Volume 5, Issue 4, April 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Hidden Routing in Mobile Ad Hoc Networks

T. Kiran,
M.E. Student
Department of CSE

T. P. Anish
Assistant Professoor
Department of CSE

St.Peter's college of engineering and technology,
Chennai, India

Abstract*— Number of techniques has been used based on packet encryption to protect the data forwarding in MANETs, Still MANETs are attacked by hackers. To get over these attack a new technique called statistical traffic pattern discovery system can be used. It is an approach to discover entire raw traffic by using probability of traffic characteristics. It discover the relationships of source to destination communication. Maximum in wireless ad hoc network, it will always choose shortest path in prior. So attackers shall enter the network freely, because if the node monitors the packet forwarding mechanism it can easily identify the entire traffic pattern in the system. Based on the activity of hacker will enter the network effectively. It can be helpful for dropping or modifying data. But here we choose the second shortest path for data forwarding. In our scenario when we change to select the routing path hackers can't be capture the current routing path.

Keywords*—Traffic Analysis, Traffic Pattern, Routing, Hacker, MANET's

I. INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes, i.e., routing functionality will be incorporated into mobile nodes.

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where

Network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies.

Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources.

In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it.

There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might

(i) misuse routing information to other nodes or
(ii) act on applicative data in order to induce service failures.

The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today. Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into internal attacks and external attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques.

II. RELATED WORK

A. Traffic Analysis

Traffic analysis is a special type of inference attack technique that looks at communication patterns between entities in a system. "Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security. Knowing who's talking to whom, when, and for how long, can sometimes clue an attacker in to information of which you'd rather it's not be aware. The size of packets being exchanged between two hosts can also be valuable information for an attacker, even if they aren't able to view the contents of the traffic (being encrypted or otherwise unavailable). Seeing a short flurry of single byte payload packets with consistent pauses between each packet might indicate an interactive session between two hosts, where each packet indicates a single keystroke. Large packets sustained over time tend to indicate file transfers between hosts, also indicating which host is sending and which host is receiving the file.

Attackers would commonly use traffic analysis in addition to some other method of attack, it is most useful for reconnaissance, to find vulnerable hosts for instance, or potentially in competitive intelligence to determine characteristics of someone else's system. However, in the case of insiders or authorized users you have the "inference problem, wherein authorized users are able to make valid deductions, based only on data they are authorized to access, about data they are not authorized to access.

Fortunately, traffic analysis can also be used as a defensive technique by identifying anomalies in traffic patterns.

B. Manets Vulnerabilities

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 centralized monitor server. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network.

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

1. Dynamic topology

Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

2. Resource availability

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

3. Scalability

Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

III. PROPOSED SYSTEM

The proposed method involves two major steps to achieve our goals. Build point to point traffic matrices using the time slicing technique; derive end to end traffic matrices with a set of traffic filtering rules and a heuristic approach to identify actual source and destination nodes. The system provides the enhance secure routing mechanism, source always select a path which has least hop count. Here source will select multipath routing. It will periodically change the path and also check the condition whether it is optimal or not. So disclosure nodes can't monitor the same path continuously. But the path is chosen based on optimal length and optimal cost. So improve both security and QOS without more complexes.

Advantages:

- Hidden traffic pattern can be discovered.
- Identify all source and destination and find their relationship.
- Fewer Complexes to find optimum route.
- Less delay and high secured.
- Dummy traffic and delay are restricted.
- Traffic delay reduced.

Modules:

1) Data Communication
2) Attacker Model
3) Star
4) AOMDV
5) Optimum Route Selection

Data Communication

Initially, we are placing nodes in the network and we choose a source and destination. If the source has no route to the destination, then source A initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node. If a closer neighbor node is available, the RREQ packet is forwarded to that node. If no closer neighbor node is the RREQ packet is flooded to all neighbor node. When destinations receive the RREQ, it will generate RREP and it will send the same path. Finally we establish the route for data traffic.

Attacker model

To monitor all the possible traffic patterns in the whole network here included an attacker node. This attack is known as disclosure attack. Disclosure attack is a special kind of attack, it won't change the network infrastructure instead of that it collects all the information about a network. Attackers only need to collect information and perform analysis quietly without changing the network behavior (such as injecting or modifying packets).

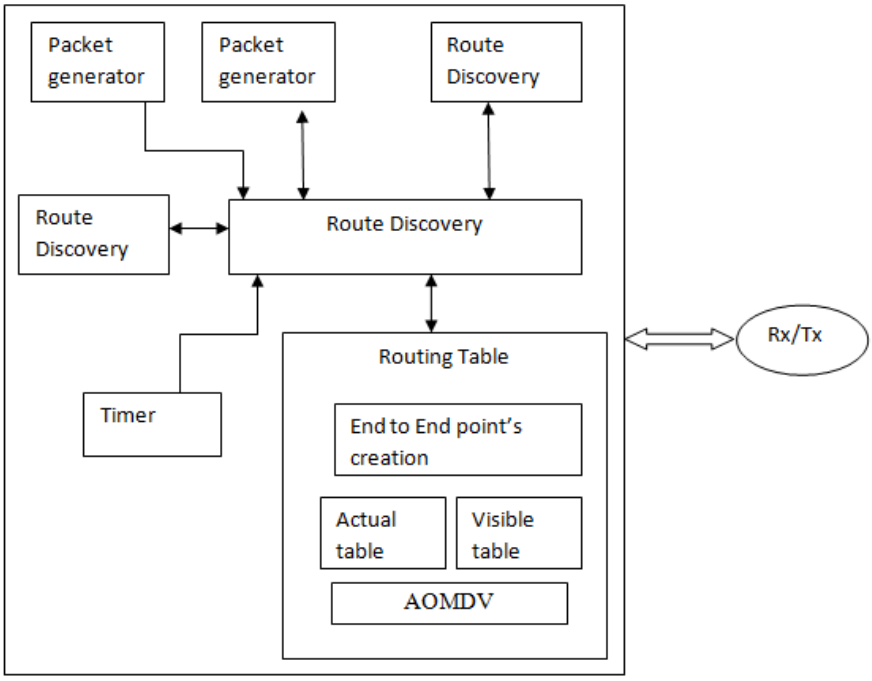


Fig : System Architecture

Star

Star is the technique called statistical traffic pattern discovery system, it will create source/destination probability distribution for each and every node to be a message source and destination and the end-to-end link probability distribution (the probability for each node to be an end-to-end communication pair).

AOMDV

The Ad hoc On Demand Multipath Distance Vector (AOMDV) routing algorithm is a routing protocol designed for ad hoc mobile networks. It is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. In each route discovery, find multiple routes between source and destination. AOMDV uses alternate routes on a route failure.

Optimum Route Selection

In this module AOMDV always select multipath route for data forwarding. Source generally selects a path which at least counts. For enhance secure, we propose multipath data forwarding depends on optimum route length and optimum route cost. Periodically route changes occur and also check whether route is optimum or not. Hence, QOS and security is maintained.

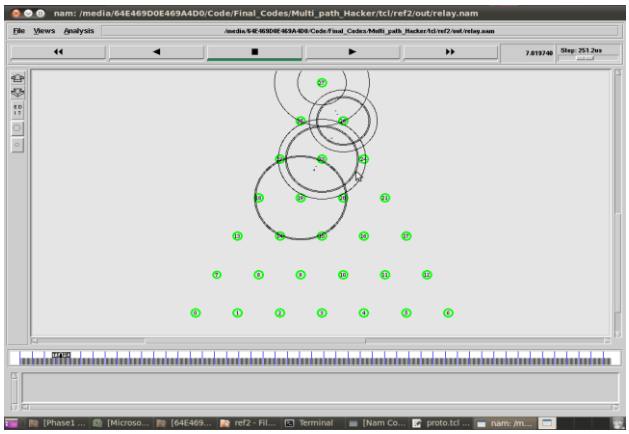
IV. SYSTEM IMPLEMENTATION

The concept of implementation deals with to change hides Traffic Hidden Network from disclosure attacks. Avoiding this node, we use a new hidden scheme done by following methodologies, every node in the network act as message source and message destination. Based on this technique easily hide the traffic from disclosure nodes. After that we are going to change the protocol. The AOMDV (Ad Hoc On Demand Multipath Distance Vector)it finds multiple routes in entire raw traffic, and then it will always choose shortest path in prior. So attackers shall enter the network freely, because if the node monitor the current traffic pattern of a network. It can be helpful for dropping or modifying data. But here we choose the second shortest path for data forwarding. By choosing this second shortest path we can avoid hackers when we change the routing path.

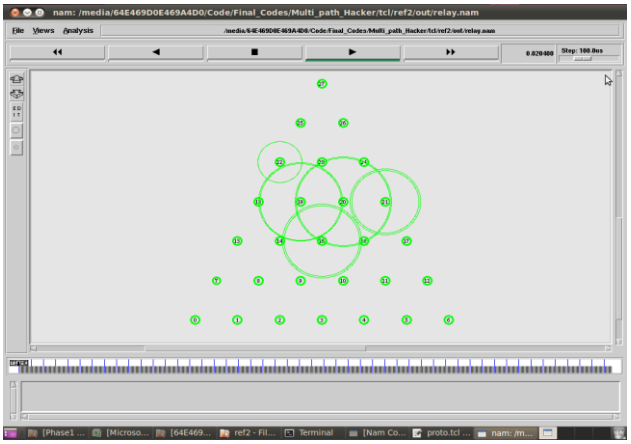
V. CONCLUSION

In this paper the secure hidden traffic is implemented through disclosure attack, i.e. it collects all the information about the traffic pattern without changing the network behavior. A hidden scheme is used to avoid the hacker by the changing the route.

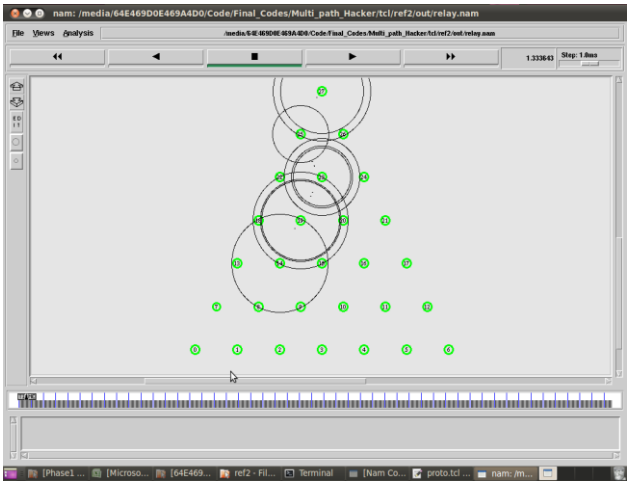
A. Data flow:



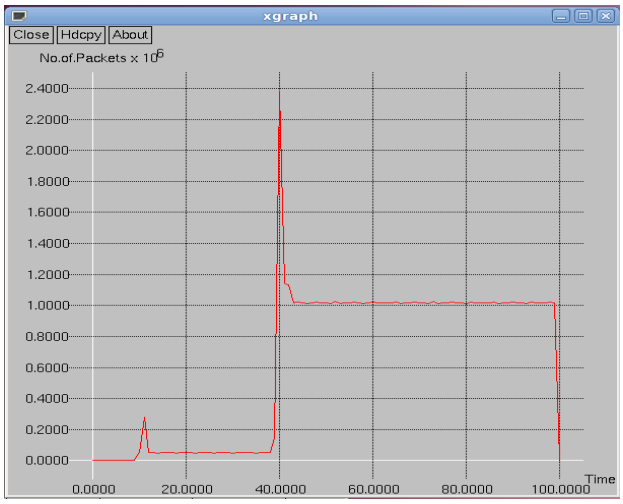
B. Data Transfer:



C. Position Update:



D. Xgraph:



REFERENCES

[1] Danezis.G, "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.

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

[3] Kong.J, Hong.X, and Gerla.M, "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] Liu Y, Zhang .R, Shi.J, and Zhang.Y, "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.

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

[6] Seys.S and Preneel.B, "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.

[7] Troncoso.C, Gierlichs.B, Preneel.B, and Verbauwhede .I, "Perfect Matching Disclosure Attacks," Proc. Eighth Int'l Symp. Privacy Enhancing Technologies, pp. 2-23, 2008.

[8] Wright .M, Adler .M, Levine .B, and Shields .C, "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.

[9] Zhang. Y, Liu. W, Lou. W and Fang. Y, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," IEEE Trans.Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.

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

