Secure and Efficient Traffic Pattern Discovery in MANETs

Soumya. M[1], Savitha.G[2], Dr. Vibha lakshmikantha[3]

[1]PG student, [2]Associate Professor, [3]Professor

Computer Science and Engineering Department

B.N.M Institute of Technology, Bengaluru, India

Email: soumya.mgowda@gmail.com[1], savithamadhusudan@gmail.com[2], vibhal1@rediffmail.com[3]

Abstract— Anonymous Communication is a critical issue in case of mobile ad-hoc networks (MANETs). It is very tough to learn the source and destination of the communication link and the other intermediate nodes that are involved in the communication. Many techniques are proposed to improve the anonymous communication in case of MANETs. However, MANETs are vulnerable under certain situations like passive attacks and traffic analysis attacks. Here the traffic analysis problem, expose some of the methods and attacks that could conclude that MANETs are weak under the passive attacks. To clearly show how to find the hidden traffic patterns without decrypting the caught packets, Secure and Efficient Traffic Pattern Discovery (SETPD) in MANETs is proposed. In order to discover the communication patterns SETPD works passively and carries out the traffic analysis depending upon the statistical features of the caught raw traffic. SETPD has the ability to find the source node, destination node and the end-to-end communication path in case of mobile ad-hoc networks.

Keywords— Anonymous Communication, Mobile ad-hoc network, Passive attack, Statistical traffic analysis, Traffic patterns, Statistical features, End-to-end communication path.

INTRODUCTION

MANET is one sort of ad-hoc network which is capable of changing its locations and composing itself. It's a group of mobile nodes communicating with one another through the wireless channels. Because of their mobile nature, wireless connections are used by them to conjoin to diverse networks. MANETs do not have fixed infrastructure and is a wireless and self-configuring network of mobile devices, where every node behaves like both host and relay. MANETs were originally designed for military tactic environments.

Anonymous Communication is a critical issue in case of MANETs. It's very tough to find out the sender or receiver of the communication link and the other intermediate nodes that are involved in it. In order to achieve anonymous communication in MANETs numerous anonymous routing protocols has been proposed like ANODR [2], MASK [3], OLAR [4] etc. In addition to these protocols many techniques are used to improve the communication anonymity in MANETs like onion routing [5] which includes multiple layers of data encryption and hides the routing information and identity of nodes from the unauthorized nodes. However the routing information can be still detected via the passive attacks.

Since 1990s, traffic analysis models have been widely used for the wired networks to track the data. For example brute force method which is an simplest approach to track a message in case of wired networks by enumerating all possible links that a message could travel has gained more importance. Now a day, statistical traffic analysis attacks have become popular because of its passive nature, i.e., the opponents just have to gather the information and quietly carry out the analysis without causing changes to the network behaviour like injecting or modifying the packets.

The predecessor attacks [6] and disclosure attacks [7] are the examples of traffic analysis attacks but they cannot efficiently analyze the traffic in MANETs due to the three characteristics of the MANETs. They are:

i) Broadcasting nature - The packets are transmitted and received by many nodes. Hence it is difficult to determine the exact destination.

ii) Ad-hoc nature - MANETs are infrastructure less and each mobile node can serve as both the sender and receiver. Hence it is tough to identify the function of a mobile node like whether it is a source or destination or simply a relay.

iii) Mobile nature - The mobility of the communication peers is not taken into consideration by many existing traffic analysis models which make the communication among the mobile nodes very complex to analyze.

Due to these unique characteristics of MANETs, very limited investigation has been carried out on traffic analysis in context to MANETs. D.Huang [8] proposed an Evidence-based Statistical Traffic Analysis (ESTA) model especially for MANETs. Here, each packet that is captured is considered as evidence that supports the point-to-point (one-hop) transmission between the source and destination. This approach creates a series of traffic matrices consisting of point-to-point transmissions and then by using them it derives the end-to-end (multi-hop) relations. It provides a best practical attacking strategy against MANETs but still leaves some important information about the communication patterns undetermined. This approach does not give a proper method to learn the actual source and destination nodes in the communication path. It only uses a naı¨ve accumulative traffic ratio to deduce the end-to-end communication relations which incurs a lot of inaccuracy in the derived probability distributions.

In order to exhibit that the MANETs are weak under passive statistical traffic analysis attacks and to clearly show how to find the hidden communication patterns without decrypting the caught traffic “Secure and Efficient Traffic Pattern Discovery in MANETs” is proposed. SETPD operates passively to carry out traffic analysis depending upon statistical features of caught raw traffic. It is an attacking system that is capable of finding the actual source node, destination node and end-to-end communication path between them. SETPD is the first statistical traffic analysis approach that considers the prominent characteristics of MANETs: the broadcasting, ad-hoc and mobile nature. Most of the previous works use only partial attacks, where they cannot find both the source and destination nodes at the same time for any given network. But SETPD is a complete attacking system which identifies the actual source node, destination node and the end-to-end communication path between them. It gives an idea of attacking MANETs because of communication anonymity in MANETs. MANET systems can achieve very restricted anonymous communication under the attack of SETPD.

LITERATURE SURVEY

J. Raymond [9] presented “Traffic Analysis: Protocols, Attacks, Design Issues and Open problems”. Security is a discriminating issue on the Internet. Absence of security prompts two things, either the web's fame lessens or it turns into the most pervasive reconnaissance framework ever. The issue contemplated here is not simply a theoretic one, truth be told there are a few contentions that it is a critical one to illuminate if the online world keeps on growing and progress. From both hypothetical and down to earth view, it without a doubt should get significantly more consideration than it has gotten as such. The traffic analysis problem is exhibited and most imperative protocols, attacks and design issues are exposed. As they are for the most part concerned in proficient and viable web based protocols, a large portion of the accentuation is put on blend based developments. The bestowment is casual and there are no confounded characterizations and verifications exhibited, the objective is to offer an exhaustive acquaintance than with current profound novel experiences. The objective is to safeguard clients against traffic analysis. A related issue is that of system inconspicuousness which tries to conceal all communication patterns. System inconspicuousness shows the incapability of traffic analysis. Though message security can be picked up by utilizing encryption, it is hard to secure sender or recipient protection, particularly in vast systems. The quantity of diverse suppositions and settings is enormous which makes it hard to characterize and give a justification regarding the issue in a thorough way.

S.Seys et al., [10] proposed “Anonymous Routing Protocol (ARM)” which is an on-demand routing protocol for MANETs that succeeds the anonymity objectives while attempting to be as efficient as possible. Anonymity is a critical portion of the general security architecture as it permits clients to shroud their actions. This empowers private interchanges among clients while making it troublesome for the opponents to concentrate on their attacks. Comparable routing protocols for example: DSR and AODV are introduced that are distinctive. The fundamental thought is that the source sends a Route Request (RREQ) message going for the destination keeping in mind the end goal to find out routes to this destination. Just the destination can perceive that this RREQ was gone for it, however every other node can just check that it was not focused at them and no other data is discharged to them. Here two distinct adversaries are assumed.

1) External global passive adversary: Where an opponent can pay attention to all conceivable conversations among all the nodes in the system at any time. The objective of ARM towards this opponent is:

a) Preventing the opponent from finding the destination of the messages.
b) Preventing the opponent from finding which nodes are divisions of the way between source and destination.

2) Corrupted node inside the network: Here it is assumed that each node which is a division of the system is a potential enemy. The objective of ARM towards this opponent is:

a) A node should not have the capacity to find out whether another node in the system is the sender or the receiver of a specific message.
b) A node should not have the capacity to find out whether another node is a division of a way between the two nodes.

X.Wang et al., [11] proposed "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems" to dissect the essential impediments of flow transformations in anonymizing the packet flows by taking the part of a dynamic opponent. The key system utilized as a part of this analysis is to straightforwardly watermark the flow of the packet by somewhat altering the timing of the chosen packets. The regular issue with network information flow is the means by which to discover those network flows that have a place with any specific network information flows. This issue is characterized as network flow identification and is intrinsically associated with anonymous communication whose objective is to shroud the genuine identities and connections between the entities under conversation. Trial results demonstrate that the interim centroid based watermarking plan is exceedingly powerful in uncovering adequately long flows even after noteworthy changes have happened. In this system an anonymized packet flow can be successfully connected with the original packet flow. The central restricting component of strength of flow watermarking plan against different flow transformations is the quantity of packets in the packet flow. This attack is dependent on packet timing correlation among the first and anonymized packet flows. Since none of the viable low-latency anonymizing frameworks had the capacity to expel all the shared data from the packet timing area, this is appropriate to all viable low-latency anonymous communication frameworks.

G.Danezis et al., [12] proposed "Two-sided Statistical Disclosure Attack (TS-SDA)" aiming at anonymous communication frameworks that permit obscure and indistinct answers. It contemplates the presence of answers and the timing of messages to ascertain the reporters of an objective client and to follow the messages that they send. It is quick, as it works in time linear in the quantity of messages (O(Ks)) and just needs straightforward working on vectors and it is additionally conceivable to productively carry out in parallel or in specialized equipment. A linear approximation is proposed depicting the suitable collectors of the sent messages. Utilizing simulations the new attack is assessed given distinctive attributes and it is demonstrated that it is better than past attacks when answers are directed in the framework. TS-SDA executes well when the size of answers is great, and the time taken by the clients to answer is less. For this situation, it utilizes the timing connections among the got messages and sent answers to de-anonymize them. It is seen that the timing of the answers is crucial to the safetyness of the anonymity framework. At the point when the clients take long time to send the answers subsequent to accepting a message, it is hard to partner them with the beginning message. Thusly, key conclusion is that the safe anonymity frameworks ought to make answers cryptographically vague from ordinary messages, as well as hard to partner in time with the messages that are being answered.

Y.Liu et al., [13] proposed a novel "Traffic Inference Algorithm (TIA)" which allows a latent worldwide opponent to precisely conclude the traffic pattern in a mysterious MANET without bargaining any node. TIA chips away at existing on-demand unknown MANET routing conventions. The outcomes highlight the requirement for cross-layer plans to secure MANET against traffic analysis. The presentation of the traffic pattern and its progressions is habitually wrecking for a mission-basic MANET. For instance, a node as the source or destination of numerous end-to-end streams may be a VIP node which regularly issues strategic orders or gathers strategic data for settling on pivotal choices. Also, high-rate streams may show the connections of the two end nodes as far as rank (a node may be permitted to correspond with different nodes with rank simply above or underneath itself). Unknown routing conventions have been proposed as a cure against vindictive traffic analysis in MANETs. They all expect to block inducing the traffic pattern by concealing the genuine sources, genuine destinations and source-destination sets of caught packets. These plans can with stand a nearby rival who is unequipped for catching each radio transmission to different degrees. It stays vague whether they can beat a worldwide rival who has the capacity to eavesdrop on each radio transmission. TIA is an interarrival-based calculation whereby a latent worldwide adversary can derive the traffic pattern in spite of the utilization of some no doubt understood mysterious on-demand MANET routing conventions. TIA is assessed by broad reenactments including CBR and VBR streams taking after different rate appropriations.

SECURE AND EFFICIENT TRAFFIC PATTERN DISCOVERY

MANETs are vulnerable under certain situations like passive attacks and traffic analysis attacks. The traffic analysis problem, expose some methods and attacks that could conclude that MANETs are still weak under the passive attacks. In order to exhibit that the MANETs are weak under passive statistical traffic analysis attacks and to clearly show how to find the hidden communication patterns without decrypting the caught traffic “Secure and Efficient Traffic Pattern Discovery (SETPD) in MANETs” is proposed. SETPD operates passively to carry out traffic analysis depending upon statistical features of caught raw traffic (traffic volume). It is an attacking system that is capable of finding the actual source node, destination node and end-to-end communication path between them. It finds the neighbor node details and hidden traffic patterns in MANETs with good accuracy.

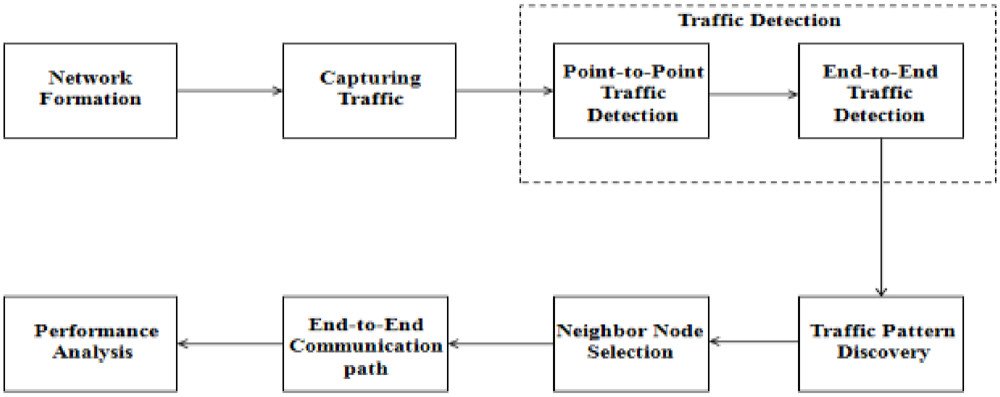

Traffic Detection
Network Formation
Capturing Traffic
Point-to-Point Traffic Detection
End-to-End Traffic Detection
Traffic Pattern Discovery
Neighbor Node Selection
End-to-End Communication path
Performance Analysis

Figure 1: Architecture Diagram of SETPD

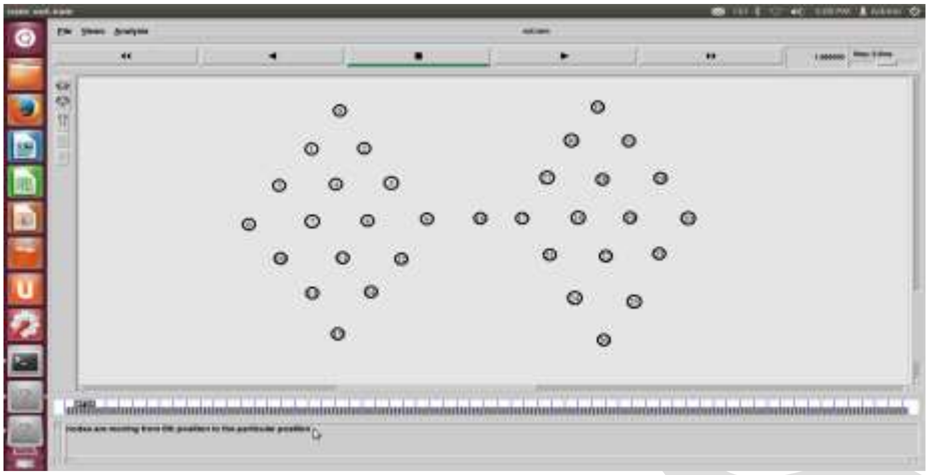
Figure 1 depicts the architecture of SETPD. Initially in network formation a number of mobile nodes are deployed in a network creating the topography for the network. And then each and every node is configured according to the required specifications.The raw traffic is captured from PHY/MAC layer of the network without looking into its contents. The captured traffic is used to build series of traffic matrices consisting of point-to-point transmissions by detecting the traffic between each point-to-point transmissions using time slicing technique. From these traffic matrices an end-to-end traffic matrix is deduced by detecting the traffic between the end-to-end transmissions utilizing a set of traffic filtering rules. Traffic pattern discovery process uses the traffic matrix and computes the possibility for a node to be the source or destination and finds the source-destination pair using the probability distribution algorithm. In the neighbor node selection process all neighbors of source and destination who are in their transmission range are found with respect to distance and link stability. Neighbor node with least distance and high link stability is selected as best neighbor for both source and destination. An optimal path between source and destination nodes is discovered through these best neighbors. The functionality of the proposed system is judged by packet delivery ratio, throughput and average packet loss.

EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

The network environment is simulated using the NS2 simulator. The results are analyzed with the help of Xgraph which is a plotting project that can be utilized to make a graphical representation of the simulation results. The nodes are placed in a 500 x 500 m^2 field area. Total simulation time is 80 seconds. The simulation parameters that are set are described in Table 1.

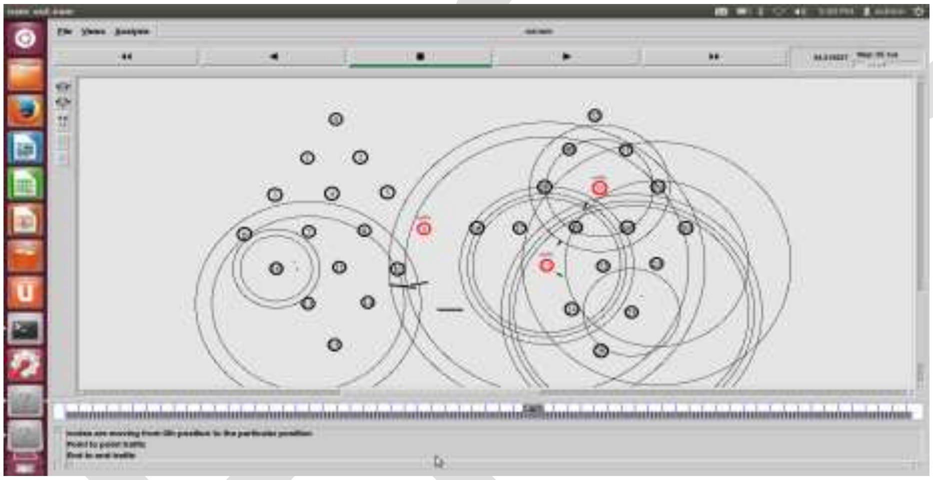
Simulation Parameters	Values
Simulator	NS 2.34
Geographical area (m^2)	500 x 500
Number of nodes	34
Channel type	Wireless Channel
Radio-propagation Model	Two Ray Ground
MAC type	802.11
Queue type	CMUPriQueue
Link layer type	LL
Antenna type	Omni Antenna
Simulation time (s)	80

Table 1: Simulation Parameters



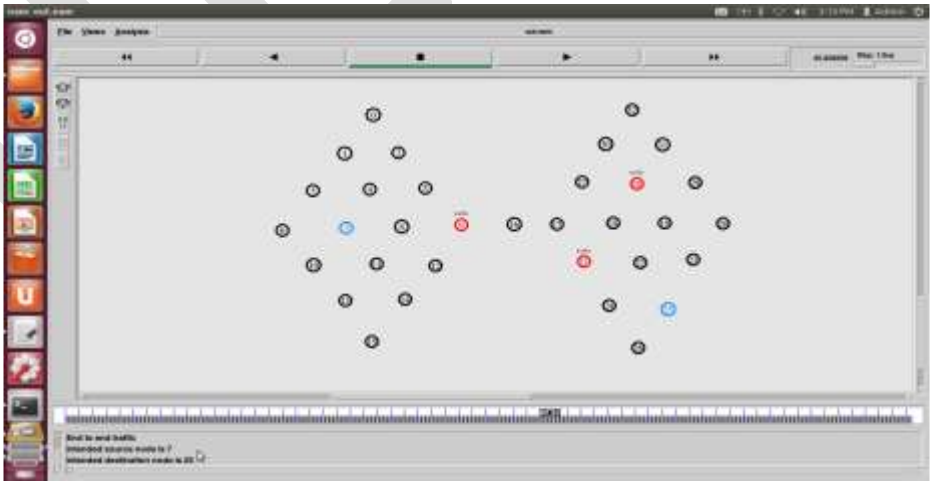
nodes are moving from 0th position to the particular position

Figure 2: Network Formation



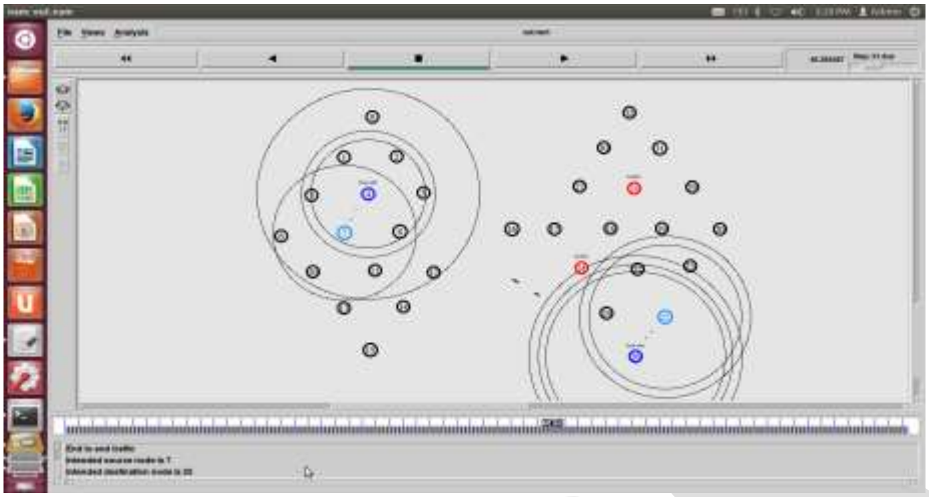
nodes are moving from 0th position to the particular position
Point to point traffic
End to end traffic

Figure 3: Simulation in progress



End to end traffic
Intended source node is 7
Intended destination node is 20

Figure 4: Intended source and destination nodes



End to end traffic
Intended source node is 7
Intended destination node is 22

Figure 5: Optimal route between source and destination

Figure 2 depicts network formation which involves deployment of mobile nodes and configuring them. Figure 3 depicts traffic analysis where traffic is detected between point-to-point and end-to-end transmissions. Once the attacker nodes obtain the traffic information from the attacked node they discover the possible source node and destination node of the network as depicted in Figure 4. Figure 5 depicts that an optimal route between the source and destination is discovered through their best neighbors.

Performance of SETPD is analyzed based on three parameters: Packet Delivery Ratio, Throughput and Average Packet Loss.

1. Packet Delivery Ratio (PDR) is characterized as the ratio of information got by the destinations to those created by the sources. It is characterized as:

$$PDR = (S1/S2) * 100$$

Where, S1 is the total number of packets got by each destination and S2 is the total number of packets produced by each source. Figure 6 depicts the relative performance of existing method (ESTA) with the implemented method (SETPD) and enhancement for Packet Delivery Ratio with varying time and pdr. As the time increases Packet Delivery Ratio also increases. It is observed that the enhancement made to the implemented method has higher Packet Delivery Ratio compared to the existing method.

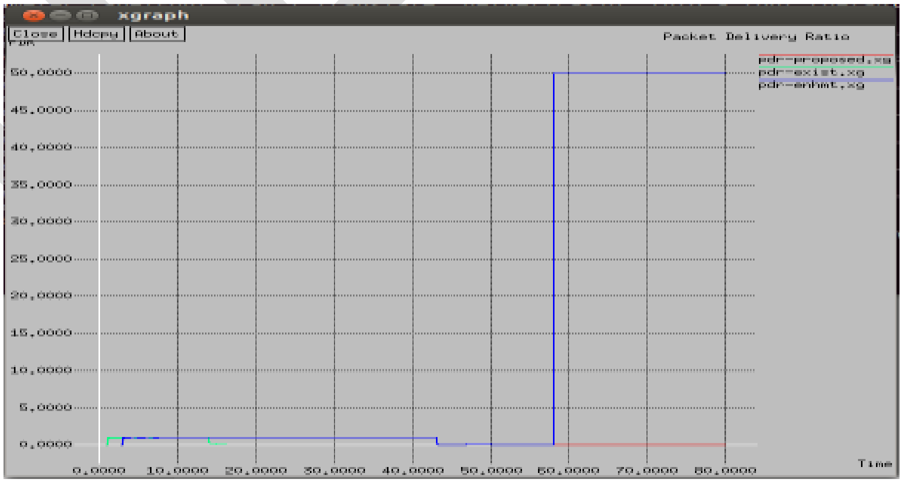


Figure 6: Packet Delivery Ratio analysis

2. Throughput is characterized as number of packets that can be transmitted over the system in a certain time. It is characterized as:

$$\text{Throughput} = N/1000$$

Where, N is the number of bits successfully got by the destination. It is measured in bits per second (bps). Figure 7 depicts the relative performance of existing method (ESTA) with the implemented method (SETPD) and enhancement for throughput with varying time and Kb/s. As the time increases throughput also increases. It is observed that the enhancement made to the implemented method has high throughput compared to the existing method.

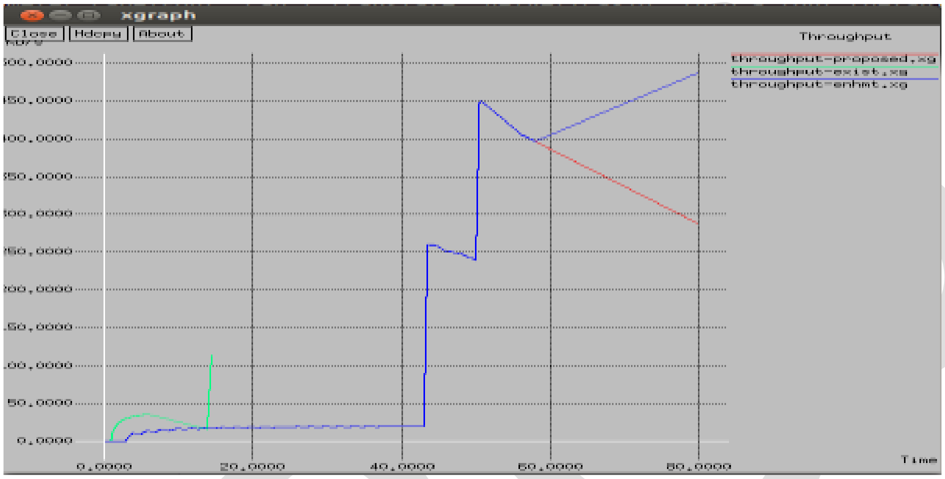


Figure 7: Throughput analysis

3. Average Packet Loss is the aggregate number of packets lost/dropped while transferring the packets over the network by the total number of packets. Figure 8 depicts the relative performance of existing method (ESTA) with the implemented method (SETPD) and enhancement for average packet loss with varying time and packets dropped. It is observed that the enhancement made to the implemented method has less packet loss compared to the existing method.

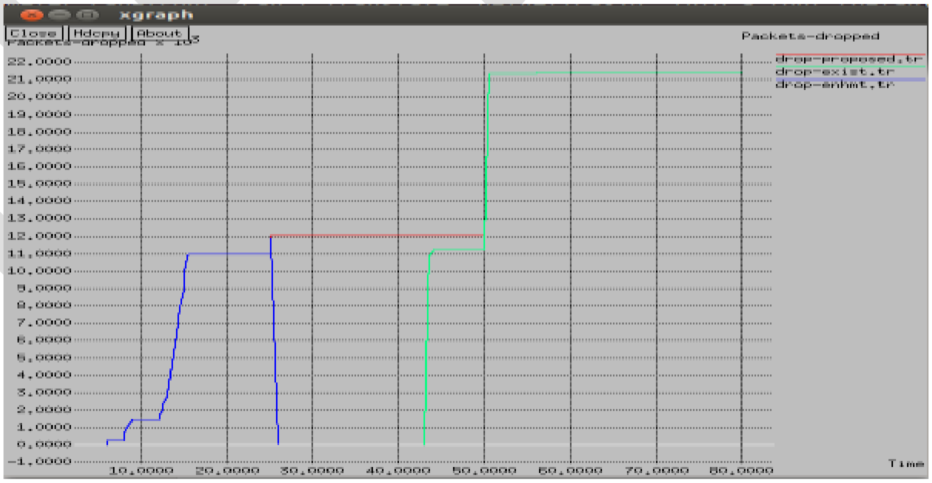


Figure 8: Average Packet Loss analysis

CONCLUSION

Secure and Efficient Traffic Pattern Discovery (SETPD) gives an idea of attacking MANETs because of communication anonymity in MANETs. It is an attacking system which works passively to carry out the traffic analysis depending upon statistical features of caught raw traffic. The raw traffic is captured from the PHY/MAC layer of the network without looking into its contents. Traffic is detected between point-to-point and end-to-end transmissions. The hidden traffic patterns i.e., actual source node, destination node and end-to-end communication path is revealed.Any network is prone to external attacker outside the network who can disrupt the network behaviour by injecting erroneous packets or modifying the packets. This attacker may not support efficient traffic pattern discovery, so it is eliminated from the network. SETPD is compared with ESTA and comparison is based on the factors such as packet delivery ratio, throughput, and average packet loss. Results indicate that the SETPD has higher packet delivery ratio, throughput and less packet drop in comparison with the ESTA.

REFERENCES:

[1] Yang Qin, Dijiang Huang, “STARS: A Statistical Traffic Pattern Discovery System for MANETs”, IEEE Trans.dependable and secure computing, vol. 11,no. 2,march/april 2014.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] G. Danezis, C. Diaz, and C. Troncoso, “Two-Sided Statistical Disclosure Attack,” Proc. Seventh Int’l Conf. Privacy Enhancing Technologies, pp. 30-44, 2007.

[13] 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