ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Revealing Packet Encrypted Communication (Anonymized) Details in Mobile Ad Hoc Networks Using Statistical Characteristics of Raw Traffic Data

Y.Padmasri
M.Tech Student
Department of CSE
Avanthi's St.Theressa College of Engineering, Technology & Management, Vijayanagaram, AP.

G.Chinnababu, M.Tech, ACCP
Associate Professor,
Department of CSE
Avanthi's St.Theressa College of Engineering, Technology & Management, Vijayanagaram, AP.

Abstract:

Anonymous Communication is the important issue in case of Mobile ad hoc Networks (MANETs). It is very difficult to find the source and destination of the communication link and the other intermediate nodes involved in it. Many enhancement techniques are proposed to enhance the anonymous communication in case of the mobile ad hoc networks (MANETs). However, MANETs are vulnerable under certain circumstances like passive attacks and traffic analysis attacks. Here we proposed the traffic analysis model; expose some of the methods and attacks that could infer MANETs are still weak under the passive attacks. To show how to discover the communication patterns without decrypting the captured packets, we present the paper Statistical traffic analysis model. In order to discover the packet patterns this model works passively and does the traffic analysis based on the statistical characteristics of the captured raw traffic. Here we can determine the source node, destination node and the end-to-end communication path in case of mobile ad hoc networks. And also accuracy of revealing the hidden traffic is more than other existing systems.

Keywords – MANETs, Anonymous Communication, Statistical Traffic Analysis, Time Slicing.

INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self- configuring infrastructure fewer networks of mobile devices connected without wires. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

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. To achieve anonymous MANET communications, many anonymous routing protocols such as ANODR [1], MASK [2], and OLAR [3] have been proposed. Though a variety of anonymity enhancing techniques like onion routing and mix-net are utilized, these protocols mostly rely on packet encryption to hide sensitive information (e.g., nodes' identities and routing information) from the adversaries. However, passive signal detectors can still eavesdrop on the wireless channels, intercept the transmissions, and then perform traffic analysis attacks.

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 behavior (such as injecting or modifying packets). The predecessor attack and disclosure attacks are two representatives. However, all these previous approaches do not work well to analyses 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.

In past, enhancing techniques of MANETs [4] are based on packet encryption to protect the communication anonymity of the mobile ad hoc networks. In Evidence-based statistical traffic analysis approach provides a practical attacking framework against MANETs but still leaves substantial information about the communication patterns undiscovered. In this approach, the system for discovering a statistical traffic in MANETs is capable of discovering the sources, the destinations, and the end-to-end communication relations.

Finally using the performance evaluation technique comparing collected traffic pattern with actual traffic pattern to calculate the false positive rate and false negative rate based on typical confusion matrix and this procedure calculates the accuracy in disclosing the hidden traffic patterns.

EXISTING SYSTEM:

Evidence-based statistical traffic analysis model, every captured packet is treated as evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. A sequence of point-to-point traffic matrices is created, and then they are used to derive end- to-end (multihop) relations. This approach provides a practical attacking framework against MANETs but still leaves substantial information about the communication patterns undiscovered. MANET systems can achieve very restricted communication anonymity under the attack of STARS.

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 behavior (such as injecting or modifying packets). The predecessor attacks and disclosure attacks are two representatives.

However, all these previous approaches do not work well to analyze 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, which 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.

DISADVANTAGES OF EXISTING SYSTEM:

- Approaches do not work well to analyze MANET traffic.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- The scheme fails to address several important constrains when deriving the end-to-end traffic from the one hop evidences.
- It does not provide a method to identify the actual source and destination nodes (or to calculate the source/destination probability distribution).
- 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.

PROPOSED SYSTEM:

We propose a novel STARS for MANETs. STARS is 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.

In this paper, we propose a novel statistical traffic pattern discovery system (STARS). 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 ofnodes 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; and

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

ADVANTAGES OF PROPOSED SYSTEM:

- The attacker can take advantage of STARS to perform traffic analysis as follows:
- Divide the entire network into multiple regions geographically;
- Deploy sensors along the boundaries of each region
- To monitor the cross-component traffic;
- Treat each region as a super node and use STARS to figure out the sources, destinations, and end-to-end communication relations; and
- Analyze the traffic even when nodes are close to each other by treating the close nodes as a super node.

SYSTEM DESIGN

The system design details and modules of each design are shown in the fig.1 below. And this section also explains the algorithms for each module for statistical traffic analysis model.

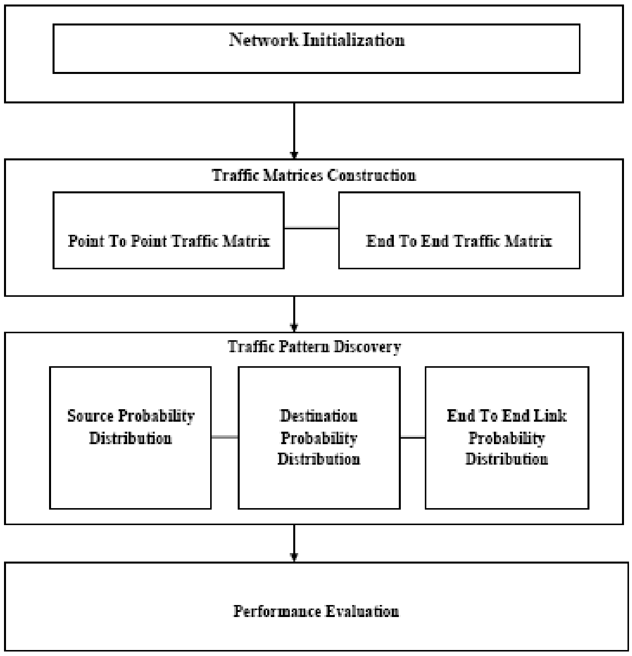

Fig.1 System Design

In Fig.1 shows there are four modules for statistical traffic analysis model for anonymous MANET. They are Network Initialization, Traffic Matrices

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Construction, Traffic pattern discovery system and finally performance evaluation.

1. Network Initialization

Network initialization is the first step in any network system design. In this module wireless network is initialized. In network initialization number of nodes, area of the network, nodes mobility model can be initialized. In network initialization module there are two models one is communication model and other one is adversary model. The assumptions for those models given as the PHY/MAC layer are 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. Padding is applied so that all MAC frames (packets) have the same size. Nobody can trace a packet according to its unique size. 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. No information about the traffic patterns is disclosed from the routing layer and above. Dummy traffic and dummy delay are not used due to the highly restricted resources in MANETs. The attackers' goal is to discover the traffic patterns among mobile nodes. Particularly, we have the following four assumptions for attackers: 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. 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. 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 techniques [5] such as triangulation, nearest sensor, or RF fingerprinting. 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. In the following of this paper, unless specifically denoted as "signal source" or "source of signal," the word "source" indicates the source of a network flow. 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.

2. Traffic Matrices Construction

To disclose the hidden traffic patterns in a MANET communication system, this system includes two major steps. First, it uses the captured traffic to construct a sequence of point to point traffic matrix matrices and then derives the end to end traffic matrix. In traffic matrix construction there are two main steps to follow. One is finding the point to point traffic and other one is to deriving the end to end traffic matrix.

Capturing point to point traffic in certain period T. Using captured traffic; build point to point traffic matrices such that each traffic matrix only contains independent one hop packets. To avoid a single point to point matrix from containing two dependent packets, then apply time slicing technique[6]. Take a snapshot of the network during time interval Δte and each snap shot is triggered by a captured packet. Constructs a traffic matrix which is an N*N one hop traffic relation matrix. A length of each time interval Δte is determined by two criteria: one is, a node can be either sender or receiver within this time interval. But it cannot be both. And the second one is each traffic matrix must correctly represent the one-hop transmissions during the corresponding time interval and avoiding same packets from different nodes. Using point to point traffic matrix, find end to end matrix.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The point to point traffic captured directly and multi hop traffic deduced from the point-to-point traffic. We can implement the point to point traffic using algorithm1 using captured traffic in the network.

Algorithm 1. —$f(\mathbf{W}|_{1\times K})$.

$\mathbf{R} = \mathbf{W}_1$
for $e = 1$ to $K - 1$ **do**
  $\mathbf{R} = g(\mathbf{R}, \mathbf{W}_{e+1}) + \mathbf{W}_{e+1}$
end for
return $\mathbf{R}$

Algorithm1 Finding Point to Point Matrix

After finding the point to point traffic we have to derive end to end traffic using the point to point traffic matrix technique. The algorithm for end to end traffic matrix is shown in Algorithm2 above.

Algorithm 2. —$g(\mathbf{R}, \mathbf{W}_{e+1})$.

$\mathbf{R}' = \mathbf{R}$
for $i = 1$ to N **do**
  for $k = 1$ to N and $k \neq i$ **do**
    for $j = 1$ to N **do**
      for each $x \in w_{e+1}(j,k).pkt$ **do**
        if $\exists\, y \in r(i,j).pkt$ s.t. $x.time - y.time < \mathcal{T}$ and $y.hop < \mathcal{H}$ **then**
          create z with $z.time = x.time$
            $z.hop = y.hop + 1$
            $z.vsize = \min\{x.vsize, y.vsize\}$
          $r'(i,k).pkt = r'(i,k).pkt \cup \{z\}$
          $r'(i,k) = r'(i,k) + z.vsize$
        end if
      end for
    end for
  end for
end for
return $\mathbf{R}'$

Algorithm 2 Finding End to End Traffic Matrix

3. Traffic Pattern Discovery

The traffic matrix R defines the deduced end-to-end traffic volume between each pair of mobile nodes. Even though we still need to perform more 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. In traffic pattern discovery system there are three sub modules to discover the traffic, they are source probability distribution, destination probability distribution and end to end link probability distributions. Each sub modules are explained as follows: After finding the traffic matrices using these matrices we have to find the source and destination probability distributions which contain several functions. All nodes within the transmitting range of a packet have the same probability to be the actual sender and receiver. Using vector space similarity assessment two nodes with higher probability to be neighbors have less impact on each other's source/destination probability distribution, which reasonably reduces the neighborhood noise. Finding the actual source using source probability distribution. Also, finding the actual destination using destination probability distribution.

The source probability distribution algorithm is shown below:

Algorithm 3. —$Src(\mathbf{R})$.

$\mathbf{S_0} = (1/N, 1/N, \ldots, 1/N)$
$n = 0$
do
  $\mathbf{S_{n+1}} = (\mathbf{\Phi}(\mathbf{R}) \cdot \mathbf{\Phi}^{\mathbf{T}}(\mathbf{R})) \cdot \mathbf{S_n}$
  normalize $\mathbf{S_{n+1}}$
  $n = n + 1$
while $\mathbf{S_n} \neq \mathbf{S_{n-1}}$
$\mathbf{S} = \mathbf{S_n}$
return $\mathbf{S}$

Algorithm 3 Finding Source Probability Distribution

Both vectors which is shown in the algorithm they are uniform probability distribution vectors. Similar approach can be applied for to find the destination probability distributions which are shown in the algorithm4 below. In this all probability distribution vectors are normalized and only the relative orders among the elements of each vector actually make sense. The actual destination can be obtained by using the algorithm4 which is shown below:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Algorithm 4. —*Dest*(R).

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

Algorithm 4 Finding Destination probability distributions

The final part of the traffic pattern discovery system is to find the end to end link between the every node in the network. The procedure and algorithm for finding the end to end link probability or end to end link between the pair of nodes is shown below: In the symmetrical way we have to apply the algorithm 5 to find the end to end link between the nodes of destination to source.

Suppress-Sender(i)
$W'|_{1\times K} = W|_{1\times K}$
for $p = 1$ to K
  for $q = 1$ to N
    $w'_p(i, q) = 0$
return $W'|_{1\times K}$

Suppress-Receiver(j)
$W'|_{1\times K} = W|_{1\times K}$
for $p = 1$ to K
  for $q = 1$ to N
    $w'_p(q, j) = 0$
return $W'|_{1\times K}$

Algorithm 5. Given a source node i, compute the probability distribution vector $L_{s-d}(i)$ for each node to be the intended destination of i.

1: $R = f(W|_{1\times K})$;
2: $D = Dest(R)$;
3: $W'|_{1\times K} =$ Suppress-Sender(i);
4: $R' = f(W'|_{1\times K})$;
5: $D^- = Dest(R')$;
6: Calculate the probability reduction vector as: $L'_{s-d}(i) = D - D^-$. If negative elements exist in $L'_{s-d}(i)$, increase each element by the absolute value of the smallest negative element;
7: Normalize $L'_{s-d}(i)$ to generate the probability vector $L_{s-d}(i)$ for each node to be the intended destination of i;
8: Return $L_{s-d}(i)$.

Algorithm 5 Finding end to end link between the sources to destination

CONCLUSION

In this traffic analysis model we can reveal the hidden traffic patterns of anonymous MANETs without decrypting the packets. The hidden traffic patterns can be revealed in good accuracy using the statistical traffic pattern analysis model, even without the number of actual sources, destinations and end to end communication relations known to the traffic analyzers. Also comparisons graphs of performance evaluation section and comparisons section proves that our proposed statistical traffic analysis model shows better accuracy for pattern detection in anonymous MANETs.

Finally the proposed traffic analysis model is detects the 80% of statistical traffic patterns of anonymous mobile ad hoc networks.

REFERENCES

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

[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]. 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.

[4]. D. Huang, “Unlinkability Measure for IEEE 802.11 Based MANETs,” IEEE Trans. Wireless Comm., vol. 7, no. 3, pp. 1025- 1034, Mar. 2008.

[5]. T. He, H. Wong, and K. Lee, “Traffic Analysis in Anonymous MANETs,” Proc. Military Comm. Conf. (MILCOM ’08), pp. 1-7, 2008.

[6]. Yang Qin, Dijiang Huang, "STARS: A Statistical Traffic Pattern Discovery System For Anonymous MANETs" IEEE Transactions On Dependable and Secure Computing, vol. 11, No. 2, March/April 2014

[7]. 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.

[8]. G. Danezis, "Statistical Disclosure Attacks: Traffic Confirmation in Open Environments," Proc. Security and Privacy in the Age of Uncertainty (SEC '03), vol. 122, pp. 421-426, 2003.

[9]. G. Danezis and A. Serjantov, "Statistical Disclosure or Intersection Attacks on Anonymity Systems," Proc. Sixth Information Hiding Workshop (IH '04), pp. 293-308, 2004.

[10]. G. Danezis, C. Diaz, and C. Troncoso, "Two-Sided Statistical Disclosure Attack," Proc. Seventh Int'l Conf. Privacy Enhancing Technologies, pp. 30-44, 2007.

[11]. 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.

[12]. 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.

[13]. 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 Workshops '06), pp. 133-137, 2006.

[14]. R. Shokri, M. Yabandeh, and N. Yazdani, "Anonymous Routing in MANET Using Random Identifiers," Proc. Sixth Int'l Conf. Networking (ICN '07), p. 2, 2007.

[15]. 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 '05), pp. 33-42, 2005.

[16]. 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.