American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-5, pp-210-216
www.ajer.org
Research Paper Open Access

Challenges in Mobile Ad Hoc Network

Reshma S. Patil[1], Dr. D.J.Pete[2]
[1](Extc Dept., Dmce College/ Mumbai University ,India)
[2](Hod Of Electronics Department, Dmce College/ Mumbai University, India)

ABSTRACT : *In MANET, the network topology can change dynamically in unpredictable manner since the nodes are free to move anywhere in network. Most of the techniques have been used to protect the data transfer in MANET which are based on packet encryption. We know that MANET's are still suffering the problem of statistical traffic analysis attack. In this paper, we proposed a statistical traffic pattern discovery system (STAR) which is used to find out communication traffic patterns without decrypting the captured packet. STARS is having capability to find actual source node and actual destination node. As well as it has capability to find end to end communication link. STARS is having good accuracy in discovering the hidden traffic.*
Keywords : *Anonymous Communication, Attacks in MANET, MANET Network, Point-To-Point Matrix, Statistical Traffic Pattern, Traffic Matrix.*

I. INTRODUCTION

Mobile Ad hoc networks are dynamic in nature and it uses wireless communication medium for data transferring. MANET provides limited resources. Communication anonymity is major problem in MANET. In MANET it is very difficult to find out actual source node and actual destination node as well as communication link between source node and destination node. MANET's are mostly used in military missions. In MANET's if nodes are present in their range of communication then these nodes are communicated with each other using point to point communication i.e directly communication takes place between these two nodes. Otherwise to deliver a packet from source node to destination node , it uses other nodes which are located in their transmission path or link. From this it is clear that there is no centralized device present between source node and destination node so that route for the packet delivery is decided by intermediate nodes from this we can say that MANET is vulnerable under traffic analysis attacks. So it is very difficult to find out the link between source node and destination node as well as intermediate nodes involves in communication. Due to this difficult to find out start time, end time, rate of communication.

To prevent traffic pattern by hiding link between source node and destination node many anonymous routing protocols are used in MANET. Such as ANDOR [2], MASK [3], OLAR [4], SDAR [4] etc. As well as Onion routing [5] & Mix- net[8] anonymity enhancing techniques are used to protect data by using packet encryption method to hide sensitive information transmitted between source & destination node. Even though such protocols are used , passive attackers still monitoring the path of data and perform traffic analysis attacks. Passive attackers are the attackers which only observe the communication between source node and destination node and collect information & perform analysis without intercepting the network behavior. There are some passive attacks such as brute force attack & predecessor attacks [6]. These two attacks are not fully successful to analyze MANET traffic due to following reason :

1. Broadcasting nature of MANET
2. The Mobile nature of MANET
3. The Ad-hoc nature of MANET.

In this paper, we described Statistical Traffic Pattern Discovery System (STARS). It is used to find actual source and actual destination node using point to point traffic matrix, end to end traffic matrix and probability distribution method. This paper is organized in following way :

Section II gives the idea about previous work in MANET. Section III describes the system. Section IV presents the traffic models. Section V described the implementation of system. Section VI presents the result of system. In Section VII we have given the conclusion of our work.

II. RELATED WORKS

In wired communication network , the traffic analysis attacks can be easily detected. There are many attacks in wireless communication system such as brute force attack [5] , in this type of attack attacker monitors that the packets coming from which node and it is transmitted to which node so that attacker will get idea that how much time is required to transmit captured packet. Attacker transmits dummy packets in the network. In this attacker follows the packet transmission path from initiator to receiver. If there are many number of receiver then it takes more time to find out information. This process is continue until all messages are transmitted to receiver. This is actually passive attack in which attacker only monitor the communication between nodes, it does not intercept any captured packet Node flushing attack [5]; this type of attack is known as spam or flooding attack . In this attack, attacker knows that nodes wait until they have ' t' no. of messages, before sending to another node attacker can send 't-1' messages in such away attacker can easily identify their own messages . In this attacker sends dummy packets to receiver node but in specific instances these dummy packets is not useful. These attacks are suitable for only wired networks instead of wireless network.

Timing attacks [1] [5]; from name it is clear that attacker attacks on transmission timing of packets, the packets are transmitted through different routs so that attacker observe the timing required to transmit packet from initiator to receiver. Even if initiator & receiver uses the constant link to transmit packets attacker can easily track the path. If paths are different he monitors the latency of each route of message and correlated with messages coming in the system as well as going out to the system by calculating there transmission latencies. But this type of attack is not suitable for wireless medium. These attacks are used to reveal who is talking to whom as well as to reveal sensitive information which is encrypted in packets. Above all attacks are suitable for wired networks. There are some statistical traffic analysis attacks which doesn't change the network behavior. For example, predecessor attack [3] [5]; in this the attacker detects an identifiable path of communication over a no. of rounds. In this attacker log into network and acts as a intermediate node and try to find actual initiator and receiver node. But this is successful only when source node does not leave the group during whole communication time period.

There are some routing protocols have been used to detect predecessor attack such as Onion Routing [2], DC net [3] & Mix net [3]. This type of attack is not useful in MANET due to Ad – hoc nature of MANET. In MANET's nodes are movable so that it changes it's location so it is difficult to find out actual source and destination node. Statistical disclosure attacks are not successful in MANET because attacker is not able to find out actual source & destination node due signal detection problem [5]. Due to unique characteristics of MANET; traffic analysis is some what difficult.

He.et.al [1] proposed timing based approach [5] in which attacker estimate the flow rate of communication path using packet matching. Then depending on this the network is divided into 2 parts. One part is the source which communicate with sufficient rate and other one which cannot be identified to estimate the potential destinations.

Liu.et.al [1] proposed a Traffic Inherence Algorithm[4]for MANET's which conclude that attacker can recognize point to point traffic using MAC control frames, end to end traffic by tracing routing frames & data frames have been used to find out actual traffic pattern. TIA has good accuracy but it is applicable for particular anonymous routing protocol not for general purpose.

III. STATISTICAL TRAFFIC PATTERN DISCOVERY SYSTEM

In this paper, we explained Statistical Traffic Pattern Discovery System for MANETs. It include two main steps: 1) By using captured packet first we construct point to point matrix and the end to end traffic matrix. 2) After analyzing end to end traffic matrix , STARs calculate the Source/ Destination Probability distribution for each pair of node.

Disadvantages of Existing System:

I Approaches do not work well to analyze MANET traffic.

II The scheme fails to address several important constrains when deriving the end-to-end traffic from the one hop evidences.

III It does not provide a method to identify the actual source and destination nodes (or to calculate the source/destination probability distribution).

IV 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 uses the concept of heuristics approach to find hidden traffic pattern in MANET. It performs the traffic analysis using the statistical nature of captured traffic. By using this method attacker observed the actual source and actual destination node & correlates source to their corresponding destination. It reused the

evidence based model and derived the source /destination probability distribution & multi hop probability distribution. These distributions are used to find hidden traffic pattern.
All previous methods are used for partial attacks; they are not able to detect both source node & destination node at the same time for any given network. STARS is the attacking system which can detects all the source & destination nodes. As well as it can trace the path or relationship between them.

Advantages of System:

I. Divide the entire network into multiple regions geographically;
II. Deploy sensors along the boundaries of each region
III. To monitor the cross-component traffic;
IV. Treat each region as a super node and use STARS to figure out the sources, destinations, and end-to-end communication relations;
V. Analyze the traffic even when nodes are close to each other by treating the close nodes as a super node.

STAR is Implemented using NS-2 (Network Simulator 2) software. NS2 offers a good platform focused on the simulation of TCP, UDP, routing and multi-cast protocols over wired and wireless networks. NS2 is based on two languages C++ and OTcl -Object Oriented Tool Command Language-. C++ is used to implement all the models and internal mechanisms of the NS2 network simulator while OTcl is used as a user interface to control and set the simulation. On the one hand, C++ is a compiled language and therefore computationally efficient when executed, however, it is slow to be changed because requires re-compilation after any change done. On the other hand, OTcl is an interpreted language and therefore does not need compilation, so changes are done very fast. However OTcl it is slower than C++. These are the reasons why they are used for different purposes inside NS2.

IV. SYSTEM MODEL

STARs adopted Two fundamental models.

1. Communication model
2. Attack Model

1. Communication Model

In this model, we assumed that combination of ant two anonymity enhancing techniques are used to protect Mobile Ad hoc Network.

a. 802.11 (a/b/g) protocol is use to controlled Phy/MAC layer. But all packets are encrypted so that attacker can't decrypt that.
b. Each an every packet should have same size so that attacker is not able to trace the packet.
c. Source & destination addresses in MAC layer & IP header are set to all 1. So that attacker cannot identify the point to point communication link.
d. Dummy traffic & delay are not used due to limited no. of resources.
e. Traffic pattern should be in hidden form.

2. Attack Model

In this model, attacker discover the traffic pattern. Assume

a. Attacker is passive attacker. He only observe the communication between nodes.
b. Attacker node is connected to other node by using additional channel so that communication between attacker node will not influence the MANET communication.
c. Any nodes are located in network in such a way they are distinct from each other so that the location tracking techniques are able to identify source of wireless signal.
d. Attacker can trace the location of each mobile node by using sensors or cameras.

V. IMPLEMENTATION OF SYSTEM

Statistical traffic pattern discovery system for MANET. For the basic idea of STARs we will use a simple structure as shown below.

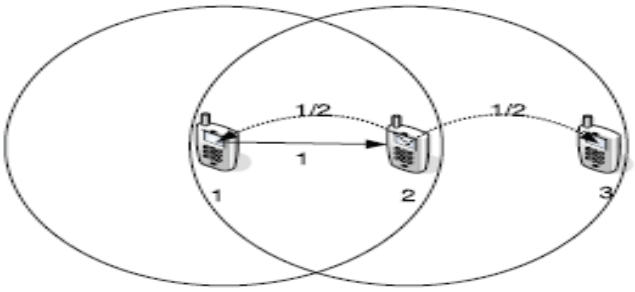


Fig. 4.1 Simple wireless Ad hoc network

In above network, there are 3 nodes (i.e. Node 1, Node 2& Node 3) which are connected to each other via wireless medium. Node 2 is located in between Node 1 & Node 3. Node 2 is in the transmission range of node 1& node 3but node 3 is located in out of the transmission range of node 1.
STARs includes two major steps.

i. Construct point to point traffic matrix & then derive end to end traffic matrix.
ii. Apply heuristics approach to find actual source & destination nodes.

4.1 Construction of Traffic Matrices

4.1.1 Point to point Matrix

In time interval 'T' we have to first develop point to point matrix such that each matrices only contains independent one hop packets. Sometimes two packets captured at different time slot may be the same packet received at different locations. For.eg. two packets sent by node 1 & node 2 at different time slot may have chances of same packets transmitted by node 1 & node 2. To avoid such problem we can apply "Time slicing" technique & develop traffic Matrix 'W' which is N x N point to point traffic relation matrix. The length of time interval can be calculated by following method :

1. At a particular time interval node can be a sender or receiver but it can't be both .
2. In particular time interval each traffic matrix must be properly represent one hop transmission of packet.

In MANETs, nodes are moving in nature.
Consider in a network there are three nodes node 1, node 2 & node 3. Assume node 1 sends packet to node 2 which is in the range of transmission of node 1 so that probability of packet transmitting from node 1 to node 2 is 1. Node 2 is transmitted the same packet to node 3as well as node 1 so the probability of transmission of packet is 0.5. as we know node 3 is not in the range of node 1 so the probability of packet transmission is 0.
Therefore the point to point probability matrix can be written as

$$W_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, W_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0.5 & 0 & 0.5 \\ 0 & 0 & 0 \end{bmatrix}.$$

Note that in W_2 original packet is transmitted by node 2 to node 3 & node 1. Therefore the virtual size is 0.5 which indicates node 1 & node 3 are equally likely to be the actual receiver.

4.1.2 End to End Traffic Matrix

End to end traffic matrix is denoted by 'R' & it is derived from point to point matrix 'W'. It includes both point to point captured traffic & multi hop traffic deduced from point to point traffic.
Let consider R = W , then g(R, W_2) should derive all possible end to end flows of communication . As we know W_2 contains packets which are send by node 2 to node 3 & node 1 having virtual size 0.5. Let P_{21} & P_{23} are the notations we are using for these two packets. Current R contains any one packet which received by node 2 from node 1 that is $P_{12.}$ For multi hop we can say packet is transmitted from node 1 to node 3 via node 2 i.e. two hop count. So that P_{13} virtual size = min {$P_{12.\ \text{virtual size}}$, $P_{23\ \text{virtual size}}$} = 0.5
Algorithm 1 is use to calculate end to end traffic matrix R.
Algorithm 1. —f ($W/_{1xK}$).

1: R =W1

2: For e = 1 to K - 1 do
3: R = g (R, W_{e+1}) + W_{e+1}
4: end for
5: return R

Function 'g' takes to input
1) End to end traffic matrix 'R' which is derive from point to point traffic matrix 'W'.
2) W_{e+1} is the next point to point traffic matrix.
The output of end to end traffic matrix is derived from W_1 to $W_{e+1.}$
We can write matrix R in following manner.

$$\mathbf{R} = \begin{bmatrix} 0 & 1 & 0.5 \\ 0.5 & 0 & 0.5 \\ 0 & 0 & 0 \end{bmatrix}.$$

From above we can say that end to end traffic matrix R contains one hop packets captured by W_1 & W_2 as well as it contains two hop flow of virtual size 0.5 from Node 1 to Node 3.

4.2 Traffic Pattern Discovery

After finding point to point traffic matrix W & end to end traffic matrix R, now we will find out actual source and destination node by using source / destination probability distribution and end to end link probability distribution.

4.2.1 Source / Destination Probability Distribution.

To investigate actual source and actual destination node first we have to derive source vector '$\overline{S}$' and destination vector '$\overline{D}$'.
Where as

$\overline{S}$ = [S_0, S_1, $S_{2.....}$ S_n]
$\overline{D}$ = [D_0,D_1,D_2…..D_n]

Without any traffic information all nodes are same that may be source node or destination node or intermediate node . we can say, a node having high probability is actual source node & the node having high probability of receiving packets from other nodes is actually a destination node.
Algorithm 2 & Algorithm 3 are used to evaluate $\overline{S}$ & $\overline{D}$.
Algorithm 2 src (R)

1: S_0 = (1/N,1/N,……..,1/N)
2: n = 0
3: do
4: S_{n+1} = (Φ(R). Φ^T(R)). S_n
5: normalize S_{n+1}
6: n = n+1
7: while $S_n \neq S_{n-1}$
8: S= S_n
9: return S

Algorithm 3 Dest ®

1: D_0 = (1/N,1/N,……..,1/N)
2: n = 0
3: do
4: D_{n+1} = (Φ^T(R). Φ(R)). D_n
5: normalize D_{n+1}
6: n = n+1
7: while $D_n \neq D_{n-1}$
8: D= D_n
9: return D

4.2.2 End to End Link Probability Distribution.

By using these we can evaluate link between actual source node and actual destination node. The many packets are transmitted from any node is known as Source node and the packets coming from any node is Zero that means that is destination node. To find out end to end probability distribution algorithms are used as well as we can refer routing table at each node so that we get idea about link between actual source node and actual destination.

Flowchart for STARS:

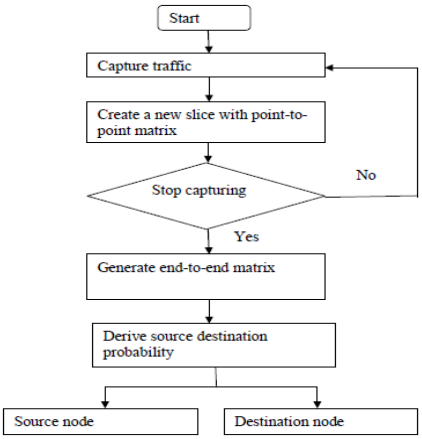


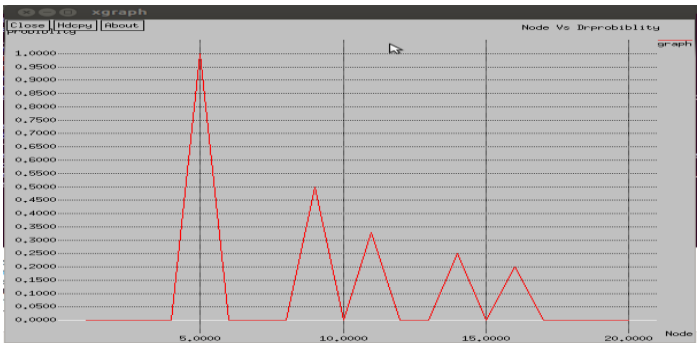
Fig. 4. 2 Work flow of STARs

VI. DEMONSTRATION & RESULT

Consider a MANET network having 20 nodes in 800X800 meter square area. There are four different scenario:

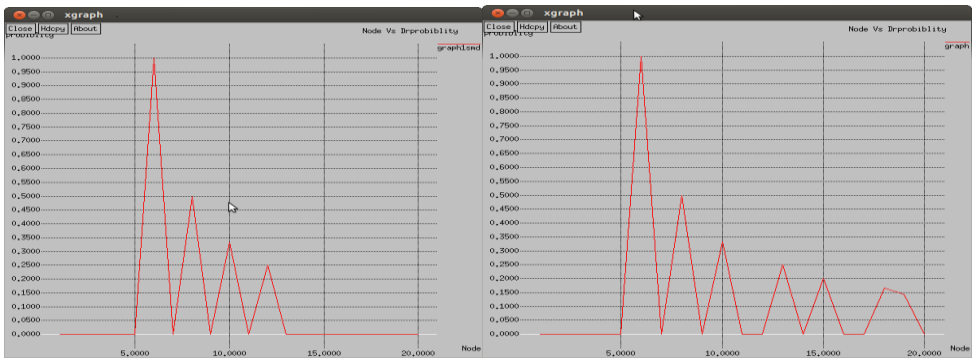
1) Single source single destination

Let us consider in this case node 5 is a source node and node 16 is destination node .



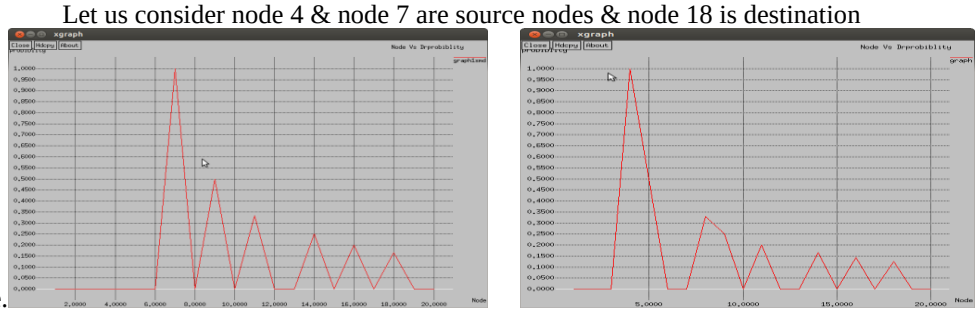
2) Single source multiple destination.

Let us consider node 6 is source node and node 12 & node 18 are destination nodes.



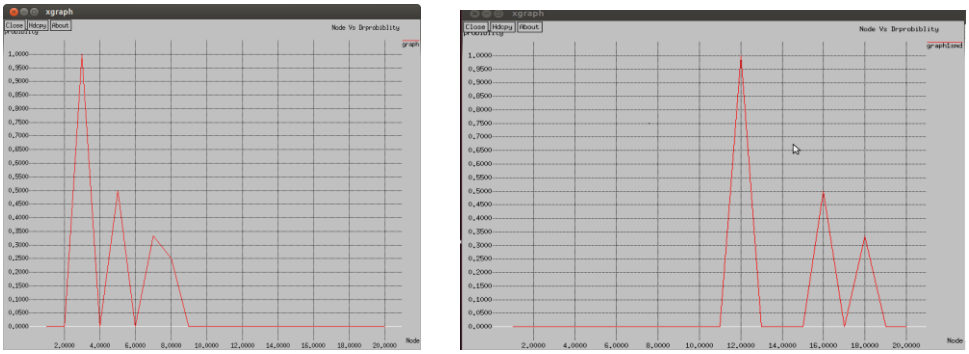
3) Multiple source single destination.

Let us consider node 4 & node 7 are source nodes & node 18 is destination node.



4) Multiple source multiple destination.

Let us consider node 3 & node 8 are source nodes & node 12 & node 18 are destination nodes.



VII. CONCLUSION

In this paper, we described a novel STARS for MANETS. Basically STARS is a attacking system which is used to find out actual source node and actual destination node. STARS system captured a raw traffic and form this it constructs point to point traffic matrix and end to end traffic matrix. The proposed system is purely passive in nature. So it doesn't require traffic analyzer. This system better result for MANET network. STARS is also used to find out hidden traffic pattern.

REFERENCES

[1]. Yang Qin, Dijiang Huang, Senior Member, IEEE, and Bing Li, Student Member, "STARS: A Statistical Traffic Pattern Discovery System for MANETs", IEEE transactions on dependable and secure computing, VOL. 11, NO. 2, pp.181-191 MARCH/APRIL 2014.

[2]. 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.

[3]. 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.

[4]. 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.

[5]. T. Parameswaran, Dr. C. Palanisamy, M.Karthigadevi, "Traffic Analysis in Anonymous MANETs," International Journal of Research in Advent Technology, Vol.2, No.10, October 2014