Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

MANET: Security Attacks and Communication Anonymity

Girish Parikh
ME Computer Networks, Savitribai Phule Pune University,
Nutan Maharashtra Institute of Engineering and Technology College, Maharashtra, India

Abstract— A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs are vulnerable to various kinds of security attacks. Communication Anonymity is one of critical security goal along with confidentiality, integrity, availability.

Keywords— Mobile ad-hoc network (MANET), Communication Anonymity, Security.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are an infrastructure-less, dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs are vulnerable to various kinds of security attacks.

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.

Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs are vulnerable to various kinds of security attacks.

There are two types of attacks - active attack and passive attack. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Active attacks are very severe attacks on the network that prevent message flow between the nodes.

MANETs are vulnerable under passive statistical traffic analysis attacks. To demonstrate this, a statistical traffic pattern discovery system (STARS) is presented. STARS works passively to perform traffic analysis based on statistical characteristics of captured raw traffic. STARS is capable of discovering the sources, the destinations, and the end-to-end communication relations.

II. LITERATURE SURVEY

2.1 MANETs characteristics [2]

- Distributed operation: There is no background network for the central control of the network operations; the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.
- Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.
- Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router. Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.
- Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.
- Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

2.2 MANET Vulnerability [2]

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:

- Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network.

- No predefined Boundary: In mobile Adhoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.
- Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation.
- Limited power supply: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.
- Adversary inside the Network: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behaviour of the node is malicious. Thus this attack is more dangerous than the external attack.

2.3 Security Goals [2]

In MANET all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

- Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.
- Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. Protection of information which is exchanging through a MANET. It should be protected against any disclosure attack like eavesdropping- unauthorized reading of message.
- Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way.. Integrity assures that a message being transferred is never corrupted.
- Authentication: Authentication is essentially assurance that participants in communication are authenticated and not impersonators. The recourses of network should be accessed by the authenticated nodes.
- Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.
- Resilience to attacks: It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.
- Freshness: It ensures that malicious node does not resend previously captured packets.

2.4 Classification of security Attacks [2]

The attacks can be categorized on the basis of behaviour of the attack i.e. Passive or Active attack

1 Passive attacks: A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic.

2 Active attacks: Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorised access to network that helps the attacker to make changes such as modification of packets.

2.5 MANET : Communication Anonymity

MOBILE ad hoc networks (MANETs) are originally designed for military tactic environments. Communication anonymity is a critical issue in MANETs, which generally consists of the following aspects:

1 Source/ destination anonymity- it is difficult to identify the sources or the destinations of the network flows.

2 End to end relationship anonymity—it is difficult to identify the end to end communication relations.

Over the past few decades, traffic analysis models have been widely investigated for static wired networks. For example, the simplest approach to track a message is to enumerate all possible links a message could traverse, namely, the brute force approach. Recently, statistical traffic analysis attacks have attracted broad interests due to their passive nature, i.e., attackers only need to collect information and perform analysis quietly without changing the network behaviour (such as injecting or modifying packets).

2.6 MANET Traffic Analysis : Challenges

It is difficult to analyse MANET traffic because of the following three natures of MANETs:

1 The broadcasting nature: In wired networks, a point-to-point message transmission usually has only one possible receiver. While in wireless networks, a message is broadcasted, this can have multiple possible receivers and so incurs additional uncertainty.

2 The ad hoc nature: MANETs lack network infrastructure, and each mobile node can serve as both a host and a router. Thus, it is difficult to determine the role of a mobile node to be a source, a destination, or just a relay.

3 The mobile nature: Most of existing traffic analysis models does not take into consideration the mobility of communication peers, which make the communication relations among mobile nodes more complex.

2.7 Anonymity Enhancing Technique

Technique	Description	Disadvantages
Onion routing [3]	Messages are encapsulated in layers of encryption. The encrypted data is transmitted through a series of network nodes called onion routers. When the final layer is decrypted, the message arrives at its destination.	Passive signal detectors can still eavesdrop on the wireless channel and can perform traffic analysis attack.
Mix networks [4]	Mix networks are routing protocols that create hard-to-trace communications by using a chain of proxy servers known as mixes which take in messages from multiple senders, shuffle them, and send them back out in random order to the next destination (possibly another mix node).	Passive signal detectors can still eavesdrop on the wireless channel and can perform traffic analysis attack.

2.8 Traffic Analysis Schemes

Traffic analysis	Description	Disadvantages
Brute force attack	The brute force attack tracks a message by enumerating all possible links a message could traverse.	Brute force attacks try as many possible answers as possible, this takes a lot of processing power.
Evidence based model	In this model, every captured packet is treated as an evidence supporting a point to point (one hop) transmission between the sender and the receiver.	It does not provide a method to identify the actual source and destination nodes (or to calculate the source / destination probability distribution).

To overcome all these inaccuracies, a novel statistical traffic pattern discovery system (STARS) is presented. STARS aims to derive the source/destination probability distribution, i.e., the probability for each node to be a message source/destination, and the end-to-end link probability distribution, i.e. the probability for each pair of nodes to be an end-to-end communication pair. To achieve its goals, STARS includes two major steps:

1. 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.
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:

1. STARS is the first statistical traffic analysis approach that considers the salient characteristics of MANETs: the broadcasting, ad hoc, and mobile nature.
2. 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 is a complete attacking system that first identifies all source and destination nodes and then determines their relationship.

III. SYSTEM MODEL

3.1 Communication Model

MANET communication system is subject to the following model:

1. The PHY/MAC layer is controlled by the commonly used 802.11(a/b/g) protocol. But all MAC frames (packets) are encrypted so that the adversaries cannot decrypt them to look into the contents.
2. Padding is applied so that all MAC frames (packets) have the same size. Nobody can trace a packet according to its unique size.
3. The "virtual carrier sensing" option is disabled. The source/destination addresses in MAC and IP headers are set to a broadcasting address (i.e., all "1") or to use identifier changing techniques. In this case, adversaries are prevented from identifying point to point communication relations.

4. No information about the traffic patterns is disclosed from the routing layer and above.
5. Dummy traffic and dummy delay are not used due to the highly restricted resources in MANETs.

3.2 Attack Model

The attacker's goal is to discover the traffic patterns among mobile nodes. Particularly, we have the following four assumptions for attackers:

1. The adversaries are passive signal detectors, i.e. they are not actively involved in the communications. They can monitor every single packet transmitted through the network.
2. The adversary nodes are connected through an additional channel which is different from the one used by the target MANET. Therefore, the communication between adversaries will not influence the MANET communication.
3. The adversaries can locate the signal source according to certain properties (e.g., transmission power and direction) of the detected signal, by using wireless location tracking technique. Note that none of these techniques can identify the source of a signal from several nodes very close to each other. Hence, this assumption actually indicates that the targeted networks are sparse in terms of the node density. In other words, any two nodes in such a network are distant from each other so that the location tracking techniques in use are able to uniquely identify the source of a wireless signal.
4. 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.

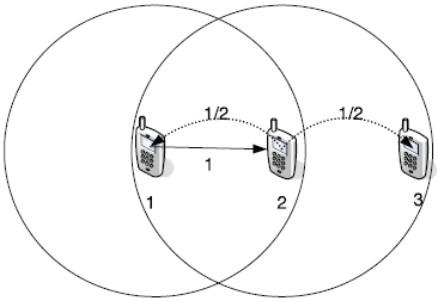

Fig 4.1 A simple Adhoc network

IV. STATISTICAL TRAFFIC PATTERN DISCOVERY SYSTEM [1]

To disclose the hidden traffic patterns in a MANET communication system, STARS includes two major steps. 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 analysing 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).

To illustrate the basic idea of STARS, we use a simple scenario shown in Fig. 4.1 above as an example. In this network, there are three wireless nodes (1, 2, and 3). Node 2 is located in the transmission range of node 1, and node 3 is located in the transmission range of node 2 (but not the transmission range of node 1). Two consecutive packets are detected: node 1 broadcasts a packet and then node 2 broadcasts a packet.

Following Fig 4.2 is the workflow of STARS. Let's go through workflow to understand the significance of each step.

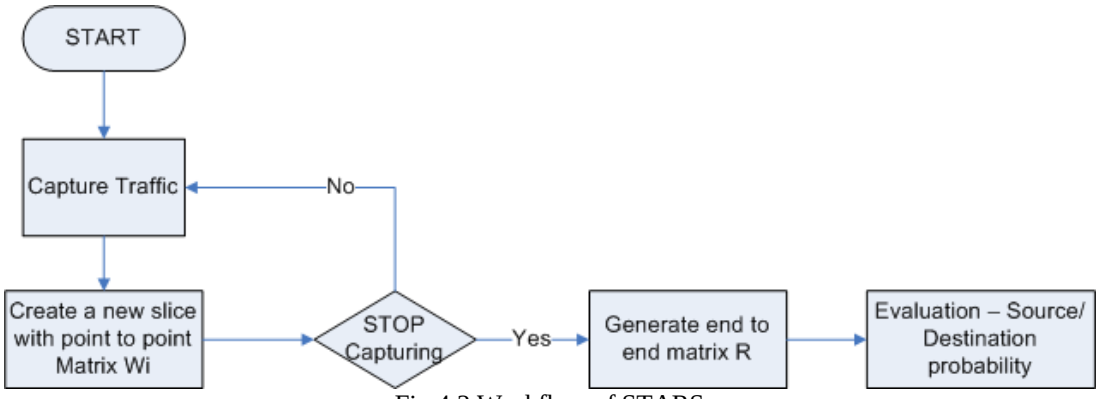

Fig 4.2 Workflow of STARS

4.1 Traffic Matrices Construction

4.1.1 Point to Point Traffic Matrix

With the captured point-to-point (one-hop) traffic in a certain period T, we first need to build point-to-point traffic matrices such that each traffic matrix only contains "independent", we apply a "time slicing" technique That is, we take snapshots of the network, and each snapshot is triggered by a captured packet.

For the example given in Fig. 4.1, we could derive:

$$\mathbf{W}_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \mathbf{W}_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0.5 & 0 & 0.5 \\ 0 & 0 & 0 \end{bmatrix}.$$

Note that in W2, a real packet sent by node 2 is divided into two sub packets of virtual size 0.5, which means nodes 1 and 3 are equally likely to be the actual receiver.

4.1.2 End to End Traffic Matrix

Given a sequence of point-to-point traffic matrices, our goal is to derive the end-to-end traffic matrix R = (r (i, j)) nxn , where r (i, j) is the accumulative traffic volume from node i to node j, including both the point-to-point traffic captured directly and multihop traffic deduced from the point-to-point traffic. We use the term accumulative traffic matrix and end-to-end traffic matrix interchangeably.

W2 contains two packets, sent from node 2 to nodes 1 and 3, respectively. Let p2x1 and p2x3 denote these two packets. The current R contains only one packet p1x2 sent from node 1 to node 2. Thus, it is possible that p1x2 and p2x3 are the same packet appearing at different hops. In this case, a new packet p1x3 is derived to represent a multihop flow from node 1 to node 3. Since the volume of a multihop flow consisting of a sequence of one-hop transmissions cannot exceed the volume of any of the transmissions, we have p1x3:vsize = min {p1x2:vsize, p2x3:vsizeg }= 0.5.
We derive the following matrix R for our presented example.

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

It can be seen that, R contains not only all the one-hop packets captured by W1 and W2, but also a derived two hop flow of size 0.5 from node 1 to node 3.

4.2 Traffic Patter Discovery

The traffic matrix R tells us the deduced end-to-end traffic volume between each pair of nodes. However, we still need to perform further investigation to discover the actual source/destination probability distribution and end-to-end link probability distribution, that is, to figure out who are the actual sources and destinations and who are communicating with whom.

4.2.1 Source/Destination Probability Distribution

We denote the actual source and destination probability distribution, respectively, as two vectors S = (s(1), s(2), s(3)…..s(N)) and D = (d (1), d(2), …. d(N)) , where s(i) and d(i) (i =1 to N) represent the probability for node i to be an actual source and destination, respectively.

To derive S and D, we compute two series of vectors which converge to S and D, respectively: the source probability distribution vector series S = (S0, S1, S2……Sn..) and the destination probability distribution vector series D = (D0, D1, D2, …..Dn..).

First, both S0 and D0 should be uniform probability distribution vectors: S0 = D0 = (1/N,1/N,…..1/N) since without any traffic information, all nodes are equally likely to be sources and destinations.

Second, we note that the ith row (r(i,j)….r(i,N)) in the matrix R is a vector of the traffic from node i to every node in the MANET. If we multiply this vector by D0 (inner product), we get

$$s'(i) = \sum_{j=1}^{N} r(i,j) \times d_0(j), \qquad (1)$$

which is the probability for node i to be a source based on the destination probability distribution D0. This is intuitive, since if a node sends a lot of packets to another node with high probability of being a destination, the node itself has a high probability of being a source. According to this, the normalized inner product of R and D0 is a vector of probabilities for nodes to be source nodes. Similarly, using S0 to denote the vector s'(1),s'(2)…..s'(N) resulted from (1) and multiplying the ith row in the transpose of R (i.e., R^T) by S', we will get

$$d_1(i) = \sum_{j=1}^{N} r(j,i) \times s'(j), \qquad (2)$$

which is the probability for node i to be a destination derived from S0 and in turn based on D0. 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. Consequently, the normalized inner product of RT and S0 generates D1 as a new probability vector for nodes to be destinations. Through this procedure, D1 is closer to the actual destination probability distribution than D0.

For the example scenario given in Fig. 1, we initialize D0 to be $(1/3,1/3,1/3)^T$, without any prior knowledge about the actual destinations. Then we compute S' = R x D0 = $(1/2, 1/3, 0)^T$, which can be normalized to S0 = $(3/5,2/5, 0)^T$. S' indicates that node 1 is most likely to be an actual source, while node 3 is definitely not a source.

V. CONCLUSION

- STARS is basically an attacking system, which only needs to capture the raw by passive attack
- From the captured packets, STARS constructs a sequence of point-to-point traffic matrices to derive the end-to-end traffic matrix, with source and destination probability
- STARS demonstrate that the existing MANET systems can achieve very restricted communication anonymity under the attack of STARS

REFERENCES

[1] Yang Qin, Dijiang Huang "STARS: A Statistical Traffic Pattern Discovery System for MANETs" IEEE Trans on Dependable and Secure Computing, VOL. 11, Mar/Apr 2014

[2] Dr S S Tyagi, Arti " Study of MANET: Characteristics, Challenges, Application and Security Attacks" International Journal of Computational Engineering Management, Volume 3, Issue 5, May 2013

[3] 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.

[4] D. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Comm. ACM, vol. 24, no. 2, pp. 84-88, 1981.

ABOUT AUTHOR

Girish Parikh has done BE in Computer Engineering from Shivaji University with Distinction. His areas of interests are Networking, Security Mechanism.

