

## PREVENTING DISCLOSING ATTACKS BY TRAFFIC HIDING TECHNIQUE IN MANETS

*Ms. R.Ramya<sup>1</sup>, Mr. V. Arnold John<sup>2</sup>, Mr.S. Suresh Krishna<sup>3</sup>, Mr.J. Paranthaman<sup>4</sup>*  
*1-PG Student, AMACE, 2, 3,4 - Assistant Professor, Department of ECE, AMACE*

**Abstract** - Maximum in wireless ad-hoc network, it will always choose shortest path in prior. So attackers shall enter the network freely, because if the node monitors the packet forwarding mechanism it can easily identify the entire traffic pattern in the system. Based on the profiles hacker will enter the network effectively. It can be helpful for dropping or modifying data. But here we choose the second shortest path for data forwarding. In our scenario when we change to select the routing path hackers can't be capture the current routing path.

**Keywords** –Traffic matrix, Routing table, hidden traffic.

### 1.INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly

and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs.

Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low

probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. MANETs are self-organizing and self re-configuring multi hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi hop forwarding.

The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to

take care of detection and prevention of anomalies. Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network.

Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources.

In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes.

This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures.

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs.

Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing

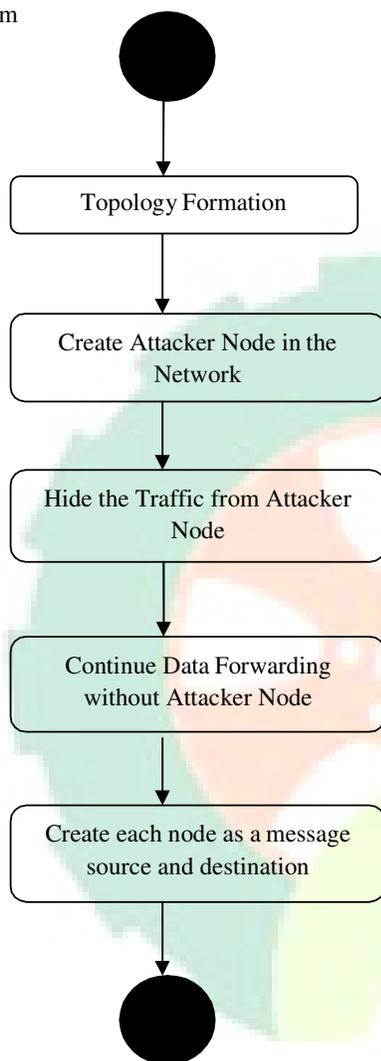
the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

## II. PROPOSED SCHEME

In STAR system every captured packet is treated as an as an evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. Statistical traffic analysis intends to discover sensitive information from the statistical characteristics of the network traffic, for example, the traffic volume. The adversaries usually do not change the network behavior (such as injecting or modifying packets). The only thing they do is to quietly collect traffic information and perform statistical calculations. Here an attacker finds himself to be on an anonymous path to the targeted destination, he increments the shared counter for its predecessor node in this path.

Number of techniques has been proposed based on packet encryption to protect the communication in MANETs, Still MANETs are vulnerable to certain statistical traffic analysis attacks. Thus present a Novel statistical traffic pattern discovery system (STARS). STARS functioning based on stastical characteristics of captured raw traffic. STARS discover the relationships of source to destination communication. Studies conclude STARS achieve good accuracy in hidden traffic pattern. STAR is a complete disclosure attack. It is a passive attack. It is hard to identify is the attack happen or not. STAR will completely monitor entire traffic and capture path of data flow. STAR is a complete target tracking mechanism. It is a type of location disclosure attack. One way can say as external attack because it never effect any nodes.

Flow Diagram



## MODULES

1.Topology Formation

2.Attacker Model

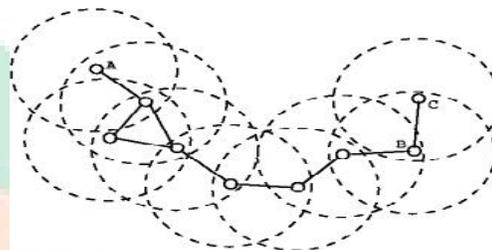
3.STAR

4.Traffic Protector

1.Topology Formation

Initially we are placing nodes in the network and we choose a source and destination. If the source has no route to the destination, then source A initiates

After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node. If a closer neighbor node is available, the RREQ packet is forwarded to that node. If no closer neighbor node is the RREQ packet is flooded to all neighbor nodes.



When destinations receive the RREQ, it will generate RREP and it will send the same path. Finally we establish the route for data traffic.

## 2.Attacker Model

Here STARS including the attacker node which one monitors all the possible traffic patterns in the whole network. This attack is known as disclosure attack. Attackers only need to collect information and perform analysis quietly without changing the network behavior (such as injecting or modifying packets).

## 3.STAR

STAR is the technique will create the route discovery in an on-demand fashion.source/destination probability distribution for each and every node to be a message source and destination and the end-to-end link probability distribution(the probability for each node to be an end-to-end communication pair).

## 4.Traffic Protector

In this module, first it uses the captured traffic to construct a sequence of point-to-point traffic

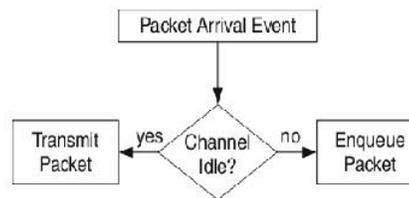
matrices and then derives the end-to-end traffic matrix.

Second, further analyzing the end-to-end traffic matrix, it calculates the probability for each node to be a source/destination (the source/destination probability distribution) and that for each pair of node to be an end-to-end communication link (the end-to-end link probability distribution). Finally it will hide the traffic pattern between actual source and destination from disclosure nodes.

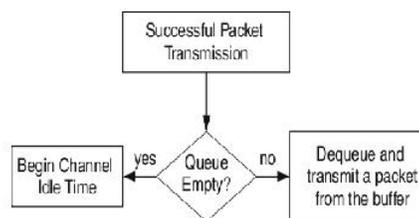
#### IV. EXPERIMENT

Simulating is a process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system. Simulation is widely-used in system modeling for applications ranging from engineering research, business analysis, manufacturing planning, and biological science experimentation, just to name a few.

Compared to analytical modeling, simulation usually requires less abstraction in the model (i.e., fewer simplifying assumptions) since almost every possible detail of the specifications of the system can be put into the simulation model to best describe the actual system. When the system is rather large and complex, a straightforward mathematical formulation may not be feasible. In this case, the simulation approach is usually preferred to the analytical approach. In common with analytical modeling, simulation modeling may leave out some details, since too many details may result in an unmanageable simulation and substantial computation effort. It is important to carefully consider a measure under consideration and not to include irrelevant detail into the simulation.

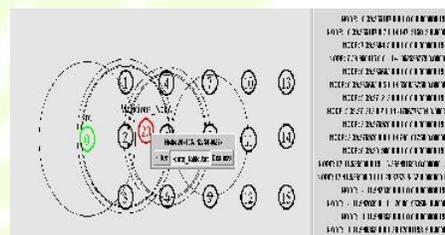


PACKET ARRIVAL EVENT



SUCCESSFUL PACKET TRANSMISSION

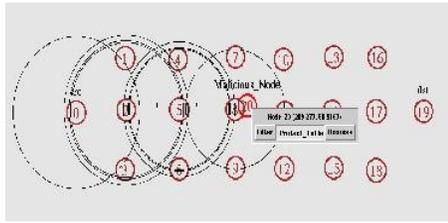
The following snap shots represent how nodes are created and data are transmitted with attacker node in (i) and(ii) and data transmission after the path is hidden in(iii) and (iv).



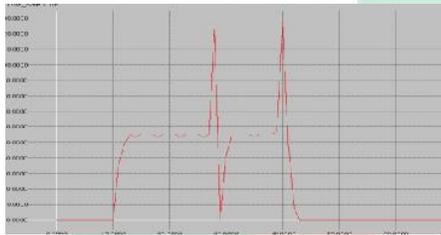
(i)



(ii)



(iii)



(iv)

## V.CONCLUSION

Source hiding technique was a type of traffic security method. In this system each point acts as source and destination. This was a form of originating point to point traffic. Thus a complete end to end anonymity will form. All this security is provided before the traffic will form. Thus prevention better than cure will come in practical. In STAR disclosure attack entire traffic path is captured. Source and destination have no idea about attack. This is a type of passive attack. Such a disclosure attack completely avoided through this source hiding security technique.

## VI. 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*, 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.*, 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)*, 2008.
- [4] M. Blaze, J. Ioannidis, A. Keromytis, T. Malkin, and A. Rubin, "WAR: Wireless Anonymous Routing," *Proc. Int'l Conf. Security Protocols*, 2005.
- [5] 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)*, 2006.
- [6] R. Shokri, M. Yabandeh, and N. Yazdani, "Anonymous Routing in MANET Using Random Identifiers," *Proc. Sixth Int'l Conf. Networking (ICN)*, 2007.
- [7] 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)*, 2005.
- [8] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE J. Selected Areas in Comm.*, May 2002.
- [9] W. Dai, "Two Attacks against a PipeNet-Like Protocol Once Used by the Freedom Service," 2013.
- [10] X. Wang, S. Chen, and S. Jajodia, "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems," *Proc. IEEE Symp. Security and Privacy*, 2007.