RESEARCHERID
THOMSON REUTERS

[Majeed* *et al.*, 6(4): April, 2017]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

INTRUSION DETECTION FOR MANETS

Insha Majeed*, Insha Altaf
* Dept. of Inforation Technology National Institute of Technology Srinagar, J&K, India
Dept. of Information Technology National Institute of Technology Srinagar, J&K, India

DOI: 10.5281/zenodo.557136

ABSTRACT

Mobile Ad hoc networks are playing very important role in the present world. They are applied to several popular wireless technologies including cellular phone services, disaster relief, emergency services, battlefield scenarios, and other applications. MANETs are decentralized networks, and the network topology is unpredictably dynamic because of node mobility. As a result, mobile nodes in MANETs act as both hosts and routers since MANETs are decentralized; all mobile nodes need to discover the dynamic topology and deliver messages by themselves. MANETs rely on the cooperation of all mobile nodes in the network to ensure reliable routing services in the presence of dynamic topology caused by their mobility. The dynamic and cooperative nature of MANETs presents substantial challenges for network security. Therefore, sufficient protection should be provided to secure MANETs to guarantee the integrity of routing messages and availability of routing services. In other words, the goal of this dissertation is to examine how to secure the routing services of MANETs in order to provide reliable communication among nodes.

KEYWORDS: Access control, routing services adhoc networks, multi authority, secure data retrieval.

INTRODUCTION

A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. The network is an autonomous transitory association of mobile nodes that communicate with each other over wireless links. Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's send range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. The devices or nodes are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes. These mobile nodes establish the routing tables by exchanging routing messages with each other and then delivering data packets for others. Generally, MANETs rely on the cooperation of all mobile nodes in the network to ensure reliable routing services in the presence of dynamic topology caused by their mobility. The dynamic and cooperative nature of MANETs presents substantial challenges for network security.

SPECIAL SECURITY ISSUES FOR MOBILE AD HOC NETWORKS

In addition to authentication, integrity, confidentiality, availability, access control and non-repudiation, which have to be addressed differently in a mobile, wireless, battery-powered and distributed environment, mobile ad hoc networks raise the following security issues:

Cooperation and fairness: There is a trade-off between good citizenship, i.e. cooperation [2], and resource consumption, so nodes have to economize on their resources.

At the same time, however, if they do not forward messages, others might not forward either, thereby denying them service. Total non-cooperation with other nodes and only exploiting their readiness to cooperate is one of several boycotting behavior patterns.

Therefore, there has to be an incentive for a node to forward messages that are not destined to itself.

Attacks include incentive mechanism exploitation by message interception, copying, or forging; incorrect forwarding; and bogus routing advertisement.

Confidentiality of location: In some scenarios, for instance in a military application, routing information can be equally or even more important than the message content itself [3].

No traffic diversion: Routes should be advertised and set up adhering to the chosen routing protocol and should truthfully reflect the knowledge of the topology of the network. By diverting the traffic in the following ways, nodes can work against that requirement:

Routing: To get information necessary for successful malicious behavior, nodes can attract traffic to themselves or their colluding nodes by means of false routing advertisements. Although only suitable for devices that have enough power, a lot of information can be gathered this way by malicious nodes for later use to enable more sophisticated attacks.

Denial-of-service attacks can be achieved by bogus routing information (injecting of incorrect routing information or replay of old routing information or 'black hole routes') or by distorting routing information to partition the network or to load the network excessively, thus causing retransmissions.

Forwarding: Nodes can decide to forward messages to partners in collusion for analysis, disclosure, or monetary benefits; or may decide not to forward messages at all, thus boycotting communications.

PROTOCOLS

Various routing protocols have been proposed to provide the secure and reliable communication among the nodes in MANET. These protocols are broadly divided in the following protocols:

[1] Reactive Protocols.
[2] Proactive Protocols.

Proactive protocols:
In this type of routing protocol, each node in a network maintains one or more routing tables which are updated regularly. Each node sends a broadcast message to the entire network if there is a change in the network topology. However, it incurs additional overhead cost due to maintaining up-to-date information and as a result; throughput of the network may be affected but it provides the actual information to the availability of the network. Distance vector (DV) protocol, Destination Sequenced Distance Vector (DSDV) protocol, Wireless Routing protocol Fisheye State Routing (FSR) protocol are the examples of Proactive protocols.

Reactive Protocols:
In this type of routing protocol, each node in a network discovers or maintains a route based on-demand. It floods a control message by global broadcast during discovering a route and when route is discovered then bandwidth is used for data transmission. The main advantage is that this protocol needs less touting information but the disadvantages are that it produces huge control packets due to route discovery during topology changes which occurs frequently in MANETs and it incurs higher latency. The examples of this type of protocol are Dynamic Source Routing (DSR), Ad-hoc On Demand Routing (AODV) and Associativity Based Routing (ABR) protocols.

Hybrid Protocols:
It is a combination of proactive and reactive protocols taking the best features from both worlds.

Distance Vector (DV) Protocol:
It is a proactive protocol that works on the principles of distance vector where each node in a network maintains a distance table that contains the shortest distance and the address of the next hop router. Initially, each node knows only the distance with the nodes that are directly connected and a distance vector is initialized with that distance. Initially, distance to all others nodes that are not directly connected are initialized to infinity. When a change occurs in the network, each node updates its directly connected neighbors to the least cost distance vector. This process continues until convergence.

The advantages of distant vector protocol are 1) No need for global broadcasting and 2) Short route acquisition delay since all information for each node are available in the routing table.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

The disadvantages are 1) Long convergence time which may cause counting to infinity problem for large networks, 2) Non-availability of alternative paths.

Wireless Routing Protocol (WRP):
It is an improved version of the distant vector protocol that eliminates the count-to-infinity problems and thereby decreasing the convergence time. It has some disadvantages also. It requires larger memory and greater processing. It is also not suitable for large networks with mobility. However, in WRP, each node in a network maintains the following four tables:
1. Link Cost Table: Each node contains cost and other information like identifier to the directly connected nodes. The cost of a broken link is identified by infinity.
2. Distance Table: In this table, each node contains information to the nodes that are not directly connected.
3. Routing Table: It contains the shortest distance and the up-to-date information of all destinations.
4. Message Retransmission List (MRL): Each node in a network sends a hello message to its neighbors and informs them that he is alive and waits for the acknowledgement (ACK) from its neighbors. If it does get any ACK from any neighbors within a certain time, then keeps this information to MRL list. Next time it will send update message to nodes only that did not reply to the hello message.

Dynamic Source Routing (DSR) Protocol:
It is a reactive protocol that creates a route on demand using source routing protocol i.e. it requires a full series of paths to be established between source and destination nodes to transmit packets and each packet follows the same path. The major motivations of this protocol are to limit the bandwidth by avoiding the periodic table updates and long convergence time. The underline fact to this protocol is that it floods a route request message in the network to establish a route and it consists of two procedures: Route Discovery and Route Maintenance.

MANETs by their very nature are more vulnerable to attack than wired net-works. The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices (which have generally different resource and computational capacities, and run usually on battery power) introduces new security risks. As part of rational risk management we must be able to identify these risks and take appropriate action. We must be able to identify the risks or intruders and take the appropriate actions.

INTRUSION DETECTION SYSTEM

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource [4] and an intrusion detection system (IDS) is a system for the detection of such intrusions. There are three main components of an IDS: data collection, detection, and response.

The *data collection component* is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and sending data to the detection module [6]. IDS can use different data sources as inputs to the system: system logs, network packets, etc. In the *detection component* data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the *response component*.

In the literature, three intrusion detection techniques are used. The first technique is *anomaly-based intrusion detection* which profiles the symptoms of nor-mal behaviors of the system such as usage frequency of commands, CPU usage for programs, and the like. It detects intrusions as anomalies, i.e. deviations from the normal behaviors. Various techniques have been applied for anomaly detection, e.g. statistical approaches and artificial intelligence techniques like data mining and neural networks. Defining normal behavior is a major challenge. Normal behavior can change over time and intrusion detection systems must be kept up to date. False positives – the normal activities which are detected as anomalies by IDS – can be high in anomaly-based detection. On the other hand, it is capable of detecting previously unknown attacks. This is very important in an environment where new attacks and new vulnerabilities of systems are announced constantly.

Misuse-based intrusion detection compares known attack signatures with cur-rent system activities. It is generally preferred by commercial IDSs since it is effi-cient and has a low false positive rate. The drawback of this approach is that it cannot detect new attacks. The system is only as strong as its signature database and this needs frequent updating for new attacks. Both anomaly-based and misuse-based approaches have their strengths and weaknesses. Therefore, both techniques are generally employed for effective intrusion detection.

The last technique is *specification-based intrusion detection*. In this approach, a set of constraints on a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. It is introduced as a promising alternative that combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with a lower false positive rate [26]. It can detect new attacks that do not follow the system specifications. Moreover, it does not trigger false alarms when the program or protocol has unusual but legitimate behavior, since it uses the legitimate specifications of the program or protocol [8]. It has been applied to ARP (Address Resolution Protocol), DHCP (Dynamic Host Configuration Protocol) [7] and many MANET routing protocols. Defining detailed specifications for each pro-gram/protocol can be a very time consuming job. New specifications are also needed for each new program/protocol and the approach cannot detect some kind of attacks such as DoS (Denial of Service) attacks since these do not violate pro-gram specifications directly [5].

REFERENCES

[1] *Alireza Shams Shafigh, Alireza Soleimany, Hekmat 1 2 3 Mohammadzadeh and 1Shima Mohseni* World "**A Persuading Approach for Cooperating Nodes in Mobile Ad Hoc Networks**"Applied Sciences Journal 15 (7): 921-932, 2011**,**ISSN 1818-4952© IDOSI Publications, 2011
[2] S. Buchegger, C. Tissieres, and J.Y. Le Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-Hoc Networks -- How Much Can Watchdogs Really Do?" *Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA '04),* 2004.
[3] Heady R, Luger G, Maccabe A, Servilla M (1990) The architecture of a net-work level intrusion detection system. Technical Report, Computer Science Department, University of New Mexico
[4] Huang Y, Lee W (2004) Attack Analysis and Detection for Ad Hoc Routing Protocols. In Proc of Recent Adv in Intrusion Detect LNCS 3224:125-145
[5] undin E, Jonsson E. (2002) Survey of Intrusion Detection Research. Techni-cal report 02-04, Dept. of Computer Engineering, Chalmers University of Technology
[6] Tseng C-Y, Balasubramayan P et al (2003) A Specification-Based Intrusion Detection System for AODV. In Proc of the ACM Workshop on Secur in Ad Hoc and Sens Netw (SASN)
[7] Uppuluri P, Sekar R (2001) Experiences with Specification-based Intrusion Detection. In Proc of the 4th Int Symp on Recent Adv in Intrusion Detect LNCS 2212: 172-189