Statistical Rigorous Traffic Pattern Protection Process against Hacking in MANETS

J. Jeya Pratha, I. Muthumani
Department of Electronics and Communication Engineering, ACCET, Karaikudi, Tamil Nadu, India

Article Info
Article history:
Received 5 February 2015
Received in revised form
20 February 2015
Accepted 28 February 2015
Available online 6 March 2015

Keywords
Ad hoc,
On Demand Distance Vector Protocol,
Packet Delivery Ratio,
MAC protocol,
MANETs,
UDP,
Constant Bit Rate,
Rigorous Algorithm

Abstract
The advance division of wireless networks in mobile ad hoc network, which is a network without infrastructure and it is formed without any central administration consisting of mobile nodes. Ad hoc networks are defined as peer=to-peeer networks between wireless computers that do not have an access point to communicate. While these types of networks, usually has some little protection by encryption methods to guide the network path. Hackers can find the particular wireless network to corrupt or collecting the data to collapse the data delivery. By utilizing the MAC protocol, the appropriate shortest path is determined through traffic matrix pattern formation. Through the virtual carrier sensing disable option of MAC layer, the network communication is protected from hackers.

1. Introduction

Mobile ad hoc is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless channel [10]. When the nodes of a topology are in moving condition, the topology may change randomly and incalculably at any time [1]. The network is decentralized and all the network behaviors like recognizing the topology and propagation of messages must be executed by the nodes themselves . Ad-hoc networks having the function of self-organization and self-re-construction of multi hop wireless networks. These network nodes perform by the same random access wireless link, forwarding the data in multi hop function.

Ad hoc networks rely on wireless transmission, the protected message transmission is important to secure the privacy of the data. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies [3], [4]. Disclosure hacking [6] is an attacking system that can collect the overall information and analyze the performance, which is done by without changing the network behavior.

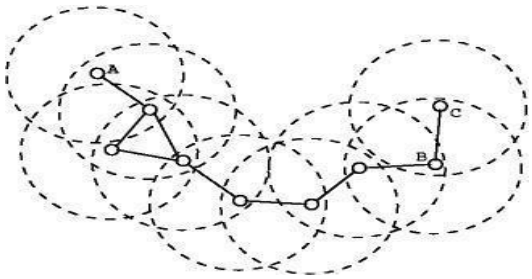


Fig: 1. When destinations receive the RREQ, it will generate RREP and it will send to the source through same path. Finally we establish the route for data traffic.

Corresponding Author,
E-mail address: jeyaprathajeganathan@gmail.com

The first stage of disclosure hacker [8] is to find the source node. From this it can forms a source node table, by analyzing the information. Second it can identify the destination and path.

In this disclosure hack, the attacker only performs some kind of monitoring on particular paths to collect information about the traffic without injecting any fake information. It serves the intruder [7] to gain information an d makes the footprint of the invaded network in order to apply the hacking process successfully

2. Related Work

In existing 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. Many appropriate routing protocols, such as ANODR, MA SK [2] and OLAR [9] were proposed to achieve anonymous MANET communication. For this, a variety of anonymity protecting techniques like onion routing [6] and mix-net [4] are utilized, these protocols mainly has an purpose of packet encryption to hide sensitive information from the attackers. Recently, statistical rigorous traffic analysis attacks have attracted broad interests due to their passive characteristics. Under the passive attacks, the predecessor attacks and disclosure attacks are the two representatives.

An evidence-based traffic analysis model specially enhanced to attack the data transmission. In this analysis every captured packet is treated as an evidence for the point-to-point transmission between the sender and the receiver [7]. It is a practical attacking framework against MANETs but still leaves substantial information about the communication patterns undiscovered. First, the scheme [1] fails to address several important constrains (e.g., maximum hop-count of a packet) when deriving the end -to-end traffic for m the captured packets. It does not provide a method to identify the actual source and destination nodes (or to calculate the source/destination probability

distribution).

The brute force attack proposed in tries to track a message by enumerating all possible links to traverse a message. In node flushing attack [8], the attacker sends a large quantity of messages to the targeted anonymous system (which is called a mix-net). The message tagging attacks require attackers to occupy at least one node that works as a router in the data path. In this way, they can tag some of the forwarded messages to analyze the network. The watermarking attacks are actually different for m the message tagging attacks; in this they reveal the final end -to-end possible relations by purposely introducing delay to selected packets. Timing -based method was proposed by The et al. In this, they estimate the flow rates of communication paths using packet matching by the assumption of transmission delay.

3. Proposed Methodology

Proposed method involves two major steps to achieve our goals.

1. Build point to point traffic matrices using the time slicing technique.
2. Derive end to end traffic matrices with a set of traffic filtering rules and a heuristic approach to identify actual source and destination modes.

Here all the MAC frames [3], [4] are encrypted so that the adversaries cannot decrypt them to look into the contents. For this padding technique is employed to all MAC frames have same size. Here MAC is set to broadcasting the address.

A. Protection Process

Statistical Traffic pattern Analysis in Rigorous is the technique; it will create source/destination probability distribution for each and every node to be a message source and destination and the end -to-end lin k probability distribution (the probability for each node to be an end -to-end communication pair).

In this module [8], first it uses the captured traffic to construct a sequence of point-to-point traffic matrices. Second, it derives the end-to-end traffic matrix, and then it analyzes the end -to-end traffic matrix. Third, it derives the source/destination probability distribution and that for each pair of node to be an end-to-end communication link. Finally actual source and the destination rigorously identified by traffic matrix pattern. This MAC protocol used to identify the actual path based on energy of each node in the possibilities of every path.

B. MAC Protocol

By the identification actual source and the destination, there is no possibility to inject or mod ify the data through the attackers. Other than attackers, hackers only track the message overview without c hanging the network characteristics [5]. To avoid data hacking, MAC protocol used to disable the virtual carrier sensing option on the MAC layer. At last the flow of data depends on the MAC protocol routing table which is having the next hop information.

C. MAC Characteristics

1. The PHY/MAC layer [2] is controlled by the commonly used 802.11(a/b/g) protocol. But all MAC frames (packets) are encrypted so that the hackers cannot decrypt and read them to look into the contents.
2. Padding is applied so that all MAC packets have the same size So that any hacker cannot trace a packet according to its unique size.
3. The "virtual carrier sensing" of each node in path option is disabled (off). The source address, destination address in MAC and IP headers are set to a broadcasting address (all "1"). By this way, the intruders are prohibited from identifying point-to point communication relations.

4. Algorithm Steps

To start a new simulator we write
Set ns [new Simulator]

A. Creating the Output Files

1. #to create the trace files we write
2. set tracefile1 [open out.tr w]
3. $ns trace-all $tracefile1
4. #to create the nam files we write
5. set namfile1 [open out.nam w]
6. $ns namtrace-all $namfile

In ns we end the program by calling the 'finish' procedure

1. #end the program
2. $ns at 50.0 "finish"

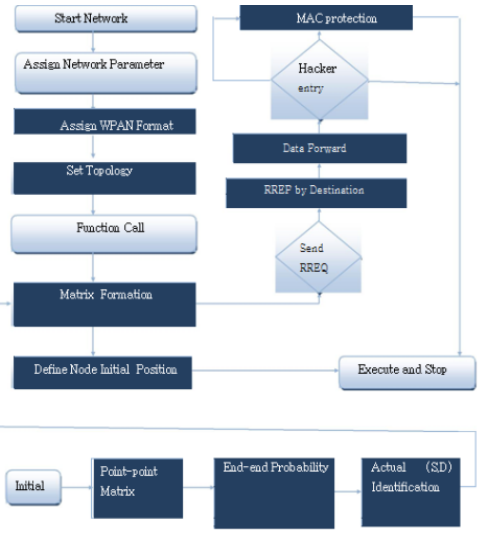
Thus the entire approach ends at 50 seconds

B. Agents and Applications

UDP

UDP [8] provides an unreliable service and the datagrams may appear duplicated or escape without notice. It assumes that error checking and correction is either not necessary or performed in the application. The field size limit for the UDP datagrams is 65,535 bytes(8 byte header + 65,527bytes of data).

C. Workflow



Constant Bit Rate (CBR)

Constant Bit Rate (CBR) is a term used in telecommunications, which define the quality of service. CBR is useful for streaming mu ltimedia content on limited capacity links since it is the maximum it rate that matters, not the average, so CBR [23] has the advantage of all of the capacity. CBR would not be the appropriate choice for storage as it does not allocate enough data for complex sections while wasting data on simple sections.

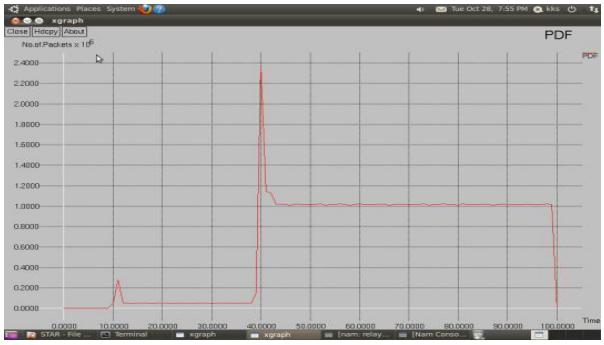
D. Traffic Matrix Formation

```
Set nk 1.8
For {set nd 0} {$nd<21} {incr nd} {If {$nd! = 20} {
Set M k [expr $nd+$kl] Set nk [expr $nk+0.5]
$ns_ at 2 "$node_ ($nd) setdest [lindex $lst $Mk] [lindex
$lst [expr $Mk+1]] 40"
Incr kl
    }
```

Table: 1.

Parameter	Value
number of nodes	21
topography dimension	1000 x 1000
Traffic type	cbr
radio propagation	two-ray ground
model	model
mac type	802.11_mac layer
mobility model	random way point
antenna type	omni directional
transmission range	250m
bandwidth	20 mhz
transmission speed	1.2 mbps
max package	50
queuing policy	fifo
packet size	512 bytes
constant bit rate	0.01

E. Graphical Repres Entation



5. Conclusion

This is basically a harmful system, which only needs to capture the selective traffic from the PHY/MA C layer without looking into the contents of the encrypted packets. From the captured packets, it constructs a sequence of point-to-point traffic matrices to derive the end-to-end traffic matrix and also MAC protocol used to expose the hidden traffic patterns from the end to end probability distribution. From this, the shortest path is obtained. At the time of hacker enters, virtual carrier sensing disabled option used for data forwarding. It is done by the proceeding function of matrix formation. Through the MAC layer protection, disclosure hacking can be prohibited. By using AODV protocol, the disadvantage of delay can be used as efficient property to analyze. This AODV [2], [3], [4], [5] gives better performance for energy conservation than the MAC protocol

6. Acknowledgement

I like to express heart full thanks to Prof. I. Muthumani. Head Of the Department, Department of ECE, to spend her valuable time to do this project and also I want to thank to my college and my friends for their support.

References

[1] R. Akbani, T. Korkmaz, G. V. S. Raju, Mobile Ad hoc Network Security, Lecture Notes in Electrical Engineering, New York: Springer-Verlag, 127, 2012, 659–666

[2] Y. Zhang, W. Liu, W. Lou, Y. Fang, MASK: Anonymous On - Demand Routing in Mobile Ad Hoc Net works, IEEE Trans. Wireless Comm., 5(9), 2006, 2376 -2385

[3] Y. Qin, D. Huang, OLAR: On -Demand Lightweight Anonymous Routing in MANET s, Proc. Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking (ICMU '08), 2008, 72-79

[4] M. Blaze, J. Ioannidis, A. Kero mytis, T. Malkin, A. Rubin, WAR: Wireless Anonymous Routing, Proc. Int'l Conf. Security Protocols, 2005, 218-232

[5] A. Boukerche, K. El-Khatib, L. Xu, L. Korba, SDA R: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks, Proc. IEEE 29th Ann. Int'l Conf. Local Co mputer Net works (LCN '04), 2004, 618 -624

[6] Kuldeep Sharma, Neha Khandelwal, Prabhakar. M. An Overview Of security Problems in MANET

[7] Wenjia Li, A. Joshi, Security Issues in Mobile Ad Hoc Networks - A Survey

[8] Yih Chun, Hu, Adrian Perrig, Dav id B. Johnson, Rushing Attacks and Defense in Wireless Ad -Hoc Network Routing Protocols, WiSe 2003, San Diego, California, USA, 2003