Asian Journal of Information Technology 6 (7): 758-761, 2007
ISSN: 1682-3915

Detecting Intrusion Attacks in ADHOC Networks

[1]R. Ranjana and [2]M. RajaRam
[1]Department of Information Technology, Sri Sairam Engineering College,
Anna University, Saileo Nagar, West Tambara, Chennai, India
[2]AP/EEE, Thanthai Periyar Government Institute of Technology, Vellore, India

Abstract: In the recent years, wireless technology has tremendous rise in popularity and usage opening new fields of applications in the domain of networking. One such field concerns mobile ADHOC networks (MANET) where the participating nodes do not rely on any existing network infrastructure. Security is hard to achieve due to their dynamic nature and limitations of the wireless transmissions medium. The proposed Intrusion Detection System for ADHOC Networks system is a novel architecture that uses intrusion detection techniques to detect active attacks that an adversary can perform against the routing fabric of mobile ad hoc networks. Moreover, the system is designed to take countermeasures to attacks. The proposed system does not introduce any changes to the underlying routing protocol and operates as an intermediate component between the network traffic and the routing protocol. The system was developed and tested to operate in ADHOC On Demand Distance Vector Routing (AODV) enabled networks using the network simulator (ns-2). The system has been designed to detect resource consumption attack, packet-dropping attack and fabrication attacks.

Key words: Adhoc networks, intrusion detection, AODV

INTRODUCTION

Security in mobile ad hoc networks is a hard to achieve due to dynamically changing and fully decentralized topology as well as the vulnerabilities and limitations of wireless data transmissions. Existing solutions that are applied in wired networks can be used to obtain a certain level of security. One of the major factors is that the wireless medium is inherently less secure than their wired counterpart. Most traditional applications do not provide user level security schemes based on the fact that physical network wiring provides some level of security. The routing protocol sets the upper limit to security in any packet network. If routing can be misdirected, the entire network can be paralyzed. This problem is enlarged in ad hoc networks since routing usually needs to rely on the trustworthiness of all nodes that are participating in the routing process. An additional difficulty is that it is hard to distinguish compromised nodes from nodes that are suffering from broken links.

AODV and intrusion detection: ADHOC On Demand Distance Vector Routing (AODV) is an improvement of Destination Sequenced Distance Vector Routing (DSDV) as it minimizes the number of required broadcasts as it creates routes in an on-demand basis, in contrast to distance DSDV which maintains a complete set of routes (Johnson *et al*., 2002).

When a node needs a route to a destination it broadcasts a Route Request (RREQ) message. The RREQ message is spread throughout the network and as soon as the message reaches a node with a fresh enough route to the specific destination or the destination node itself, a Route Reply (RREP) message is unicast back to the requesting node (Peng and Kun, 2003).

Intrusion Detection Systems (IDS) are mainly used to detect and call attention to suspicious behavior. The first intrusion detection model was developed in 1987 in which Denning proposed a model based on the hypothesis that security violations can be detected by monitoring a system check records for abnormal patterns of system usage (Denning, 1987).

Current approaches to intrusion detection can be broadly classified into two types: Behavior based intrusion detection and knowledge based intrusion detection.

MATERIALS AND METHODS

The proposed system can be characterized as an architecture model for intrusion detection in wireless ADHOC networks, while its implementation targets specifically the ADHOC On Demand Distance Vector Routing (AODV) routing protocol. The reason why it can be classified, as an architecture model is that it does not perform any changes in the underlying routing protocol

Corresponding Author: R. Ranjana, Department of Information Technology, Sri Sairam Engineering College, Anna University, Saileo Nagar, West Tambara, Chennai, India

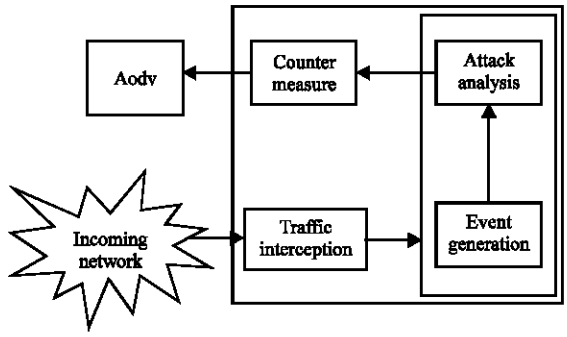

Fig. 1: Proposed intrusion

but it intercepts routing and application traffic. The security component operates in a different layer without interfering with the normal operation of the routing protocol. The system does not utilize any cryptographic mechanism to ensure protection from malicious activities and so it does not introduce any additional computation overhead to the routing process and does not consume additional bandwidth. Its logical components are shown in Fig. 1.

The traffic interception module captures the incoming traffic from the network and selects which of these packets should be further processed. The event generation module is responsible for abstracting the essential information required for the attack analysis module to determine if there is malicious activity in the network Extract the information about sequence number, time, IP address of the node, hop count, packet size.

The attack analysis module detects and classifies the type of attack. The possible attacks can be fabrication attack, Dropping Routing Traffic Attack and Resource Consumption Attack.

ATTACK DETECTION

Fabrication attack: The source node initiates a route discovery process directed to the destination node by sending a RREQ packet. When the malicious node receives the RREQ even if it does not have a fresh enough route in its routing table it creates a RREP with forged information about the sequence number and the next hop. The malicious node puts a high sequence number to the destination sequence number field. If the RREP from the malicious node is received before the one from the legitimate source node then it manages to put itself in the route and it can change the source address thereby fabricating a source. Even if the malicious RREP does not reach the source node first it will eventually reach it and because the destination sequence number will be greater the forged route will replace the original route.

Fabrication attack detection algorithm:

Step 1: Malicious node attempt to send false route reply packets to source.

Step 2: Repeatedly transmits route reply packets until accept the reply.

Step 3: Malicious node try to act as original neighbor by incrementing sequence number by large value comparatively destination sequence number.

Step 4: Malicious node accept packet and transmit to some other node as source node to alter source and destination path.

Step 5: Event generation module fetches sequence number and transmit to attack analysis module.

Step 6: Attack analysis module check sequence number with previous sequence number with adding threshold value of 5.

Step 7: Condition not satisfied then inform to counter measure module to discard the packet. This node information is not updated in routing table.

Dropping routing traffic attack: Mobile nodes due to limited battery life and limited-processing capabilities may decide not to participate in the routing process in order to conserve energy. Thus, a malicious node upon receiving a routing packet that is not destined for it drops it. The node by acting selfishly conserves energy but it may also cause network segmentation. If the some of the participating nodes are connected only with the malicious node then they become unreachable and isolated from the rest of the network.

Dropping Routing Packets Attack Detection algorithm:

Step 1: A node sends or forwards a RREQ or a RREP packet. It waits for time t for the node to forward/reply to the routing packet.

Step 2: If the node fails to reply or forwards the packet it suspects it to be malicious and waits for some more time t.

Step 3: If the node manages to respond appropriately by forwarding the routing traffic or by replying to a RREQ it is removed from the suspected nodes list.

Step 4: Otherwise, the node is marked as malicious and is prevented from forwarding any kind of traffic.

Resource consumption attack: In this attack the malicious node attempts to consume both the network and node resources by generating and sending frequent unnecessary routing traffic. This routing traffic can only be RREQ and RERR packets since all false RREP are automatically discarded by the specification of the AODV protocol. The goal of this attack is to flood the network with false routing packets to consume all the available network bandwidth with irrelevant traffic and to consume energy and processing power from the nodes.

Resource consumption attack detection algorithm

Step 1: All nodes that sends a routing packet is observed with a list.

Step 2: the list contains all the nodes from which it has recently received routing traffic along with a counter that signifies the number of packets that the specific node has sent and a timer.

Step 3: The counter is incremented for every new routing packet received from this node.

If the counter reaches the threshold value it means that it has detected abnormal traffic generation and drops all the incoming routing traffic from the offending node for finite time interval.

SIMULATION ENVIRONMENT

The proposed Intrusion Detection System for ADHOC Network was implemented in the network simulator (ns-2). The utilized version of ADHOC On Demand Distance Vector Routing (AODV) was the default one included in ns-2. The three attacks and the proposed Intrusion Detection System for ADHOC Network were developed as new routing agents based on the implementation of AODV included in ns-2. In order to realize the appropriate behavior several methods of the default AODV routing agent were extended. Every routing agent inherits the methods and attributes of the normal AODV implementation and modifies only the methods required to the intrusion detection component. The main operation of ADHOC On Demand Distance Vector Routing (AODV) is implemented in the header file named aodv.h and in the C++ file named aodv.cc. For every packet that is received the node introduced intruder send only reply packet to enter into routing.

The simulation was performed with 20 mobile nodes with transmission range of 250 m and maximum speed of 5-20 m sec^{-1}. A CBR traffic type with a payload of 512 bytes at a rate of 2 pkt sec^{-1} was used. A single node was simulated to be a malicious node.

RESULTS AND DISCUSSION

The throughput has been compared for all the attacks with normal AODV and AODV with the proposed

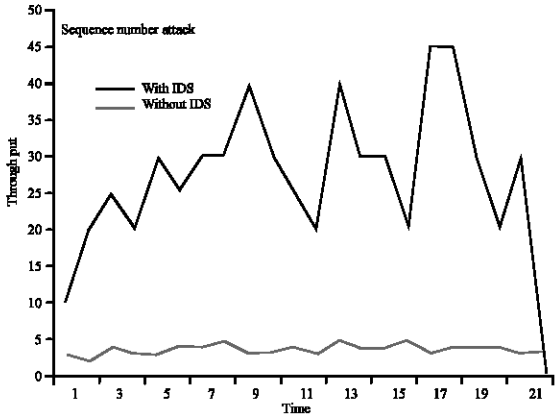

Fig. 2: Sequence number attack graph

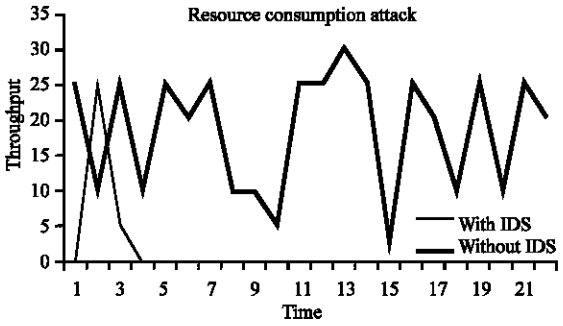

Fig. 3: Resource consumption attack graph-throughput (bits sec^{-1}) vs time (sec)

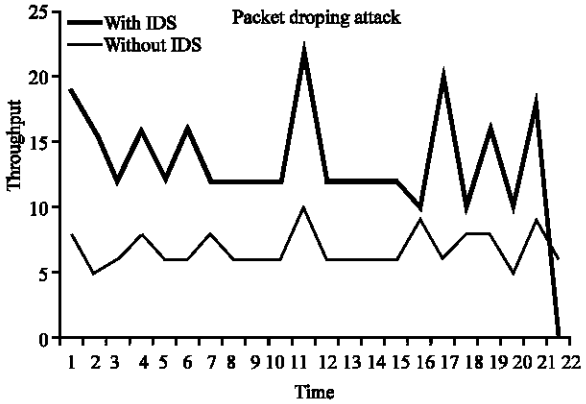

Fig. 4: Packet dropping attack graph throughput (bits sec^{-1}) vs time (sec)

intrusion detection system. The resultant graphs Fig. 2-4 show that the proposed system helps to increase the throughput over time.

CONCLUSION

The proposed system is a intrusion detection component for wireless Ad Hoc networks that find attacks of Resource Consumption attacks, Packet Dropping attacks, Fabrication Attack. The performance has been compared with the default routing protocol and the simulation results show that the new system performs better. Future enhancements would be to extend the system to detect attacks like node isolation, route invasion and Flooding attack.

REFERENCES

Denning, D.E., 1987. An Intrusion Detection Modelbe, IEEE. Trans. Software Eng., pp: 13.

Johnson, D.B., D.A. Maltz, Y.C. Hu and J.G. Jetcheva, 2002. The dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet Draft, draft-ietf-manet-dsr-07.txt, work in progress.

Peng Ning and Kun Sun, 2003. How to misuse AODV: Case Study of Insider attack against Mobile ADHOC Networks, IEEE., pp:1509-1518.