traffic. From this approach we can identify the actual source node and destination nodes, and then correlate the source node with their corresponding destination. To the best of our knowledge, MTPD is the statistical traffic analysis approach that takes the salient characteristics os 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.

Advantages:

- works passively for identifying traffic pattern

Traffic Inference in Anonymous MANETs [10]

Author: Yunzhong Liu, Rui Zhang , Jing Shi, and Yanchao zhang

The open wireless medium in a mobile ad-hoc network (MANET) enables malicious traffic analysis to dynamically infer the network traffic pattern in hostile environments. The disclosure of the traffic pattern and its changes is often devastating in a mission-critical MANET. A number of anonymous routing protocols have been recently proposed as an effective countermeasure against traffic analysis in MANETs. In this paper, we propose a novel traffic inference algorithm, called TIA, which enables a passive global adversary to accurately infer the traffic pattern in an anonymous MANET without compromising any node. As the first work of its kind, TIA works on existing on-demand anonymous MANET routing protocols. Detailed simulations show that TIA can infer the traffic pattern with an accuracy as high as 95%. Our results in this paper highlight the necessity for cross-layer designs to defend a MANET against traffic analysis. In this paper, we propose a novel traffic inference algorithm called TIA. Which enables a passive global adversary to accurately infer the traffic pattern in an anonymous MANET without compromising any node.

Advantages:

- TIA works on on-demand Anonymous MANET routing

Disadvantages:

- Complex to implement and difficult to compare with other methods

Traffic Analysis in Anonymous MANETs [9]

Author: Ting Hi, Ho Yin Wong, and Kang –Won Lee

This paper addresses the problem of non-intrusive traffic analysis of anonymous mobile ad hoc networks (MANETs). The goal is to trace down the destination of a some source node with the least dependency on the essential network infrastructure. Specifically, it is assumed that nodes in the network do not participate in tracing, the eavesdropper is not allowed to tamper traffic, and both the payload and the packet headers are encrypted at every hop. To deal with these constraints, a timing-based approach is taken, which identifies potential destinations by estimating end-to-end flow rates based on node transmission activities. Furthermore, it is shown that as routes change due to node movement, the tracing method quickly converges to the true destination by exploring topology diversity. The proposed method is proved to be consistent under mild conditions and shown to perform

well even in the presence of intersecting flows and chaff traffic.

Advantages:

- Provides efficient network monitoring

Disadvantages:

- Protecting user privacy against eavesdroppers
- Not robust against dummy request packets

ASTATISTICAL TRAFFIC PATTERN DISCOVERY SYSTEM FOR MANETs [11]

Author: Yang Qin and Dijiang Huang Arizona State University

Anonymous MANET routing relies on techniques such as re-encryption on each hop to hide end-to-end communication relations. However, passive signal detectors and traffic analyzers can still retrieve sensitive information from PHY and MAC layers through statistical traffic analysis. In this paper, we propose a statistical traffic pattern discovery (STPD) system. STPD intends to find out the sources and destinations of captured packets and discover the end-to-end communication relations. The proposed approach does not require analyzers to be actively involved in MANET transmissions or to decrypt the traffic. We present theoretical models as well as extensive simulations to demonstrate our solutions.

Advantages:

- This model avoids the exponential complexity of using evidence theory based approach.
- The proposed solution scalable for large scale MANETs.

Disadvantages:

- The negative effects of the forwarders in the network.
- The proposed system is hardly able to distinguish the forwarders from the source and destination.

Security Attacks in Mobile Ad-hoc Networks – A Literature Survey [13]

Author: T. Navaneethan, M. Lalli

A MANET (Mobile Ad-hoc Network) is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Wireless networks are vulnerable to security attacks, which allows for many other forms of attacks on the networks. By providing communications in the absence of a fixed infra-structure MANETs are an attractive technology for many applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. Security is a major concern for protected communication between mobile nodes in an unfriendly environment. In the presence of malicious nodes, one of the main challenges in MANET is to design the strong security solution that can protect MANET from various attacks such as spoofing, black hole, worm hole, flooding, eavesdropping and so on. This paper provides different kinds of attacks in MANET. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad hoc network is self organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to keep connections to the network as well as simply adding and removing devices to and from the network. The set of applications for MANETs is different, ranging from wide-ranging, mobile, highly dynamic networks, to small, fixed networks that are controlled by power sources. Besides the legacy applications that move from conventional infrastructure environment into the ad hoc context, a large arrangement of new services can and will be generated for the new environment. It includes Military Battlefield, Sensor Networks, Medical Service and Personal Area Network. Routing Security in Wireless Ad Hoc Networks [14]

Author: Hongmei Deng, Wei Li, and Dharma P. Agrawal

A MANET is a set of wireless mobile nodes that are able to Communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In this article we study the routing security issues of MANETs, and analyze in detail one type of attack the "black hole" problem that can easily be employed against the MANETs. We also propose a solution forthe black hole problem for ad hoc on-demand distance vector routing protocol. Routing table overflow: The attacker attempts to create routes to absent nodes. The aim is to have enough routes so that making of new routes is prevented or the performance of routing protocol is overwhelmed. Impersonation: A malicious node may copy another node while sending the control packets to create a variance update in the routing table. Energy consummation: Energy is a essential parameter in the MANET. Battery-powered devices aim to save energy by transmitting only when necessary. An attacker can attempt to utilize batteries by requesting routes or forwarding unnecessary packets to a node. Information disclosure: The malicious node may uncover confidential information to legitimate users in the network, such as routing or location information. In the end, the attacker knows which nodes are located on the target route.

Advantages:

- Reduces memory requirements and needless duplications.
- Fast response to link breakage in active routes.

Disadvantages:

- The source node cannot identify if the reply message is really from the destination node.

2. CONCLUSION

This paper surveys and compares various Existing Methods available to analyze statistical traffic from MANETs. Our empirical study demonstrates that the existing MANET systems can achieve very restricted

communication anonymity under the attack of STARS. In STARS, the actual receiver of a point-to-point transmission is not identifiable among all the potential receivers within the sender's transmitting range.

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] 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.

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

[10] 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.

[11] Yang Qin and Dijiang Huang "STARS: A Statistical Traffic Pattern Discovery System for Anonymous MANET Communications", Arizona State University,2009

[12] Arunkumar R, Bharateshhegde, Ganeshprasad, Manoj C Jagatap, Vishwas S, "MTPD: MANET Traffic Pattern Discovery –A Heuristic Aproach" Volume No.02, Issue No. 06, June 2014

[13] T. Navaneethan, M. Lalli, "Security Attacks in Mobile Ad-hoc Networks – A Literature Survey" T. Navaneethan et al, International Journal of Computer Science and Mobile Applications,Vol.2 Issue. 4, April- 2014, pg. 1-7

[14] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks" University of Cincinnati.

[15] Yang Qin, Dijiang Huang, "STARS: A Statistical Traffic Pattern Discovery System For Anonymous MANETs" IEEE Transactions On Dependable and Secure Computing, vol. 11, No. 2, March/April 2014