Journal of Computer Science 4 (3): 245-251, 2008
ISSN 1549-3636

An Approach for Detecting Attacks in Mobile Adhoc Networks

[1]V. Madhu Viswanatham and [2]A.A. Chari
[1]School of Computing Sciences, VIT University, Vellore, TN, India
[2]Department of OR & SQC, SKU PG Center, S K University, Kurnool, AP, India

Abstract: The security of data becomes more important with the increased use of commercial applications over wireless network environments. We presented an approach to handle various attacks for wireless networks. There were several problems of security in wireless networks due to intruders and different type of attacks such as Node Isolation, Route Disruption and Resource Consumption. There were better methods and intruder handling procedures available for fixed networks but it was difficult to analyze attacks in the mobile adhoc environments. The reason was due high mobility of network nodes and lack of fixed infrastructure. Normally, attacks by an intruder cause unauthorized use of the wireless network so that the whole network will be suffered from packet losses and reduced throughput. So, we have performed a study on various issues of threats for Mobile Adhoc Networks and presented an approach to handle such threats efficiently. The main principle was to use my-AODV agent to introduce various attacks on existing AODV MANET routing protocol.

Keywords: MANET, attacks, detection, node isolation, route disruption, resource consumption

INTRODUCTION

A Mobile Adhoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end-system but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. MANET does not require any fixed infrastructure such as base stations; therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. Most existent protocols, applications and services for Mobile AdHoc Networks (MANETs) assume a cooperative and friendly network environment and do not accommodate security. Therefore, the number of attacks in this environment is more and we aim to address the problem of attacks on mobile nodes. Here we presented some popular methods used to detect attacks on mobile nodes.

Host centric methods usually analyze data collected from operating system's audit trails, system and application logs or audit data generated by loadable-kernel modules that intercept system calls to detect the attacks. Next, Network centric methods analyze data packets that travel over the actual network. These packets are examined and sometimes compared with empirical data to verify their nature: malicious. Another approach is Signature-based detection. In this misuse detection identifies attacks through attack pattern (i.e., *signature*) matching. Various data sources and types of pattern recognition techniques are used to separate attacks signals from normal usage noise. An attack signature is a known attack footprint abstraction. In other words, it is a descriptive material on known abnormal behavior. In general, signature detection designs have an acceptable accuracy and they tend to produce fewer false positives (i.e., classifying an action as malicious when in fact it is not) than anomaly detection designs. The systems are easier to implement and simpler to configure, especially in large production networks. However, signature detection is unable to detect novel attacks whose signatures are unknown. In addition, it requires updating signatures regularly due to the emergence of new variants of known attacks.

Anomaly detection, in contrast to signature detection, is able to detect novel attacks by recognizing any deviance from norm which characterizes network/system/user's normal behaviors. Anomaly detection techniques can be subcategories by the way of characterizing normal behaviors. They can be divided into two categories: profile-based detection and specification-based detection.

Profile-based detection: Profile-based detection is also known as behavior-based detection. Profile-based detection defines a profile of normal behavior and classifies any deviation of that profile as an anomaly. The assumption of this type of detection is that attacks

Corresponding Author: V. Madhu Viswanatham, School of Computing Sciences, VIT University, Vellore, TN, India

are events distinguishable from normal legitimate use of system resources. Although this type of anomaly detectors are able to detect novel attacks, they are prune to high false positive rate due to the difficulty of clear segmentation between normal and abnormal activities and the use of insufficient or inadequate features to profile normal behaviors.

Specification-based detection: Specification-based detection defines a set of constraints that describe the correct operation of a program or protocol and monitors the execution of the program with respect to the defined constraints. It has been show that specification-based techniques live up to their promise of detecting known as well as unknown attacks, while maintaining a very low rate of false positives. Since the increasing popularity of wireless networks to that of wired networks, security is being considered as a major threat in them. Wireless network exposes a risk that an unauthorized user can exploit and severely compromise the network.

There can be different possible attacks in wireless network viz., active and passive attacks. So there is a need for secured wireless system to analyze and detect number of attacks.

BACKGROUND

Intrusion detection techniques are widely used in wired networks to protect networked systems. Intrusion detection techniques geared towards wired networks cannot, however, is applied directly to wireless networks. This is especially because of the latter's lack of a fixed infrastructure, mobility, the vulnerability of wireless transmissions to eavesdropping and the lack of a clear separation between normal and abnormal behavior of the nodes. Installing a Wireless network is easier than the installation of traditional network both in residential and corporate environments. However, these wireless networks have some disadvantages[4]. Use of wireless links renders an ad-hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting data, injecting wrong messages; impersonate a node etc. thus violating availability, integrity, authentication and non-repudiation. It exposes a risk that the other user can share the same channel and misuse it. So there is a problem of security in wireless networks[1].

Hence there is a need for efficient wireless network technology to provide safe network access to users and also the efficient Wireless Intrusion Detection System (WIDS)[5] that not only detects different possible attacks but also to recover from them. Intrusion detection systems have performed well for fixed networks, but in Ad-hoc network it met lot of difficulties due to the following reasons[2]:

- There is no central point to control all the activities in the network
- Dynamically changing network topology and behavior
- Limited power level of mobile devices

The basic requirements for IDS to be implemented in ad hoc networks are.

The IDS should not introduce a new weakness in the MANET[1,3]. That is, the IDS itself should not make a node any weaker than it already is:

- IDS should run continuously and remain transparent to the system and users
- The IDS should use as little system resources as possible to detect and prevent intrusions. IDS that require excessive communication among nodes or run complex algorithms are not desirable
- It must be fault-tolerant in the sense that it must be able to recover from system crashes, hopefully recover to the previous state and resume the operations before the crash
- Apart from detecting and responding to intrusions, IDS should also resist subversion. It should monitor itself and detect if it has been compromised by an attacker
- IDS should have a proper response. In other words, an IDS should not only detect but also respond to detected intrusions, preferably without human intervention
- Accuracy of the IDS is another major factor in MANETs. Fewer false positives and false negatives are desired

The proposed Wireless Intrusion Detection System has been simulated using NS-2 environment in Linux platform.

SYSTEM DESIGN

The main design goal is to identify various possible attacks in wireless network systems and to propose a method for detecting attacks in MANETs. The proposed work can be performed by modifying Ad Hoc On-demand Distant Vector (AODV) routing protocol using MYAODV agent. There is also a possibility of inside attacker which acts on the AODV routing protocol. Some of the inside attackers are Node Isolation, Route Disruption and Resource Consumption.

Recovery is the next logical step after an intrusion has been detected. As part of the recovery phase, the victim should be isolated. In this state, the victim is connected to neither the attacker nor the valid system. This ensures that the attacker does not have any influence on the victim. However, this will completely shut out victim from accessing the network. When a traffic flow has been identified as vulnerable to attacks, system instructs the access router to block the flow to prevent possible attacks to that flow. A detection system should have both types of capabilities.

When a traffic flow has been identified as vulnerable to attacks, system instructs the access router to block the specific flow to prevent possible attacks to that flow. Ideally, a detection system should have both types of capabilities.

The proposed work can be divided into three modules based on the packets transfer under normal and attack mode. Modules can be divided mainly into two phases namely detection and recovery part. In the two phases, detection part used to identify the possible intruder in the network environment which can be further sub-divided into normal mode and attack mode. Under normal mode there is no action of attack. Here packet transfer between the nodes takes place randomly without any intruder act over them. Under attack mode, the three different attacks had been introduced to perform intruder attack over the system. These Intruders responsible for the drop of packets while transferring between the nodes. The next step is recovery process, where the intruder which has been detected in the detection phase should be isolated from the network. The intruders have no action in the network environment since it has been isolated as the individual victim. Now the network environment is free from the action of intruder and thus results in the secure communication. The different module which consists of detection and recovery phase are explained under as follows.

Detection Phase

Packets transfer (under normal mode): This process can be explained by considering 20 different wireless nodes in the network environment[6]. Each different node sends and receives the packets randomly. Each packet size is of about 512 kb. The communication range between different nodes exists as predetermined. This mode considered as normal mode, since each node while transferring data only there is a less number of chance that the packets drop in the intermediate. In normal mode also there is a packet loss but which is very small. This packet loss normally occurs in the wireless environment. Here it is considered there is no attacker. The packets which we sent from the source reaches destination but only minor loss. These can be verified by checking sent amount of packets with that of received packets and by plotting the graph using which gives details about network information, i.e., the number of packets sent and number of packets received between different nodes. From graphs also these details become clear.

Packets transfer (under attack mode): Packet transfer method can be explained by considering same 20 different wireless nodes in the network environment. Each different node sends and receives the packets randomly. Each packet size is of about 512 kb. The communication range between different nodes exists as predetermined. This mode considered as attack mode since there is more chances of the packets drop. The packets which we sent from the source reaches destination with major loss. These can be verified by checking sent amount of packets with that of received packets and by plotting the graph using which gives details about network information, i.e., the number of packets sent, number of packets received and number of dropped packets between different nodes. From graphs also these details become clear. In this method we introduced attacks in the network environment to check how an intruder acts as an attacker and allowing the packets to drop. The attack which we introduced are generally the inside attackers.

The three different attacks which are introduced as follows:

- Route Disruption
- Node Isolation
- Resource Consumption

Recovery phase

Recovery from attacks: Recovery from attacks can be explained by considering same 20 different wireless nodes in the network environment. Each different node sends and receives the packets randomly. Each packet size is of about 512 kb. The communication range between different nodes exists as predetermined. In this

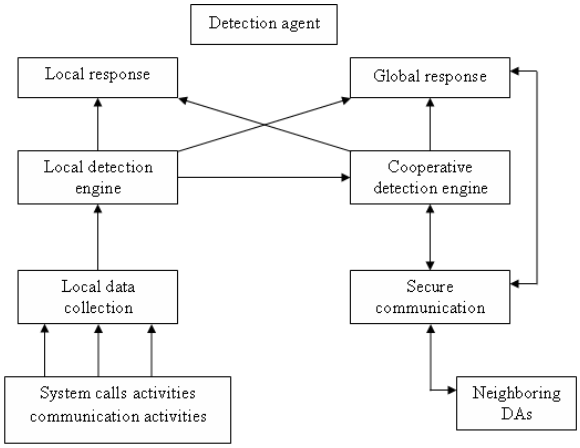

Fig. 1: A conceptual model of the system

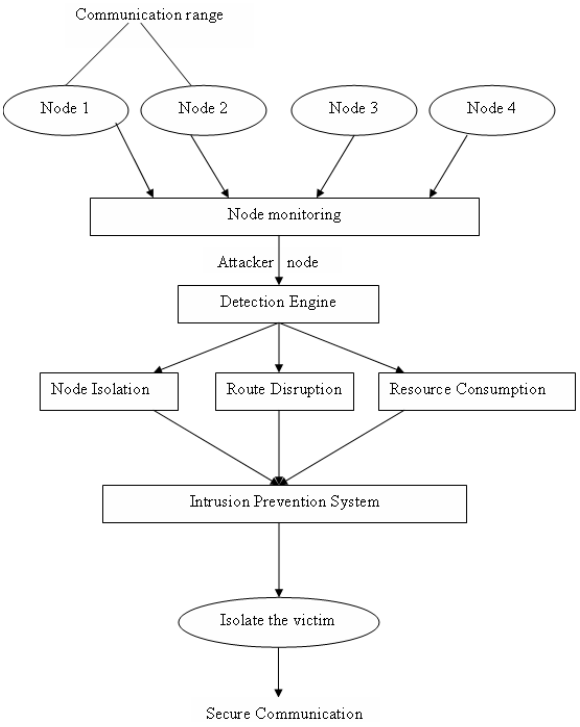

Fig. 2: Overveiw of the system

module, the node which has been detected as the intruder should be isolated from the network environment. Also the route which has detected prone to attack should be diverted from the normal path. Hence further possible attacks can be easily prevented.

System Architecture: The Fig. 1 shown below predicts a conceptual model of the system. The overall system architecture has been shown in Fig. 2. Over-all system

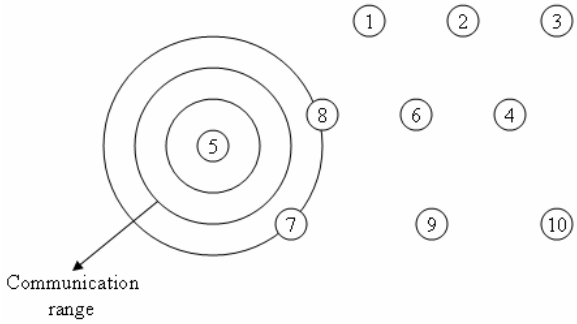

Fig. 3: Wireless node scenario

design includes different nodes of about 20. Each node can communicate with other nodes randomly and also based on the communication range. Nodes are positioned randomly in any order but are separated from other one.

Node monitoring: The different nodes positioned in the network environment are monitored by simulation setup. Each node setup sends packets based on the communication range and node connectivity. The transfer of packets between different nodes could be easily visualized under the simulation environment. The route discovery between the nodes for sending packets could also be easily visualized. Under normal mode, there could be less number of packets being dropped. Under attack mode, there could be more packet drop which could be easily identified. The Fig. 3 below shows the simple wireless topology of different nodes. Each small circle marked alphabetically shows each node and its position in the network environment. The big circle shows the communication range between the nodes.

Detection engine: The main work of the detection engine is to detect the intruder in the network environment. In general, the three different attacks considered in the wireless network are:

- Routing disruption attacks
- Node Isolation attacks
- Resource Consumption attacks

Routing disruption attacks: In a routing disruption attack, a malicious node intentionally drops control packets, misroutes data, or disseminates incorrect information about its neighbors and/or its pre-discovered routing capabilities to particular destinations. This is shown in Fig. 4. An attacker might try to:

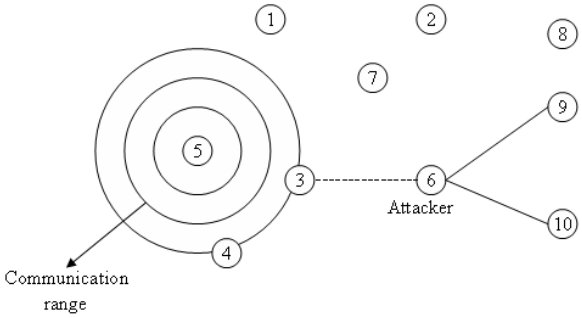

Fig. 4: Node disruption scenario

- Forge messages by spoofing originator or destination addresses
- Signal false route errors or modify route error messages
- Alter or replace originator, destination or sender addresses in routed messages

Node isolation attacks: Node isolation refers to preventing a given node from communicating with any other node in the network. It differs from Route Disruption in that Route Disruption is targeting at a route with two given endpoints, while node isolation is aiming at all possible routes.

Resource consumption attacks: In a resource consumption attack also known as resource exhaustion attacks, an attacker might try to consume network resources by:

- Initiating large number of route requests to bogus destinations in order to exhaust the resources of the network, or
- Playing the "gray hole attack" or "selective dropping" of packets, resulting in increased number of route requests from neighbor nodes that have limited routing capabilities, exhausting neighbors' resources.

Intrusion prevention system: In the prevention system, the node which has been identified as an attacker should be isolated from the network environment as shown in Fig. 5.

First there is a need to find in which route the attacker node is present or where the attacker node exactly located in the network environment by visualizing the network topology. The node that highly drops the packets, the node which disrupts the existing

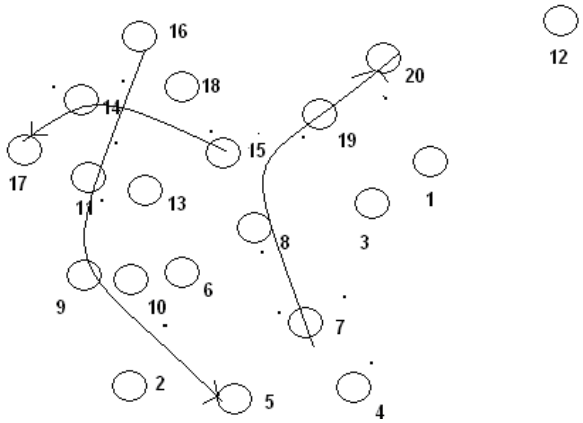

Fig. 5: Intrusion Prevention System - an example

route of packet transfer between nodes and the one which consumes more resources i.e., which by default receives more packets but not transferring the packets are generally said to be attacker. These nodes are pointed as attackers in the simulation environment and are isolated from the network topology. Thus prevents the action of attacker on the packet transfer.

In the Fig. 5, arrow line arrows represent the route discovery between the nodes; small circles represent the node position. The small black dots represent the transfer of packet between different nodes. Each packet is of size 512 kb. The route discovered between the nodes takes place randomly particularly for the transfer of packets. As the twelfth node found to be attacker it has been isolated from the victim. As the intruder been isolated from the network topology now the safer communication is possible between the nodes and the packet loss is reduced.

PERFORMANCE ANALYSIS

The simulation experiments are conducted on the ns2 platform. Consider a network in a 1000×1000 m square area with a fixed 20 mobile nodes. For each traffic flow, a source/destination pair is randomly selected from the node set and the transmission rate is 2 packets per second with a packet size of 512 bytes. A fixed 64-packet send buffer is maintained at each node for packets waiting for available routes. Some regarding simulation environment is given in Table.2.

An important property of a mobile ad hoc network is dynamic network topology. Since every node can move arbitrarily, the network topology changes from time to time and the communication links between mobile nodes break frequently. During the simulation, each node randomly selects a destination in the network

Table 1: Simulation Parameters

Parameters	Value
Simulation duration	100 seconds
Topology	1000m * 1000 m
Number of mobile nodes	20
Transmission range	250 m
Node Movement model	Random waypoint model
Traffic type	CBR (UDP)
Data payload	512 bytes

Table 2: Packets drop (Route Disruption Attack)

Under-Normal	Under-Attack
423	32
373	21
376	18
442	26
387	33
383	12
385	17
311	14

and moves toward the destination at a speed that is randomly selected from the range [0, maxspeed], where maxspeed represent node max movement speed. When the destination is reached, another destination location is chosen after a short pause. By adjusting the values of maxspeed and pause time, different network topologies can be simulated. To prevent all traffic flows start at the same time, each source node chooses a random start time of sending packets from the range of [0, stime], where stime is set to 10 sec.

Simulated attacks: Under Simulated environment, the three different attacks have been introduced and their corresponding actions in the network topology with packet losses are predicted in the following section.

Route Disruption (RD) attack: The action of Route Disruption is breaking of an existing route or preventing a new route from being established. Under this attack, due to breaking of existing route, dropping of packets occurs. By implementing this attack in ns-2, the packet drop at different stages can be predicted in a tabulated manner as shown in Table 2.

From the above table, under normal mode 8 different packet sizes are predicted and under attack mode the other packet sizes are predicted. First result shows 423 packets are sent under normal mode while under attack mode only 32 packets are sent, which clearly distinguishes the action of attacker from that of normal mode. The reduction in packet size could be easily understood which exactly depicts the action of RD-attacker over the system.

Node Isolation (NI) attack: The action of NI-attack is preventing a node from communicating with any other

Table 3: Packets drop (Node Isolation Attack)

Under-Normal	Under-Attack
751	91
614	56
724	218
734	181
810	174
759	212
580	112
577	124

Table 4: Packets drop (Resource Consumption Attack)

Under-Normal	Under-Attack
0	14603
5432	156712
3675	223156
2443	265481
3981	332145
2123	277451
3671	288165
9832	185457

node. Under this attack the node gets isolated from the network topology due to the action of attacker over the system. By implementing this attack in ns-2, the packet drop at different stages is predicted in a Table 3.

From the above table, the results of 8 different nodes attack are predicted. First result shows 751 packets are sent under normal mode while under attack mode only 91 packets are sent, which clearly distinguishes the action of attacker from that of normal mode. This attack though performing the of similar action of RI attack, from the above predicted values the difference in dropped packets is more compared to that of Route Disruption attack. The results have also been shown for other different nodes. The reduction in packet size could be easily understood which exactly depicts the action of NI-attacker over the system.

Resource Consumption (RC) attack: In RC attack, an attacker tries to consume more network bandwidth or storage space. Under this attack, the particular node consumes more bandwidth and also occupies more storage spaces without providing them to the other nodes. The results calculated for packets drop in this attack are shown in Table 4.

From the table action on 8 different nodes are predicted. First result shows 0 packets send in normal mode. Under attack mode 14603 packets have been predicted as sent packets. Actually, it consumes that much amount of packets under attack mode due to the action of attacker rather to be zero as in normal mode. So that huge resource it tends to occupy not providing to other nodes. Thus the resource consumption attack over the network nodes is predicted.

CONCLUSIONS

An approach for detecting and analyzing various attacks on MANET has been studied and performance is analyzed. These attacks have been performed using My-Aodv agent in ns-2 simulator. This My-Aodv agent is used to introduce attacks in the network topology. The particular node dropping the packets, diverting the route and consuming more resources have been detected by the proposed system. Also, a recovery procedure is discussed for the MANET under various attacks. The recovery has been provided by finding the attacker node and isolating that particular node from the network topology. It was shown that the performance of the proposed system increases significantly by measuring packet drops for various attacks.

In the future enhancement, simulation can be performed for some complicated attacks. The attacks such as Denial of Service (DOS) Man in the Middle could be performed using some security based cryptographic algorithms. Also as the future work, the recovery phase can be more concentrated. Recovery can be shown in the different way without isolation the attacker node, the action of attack can be reduced by using some sophisticated algorithmic techniques.

Also Mobile devices have less battery power and memory. In Addition the wireless environment is less secured, any one can intercept the message, and hence they require more security. The security of any system depends on its key management. If key is large, more secure. An Elliptic Curve Cryptography provides the same level of security for far less key sizes as compared to the traditional cryptosystems, but it is ideal for MANNET to provide security using ECC. An ECC approach reduces the node's limited resource utilization.

REFERENCES

1. Anand, R., Nachiketh R. Potlapally, 2006. A study of the energy consumption characteristics of Cryptographic Algorithms and Security Protocols. IEEE Trans. Mob. Comput., 5(2), pp: 128-143. doi: 10.1109/TMC.2006.16
2. Yang, H. Ricciato, F. Lu, S. Zhang, L. 2006. Securing a wireless world. Proc. of IEEE, 94(2): 442-454. doi: 10.1109/JPROC.2005.862321
3. Anjum, F. Das, S. Gopalakrishnan, P. Kant, L. Byungsuk Kim , 2005. Security in an insecure WLAN network. Int. Conf. Wireless Networks, Commun. Mob. Computing, Telcordia Technol. Inc., pp: 292-297. doi: 10.1109/WIRLES.2005.1549425
4. Karnik, A. Passerini, K. , 2006. Wireless network security: A discussion from a business perspective. Proceedings of wireless Telecommun. Symposium, Institute of Technology, New Jersey, April 28-30, 2005 pp: 261-267. doi: 10.1109/WTS.2005.1524796
5. Lim. Y, Schmoyer. T, Levin. J and H.L. Owen and, 2003. Wireless intrusion detection and response. Proceedings of the 2003, IEEE Workshop on Inf. Assurance, West Point, NY, June 2003, pp: 68-75. http://users.ece.gatech.edu/~owen/Research/Conference%20Publications/wireless_IAW2003.pdf
6. William, S., 2003. Cryptography and Network Security: Principles and Practices, 3rd Edition Prentice Hall, USA.