International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
www.ioirp.com ISSN: 2394-6364, Volume – 1, Issue – 6. May 2015

STATISTICAL TRAFFIC ANALYSIS ATTACKS ON END TO END COMMUNICATIONS

M.Abinaya
M.E (Computer Science and Engineering), Idhaya Engineering College for Women, Chinnasalem, India

***Abstract*— Privacy and security have emerged as an important research issue in mobile Ad Hoc Networks (MANET). We proposed how to discover the communication channels without changing the packet content as plaintext, so we present a novel statistical traffic pattern discovery system (STARS). By using the STARS to identify the Source/destination anonymity and end-to-end anonymity. MANET systems can achieve very restricted communication anonymity under the attack of STARS.**

I. INTRODUCTION

Compared to wired networks, MANETs are more vulnerable to both active and passive attacks. Wireless transmissions are easy to capture remotely and undetected, while the lack of central management and monitoring make network nodes susceptible to active attacks. A sequence of point-to-point traffic matrices is created, and then they are used to derive end-to-end (multihop) relations. First, the scheme fails to address several important constrains when deriving the end-to-end traffic from the one-hop evidences. Second, it does not provide a method to identify the actual source and destination nodes (or to calculate the source/destination probability distribution). They collectively maintain a single predecessor counter for each legitimate node in the system. When 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. The counters are then used for the attackers to infer the possible source nodes of the given destination. The adversaries can trace the movement of each mobile node, by using cameras or other types of sensors. In this case, the signals (packets) transmitted by a node can always be associated with it even when the node moves from one spot to another. We propose a novel secure distributed path construction protocol for anonymous communication and wireless ad hoc networks. As opposed to previous related protocols, the proposed protocol does not require the source node to gather and store information about the network topology. Instead, the source node initiates a path establishment process by broadcasting a path discovery message with certain trust requirements to all of neighboring nodes. Intermediate nodes satisfying these trust requirements insert their identification (IDs) and a session key into the path discovery message and forward copies of this message to their selected neighbors until the message gets to its destination. The intermediate nodes encrypt this information before adding it to the message, and only the selected neighbor nodes are able to decrypt it. Once the receiver node receives the message, it retrieves from the message the information about all intermediate nodes, encapsulates this information in a multi-layered message, and sends it along a reverse path in the dissemination tree back to the source node. Each intermediate node along the reverse path removes one encrypted layer from the message, and forwards the message to its ancestor node until the message reaches the source node. When the protocol terminates, the source node ends-up with information about all the trusted intermediate nodes on the discovered route as well as the session keys to encrypt the data transmitted through each of these nodes.

- **Modules:**

1. Network Infrastructure
2. Global traffic detection
3. Probability distribution
4. Recover packets

A. Network Infrastructure:

In this network, point to point message transmission between the nodes, usually nodes can serve as both a host and a router. In this model, every captured packet is treated as evidence supporting a point-to-point transmission between the sender and

the receiver. The sender can able to send a message and transmit to destination via multi-hop with split the messages into multiple numbers of packets. The packets can be split based on the size of the file.

B. Global Traffic detection:

In this project, to build point-to-point traffic matrices such 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. A node can be either a sender or a receiver within this time interval. But it cannot be both. Identify those events in the network. Each traffic matrix must correctly represent the one-hop transmissions during the corresponding time interval. The "time slicing" has to make sure that all packets captured in any of the time intervals are independent with each other. In other words, two packets residing in different entries of the same matrix must not be the same packet transmitted through multiple hops.

C. Probability distribution:

In this module, source/destination and end-end link approaches are partial attacks in the sense that they either only tries to identify the source or destination nodes or to find out the corresponding destination/source nodes for given particular source or destination nodes. The adversaries are not able to determine whether a particular node is a destination depending on whether the node sends out traffic. By using these approaches we find out the actual source and destination of the particular packet and then send the packet to the correct destination.

D. Recover Packets:

In this module, this claim is based on the fact that if a node receives a lot of packets from a node with high probability of being a source, the node itself has a high probability of being a destination. If the packets are missing intimate to the source otherwise merge the packets and store it to the desired location. The packet counts starts from 0.

- **Super Node:**

Analyze the traffic in the network, even when nodes are close to each other by treating the close nodes as a super node. GSTARS does not need the signal detectors to be able to precisely locate the signal source. They are only required to determine which super node (region) the signals are sent from. Moreover, in STARS, 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 GSTARS because most potential receivers of a packet will be contained within one or a few super nodes.

II. PROBLEM DEFINITION

The statistical disclosure attacks cannot be applied to MANETs either, because the attackers cannot easily identify the actual source nodes in MANETs. 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. Dummy traffic and dummy delay are not used due to the highly restricted resources in MANETs.

III. EXISTING SYSTEM

In existing system, the brute force attack tries to track a message by enumerating all possible links a message could traverse. In blending attacks, attacker easily modifies messages and reordered by the system. 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. Moreover, in a MANET protected by anonymity enhancing techniques, it is a difficult task itself to identify an actual destination node as the target due to the ad hoc nature. The adversaries are not able to determine whether a particular node is a destination depending on whether the node sends out traffic. Nonetheless, the statistical disclosure attacks cannot be applied to MANETs either, because the attackers cannot easily identify the actual source nodes in MANETs.

A. Disadvantage:

- It's difficult to identify the actual destination.

- Attacker able to figure out the destination of the given source.

IV. PROPOSED SYSTEM

In this paper, we propose a novel statistical traffic pattern discovery system (STARS). STARS aims to derive the source/destination probability distribution, each node to be a message source/destination, and the end-to-end link probability distribution, i.e., the probability for each pair of To achieve its goals, STARS includes two major steps: 1) time slicing technique is used to construct point-to-point traffic matrices, 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. The contribution of STARS is 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 are a complete attacking system that first identifies all source and destination nodes and then determines their relationship.

A. Advantage:

- Easily identifies the destination.
- Able to detect the traffic between the mobile nodes.
- 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.

V. CONCLUSION

In this paper, we propose a novel STARS for MANETs. STARS are 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, STARS 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 STARS.

A. Future Work:

Furthermore, we have to analyze the traffic before sending the packets to destination. For single destination we have many paths to reach from source. So in case of traffic, user can choose an alternate way to send a message to destination.

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,vol. 6, no. 8,pp. 888-902, Aug. 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.,vol. 5, no. 9, pp. 2376-2385, Sept. 2006.

[3] Y. Qin and D. Huang, “OLAR: On-Demand Lightweight Anonymous Routing in MANETs,”Proc. Fourth Int’l Conf. MobileComputing and Ubiquitous Networking (ICMU ’08),pp. 72-79, 2008.

[4] M. Blaze, J. Ioannidis, A. Keromytis, T. Malkin, and A. Rubin,“WAR: Wireless Anonymous Routing,”Proc. Int’l Conf. SecurityProtocols,pp. 218-232, 2005.

[5] 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.

www.ioirp.com