Sabale M. R, Prof. Kalavadekar P. N / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.1552-1555

Intrusion Detection System For Wireless Network

Sabale M. R[1], Prof. Kalavadekar P. N[2]
[1, 2] (Department of Computer Engineering, Pune University,

ABSTRACT

DOS (Denial-of-Service) attacks, and jamming are a threat to wire or wireless networks because they are at the same time easy to mount and difficult to detect and stop. I discuss intrusion detection system for wireless network in which each node monitors the traffic flow on the network and collects relevant statistics about it. By collaborating each node's. I able to tell if (and which type of) an attack happened on our network any wireless network open the possibility of misuse. However, this system closes the possibility for misuse. I discuss the impact of the misuse on the system and the provide security for each user.

Keywords **-** Global list, Local list, KDD, Distribution Detection, Node Monitor, Intrusion Detection System.

I. INTRODUCTION

Networks are protected using many firewalls, encryption software's and various network tools. But many of them are not sufficient and effective. Most IDS(intrusion detection systems) for ad hoc networks are focusing on either routing protocols or its efficiency, but it is fails to address the security issues. Sometime one of the nodes may be selfish, for example, it does not forwarding the packets to the destination, because of saving the battery power for future working. Some others may act malicious by launching security attacks like denial of service or hack the information. The main goal of the security service for wireless networks is to provide security services which are authentication, confidentiality, integrity, anonymity, and availability for users. This paper incorporates agents and data mining techniques to prevent anomaly intrusion in wireless adhoc networks. Home user present in each system collects the data from its own system and using data mining techniques to observe the local attack. The user in network monitoring the neighboring nodes and collect the information from neighboring to determine the co-ordination among the observed anomalous patterns before it will send the data. The goal this system was able to stop all of the successful attacks in an wireless adhoc networks and reduce the false alarm positives.

1.1 Vulnerabilities of Mobile Wireless Networks

The nature of wireless network environment makes it very vulnerable to an adversary's malicious attacks. First all, the use of wireless links renders the network susceptible to attacks ranging from passive to active interfering. In wired networks where adversary must gain physical access to the network wires or pass through several lines of defense at firewall sand gateways, attacks on a wireless network can come from all directions and target at any node. Damages can include leaking of main or secret information, message contamination, and node architecture. All of these mean that a wireless ad-hoc network will not have any clear line of defense, and each and every node must be preparing for encounters indirectly.

Second, nodes are autonomous units and which are capable for independently. That means the nodes with inadequate physical protection are receptive to being capturing, compromising, and hijacking. So Tracking down a particular node in a global large scale network cannot be done easily, The attacks by a compromised node from within the network are far more damaging and much difficult to detect. Therefore, nodes and the structure must be prepared to operate in which mode that do not trusts peer.

Third, decision-making in wireless networking environment is sometimes decentralized and some wireless network algorithms rely on the cooperative participation of all nodes and the structure of architecture. The lack of centralized authority means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms.

To summarize, a wireless network is vulnerable due to its features of open medium, dynamic changing network topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense.

1.2 The Need for Intrusion Detection

Intrusion prevention measures, such as encryption and authentication and various network security tool, can be used in ad-hoc networks to reduce intrusions, but difficult to remove them. For example, encryption and authentication cannot provide security wireless nodes, which often carry the private keys. Integrity checking using redundant information (from different nodes), such as which are being used in secure routing, also relies on the other nodes, which could likewise be weak link for sophisticated attacks. To secure wireless network applications, we need to add intrusion detection and powerfull techniques, and future research is necessary to add these techniques to the new environment, where original applications in fixed

wired network. In this paper, we focus on particular type of wireless network environment called ad-hoc networks and propose a new model for intrusion detection and response for this environment. I will first give a background detail on intrusion detection, and then give detail our new architecture.

1.3RelatedWork:

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The nature of wireless network that creates new vulnerabilities that do not exist in a wired network, and yet many of the proven security technique is be ineffective. So, the old or traditional way of protecting networks with firewalls and encryption and other security software is no longer sufficient. I need to develop new architecture and mechanisms to protect the wireless networks and mobile computing applications.

II. WIDS MODEL

2.1 DETECTION OF THE INTRUDER

The first process is the training process in which source sends the packet with events to all the nodes in the network to detect the intruder. This process is called as multicasting. For sending any data, before it sending the packets to all nodes, the source node first initiates the timestamp for the packets. Then this training process is stored as an initial event list 1(FIRST) in the source node. For receivers it receives the packets which contain the timestamp and send appropriate ACK replies. Then receivers store the received packets in their event list. Then after receiving all the packets from source. Receivers send the reply ACK .It is done by using multicast method. Intruder detection (ID) is done by checking the received ACK packets . This is done by the matching algorithm.

2.2 MATCHING THE LIST OF EVENTS

The basic of matching algorithm is to be match two lists of events is as follows: First we start from the first list and for each and every event (packet or channel idle) this will be try to find a matching event on the second list. Now we find is that for every packet on the first list we find it on the second one if the network worked fine otherwise, we need find a channel idle event if some problem like jamming or malfunctioning happened. Continuing the example above, we'd have transmitted packets on the first event list and channel idle (together with a high number of dropped packets) on the second one. Now we can find unmatched events on the second list at the end (for example if the first node was jammed), then we swap the 2 lists and run the matching algorithm again .Then the final output is a single list of events which combines of this two list. Jamming and channel failure have the same basic signature, but differentiate on their position in the event list. A few packets disappearing here and there are index of channel failures, while a sequence of disappearing packets is considered as jamming attack. Large number of non-consecutive channel failures is index of bad Quality of service. So all nodes participate in the detection process, we extend it in order to match more than one lists. The idea is to merge one list at a time with the result of the previous merge. In other words, we merge lists #1 and #2, and then we match the result with list #3, until we generate every list. We obtain in this way an final aggregated list of all events which available in the network in a given time frame. Here we need to notice here that a node might not overhear the traffic of every other node because of different range. We assumed that each node has relevant or original information to offer, but this is not always true.

The basic feature here is that the monitoring system is distributed means it do not running on single machine. A single station alone cannot tell if it is experiencing an attack or just a temporary network failure, and cooperation among all nodes is required for the nodes to understand what is going on our wireless network. Finally the event lists are shared among all nodes in the network.

Each and every node sends their evidences to each and every other node in the network. Every node executes the matching algorithm to generate the aggregated event list that they clear view of what happened in the network in the given time frame.

2.3 MULTICAST THE INTRUDER TO THE NEIGHBOURING NODES

The matching algorithm will working after receiving reply events from the each in the network. Then it compares events from the other nodes which are initiator. If anyone from the received ACK packets is not matched with list, then that particular node is the intruder to be found. Then the intruder is detected the IP address of the intruder is sent to the entire network by multicasting. Finally neighbor nodes receive the IP address of the intruder and store it in the event lists (local List) to prevent future attacks from that node in the network. The multicasting of the intruder address is done source address.

2.4 SENDING DATA TO THE DESTINATION

The data send process is done by dividing the selected text file into number of packets for transmission in wireless network. The data sending process is start after the source finds out an intruder free path. In the case of jamming/network malfunction, then the source waits till the network is restored, it starts the training process to find the intruders and if any detected as intruder, then it selects a path which free from intrusion. Then the path selection is done by the Dynamic Source Routing Protocol (DSR). The source sends the data

directly to the destination through the 'safe' path. Destination receives the data in the form of packets and checks for anomalies to detect any loss of data in the data due to intrusion.

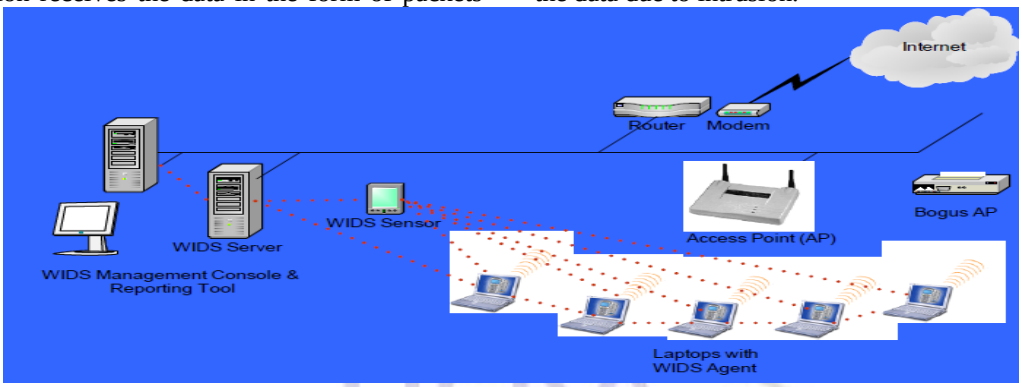

Fig.1 WIDS MODEL

III. DATA INDEPENDENCE AND DATA FLOW

A DFD provides no information about the ordering of processes, or about whether processes will operate in sequence or in parallel. There is quite different from a flowchart, which shows the flow of control through an algorithm, It allowing a reader to determine what operations will be performed, in which order, and under which condition, but not what kinds of data will be input to and output from the system, nor where the data will come from and go to, nor where the data will be stored (all of which are shown on a DFD). A data-flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. DFDs can also be used for the visualization of data processing or structured design.

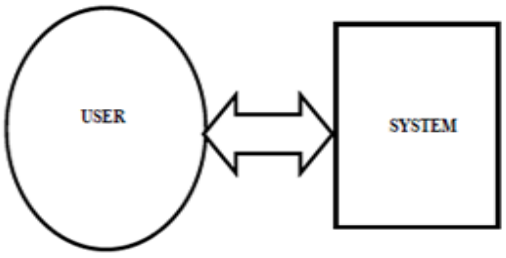

Fig.2: DFD 0Leval

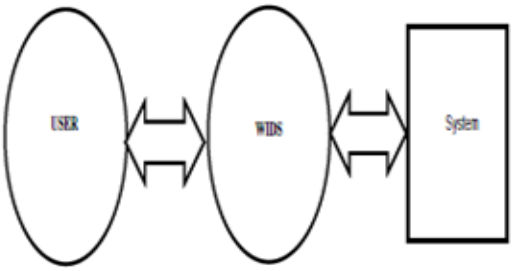

Fig 3. DFD 1 Leval

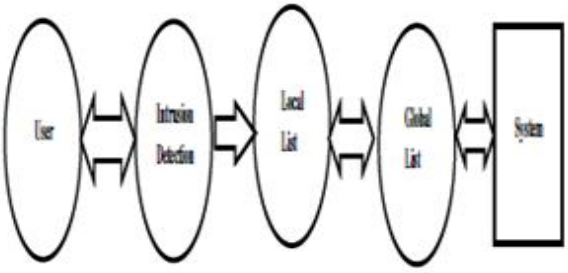

Fig. 4: DFD 2 Level

IV. RESULT AND DISCUSSION

Result of algorithm show the efficiency .Result showing data regarding the algorithmic efficiency parameters and comparative discussion related to efficiency of the algorithm proposed.

I propose a wireless network system made of many cells, with a given population, and with variable distribution of population into cells, ranging from uniform to very narrow Gaussian. I propose a percentage of cheaters varying from 10 to 35%. Cheaters coordinate their efforts: a single cell is assigned a value equal to its size (for example, a cell containing 60 users has a value of 60) and a weight equal to half of its size that cheaters must be the absolute majority in a cell to subvert it. This is an instance of the 0-1 knapsack problem, and results for its simulation are reported in Appendix A. The number reported as score is the sum of the values of all objects taken, in this case its the total number of affected users to whom the operator will have to pay the fee. What we can observe at first is that the results are independent from both the size of the cells and the number of population. From the results we obtain the following experimental relationship:

$m = 2(Pc+u)€$…….. (2)

where m is the amount of cheating, expressed as percentage of the users who get the fee. Pc+u epsilon , as this is the input range we used in the simulations.

Evolution of user population:

Under a cheating attack honest users are not immediately affected, as the operator might reduce its

QoS as a consequence of the fees it has to pay. This way its network will be even more undersized, with more problems and more honest users becoming cheaters. However, this trend cannot go forever as the operator will at some point shut the network down, giving no more service nor more fees back. I model the idea in this way: in our system we have a fixed percentage of cheaters, Pc, and a percentage of cheating users, Pc+u which depends on the QoS, x, as in equation 1. Equation 2 outlines the relation between the amount of cheating and the percentage of cheating users. Includes some useful equations that model the operators revenue, costs and fees. t is the number of users, k.1, k.2, k.3, k.4 and k.5 are all constants of proportionality. Costs are proportional to the number of users and the QoS, plus a fixed value 1. I can now calculate the the operators profit (gain) function, G, as G = income − costs − fees. Substituting the formulae, replacing t and y with their respective functions and using Equations 1 and 2 we obtain:\\

G = -(k.2)(k.5)(x.2) +[k.1 k.5 +2(k.4(1-Pc)] x - (k.3 +2 k.4) (3)

1 For example, the cost of governance licenses to provide the service which is a quadratic relation between the gain and the QoS, aimed towards bottom. x epsilon[0,1]. Since the y axis represents the operators gain, we can assume that the functions vertex represents a positive value of G and thus there are 2 intersections with the axis x. The functions maximum is

x = k.1 k.5 + 2 k.4(1 - Pc)*2 (k.2* k.5)

which is positive as all constants are positive. We can assume to have a profit when x=1. Also, when x=0 we have a profit of G = -k.3 - 2 k.4, thus a negative value. Given these characteristics of our function, we can say that the maximum is located either in our domain or at Xmas = 1. From here we can see that the operator tends to keep the QoS at maximum as it maximizes G. The cheaters impact will make the QoS decrease, thus making the number of unhappy users rise and operators gain decrease. If the gain approaches zero or goes below it, the operator can either shut the service down or operate in loss for some time to lower the number of unhappy users. The first choice is against cheaters interests as well, as I said they are interested in the service as well and not only on the fees. The second choice can be kept for a little time only, as the cheating level should lower after a while as it usually comes from a small number of real cheaters and a higher number of unhappy users .Where alpha is parameter which represent shape of cell.

Table I. Simulator result for 32 cells and 100 user.

Alpha	% Cheater	Score
0.1	0.1	193
0.1	0.2	395
0.1	0.3	594
0.1	0.4	788
0.5	0.1	195
0.5	0.2	388
0.5	0.3	880
0.5	0.4	771
1	0.1	190
1	0.2	380
1	0.3	566
1	0.4	755

V. CONCLUSION

IDS(Intrusion detection system) for wireless network based on distributed collection of relevant information, and showing that it will also detect different types of attacks like jamming, DOS(Denial-of-Service) etc. I also suggest a commercial use of the system, in order to provide a better service and security to customers. Anyway, their impact is limited: I showing that the operator will lower the quality of service under a certain threshold (as without such a system), otherwise unhappy users will take over and get a pay back. I also showing cheating users push too much, otherwise the system will go towards the total shutdown.

I achieve two goals:

first is detect more attacks and force the operator to give a decent service and second is allow cheaters to come into play, but their impact is self-limiting as a working network is needed for them to play.

REFERENCES

[1] Ethereal: a network protocol analyzer. http://www.ethereal.com.

[2] M. Aime and G. Calandriello. Distributed monitoring of wifi channel. Technical report, Politecnico di Torino, 2005.

[3] Y. an Huang and W. Lee. A cooperative intrusion detection system for ad hoc networks. In *SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 135–147, Fairfax (VA), USA, 2003.

[4] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *Proceedings of the 11th USENIX Security Symposium*, pages 15–28, Washington D.C, USA, 2003.

[5] M. Raya, J.-P. Hubaux, and I. Aad. Domino: A system to detect greedy behavior in ieee 802.11 hotspots. In *Proceedings of ACM MobiSys*, Boston (MA), USA, 2004.

[6] N. B. Salem, J.-P. Hubaux, and M. Jakobsson. Reputationbased wi-fi deployment. *SIGMOBILE Mob. Comput. Commun. Rev.*, 9(3):69–81, 2005.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57, Urbana-Champaign (IL), USA, 2005.

[8] Y. Zhang, W. Lee, and Y.-A. Huang. Intrusion detection techniques for mobile wireless networks. *WirelessNetwork.*