STATISTICAL DISCLOSURE OF TRAFFIC ON ANONYMOUS SYSTEM USING MANETs

Vandana Kumari[1] , S. Raj Anand[2], Suganya.V[3]

[1,3] PG. Scholar, Department of MCA, VelTech HighTech Engineering college
[2] Department of MCA, VelTech HighTech Engineering college

Abstract

Mobile communication with safety encryption is a needed affair and plays the vital role. To protect the communication anonymity of mobile ad hoc networks (MANETs) the different anonymity techniques have been proposed based on packet encryption. The paper shows that under passive statistical traffic attack, MANETs are vulnerable. To demonstrate the communication patterns , a novel statistical disclosure of traffic on anonymous system using MANETs (STAM) is presented and it performs traffic analysis which works to find the capacity of the nearest node from the sender. The proposed system will be able to find the source, the destination and the end to end relationship without traffic and it condense time also .To overcome the existing attacks such as forerunner attack and revelation attack, the proposed work uses Brute Force attack and Node Flushing attack. The results show that STAM achieves better accuracy to disclose the hidden traffic pattern.

KEYWORDS

Anonymity, MANET, STAM

1.Introduction

Mobile ad hoc network (MANETs) are a kind of wireless ad hoc network that usually has a routable networking environments on top of a link layer ad hoc network. MANET consist of a per-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. The device of the MANET has the power to move independently in any direction[6], and can change its links to other devices frequently. The design of MANET was originally for military environments. The communication using MANET includes the source/destination and end-to-end relationship.

In an adverse environment, to provide security and privacy for data communication, a number of protocols have been compromised by the attackers. In this paper, to ensure security and privacy, the concept of anonymity and pseudonymity has been introduced. The SOT (Secure Onion Throat) protocol [1] is proposed based on the combination of group signature and onion routing with ID-based encryption for route discovery.

The MANET exists in two types[5]: open and closed. All nodes in closed MANETs work for a common goal and can be controlled easily but open MANETs have different goals. Both types of MANETs have two main problems namely fixed infrastructure support and the frequent changes in network topology [7] [8].

The nature of MANETs is dynamic[14] which have a wireless radio medium with limited resources. The source node, destination node, and their relationship are very hard to observe. In

DOI: 10.5121/ijcacs.2016.1103

this paper, the traffic analysis, the attacks, and how could they infer is been described [2]. A STAR (Statistical Traffic Pattern Discovery System) detects all source, destination and then finds out their communication relationship.

In MANETs, different anonymous routing protocols have been proposed and one such protocol is TIA (Traffic Interference Algorithm) to enable passive global adversary to accurately infer the traffic pattern in anonymous MANET [3]. The result of the TIA infer traffic pattern with 95% accuracy. The two sided statistical disclosure attack [4] is a traffic analysis attack which tries to uncover the receivers of messages sent through an anonymizing network supporting anonymous replies. In this paper, simulation evaluate that the new attack is superior to previous attacks when replies are routed in the system.

2. Related Work

To discuss the anonymous traffic pattern proposed for MANETs is the major focus. To provide unlinkability and anonymity for routing in MANET, Kong and Hong propose an Anonymous On-Demand Routing (ANODR)[10] protocol. The unobservability is failed but uses one time public/private key pairs to achieve anonymity and unlinkability in ANODR. The many anonymous MANET routing protocols like [10-13] [15] are adaptations of on demand routing protocols such as AODV or DSR where routes are discovered. The performance of routing changes significantly when different cryptosystems are used to implement the same function is the add on advantage for ANODR is seen in efficient anonymous routing for MANET by Kong et al. A small set[9][16] of special nodes data packets from different end-to-end connections by reordering and re encrypting the packets such that incoming and outgoing data packets cannot be related.

3. Overall Architecture

The figure 3.1 shows the architecture in which message is sent from the physical server such as mobile. That message is broken into several small data packets and managed by the resource controller. The resource controller manages all the data according to the size of the tower. For instance, if the capacity of the tower is 100 GB and the size of the message is 200 GB then the 200 GB message will be divided in 100 GB and that 100 GB will be sent to the tower. The sending and receiving of message is done vice versa. The network provider scans all the messages and verifies their performance. When it is done, the data packets are sent to the physical server(tower) and this process is repeated till the messages are received by the receiver(destination).

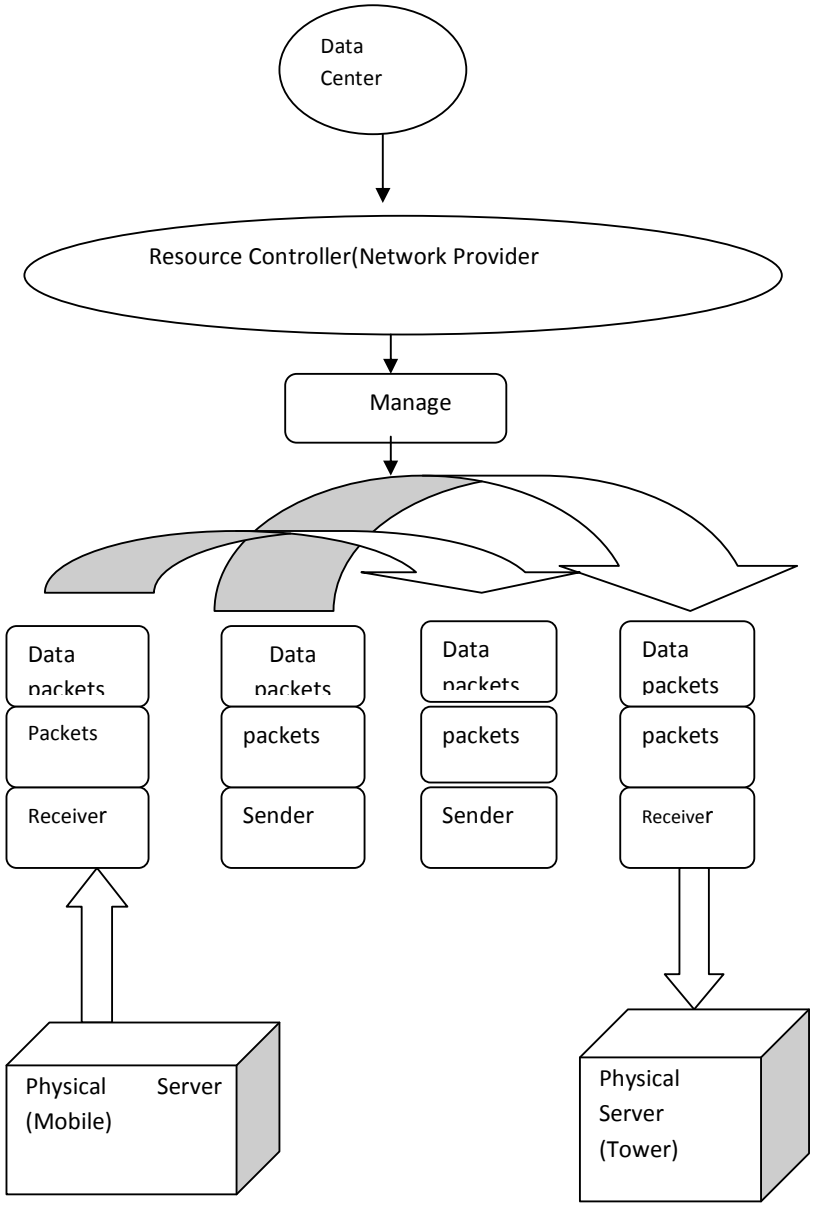

Figure 3.1 Architecture of Message Sending from Source to Destination

4. Earlier Approach Of Traffic On Anonymous System

From the past few years, traffic analysis models have been widely investigated for static wired networks. The simplest approach is the brute force in which a message is traced by enumerating all doable links in which a message may traverse. But these attacks did not work properly. Previously, attackers collect information and analysis is performed quietly while not changing the behavior of the network flow. The forerunner attack and the revelation attack are the two representatives. To overcome this, the new numerous techniques have been employed in this paper. The two problems which incurred in the existing paper such as offered mobile computing

services in a very commercially viable manner, however terribly difficult as on lives money issue. The next main challenge of MANET is to find the best tradeoff between two contradicting objectives: reducing the packet drop and increasing response over the service and also satisfactory computing demands for high end network technique, which may incur huge financial burden.

5. Proposed Approach Of Traffic On Anonymous System

In the planned system, traffic is analyzed against the static wired networks. The brute force attack planned, tries to trace a message by enumerating all attainable links which a message may traverse. In node flushing attacks, the arrangement of sending oversized message to the anonymous system is overcome in every communication path. If the wrong doer will track the latency of every path, it will correlate the messages coming back in and out of the system by analyzing their transmission latencies. The figure 5.1 shows the communication of the mobile server receives the data packets without any drop. The message tagging attacks need attackers to occupy at least one node that works as a router within the communication path so they will tag a number of the forwarded messages for traffic analysis. By recognizing the tags in latter transmission hops, attackers will track the traffic flow. The water marking attacks are literally variants of the message tagging attacks. They reveal the end to end communication relation too.

The Brute Force attack and the Node Flushing attacks are the attack which are used to find the hidden traffic from the source to the destination. The general problem can be solved by tracking all the attainable links with which the data can be transferred without any loss and it checks the problem at every stage that is at all the nodes.

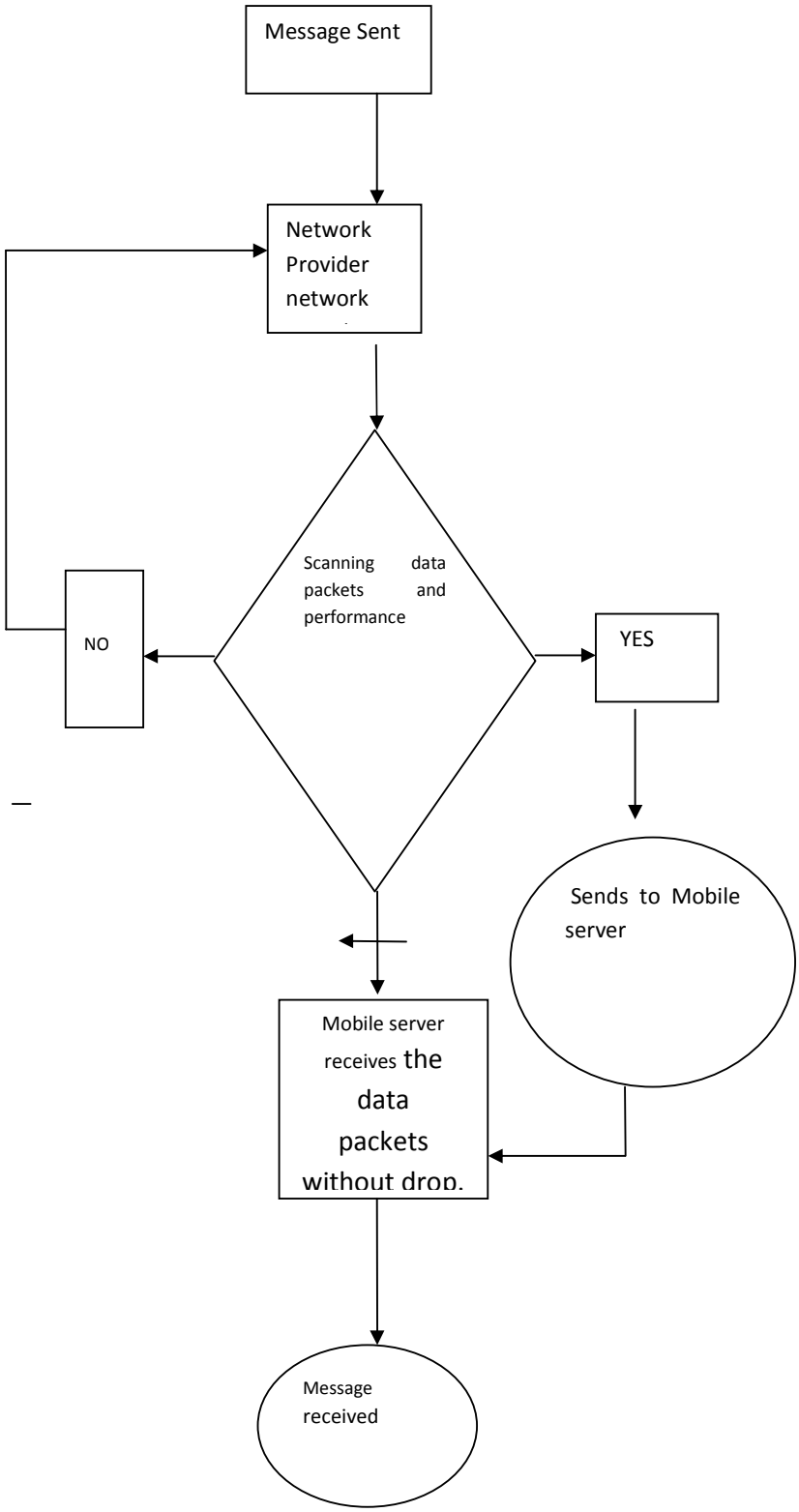

Figure 5.1 Performance of Packet Transmission in Mobile Server

6. Methodology Of Stam

Step1: The data is sent from the source.
Step2: The data is passed through the network provider which verifies the sent data.
Step3: The data is divided into several small packets according to thesize of the nearest node.
Step4: The small packets of data are scanned
and their performance is checked.
Step5: If the size of the packet match the size of the node, it will be sent to the node.
Step6: If the size of the packet do not match the size of the node, it will be again sent to the network provider for verifying.
Step7: The matched packet of data is sent to the mobile.
Step8: The mobile server receives the data without any drop.
Step9: The data is sent to the destination.

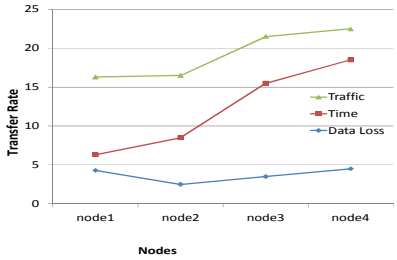

Figure6.1: Comparison of STAM with Earlier Approach

The figure 6.1 shows that the earlier work of paper when compared with the transfer rate and the nodes through which the data passes tells that data is transferred from one node to another node in long time, there is lot of traffic from one node to another node and there is also some loss of data. The data is transferred by attaining all doable links through which the data may traverse. The node1 is the source from which the data is sent and the node4 is the destination. The graph denotes that the traffic is high when the data reaches destination and due to this time is increased. The rate of transfer of data is low as some drop in the data may occur.

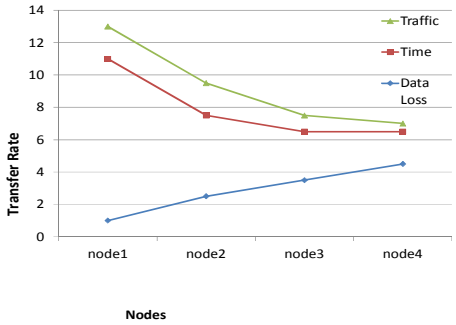

Fig6.2: Proposed Approach of STAM in Present Scenarios

The figure 6.2shows that the present scenario of STAM which overcomes the existing problem by attaining all the attainable links to transfer the data from one node to another node. The node1 represents the source and the node 4 as destination. In this there is no loss of data , the time is also condensed to reach to the destination and the traffic is less compared to earlier work. This is

because of Brute Force attack with which the data is transferred with low traffic and reduced time and the drop of data is also reduced.

7.Brute Force and Node Flushing Attacks

The systematic, exhaustive testing of all possible methods that can be used to break a security system. Brute-force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when he/she has cracked the code. Brute-force attacks are an application of brute force search, to complicate the adversary process dummy messages are sent and to overcome those attacks brute force and node flushing attacks are used in this paper.

8.Conclusion

In this paper, the main challenge is been overcome for mobile computing suppliers to search out the most effective trade-off between two contradicting objectives: reducing the traffic redundancy and increasing packet information transfer rate without break. The performance of knowledge transfer has been overcome. The time efficiency is condensed and the packet of data is transferred without any drop and the hidden traffic has been achieved with good accuracy.

References

[1] M.Gunasekharan, K.Premalatha "An anonymity based secure on demand routing for mobile ad hoc networks," International scholarity and Scientific Research & Innovation, Vol8, pp 94-95, 2014.
[2] T.Parameswaran, Dr. C.Plalanisamy, M.Karthigadevi, "University regional center Coimbatore", Vol2, pp152 ,2014.
[3] Yunzhong Liu, Rui Zhang, Jing Shi, Yanchao Zhang, Traffic Interference in Anonymous MANETs" New Jersey Institute of Technology, IEEE Communication Society ,Vol1 , pp978, 2010.
[4] K.U.Leuven,"Two-sided statistical disclosure attack", Vol10 pp1-2, 2012, Belgium.
[5] George danezis, " Statistical Disclosure attacks, Traffic confirmation in open environments," University of Cambridge, Computer Laboratory, Vol1 pp 1-2, 2008.
[6] Yang Qin, dijiang Huang, " STARS: A statistical traffic pattern discovery system for MANETs", Senior Member IEEE, Vol1, pp 1-2, 2014.
[7] S.Buruhanudeen, M.Othman and B.M.Ali, " Existing MANET routing protocols and metrics used towards the efficiency and reliability-an overview," IEEE International conference on telecommunication, Vol1 pp,231-232, 2007.
[8] F.Maan, "MANET routing protocols Vs Mobility Models performance evaluation," 3rd International conference on ubiquitous and future networks, Dalian, Vol1 pp1, 79-180, 2011.
[9] DARPA, "Research challenges in high confidence networking," White paper, Arlington, VA, Vol1, pp1-2, 1998.
[10] J.Kong and X.Hong, "ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks", in ACM MobiHoc'03. Annapolis, MD, Vol1 pp 1-2, 2003.
[11] B. Zhu, Z. Wan, M. S. Kankanhalli. F, Bao, and R. H. Deng, "Anonymous secure routing in mobile ad-hoc networks," in LCN'04, Vol1, pp102-103, 2004.
[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," in IEEE LCN'04, Vol1, pp618-619, 2004.
[13] R.Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in SASN'05, Vol1, pp 1-2, 2005.
[14] X. Wu and B. Bhargava, "AO2P: Ad hoc on-demand position-based private routing protocol," IEEE Trans. Mobile Computing, Vol1, pp 335, 2005.
[15] Y.Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in IEEE INFOCOM'05, Miami, FL, Vol1, pp 1940, 2005.
[16] S. Jiang, N. H. Vaidya. And W. Zhao, "A mix route algorithm for mix net in wireless mobile and ad hoc networks," in MASS'04, Vol1, pp406, 2004.