TP-DS: A Heuristic Approach for Traffic Pattern Discovery System in MANET's

Shweta M Nirmanik,
Citech,
Bangalore-560 036

Abstract:- As mobile ad hoc network (MANET) systems research has matured and several testbeds have been built to study MANETs, research has focused on developing new MANET applications such as collaborative games, collaborative computing, messaging systems, distributed security schemes, MANET middleware, peer-to-peer file sharing systems, voting systems, resource management and discovery, vehicular computing and collaborative education systems. 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. Traffic analysis problem expose some of the methods and attacks that could infer MANETs are still weak under the passive attacks. In this Research, proposed 'Traffic pattern Discovery System in MANET's, aheuristic approach(TP-DS) , enables a passive global adversary to accurately infer the traffic pattern in an anonymous MANET without compromising any node.

TP-DS works well on existing on-demand anonymous MANET routing protocols to determine the source node, destination node and the end-to-end communication path. Detailed simulations show that TP-DS can infer the hidden traffic pattern with accuracy as high than the TP-DS and gives the result with accuracy of 95%.

____*****____

I. INTRODUCTION

MANET Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc Network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

MANET (Mobile ad hoc network) is an infrastructure less, wireless and self-configuring network of mobile devices. These are mainly used in defense field. Anonymous 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.

`The predecessor attack and disclosure attacks 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:

1. The broadcasting nature - where the packets are transmitted and received by many nodes hence it is difficult to identify the exact destination,
2. 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.
3. The mobile nature – here the nodes are movable and hence the communication between the mobile nodes are very complex to analyze.

The proposed evidence based statistical traffic analysis model especially for MANETs . Here, every packet that is captured is treated as evidence supporting a point-to-point transmission between the source node and destination node. Reusing the evidence-based model, in this paper, we propose a novel traffic pattern discovery system (TP-DS).TP-DS 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, TP-DS 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.

II. RELATED WORK

As proposed earlier [1], it takes to provide secure communication in hostile and suspicious MANETs. To this end, we construct a framework for Anonymous Location-Aided Routing in MANETs (ALARM) which demonstrates the feasibility of obtaining, at the same time, both strong privacy and strong security properties. By privacy properties we mean node anonymity and resistance to tracking. Whereas, security properties include node/origin authentication and location integrity. The advantage of this lies in, MANET is a strong privacy and strong security. MANET node could easily create fraudulent phantom node-location entries and propagate to the entire MANET. It is flexible and efficient. But its drawbacks are do not consider jamming and denial-of- service (DoS) attacks. Such attacks are impossible to combat at the network layer. A node will not accept a LAM unless it contains the correct time-stamp of the current time slot.

A number of anonymous routing protocols have been recently proposed as an effective counter measure against traffic analysis in MANETs[2]. 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. It routing frames and data-frame interarrival times are effective metrics to recognize and trace anonymous MANET flows. More than 400 nodes with the same transmission range are needed to ensure sufficiently high network connectivity. Most anonymous routing protocols require each node to not use its true MAC address in MAC-layer Communications.

We can take the all mix system[3] that requires that the messages to be anonymized should be relayed through a sequence of trusted intermediary nodes. These nodes, called mixes, hide the correspondence between their input and output messages. Although originally it was proposed that all participants should act as mixes, subsequent systems developed and deployed make a distinction between clients simply using the network, and mix nodes that form its core. An analysis of the applicability and efficiency of the statistical disclosure attack. It requires less computational effort by the attacker and yields the same results.

A two-step unlink ability measuring approach for MANET, evidence collection using statistical packet-counting traffic analysis[4], evidence theory-based unlink ability measure. We use IEEE 802.11b-based MANETs as our analytical systems. Using our approach and then we can apply the evidence theory-based unlink ability measuring methods to derive the unlink ability evaluations of the 802.11b MANET. Minimizes their deployment time, reduces the cost and high latency. Thus the mobile Ad hoc network (MANET) is a self-configuring network that does not require any preexistent (fixed) Infrastructure and of lower capacity.

III. PROPOSED SYSTEM

TP-DS estimates the probability of any node being a source or destination and the probability of any two nodes communicating with each other, but the actual traffic pattern still remains secret. The traffic inside each super node can be ignored, since it will not affect the inter-region traffic patterns. Point-to-point transmission is not identifiable among all the potential receivers' leads to inaccuracy of the traffic pattern. In this paper, we propose a novel TP-DS for MANETs.

TP-DS 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, TP-DS 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.

To perform TP-DS, the adversaries only need to monitor the nodes beside the boundaries of the super nodes. The traffic inside each super node can be ignored, since it will not affect the inter-region traffic patterns. In addition, TP-DS does not need the signal detectors to be able to precisely locate the signal source. Moreover, in TP-DS, the actual receiver of a point-to-point transmission is not identifiable among all the potential receivers within the sender's transmitting range. This inaccuracy can be mitigated in TP-DS because most potential receivers of a packet will be contained within one or a few super nodes. TP-DS 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. The existing MANET systems can achieve very restricted communication anonymity under the attack of TP-DS.
TP-DS consists of three key components as follows

1. *Flow Recognition Algorithm* is used to validate routing frames and data-frame inter-arrival times are effective metrics to recognize and trace anonymous MANET flows.
2. Develop an *inter-arrival-based algorithm*, called TP-DS, whereby a passive global adversary can infer the traffic pattern despite the use of some well-known anonymous on-demand MANET routing protocols.
3. Evaluate TP-DS by extensive simulations involving *CBR* and *VBR* flows following various rate distributions. Our simulation results show that TIA can infer the traffic pattern with an accuracy as high as 95%.

The attacker can take advantage of TP-DS to perform traffic analysis as follows, divide the entire network into multiple regions geographically. Deploy sensors along the boundaries of each region to monitor the cross-component traffic. Treat each region as a super node and use TP-DS to figure out the sources, destinations, and end-to-end communication relations; and analyze the traffic even when nodes are close to each other by treating the close nodes as a super node.

IV. SYSTEM OVERVIEW

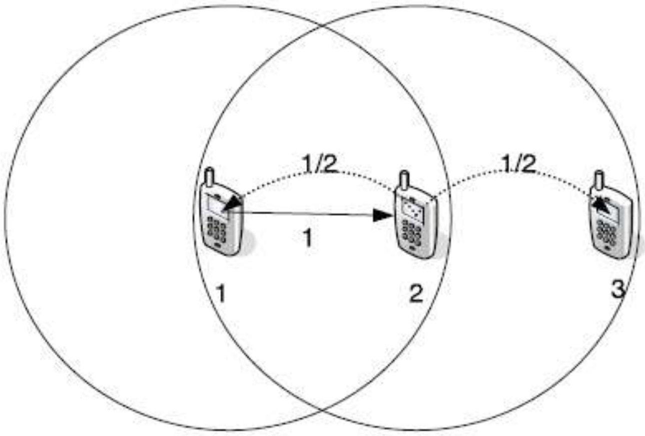

Fig 1: A simple wireless adhoc networks

There are two matrix formation which are called as point to point matrix and end to end matrix. In point to point matrix, with the captured point-to-point (one-hop) traffic in a certain period T, we first build point-to-point traffic matrices such that each traffic matrix only contains “independent” one-hop packets. Note that two packets captured at different time could be the same packet appearing at different locations, such as the two packets sent by node 1 and node 2 consecutively in Fig. 1, so they are “dependent” on each other. But as shown in the figure, node 3 is also in the same location and receives the packet directly from the node 2. The node 2 acts like a intermediate node between node 1 and node 2. Hence there is a one hop packet distance between node 1 and node 3. Therefore node 1 can send the packet to node 3 after constructing the point to point matrix and end to end matrix and after solving using time slicing technique.

The length of each time interval is determined by two criteria: A node can be either a sender or a receiver within this time interval. But it cannot be both. Each traffic matrix must correctly represent the one-hop transmissions during the corresponding time interval. In this way, the construction of matrices will automatically involve mobility in the traffic matrices constructions.

V. SYSTEM ARCHITECTURE

First File has been spitted. More information can be send to sources and destination. At the same time traffic may be occurring. After that overcome the traffic by using greedy algorithm. Encrypt the data by using Encrypt AES Algorithm. Thus the data send through packet. Finally decrypt the data by using Decrypt Algorithm. Comparison between existing and proposed system by using Probability distribution algorithm executed in graph.

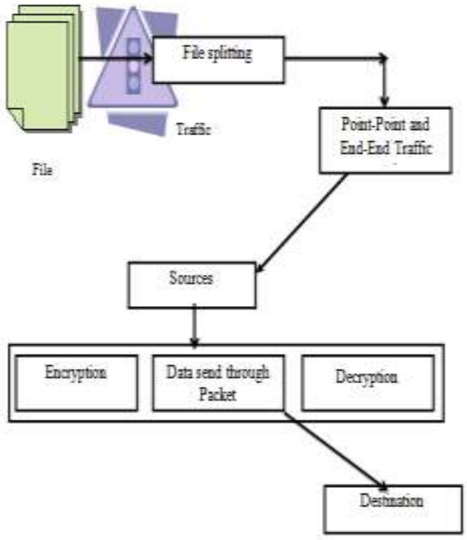

Fig 2: Process of Functioning.

File splitting is an approach to protecting sensitive data from unauthorized access by encrypting the data and storing different portions of a file on different servers. It is selection of some files in this Location. In traffic analysis, network traffic information can usually be easily retrieved from various network devices without affecting network performance or service availability too much. Time-sensitive data may be given priority over traffic that can be delayed briefly with little-to-no ill effect.

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Decrypt the message without possessing the key for a well-designed encryption scheme. large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key, provided by the originator to recipients but not to unauthorized interceptors.

In node creation process, it creates some nodes; it can identify the sources and destination. It is used to End-End and Point-Point link probability distribution. Data is extracted from the given input file. Decryption is the process of converting ciphertext back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. The algorithms that can be used are encrypting AES Algorithm, Greedy Algorithm, Distributed Algorithm and Decrypt Algorithm.

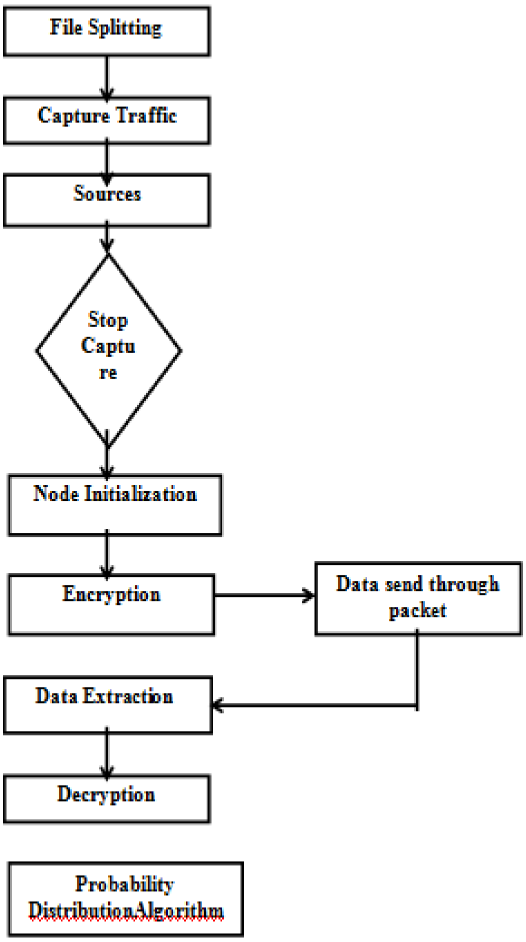

Fig 3: flow diagram for TP-DS.

VI. FUTURE WORK

The adversarial model presented, assumes that the adversaries can globally monitor the traffic across the entire network region. This assumption is conservative from the network users' point of view. Usually, it is difficult for the attackers to perform such global traffic detection. However, even though the adversaries are not able to monitor the entire network, they can monitor several parts of the network simultaneously. For example, an attacker can deploy sensors (signal detectors) around some particular mobile nodes to track their movements and eavesdrop all of their traffic. These sensors may even move accordingly.

We call this variant of TP-DS as the Generalize TP-DS (GTP-DS). To perform GTP-DS, the adversaries only need to monitor the nodes beside the boundaries of the supernodes. The traffic inside each supernode can be ignored, since it will not affect the inter-region traffic patterns. In addition, GTP-DS does not need the signal detectors to be able to precisely locate the signal source. They are only required to determine which supernode (region) the signals are sent from. Moreover, in TP-DS, the actual receiver of a point-to-point transmission is not identifiable among all the potential receivers within the sender's transmitting range. This inaccuracy can be mitigated in GTP-DS because most potential receivers of a packet will be contained within one or a few supernodes. GTP-DS will be the direction of our future research.

VII. CONCLUSION

In this paper, we propose a novel TP-DS for MANETs. TP-DS 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, TP-DS 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 TP-DS.

REFERENCES

[1] 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**.**

[2] 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.

[3] 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.

[4] D. Huang, "Unlinkability Measure for IEEE 802.11 Based MANETs," IEEE Trans. Wireless Comm., vol. 7, no. 3, pp. 1025- 1034, Mar. 2008.

[5] TP-DS: A Statistical Traffic Pattern Discovery System for MANETs Yang Qin, Dijiang Huang, Senior Member, IEEE, and Bing Li, Student Member, IEEE

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, 1981.

[16] 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

[17] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transactions,"ACM Trans. Information and System Security, vol. 1, no. 1,pp. 66-92, 1998.

[18] Balasubramanian, R. Mahajan, and A. Venkataramani,"Augmenting mobile 3G using WiFi," in Proc. MobiSys, San Francisco, CA, USA, 2010.

[19] S. Dimatteo, P. Hui, B. Han, and V. O. K. Li, "Cellular trafficoffloading through WiFi

networks," in Proc. IEEE 8th Int. Conf. MASS, Valencia, Spain, 2011.

[20] R. L. Cruz and A. V. Santhanam, "Optimal routing, link scheduling and power control in multihop wireless networks," in Proc. IEEE Soc. INFOCOM, 2003.

[21] W. Gao and G. Cao, "User-centric data dissemination in disruption tolerant networks," in Proc. IEEE INFOCOM, 2011.

[22] U. G. Acer, P. Giaccone, D. Hay, G. Neglia, and S. Tarapiah,"Timely data delivery in a realistic bus network," in Proc. INFOCOM, Shanghai, China, 2011.

[23] P. Deshpande, A. Kashyap, C. Sung, and S. R. Das, "Predictivemethods for improved vehicular WiFi access," in Proc. Mobisys,Kraków, Poland, 2009.

[24] X. Li, X. Yu, A. Wagh, and C. Qiao, "Human factors-aware service scheduling in vehicular cyber-physical systems," in Proc. IEEE INFOCOM, Shanghai, China, 2011.

[25] C. Troncoso, B. Gierlichs, B. Preneel, and I. Verbauwhede, "PerfectMatching Disclosure Attacks," Proc. Eighth Int'l Symp. Privacy Enhancing Technologies, pp. 2-23, 2008.

[26] D. Huang, "Unlinkability Measure for IEEE 802.11 Based MANETs," IEEE Trans. Wireless Comm., vol. 7, no. 3, pp. 1025- 1034, Mar. 2008.

[27] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.

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

[29] 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.

[30] J. Wexler, "All About Wi-Fi Location Tracking," Network World, http://features.techworld.com/mobile-wireless/2374/all-aboutwi- fi-location-tracking/, 2004.

[31] Scalable Network Technologies, "QualNet Simulator," http:// www.qualnetcomm.com/, 2008.