International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

AN EFFECTIVE STATISTICAL TRAFFIC PATTERN DISCOVERY SYSTEM FOR MANETS USING DISTRIBUTED SUPER NODE SELECTION MODEL

S.Mohideen Badhusha[1] , J.Sobana[2]
[1]*Assistant Professor/ CSE department,K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu, India.*
[2]*M.E(IInd Year)/CSE,K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu, India.*

Abstract— Communication anonymity is a critical issue in MANETs, which is generally classified as Source/destination anonymity and end-to-end relationship anonymity. In this paper a novel Statistical Traffic Pattern Discovery System (STPDS) is presented to address these issues. STPDS works passively to perform traffic analysis based on statistical characteristics of captured raw traffic. STPDS is capable of discovering sources, destinations, and end-to-end communication relations. Empirical studies demonstrate that STPDS achieves good accuracy in disclosing the hidden traffic patterns. STPDS is a complete attacking system that first identifies all source and destination nodes and then determines their relationship. In addition, the STPDS is extended as Generalized STPDS (GSTPDS) which 1) divides the entire network into multiple regions geographically; 2) deploys mobile node along the boundaries of each region to monitor the cross-component traffic; 3) treats each region as a supernode and use STPDS to figure out the sources, destinations, and end-to-end communication relations, 4) analyzes the traffic even when nodes are close to each other by treating the close nodes as a supernode; Though many encryption techniques are used in video streaming applications in MANETs, which is using MDC with selective encryption technique is proposed in this work for enhancing scalability and confidentiality.
Keywords: Anonymous communication, mobile ad hoc networks, statistical traffic analysis

I. INTRODUCTION

Mobile ad hoc networks (MANET) are originally used in military tactics environments. Communication anonymity is a critical issue in MANETs, which is usually of the following aspects: 1) source / destination - anonymity is difficult to identify the sources or targets of network flows. 2) End -to- end relationship anonymity is difficult to identify the end-to-end communication relations. In order to achieve anonymous Communication in MANETs, many anonymous routing protocols such ANODR [1], MASK [2], and OLAR [3] have been proposed. Although a variety of anonymity improvement techniques such as Onion Routing [4] and mix -net [5] are used, these protocols often rely on packet encryption (e.g., nodes' identities and routing information) to hide from the adversaries sensitive information. However, passive signal detectors yet to eavesdrop on the radio channels, intercept the transmissions, and then perform traffic analysis attacks.

Recently, statistical traffic analysis Attacks have considerably been increasing due to their passive nature, i.e., attackers need only collect information and quietly perform analysis without changing the network behavior (injection or modifying packages). The predecessor attacks and disclosure attacks are two representatives. However, all of these previous approaches do not work well to analyze MANET traffic due to the following three natures MANETs: 1) The broadcasting nature: In wired networks [6], a point-to-point communication usually has only one possible recipient, In wireless networks, while a

message is sent, multiple users can receive it simultaneously. 2) In MANETs which each mobile node can serve as a host and a router both. Thus, it is difficult to determine the role of a mobile node to be a source, a destination or a relay. 3) The mobile nature: Most of the existing traffic analysis models do not consider the mobility of the communication peers which makes the communication relationship between mobile nodes complex.

An evidence-based statistical traffic analysis model is specifically developed in MANETs. In this model, each and every captured packet is treated as evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. A sequence of point -to-point traffic matrices is created, and then they are used to derive end-to- end (multihop) relations [7]. This approach offers a practical attack against MANETs frame, but still significant information about the communication patterns undiscovered leaves. First, the system suggests several important constraints to address (for example, the maximum hop -Count of the package) , when the derivative of the end-to -end traffic from one hop evidence . Secondly, it is not a method to identify the actual source and destination nodes (the source / target probability distribution to calculate) .

STPDS aims to derive the source / derived destination probability distribution, i.e., the probability of each node to a message source / destination , and the end-to-end connection probability distribution , i.e., the probability for each pair of nodes to end- to-end communications pair . To achieve its objectives , STPDS comprises two main steps [7] : 1) Construct point -to-point traffic matrices are constructed using the time slice technique , and then the end-to-end traffic matrix is derived with a number of traffic filtering rules and 2) a heuristic approach is used to identify the actual source and destination nodes and then to correlate the source nodes with their corresponding destinations.

The contribution of STPDS is at twofold: 1) To the best of our knowledge, STPDS 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. STPDS are a complete attacking system that first identifies all source and destination nodes and then determines their relationship.

There are generally two types of MANETs namely open and closed MANETs. [13] Closed MANETs don’t have problems because all nodes are working toward a common goal and can be easily controlled. Open MANETs share their resources to ensure global connectivity but they many have different goals. The nodes in open MANETs are operated by multiple users, and they must not be forced to cooperate. However, both types of MANET cause two main problems which are not normally faced by traditional fixed network routing protocols. These are the lack of fixed infrastructure -Support and the frequent changes in network topology. There are various secure routing protocols [14,15] have been proposed to secure ad hoc networks from security threats and improve routing performance, but these protocols are vulnerable in many ways and most of these mechanisms to discuss only reliability not for anonymity.

In MANET, video streaming transmission means continuous stream of video packets at a certain interval. Video streaming with the problem of transfer of video data as a continuous stream. The challenge of providing real-time video streams in infrastructure-less wireless networks, such as MANETs, efficiently addressed by Scalable Video Coding (SVC) or Multiple Description Coding (MDC). The video streaming over mobile ad hoc networks is more difficult than the other networks due to dynamic changes in the network topology with unreliable wireless channels [17]. In video streaming,

we can apply the cryptographic method of encryption and decryption. The method for data encryption and decryption are divided into symmetric encryption and asymmetric encryption[18]. Encryption is the process of encoding plaintext into ciphertext and decryption is the reverse process. Using encryption and decryption, the protection of data confidentiality and integrity are achieved. Based on the characteristics of wireless devices, but a wireless ad hoc network has special security and efficiency requirements conventional cryptographic algorithms. *Selective encryption algorithms* are applied mainly in large-scale data transmission such as multimedia communications, mobile ad hoc networks.

II. RELATED WORK

Traffic analysis attacks against the static wired networks have been well investigated. The brute force attack proposed in [8] tries to track a message by enumerating all possible links a message could traverse.

In node flushing attacks [9], the attacker sends a large quantity of messages to the targeted anonymous system (which is called a mix-net). Since most of the messages modified and reordered by the system are generated by the attacker, the attacker can track the rest a few (normal) messages.

The timing attacks as proposed in [10] focus on the delay on each communication path. If the attacker can monitor the latency of each path, he can correlate the messages coming in and out of the system by analyzing their transmission latencies.

A timing-based approach in [11] to trace down the potential destinations given a known source. In this approach, assuming the transmission delays are bounded at each relay node, they estimate the flow rates of communication paths using packet matching. Then based on the estimated flow rates, a set of nodes that partition the network into two parts, one part to which the source can communicate in sufficient rate and the other to which it cannot, are identified to estimate the potential destinations.

An Anonymous On-Demand Routing (ANODR) Protocol [12], is the first one to provide anonymity and unlinkability for routing in MANETs. ANODR uses one-time public/private key pairs to achieve anonymity and unlinkability but fail to guarantee content unobservability.

An On-Demand Lightweight Anonymous Routing (OLAR)[16] scheme which applies the secret sharing scheme based on the properties of polynomial interpolation mechanism to achieve anonymous message transfer without per-hop encryptions and decryptions. The only task for a forwarder is to perform additions and multiplications, which cost much less than traditional cryptographic operations.

III. STATISTICAL TRAFFIC PATTERN DISCOVERY SYSTEM

To disclose the hidden traffic patterns in a MANET communication system, STPDS comprises two main steps: First, it uses the captured traffic, constructs a sequence of point -to-point traffic matrices and then forwards the end – to-end traffic matrix . Second further analysis of end- to-end traffic matrix , the probability for each node calculates a source / destination (the source / target probability distribution) , and that its for each pair of nodes , an end-to -end communication links (end -to -end link probability distribution) .

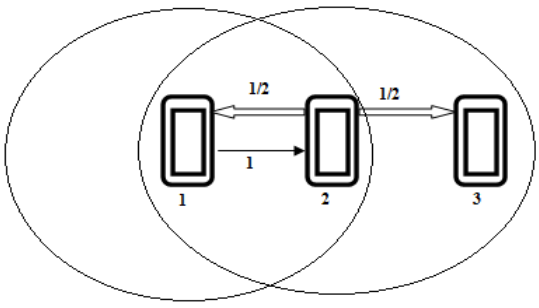

Fig. 1. A simple wireless ad hoc network

To illustrate the basic idea of STPDS, a simple scenario is used as show in Fig.1. In this network, there are three wireless nodes (1, 2 and 3). Node 2 is located in the transmission range of the node 1 and the node 3 is located in the transmission range of node 2 (but not the transmission range of node 1) . Two consecutive packages are identified : node 1 sends a packet and then node 2 sends a packet .

IV. TRAFFIC PATTERN DISCOVERY

Traffic matrix tells us the deduced end-to-end traffic volume between each pair of nodes . However, we need further studies to be carried out to discover the probability distribution and end-to-end link probability distribution , the actual source / target ,i.e.,, to find out who the actual sources and destinations , and who are communicating with whom.

V. SELECTIVE ENCRYPTION

In selective encryption, not all messages are necessarily, encrypted while the entire data transmission can be viewed to be secure on the whole. Selective encryption is able to improve the scalability of the data transfer and reduces the processing time. Encryption is a process that is used to secure the data and the encryption algorithms play an important role in the efficient information security systems. Full encryption techniques are slow. Selective encryption is used to save computing power and time reduces, overhead and increase speed. This technique also provides a better security by encrypting only a selected portion of a bit stream. Since full encryption of the transmitted data streams may place a heavy burden on the signal processing and incoming node, which leads to consider the concept of partial encryption of data streams. In the partial encryption, only a percentage of the transmitted data stream is processed by an encryption algorithm, with the remainder of the data stream are sent in clear.

VI. EXPERIMENTAL RESULTS

The following Table 6.1 and Fig 6.1 describe experimental result of existing system (EM-STPDS) and proposed system (PM-GSTPDS) in successive transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown

S.NO	Pass Time (Min)	Ratio of Successive Transmission Node (Existing System)	Ratio of Successive Transmission Node With Selective Encryption (Proposed System)
1	10	0.43	0.48
2	20	0.52	0.57
3	30	0.61	0.66
4	40	0.69	0.72
5	50	0.74	0.77
6	60	0.80	0.83
7	70	0.86	0.89
8	80	0.90	0.92
9	90	0.93	0.95
10	100	0.97	0.98

Table 6.1 Ratio of Successive Transmission Node

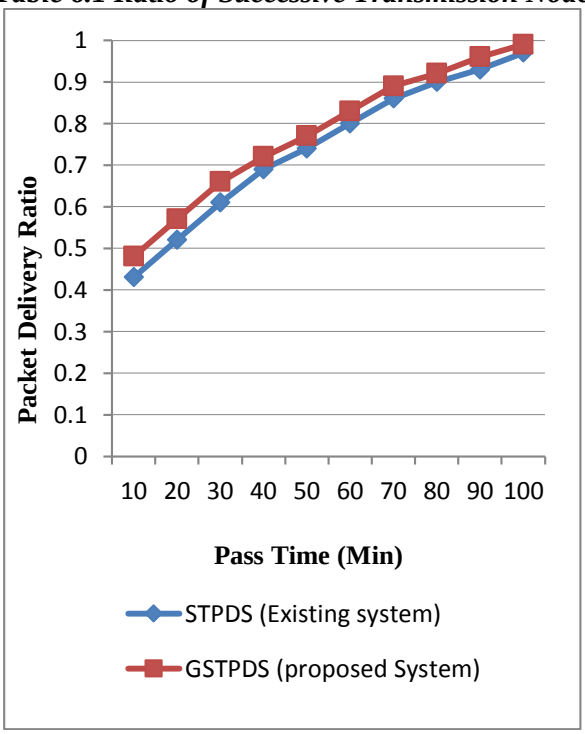

Fig 6.1 Ratio of Successive Transmission Node

VII. CONCLUSION

Video streaming is recently emerging as an important research area in MANETs. STPDS is basically an attacking system, which only needs to capture the raw data traffic from the PHY / MAC layer without looking into the contents of the intercepted packets constructed from the captured packets, STPDS a sequence of point-to-point traffic matrices are used to derive the end-to-end traffic matrix, and then uses a heuristic data processing model to reveal the hidden traffic patterns of end-to-end matrix. It is observed that MANETs are only restricted communication to achieve anonymity under the attack of the STPDS. Moreover STPDS is extending geographically GSTPDS which divides the entire network into multiple regions; and deploys sensors along the boundaries of each region to monitor the cross-component traffic. Also, each region is treated as a supernode and use STPDS to find out the sources, destinations, and end-to-end- communication relationships.

Selective encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile networks. to data protection more effectively to achieve a novel solution for selective encryption with a reasonable cost. They can reduce the overhead data encryption / decryption times and improve the network efficiency. The result shows that the proposed GSTPDS and Selective encryption gives 3.2% higher performance than the existing work.

REFERENCES

i. 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.
ii. 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.
iii. 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.

iv. 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.
v. 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.
vi. Yang Qin, Dijiang Huang "STARS: A Statistical Traffic Pattern Discovery System for MANETs", IEEE Transactions On Dependable And Secure Computing, Vol. 11, No. 2, March/April 2014.
vii. D. Huang "Unlinkability Measure for IEEE 802.11 Based MANETs", IEEE Trans. Wireless Comm., vol. 7, no. 3, pp. 1025- 1034, Mar. 2008.
viii. 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.
ix. D. Chaum "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Comm. ACM, vol. 24, no. 2, pp. 84-88, 1981.
x. 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.
xi. T. He, H. Wong, and K. Lee "Traffic Analysis in Anonymous MANETs", Proc. Military Comm. Conf. (MILCOM '08), pp. 1-7, 2008.
xii. J. Kong, and X. Hong "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks", in Proc. 4th International Symposium on Mobile Ad Hoc Networking & Computing, New York, 2003, pp. 291-302.
xiii. H. Miranda, and L. Rodrigues "Preventing Selfishness in Open Mobile Ad Hoc Networks", in Proc. 7th CaberNet Radicals Workshop, Portugal, , pp. 440-445, 2002.
xiv. L. Abusalah, Khokhar, and M. Guizani "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE Communications Surveys and Tutorials,Vol. 10, No. 4, pp. 78-93, Jan. 2008.
xv. T. R. Andel, and A. Yasinsac "Surveying Security Analysis Techniques in MANET Routing Protocols", IEEE Communications Surveys andTutorials, Vol. 9, No. 4, pp. 70-84, Feb. 2007.
xvi. Q. Yang, H. Dijiang, and K. Vinayak "OLAR: On-demand Lightweight Anonymous Routing in MANETs", in Proc. 4th International Conference on Mobile Computing and Ubiquitous Networking, Tokyo, 2008, pp. 72-79.
xvii. S. Mohideen Badhusha, K. Duraiswamy"Secure Low-Bandwidth Video Streaming through Reliable Multipath Propagation in MANETs" International Scholarly and Scientific Research & Innovation, Vol:9, No:6, 2015
xviii. Patil Ganesh G & Madhumita A Chatterjee "Selective Encryption Algorithm for Wireless Ad-hoc Networks "International Journal on Advanced Computer Theory and Engineering (IJACTE), ISSN (Print) : 2319 – 2526, Volume-1, Issue-1, 2012

