Wireless Intrusion Detection System Using a Lightweight Agent

Fariba Haddadi
Electrical and Computer Engineering Department
Yazd University
Yazd, Iran
f.haddadi@stu.yazduni.ac.ir

Dr. Mehdi A. Sarram
Electrical and Computer Engineering Department
Yazd University
Yazd, Iran
mehdi.sarram@yazduni.ac.ir

Abstract— **The exponential growth in wireless network faults, vulnerabilities, and attacks make the Wireless Local Area Network (WLAN) security management a challenging research area. Deficiencies of security methods like cryptography (e.g. WEP) and firewalls, causes the use of more complex security systems, such as Intrusion Detection Systems, to be crucial. In this paper, we present a hybrid wireless intrusion detection system (WIDS). To implement the WIDS, we designed a simple lightweight agent. The proposed agent detect the most destroying and serious attacks; Man-In-The-Middle and Denial-of-Service; with the minimum selected feature set. To evaluate our proposed WIDS and its agent, we collect a complete data-set using open source attack generator softwares. Experimental results show that in comparison with similar systems, in addition of more simplicity, our WIDS provides high performance and precision.**

Intrusion detection system; Wireless Local Area Network; Wireless network attacks; Security;

I. INTRODUCTION

Low cost of wireless networks and relative ease of use, cause organizations to invest in wireless networks as opposed to traditional LANs. Although so many attempts have been made to secure these networks, the technology is still highly insecure and susceptible to active and passive intrusions. Security methods like cryptography and firewalls do not satisfy user's needs. This causes the use of more complex security systems, such as Intrusion Detection Systems (IDSes), to be crucial.

Due to the long history of wired LANs, so many IDSes have been developed. Although the traditional wired-IDSes are powerful systems, unfortunately they do little for the wireless world. Different nature of the transmission medium, different protocol specification in lower layer, different lower layer functionality of intruders and users and etc. causes huge different in wired and wireless networks and also their intrusion detection systems[1].

In [2], a prototype implementation of a wireless intrusion detection and active response system is described. In [3] the author devised an innovative solution by developing a proactive wireless IDS by utilizing short message service (SMS) and proactive techniques. Yand et. al. in [4] focus on intrusion detection and security consideration in wireless local area networks. This paper propose a conceptual model for IDS agents. [5] present a novel approach based on multi channel monitoring and anomaly analysis of station localization, packet analysis and state tracking to detect wireless attacks. [6] discuss the major wireless attack categories concerning IEEE 802.11 family networks and propose a wireless IDS that can effectively handle these attacks.

As in wired networks, wireless intrusion detection systems can be classified in to anomaly detection and misuse detection. Misuse methods [7] detect attacks if their signitures match well-known predefined signatures. Anomaly based methods [8] label any traffic outside the present normal contour as an abnormal traffic.

Modeling normal behavior of a system, in anomaly IDSes, is so cumbersome due to its complexity. But in other hand, they are best suited to detect new attacks. Due to the predefined pattern of previous attacks, misuse IDSes are vulnerable to new ones. Hybrid IDSes take advantages of two previous systems to resolve their deficiencies.

In this paper we present a hybrid wireless-IDS. The proposed system can distinguish abnormal traffic and attacks. Also it is able to classify attacks into five major known types.

The paper is organized as follows: section 2, gives a brief overview of the most common security attacks in IEEE 802.11 networks. section 2, demonstrates the WIDS process. Section 3, evaluates the proposed system and at last, section 4, presents the conclusion of this work.

II. WIRELESS NETWORK ATTACK CATEGORIES

we classify the most common wireless network attacks in to five distinct categories: Network discovery attacks, Eavesdropping attacks, Impersonation attacks, Man-In-The-Middle (MITM) attacks and Denial-of-Service attacks[6,9].

A. *Network discovery attacks*

Wireless LAN discovery tools such as NetStumbler are designed to identify various network characteristics. Although the use of these tools in not characterized as a real attack, the derived information will be used later for launching a real attack against the network.

B. *Eavesdropping attacks*

This type of network attack occurs when an attacker monitors or capture network traffic in transit, and then interprets all unprotected data. Since all 802.11 packet headers are not encrypted and travel through the network in

978-0-7695-4042-9/10 $26.00 © 2010 IEEE
DOI 10.1109/ICCNT.2010.26

clear text format they can be easily read by potential eavesdroppers.

C. Impersonation attacks

This category of attacks considers aggressors trying to steal and imitate the characteristics of a valid user or most importantly those of a legitimate AP. The attacker would most likely trigger an eavesdropping or a network discovery attack to intercept the required characteristics from a user or an AP accordingly. Then, he can either change his MAC address to that of the valid user or utilise software tools like the well known HostAP [10] that will enable him to act as a fully legitimate AP.

D. Man-In-The-Middle attacks

The most advanced type of attack on a wireless or wired network is the "Man-In-TheMiddle" attack. The attacker attempts to insert himself as middleman between the user and an access point. The aggressor then proceeds to forward information between the user and access point, during which he collects log on information. As a result, the attacker can maliciously intercept, modify, add or even delete data.

E. Denial-of-Service attacks

A denial of service occurs when an attacker has engaged most of the resources a host or network has available, rendering it unavailable to legitimate users. More specifically, this sort of attack targets the availability of the network i.e. by blocking network access, causing excessive delays, consuming valuable network resources, etc.

III. OVERALL SYSTEM PROCESS

In fig. 1, we indicate the overall process of creating and testing our wireless intrusion detection system. Just as shown, we have three general phases: Data-set generation, IDS creation phase and test.

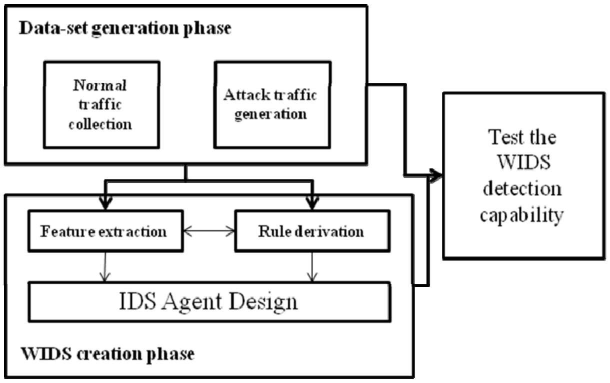
Data-set generation phase
Normal traffic collection
Attack traffic generation
Test the WIDS detection capability
Feature extraction
Rule derivation
IDS Agent Design
WIDS creation phase

Figure 1. Overall system process diagram

A. Data-set Generation Phase

DARPA project was expanded in MIT University in 1998 to provide IDS developers with a benchmark to compare their products [11]. Unfortunately, due to the considerable differences between wired and wireless networks, DARPA data-set can not be used for wireless networks.

Not having a popular benchmark, impel us to make a data-set consist of normal and attacks wireless traffic. To create this data-set, we used the Yazd university wireless network (fig. 2).

At the end of this phase, several files for normal and different attacks types will be created.

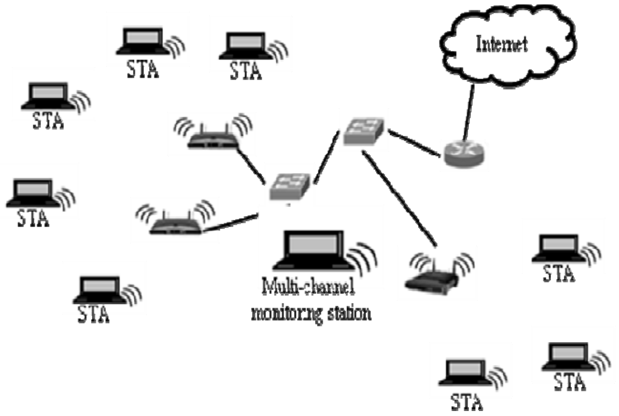

Figure 2. Wireless test bed at Yazd university

1) Normal traffic collection: To gather the normal traffic, we captured several hours of university users traffic in several days. We selected the hours and the days randomly to have a normal traffic collection as varied as possible.

2) Attack traffic generation: There are so many types of attack in wireless networks compare to wired networks. to generate these attacks, there are several softwares. Based on attack type and its generation method, the softwares should be used simply or in combination with each other. The attack types covered in this paper are: Man-In-The-Middle, Denial-of-Service, Impersonation, Eavesdropping. Table 1 show the attacks and some of their required softwares [12,13,14].

TABLE I. ATTACKS REQUIRED SOFTWARES

Attacks	Softwares
Network discovery	Netstumbler, Kismet, Airmon-ng
Eavesdropping	Wireshark, Kismet, Ethercap
Impersonation	AirJack, MonkeyJack
Man-In-The-Middle	Dsniff, Ethercap-NG
Denial-of-Service	Void11, Aireplay, FataJack

B. IDS Creation Phase

1) Principal Feature extraction and rule derivation: Considering the attacks creation methods and their functionality, in this step we extract a minimum set of feature that are required for intrusion detection. The selected feature set is shown in table 2.

TABLE II. SELECTED FEATURES SET

Feature's name	description
Frame Type/subtype	Frame types: management, control, data
Src. MAC Address	Source physical address
Des. MAC Addess	Destination physical address
BSS Id	The access point MAC address
Seq. #	Sequence number of the frame
Timestamp	Frame timestamp
Beacon interval	Interval between beacon frames
ESSID	The access point name
Channel #	Channel number[1 to 11]

2) IDS Agent Architecture Design: So many IDS agents have been designed so far. In this paper, we propose the most simple agent(fig. 3). Compare to its simplicity, our wireless IDS agent has a relatively perfect functionality with a great detection capability.

The network sniffer part of the agent, sniffs the traffic over wireless medium. Then it passes the sniffed packets to the detection engines (anomaly and misuse). Each of the engines analysis the packets, considering the principal extracted features and the network threshold that had been set based on a particular network specification (e.g. yazd university network).

The misuse detection engine, analysis the input packet via the signatures and the thresholds. If the attack is detected with adequate similarities compare to the rules, the engine call the alarm module to inform the network administrator.

The anomaly detection engine, analysis the inputs in order to find some anomalies due to the specific network normal behavior. As an example, consider the number of the Yazd university access points (X), the beacon frame intervals(Y sec.) and variation coefficient (Z%). In the normal behavior of this specific network, there is maximum (X/Y) + Z*(X/Y) beacon frame admissible per second. If the inputs beacon numbers per second go above this normal threshold, the engine should diagnose a beacon flood attack.

In both misuse and anomaly detection engine, if a series of inputs does not meet the needs of special attacks specifications or anomalies but it has some strong specification of them, the engines send it to the probable attack module for more precise examination.

The probable attack detection module collect the suspicious data. For every new entry, the module search in its database to find the previous related data, to see if a serious attack is going on or not.

If one of detection modules diagnose an anomaly or attack, they call the alarm module to inform the administrator. The alarm module has a very simple logging mechanism.

C. Test phase

Finally, in this phase, we used the data-set collected in the first phase to test the proposed wireless intrusion detection agent in phase two.

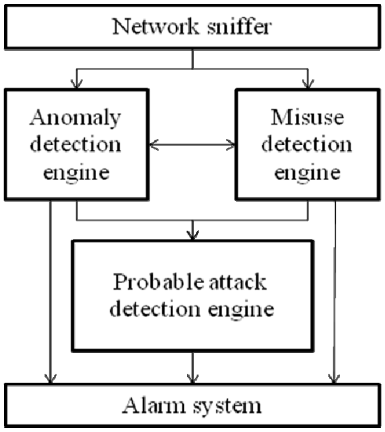

Figure 3. Wireless Intrusion Detection Engine Agent

IV. EXPERIMENTAL RESULTS

To evaluate and validate our proposed wireless IDS approach, we used the yazd university test bed (fig. 2) . The test bed consists of 3 access points includes different security methods in each environment. The test bed uses eight user machines acting as wireless stations (STA) generating normal and attack traffic.

The multi-channel monitoring station is an open suse-11.1 machine with powerful antennas, capable of monitoring all the wireless channels in use [1 to 11].

The wireless monitoring software used is the open source wireshark [13]. To generate a normal traffic, we replayed the captured normal traffic in data collection phase. Also we replayed the attack library that was collected in data collection process.

The main types of attacks that are supported in this project are: Man-In-The-Middle, Denial of Service, Impersonation and Network discovery. These are the most frequent and important types of attacks.

A. Results

Due to the wide range of attack types and their different specifications, we can not show each type separately in this section. As an example, in fig. 4 we showed a beacon flood attack from the DoS category. Considering the Yazd university network specifications, we used a threshold of 19 beacon frames per 30 second. The figure exactly illustrate that a beacon flood attack is happening in the network.

Because all the papers that proposed a WIDS, generate their distinct data-set, we can not compare our detection rate numerically. Compare to [6], our simple, lightweight proposed wireless IDS covers more attack types (table 3).

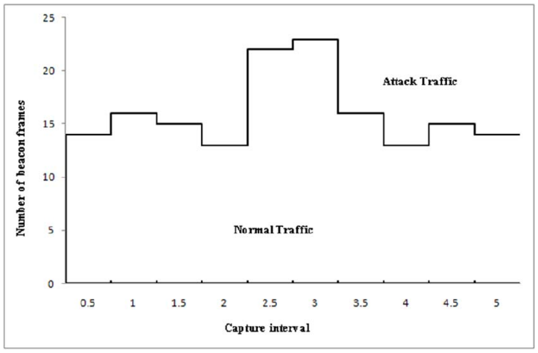

Figure 4. Number of beacon frames on all monitored channels per 30 seconds

TABLE III. RESULT COMPARISON TABLE

WIDS Attacks	[6]	Proposed WIDS
Network discovery	detected	detected
Eavesdropping	Not detected	Not detected
Impersonation	detected	detected
Man-In-The-Middle	not detected	detected
Denial-of-Service	detected	detected

V. CONCLUSION

The use of intrusion detection systems in wireless networks is a new approach in wireless security. Due to security protocol deficiencies, intrusion detection can be proved valuable. In this paper, we proposed a hybrid wireless intrusion detection system with the most simple agent. Our agent monitors the wireless network on multiple channels and uses three engines to detect different type of intrusions.

Considering the lake of a popular benchmark, we create a data-set which provides all major types of attacks. The analysis of the experimental results shows the accuracy and integrality of our wireless intrusion detection system in detecting attacks.

REFERENCES

[1] J. Dixon, “Wireless Intrusion Detection Systems including Incident Response and Wireless Policy” , unpublished.

[2] Y. X. Lim, T. Schmoyer, J. Levine, H. Owen, “Wireless Intrusion Detection and Response,” IEEE 4th Annual Information Assurance Workshop, West Point N.Y., June 2003, pp. 68-75.

[3] W.-C. Hsieh, C.-C. Lo, J.-C. Lee, and L.-T. Huang. " The Implementation of a Proactive Wireless Intrusion Detection System ", In The Fourth IEEE International Conference on Computer and Information Technology. CIT ’04. 14-16 Sept, pages 581–586, 2004.

[4] H. Yang, L. Xie and J. Sun, “Intrusion Detection Solution to WLANs” IEEE 6th CAS Symp**.** on Emerging Technologies: Mobile and Wireless Comm., pp.553-556, 2004.

[5] S.Fayssal, S. Hariri and Y. Al-Nashif, “Anomaly-Based Behavior Analysis of Wireless Network Security”, 4th annual International Conference on: Mobile and Ubiquitous Systems-networking and services,2007

[6] A. Tsakountakis, G. Kambourakis and S. Gritzalis, “Towards Effective Wireless Intrusion Detection in IEEE 802.11i”, 3th International Workshop on Security and Trust in Passive and Ubliquitous computing, pp.37-42, 2007.

[7] Y. M. Raya, J. P. Hubaux, I. Aad, “DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots” ACM MobiSys 2004, Boston USA, 2004.

[8] R Gill, J Smith & A Clark, “Specification- Based Intrusion Detection in WLANs”, 22nd Annual Computer Security Applications Conference, Miami, 2006.

[9] Ch. Barnes et.al., "Hack Proofing Your Wireless Network", Inc. Syngress, USA, 2002.

[10] Host AP driver for Intersil Prism 2/2.5/3, http://hostap.epitest.fi.

[11] MIT Lincoln Laboratory, The 1998 intrusion detection off-line evaluation plan, <http:// WWW.ll.mit.edu>, 1998.

[12] List of Wireless Network attacks –part 1, http://www.brighthub.com/computing/smb-security/articles/53949.aspx

[13] List of Wireless Network attacks –part 2, http://www.brighthub.com/computing/smb-security/articles/53950.aspx

[14] List of Wireless Network attacks –part 3, http://www.brighthub.com/computing/smb-security/articles/53951.aspx

[15] Wireshark [Website] 2007 April 10th available: http://www.wireshark.org