STATISTICAL TRAFFIC ANALYSIS FOR ROUTING PROTOCOL ON MANETs

M.Abinaya[1] R.Vasanthi[2]
[1]PG Student [2]Asst. Prof Dept. of CSE,
[1&2]Affiliated to Anna University Chennai, Dept. of Computer Science and Engineering
Idhaya Engineering College for Women
Sabari.nya@gmail.com

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

1 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. The multi-cast mechanism and the layered encryption used in the protocol ensure the anonymity of the sender and receiver nodes.

2 MANETs

A mobile ad-hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad-hoc is Latin and means "for this purpose".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller (to determine, optimize, and distribute the routing table). MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).

Multi-hop relays date back to at least 500 BC. The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

3 PROPOSED SYSTEM

Consider a novel statistical traffic pattern discovery system .It 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 communication.

To achieve its goals, it 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.

2) Apply a heuristic approach to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations.

This 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. They are a complete attacking system that first identifies all source and destination nodes and then determines their relationship.

4 SYSTEM MODEL

There are various models are available to complete the whole process.

4.1 Network Infrastructure

This specifies 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.

4.2 Global Traffic Detection

This is 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.

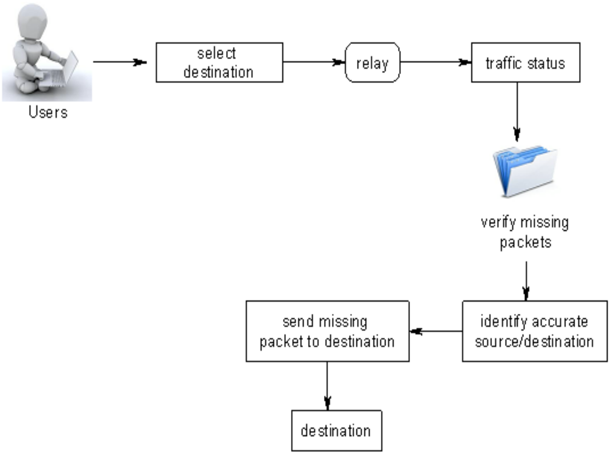
4.3 Super Node

Analyze the traffic in the network, even when nodes are close to each other by treating the close nodes as a super node. STARS 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, 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 because most potential receivers of a packet will be contained within one or a few super nodes.

4.4 Probability Distribution

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.

5 SYSTEM ARCHITECTURE



6 EXPERIMENT METHODS

6.1 Source/Destination Anonymity

To identify the sources or the destinations of the network traffic flows. A sequence of point-to-point traffic matrices is created, and then they are used to derive end- to-end relations. 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.

6.2 End-To-End Relationship Anonymity

To identify the end-to-end communication relations and to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations.

7 CONCLUSION

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, it 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. This empirical study demonstrates that the existing MANET systems can achieve very restricted communication anonymity under the attack of STARS.

8 FUTURE SCOPE

Furthermore, to analyze the traffic before sending the packets to the destination. For single destination which 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] Berthold.O, et al, (2014) In Proc. Workshop on Design Issues in Anonymity and Unobservability, ICSI TR-00-011, pp. 27–42. “The disadvantages of free mix routes and how to overcome them”.

[2] Dai.W, (2013).”Two Attacks against a pipeNet-Like Protocol Once Used by the Freedom service”

[3] Guo.S,et al,(2009).In Proceedings of the 55th Annual Reliability and Maintainability Symposium (RAMS 2009) on Fort Worth of Texas,USA,January pp.471-476 “Grid service reliability modeling on fault recovery and optimal task scheduling”.

[4] Huang.D(2008)”Unlinkability Measure for IEEE 802.11 based on MANETs “from IEEETrans.Wireless.vol.7,pp.1025-103.

[5] Kong.J,et al,(2007) “An Identity-free and On-demand Routing Scheme against the Ananymity of the presence of Threats in Mobile Computing”.vol.6,no.8,pp.888-902.

[6] ~~YangQin,et al,(2007)”Tran~~saction on the node dependable and secure computing”.