ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, January 2013

DETECTING ATTACK'S IN MOBILE AD-HOC NETWORK USING AODV ROUTING PROTOCOL

Prakash D. Naik[1], Shriram Datar[2], Raju G. Metkari[3]

Student, Department of Computer Engineering, KJ College Of Engineering, Pune, India[1,2,3]

Abstract: In mobile ad hoc networks the nodes have fully decentralized topology and they are dynamically changing. Due to the dynamic changing nature of participating nodes the vulnerabilities and wireless transmissions medium security is very hard to achieve. In this paper we propose an Intrusion and various attack's Detection Techniques and On Demand Routing for AD-HOC Networks based on a Novel Architecture. It uses intrusion detection techniques to detect active attacks that can perform against routing fabric of mobile ad hoc networks. The Intrusion Detection Technique and On Demand Routing for ADHOC Network system does not introduce any changes to the underlying routing protocol and operates as an intermediate component between the network traffic and routing protocol in the system. The system that we are going to developed and tested to operate in ADHOC on Demand Distance Vector Routing (AODV) enabled networks using the network simulator (ns-2). The proposed system has been designed to detect resource consumption attack, fabrication attack, packet dropping attack.

Keywords: MANET, ADHOC Networks, attacks, AODV, NS2, OTCL, NSG.

I. INTRODUCTION

Different networks are being used in various areas and the demand of users nowadays has increased in Mobile Ad Hoc Network (MANET). MANET is a wireless network and has dynamic topology due to its node mobility. Every single node in network will independently work as both transmitter and receiver. Ad hoc On Demand Distance Vector (AODV) is one of the routing protocols in MANET. One advantage of wireless networks is the ability to transmit data among the users in the common area while remaining mobile. Each sends its own data as well as routs and forwards data on behalf of other nodes.

In mobile ad hoc networks the nodes are dynamically changing and they have a fully decentralize topology. Hence, security is very hard to achieve due to the dynamic nature of the relationships between the participating nodes as well as the vulnerabilities and limitations of the wirelesstransmissions medium. We are going to design an Enhancement on Intrusion Detection Systems for ADHOC Networks (EIDAN) based on a novel architecture that uses intrusion detection techniques to detect active attacks in ad- hoc networks. So, the system that we are going to designed to take countermeasures to attacks. The novelties (newness) of the system enable the detection of active attacks. The Enhancement of the Intrusion Detection System for ADHOC Network (EIDAN) 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. Thesystem will developed and tested to operate in ADHOC on Demand Distance Vector Routing (AODV) enabled networks using the network simulator (ns-2). The proposed system will be designed to detect resource consumption attack, fabrication attack, packet dropping attack.

A. Issues of Ad Hoc networks

Ad hoc networks are ideal in situations where installing an Infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous infrastructure networks were destroyed. 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 used and applied in wired networks can be used to obtain a certain level of security. These solutions are not always being suitable to wireless networks. Therefore, ADHOC networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions. One of the very distinct characteristics of mobile ADHOC networks (MANET) is that all participating nodes have to be involved in the routing process. Since traditional routing protocols designed for infrastructure networks cannot be applied in ad hoc networks, ad hoc routing protocols were designed to satisfy the needs of

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, January 2013

infrastructure less networks. Due to the different characteristics of wired and wireless media, the task of providing seamless environments for wired and wireless networks is very complicated. The major factors are that wireless medium is inherently less secure than their wired counterpart. The routing protocol sets the upper limit to security in any packet switched 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. Another difficulty is that it is hard to distinguish compromised nodes from nodes that are suffering from broken links.

II. LITERATURE SURVEY

A. Intrusion Detection System

Intrusion detection is a new, retrofit approach for providing a sense of security in existing computers and data networks, while allowing them to operate in their current open mode.

The goal of intrusion detection system is to identify, preferably in real time, unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators.

approaches to intrusion detection can be broadly classified into two trends types:-

1. Behaviour-based Intrusion Detection
2. Knowledge based Intrusion Detection

1) Behaviour-based Intrusion Detection;

Behaviour-based intrusion detection systems monitor and build a reference profile of normal behaviour for the information system by using statistical methods and try to detect activity that deviates from the normal behaviour profile.

*Advantage:*It can detect attempts to exploit new and unseen vulnerabilities without having a priori Knowledge of explicit security flaws.

*Disadvantage:*This technique suffers from a high volume of false positives it means totally gives wrong system behaviour, since the entire scope of the system behaviour may not be covered during the learning phase and legitimate behaviour may change over time.

2) Knowledge-based Intrusion Detection;

Knowledge-based intrusion detection system accumulates knowledge about attacks, examine the current traffic and try to identify patterns indicating that a suspicious activity is occurring. This approach can be applied against known attacks patterns and needs to update the knowledge base activity frequently.

*Advantage:*It includes simplicity, efficiency and an excellent ability to detect known attacks.

*Disadvantage:*The system can only detect known attacks.

B. Architecture of Intrusion Detection System

1) Host- Based IDS;

In this architecture apply their detection method to activity that occurs on the host. The system was designed to detect attacks such as buffer overflows and encapsulation privileges.

Host based system have little or no view of network activities.

2) Network-Based IDS;

Apply their detection methods to network traffic. This system was designed to detect attacks such as denial of service, network probes and malformed packets. These system may have some overlap with firewalls, network based system have little or no direct view of host based attacks 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 since it creates routes in an on-demand basis, opposite to Destination sequenced distance vector routing (DSDV) which maintains a complete set of routes. It utilizes destination sequence numbers to ensure loop-freedom at all times and to avoid the count-to-infinity problem associated with classical distance-vector protocols.

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. Generally AODV offers low overhead, quick adaptation to dynamic link conditions and low processing and memory overhead. Since the AODV routing protocol is the one that it used in this research and in the development of the Enhancement of Intrusion Detection system. ADHOC On Demand Distance Vector Routing (AODV) is designed specifically to address the routing problems in ad-hoc wireless networks and provides communication between mobile nodes with minimal control overhead and minimal route. ADHOC On Demand Distance Vector Routing (AODV) being a reactive protocol does not require the maintenance of routes to destinations that are not in active communication, instead it allows the mobile nodes to obtain routes quickly to new destinations. Moreover, ADHOC On Demand Distance Vector Routing (AODV) enables mobile nodes to respond to link breakages and changes in the network topology in a timely manner. As was highlighted earlier loop-freedom is a desirable property in ad hoc routing protocols. The operation of ADHOC On Demand Distance Vector Routing (AODV) is loop-free and provides quick convergence when the network topology changes.

III. SYSTEM ARCHITECTURE

The Enhancement in Intrusion Detection System for mobile ADHOC Network (EIDAN) can be characterized as an architecture model for intrusion detection in wireless ADHOCnetworks, while its implementation targets

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, January 2013

specifically the ADHOC On Demand Distance Vector Routing (AODV) routing protocol. It can be classified, as an architecture model is that it does not perform any changes in the underlying routing protocol but it intercepts routing and application traffic. In this proposed system following four different modules are used.

A. Traffic interception module
B. Event generation module
C. Attack Analysis Module
D. Countermeasure module

The security component operates in a different layer without interfering with the normal operation of the routing protocol. The proposed system will detect the different type of attacks, which are making by malicious node in the Ad-hoc network.

The high-level architecture of the Intrusion Detection Technique and On Demand Routing for ADHOC Network system is designed to detect resource consumption attack, packet dropping attack, fabrication attack. Its logical components are shown in figure 1.

A. Traffic interception module

The traffic interception module captures the incoming traffic from the network and selects which of these packets should be further processed. Once path has established then by receiving each packet has traced by Intrusion Detection Technique and On Demand Routing System has to check the node information already present in the routing table entry. If condition not satisfied then packet is picked for further process.

B. Event generation module

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.

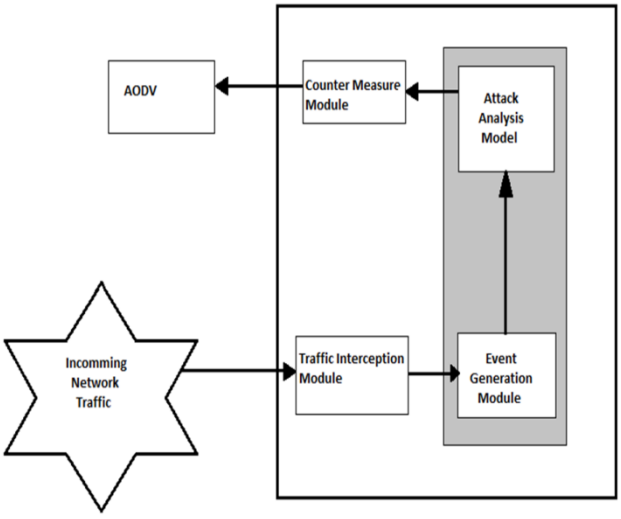

Fig 1: Intrusion detection system

C. Attack analysis module

The attack analysis module to analyses any defined attacks are to found are not if it is found then send malicious packet to counter measure module. In attack analysis module can only verify type of attack. The operation of the system process by to detect malicious packet to be analysed using existing ADHOC On Demand Distance Vector Routing (AODV) protocol. Resource consumption attack a malicious node attempt to enter into route thereby disturb already existing path to send route reply packets unnecessarily to block the route it can be analysed and informed to counter measure module to take appropriate action .Packet dropping attack a malicious node attempt to enter into route thereby disturb already existing path to send route reply by block the route it can be analysed and informed to counter measure module. Fabrication attack malicious node attempt to enter into route thereby disturb already existing path to send route reply to make false fabricated source node to alter the route by new route it can be analysed to inform countermeasure module take action.

D. Counter measure module

The final component of the architecture is the countermeasure module that is responsible for taking action to drop malicious packet get from the attack analysis module. Therefore, the Intrusion Detection Technique and On Demand Routing for ADHOC Network intrusion detection component operate between the network traffic and the routing protocol requiring no modifications to the routing protocol that is utilized in the network. The intrusion detection system runs locally in every participating node and it makes decisions upon the partial view of the traffic that it observes. Thus, the system is a host-based network intrusion detection system. The operation of the system could be a malicious node is detected, however in order to provide a more complete solution the nodes take countermeasures to deal with the isolation of the detected misbehaving node. The intrusion detection component has high rates of accuracy in detecting the malicious nodes and the countermeasures taken by the nodes.

IV. SYSTEM DESIGN

The Intrusion Detection Technique and On Demand Routing for ADHOC Network is a host-based network intrusion detection system. The operation of the system process by to detect malicious packet to be analyzed using existing ADHOC On Demand Distance Vector Routing (AODV) protocol.

A. Resource consumption attack

In this attack, an attacker tries to consume or waste away resources of other nodes present in the network. The resources are targeted with the three factors that are bandwidth, computational power, and battery power which are only limitedly available in ad-hoc networks. The

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, January 2013

attacks could be in the form of unnecessary route requests (RREQ) for routes, very frequent generation of (beacon) packets, or forwarding of (stale) packets to other nodes. Using the battery power level of another node by keeping that node always busy by continuously pumping the packets to that node is known as a sleep deprivation attack. So automatically that node consumes a lot more battery power and loose energy.

1) Algorithm;

Step 1: Check malicious node already source destination path is established.

Step 2:Malicious node tries to enter into already existing path. From route table to get information about source and destination route was found.

Step 3: Malicious node generate route reply packet to existing source.

Step 4: Malicious node try to act as original neighbor by incrementing sequence number by large value comparatively designation sequence number.

Step 5: Malicious node enters into route there by transmitting unnecessary packet to neighbors.

Step6: Attack analysis module set threshold time receiving packet with five seconds only below five packets if it exceed the number packet more than five packets then confirmed as malicious node to inform counter measure to drop the packets.

B. Packet dropping attack

Malicious node attempt to enter into route thereby disturb already existing path to send route reply by block the route. When it gains access in the network it drops all the packets incoming from sender hence completely blocking the communication from happening. Because packets are routinely dropped from a lousy network, the packet drop attack is very hard to detect and prevent because from many ways the packets can be dropped in ad-hoc networks.

1) Algorithm;

Step 1: Check malicious node already source destination path is established.

Step 2: Malicious node attempt to send false route reply packets to source.

Step 3: Repeatedly transmitting route reply packets until accept the reply.

Step 4: Malicious node try to act as original neighbor by incrementing sequence number by large value comparatively designation sequence number.

Step 5: Malicious node accept packet and drop it.

Step 7: System wait for the route reply packet from the neighbors already established path.

Step 8: If neighbors not transmitting route reply packets within the threshold time then system assume packet dropping attack.

C. Fabrication attack

In fabrication attack sender send the packet to the receiver. Somewhere in the communication path, malicious node entered into route as an original node and tries to change the already existing path. At the receiver side the malicious node act as a sender and send packet to the receiver as sender by changing complete route path. In short, malicious node attempt to enter into route thereby disturb already existing path to send route reply to make false fabricated source node to alter the route.

1)Algorithm;

Step 1: Check malicious node already source destination path is established.

Step 2: Malicious node attempt to send false route reply packets to source.

Step 3: Repeatedly transmitting route reply packets until accept the reply.

Step 4: Malicious node try to act as original neighbor by incrementing sequence number by large value comparatively designation sequence number.

Step 5: Malicious node accept packet and transmit to some other node as source node to alter source and destination path.

Step 6: System of event generation module fetch sequence number and transmit to attack analysis module.

Step 7: Attack analysis module check sequence number with previous sequence number with adding threshold value of five.

Step 8: Condition not satisfied then inform to counter measure module to discard the packet. This node information will not be updated in routing table.

D. Malicious Node Detection using Trust based System

In our proposed system's protocol, by dynamically calculating the "nodes trust counter values", the source node will be able to select the more trusted routes rather than selecting the shorter routes. This proposed system should marks and isolates the malicious nodes from participating in the network. So that potential damage caused by the malicious nodes or hackers node is reduced. We are going to make changes to the AODV routing protocol. An additional data overhead called Neighbour Trust Counter Table (NTT) is maintained by each network node.Let {Tc1, Tc2…} be the initial trust counters of the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, January 2013

nodes {n1, n2…} along the route R1 from a source S to the destination D.

Since the node does not have any information about the reliability of its neighbors in the starting, nodes cannot either be fully trusted or be fully distrusted. When a source 'S' wants to establish a route to the destination D, it sends route request (RREQ) packets. Each node keeps track of the number of packet it has forwarded through a route using a forward counter (FC).

Each time, when node nk receives a packet from a node ni, then nk increases forward counter of node ni .

FCni = FCni + 1, i=1, 2…… (1)

Then the NTT of node nk is modified with the values of FCni .Similarly each node determines its NTT and finally the packets reach the destination D.

When the destination D receives the accumulated RREQ messages, it calculates the number of packets received (Prec). Then it constructs a MAC on Prec with the key shared by the sender and destination. The RREP contains the source and the

Destination ids, The MAC of Prec, accumulated route from RREQ, which are digitally signed by the destination. RREP is sent towards the source on the reverse route R1. Each intermediate node along the with reverse route from D to S checks the RREP packet to compute success ratio as,

SRi = FCni / Prec……. (2)

Where Prec is the number of packets received at D in time interval t1. The [FCni] values of ni can be got from the corresponding NTT of node. The success ratio value [Sri] is then added with RREP packet.

The intermediate node then verifies the digital signature of destination node stored in RREP packet, is valid. If the verification fails, then RREP Packet is dropped. Otherwise, it is signed by intermediate node and forwarded to the next node in reverse route.

When the source S receives the RREP packet, if first verifies that first id of the route stored by RREP is its neighbour. If it is true, then it verifies all the digital signatures of the intermediate nodes, in RREP packet. If all these verifications are successful, then the trust counter values of the releted nodes are incremented as

Tci = Tci + δ1 …….(3)

If the verification is failed, then

Tci = Tci - δ1…… (4)

Where, δ1 is the step value which can be assigned a small fractional value during the simulation experiments. After this verification stage, source S will check the success ratio values SRi of the nodes ni.

For any node nk, if SRk<SRmin, where SRmin is the minimum threshold value, its trust value counter is decremented further as

Tci = Tci – δ2 …….(5)

For all the other nodes with SRk>SRmin, the trust counter

values are further incremented as

Tci = Tci + δ2…… (6)

Where, δ2 is another step value with δ2 < δ1. For a node nk, if Tck<Tcthr, where Tcthr is the trust threshold value, then that node is assumed or considered and marked as "malicious node".

If the source does not get the RREP packet for a time period of [t] seconds, it will be considered as route breakage or failure. Then route discovery process is initiated and started by the source again. The same procedure is again repeated for the other routes R2, R3 and either a route without a malicious node or with least number of malicious nodes, is selected as reliable route.

In this proposed system's protocol, authentication is performed for route reply operation. Also, nodes which are stored in the current route need to perform these cryptographic computations. So the proposed system is efficient and more secure than the existing system

V. SYSTEM IMPLEMENTATION

The Intrusion Detection Technique and On Demand Routing for ADHOC Network system 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 Intrusion Detection System for ADHOC Network intrusion detection component 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 ADHOC On Demand Distance Vector Routing (AODV) routing agent were extended. Every routing agent inherits the methods and attributes of the normal ADHOC On Demand Distance Vector Routing (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 method analyses the header and checks whether the received packet is a normal routing packet or malicious routing packet.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, January 2013

VI. CONCLUSION AND FUTURE WORK

The proposed system will be reliable than any other Intrusion detection system. It will detect the attacks and nullify them. In this way provides security to the mobile ad hoc network.The proposed system can find Fabrication, Resource Consumption attacks and Packet Dropping attacks. It also detects the malicious node and enhances the AODV protocol.

In the future work the system will be enhanced by adding more than three attacks. Also try to improve the performance of the routing Agent.

ACKNOWLEDGMENTS

First and foremost, we would like to thank our guide Prof.Suhas M.Patil, for his guidance and support. We will forever remain grateful for the constant support and guidance extended by guide, for completion of project report. Through our many discussions, he helped us to form and solidify ideas. The invaluable discussions We had with him, the penetrating questions he has put to me and the constant motivation, has all led to the development of this project.We are also thankful to our family members for encouragement and support in this project work.We wish to express our sincere thanks to the project coordinator Prof.S.A.Hirve, as well as our principal Dr.SanjeevJ.Wagh and the departmental staff members for their support.We would also like to thank to our friends for listening to our ideas and the suggestions to those ideas and providing feedback for improving our ideas.

REFERENCES

[1] L.PremaRajeswari, R. Arokia Xavier Annie, A. Kannan; *Enhanced Intrusion Detection Techniques for Mobile Ad-Hoc Network*;IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007).

[2] Yuvraj Singh and Sanjay Kumar Jena; *Intrusion Detection System for DetectingMalicious Nodes in Mobile Ad hoc Networks*; International Conference on Parallel,Distributed Computing technologies and Applications (PDCTA-2011) ISSN 1865-0929 .

[3] [3] MahaAbdelhaq, Rosilah Hassan, Mahamod Ismail and DaudIsraf; *Detecting Resource Consumption Attack over MANET using an Arti_cial Immune Algorithm*;Research Journal of Applied Sciences, Engineering and Technology 3(9): 1026-1033,2011

[4] HolgerDreger, AnjaFeldmann, Vern Paxson and Robin Sommer; *Predicting theResource Consumption of Network Intrusion Detection Systems*; R. Lippmann, E.Kirda, and A. Trachtenberg (Eds.): RAID 2008, LNCS 5230, pp. 135154, 2008.

[5] VenkatesanBalakrishnan and Vijay Varadharajan; *Packet Drop Attack:A Serious Threat To Operational Mobile Ad- Hoc Networks*; Information and Networked System Security Research Group Department of Computing Macquarie University Sydney, Australia venkat,vijay@ics.mq.edu.au

[6] D.Karun Kumar Reddy, K.Sandhya Rani Kundra, M.RatnakarBabu ,Dr.L.Prasanna Kumar; *Prevention of Routing Attack in Mobile Ad-vHoc Networks: A comparative study*; International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 5,October 2012.

[7] AishwaryaSagarAnandUkey, MeenuChawla; *Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET*; IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010

[8] A. Rajaram, Dr. S. Palaniswami; *Malicious Node Detection System For Mobile Adhoc Network*; (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010