A Modular Approach for Intrusion Detection System in Wireless Networks

Tapas Badal
Department of Computer Science and Engineering,
Shri Shankaracharya Institute of Technology & Management,
Bhilai (C.G), India
tapasbadal@gmail.com,

Dipti Verma
Department of Computer Science and Engineering
Shri Shankaracharya Institute of Technology & Management,
Bhilai (C.G), India
diptiverma.sac@gmail.com

Abstract: The increasing reliance upon wireless networks has put tremendous emphasis on wireless network security. Intrusion detection in wireless network has become an indispensable component of any useful wireless network security system, and has recently gained attention in both research and industry communities due to widespread use of wireless local area network (WLAN). Although some intrusion prevention systems have recently appeared in the market, their intrusion detection capabilities are limited. This paper focus on detecting intrusion or anomalous behavior of nodes in WLAN's using modular technique. We explore the security vulnerabilities of 802.11, numerous intrusion detection techniques, and different network traffic metrics also called as features. Based on the study of metrics we propose a modular based intrusion detection approach.

Keyword- **Intrusion detection system*(IDS),* Signature based Intrusion Detection (SID), Anomaly based Intrusion Detection (AID)**

I. INTRODCTION

Wireless networks do not rely on a preexisting network infrastructure, and are characterized by wireless multi-hop communication. Unlike fixed wired networks, wireless networks have many operational limitations. For example, the wireless link is constrained by transmission range and bandwidth, and the mobile nodes may be constrained by battery life, CPU, and memory. Wireless networks are used in situations where a network must be deployed rapidly, without an existing infrastructure. Applications of wireless networks include the tactical battlefield, emergency search and rescue missions, as well as civilian ad-hoc situations, such as conferences and classrooms. Wireless networks are vulnerable to additional threats above those for a fixed wired network, due to the wireless communication link and the dynamic and cooperative nature of the routing infrastructure. The wireless link does not provide the same level of Protection for data transmission as a wired link, allowing adversaries within radio transmission range to make attacks against the data transmitted over the wireless link without gaining physical access to the link [1].

II. INTRUSION DETECTION SYSTEM (IDS)

Intrusion Detection is the process of monitoring computers or networks for unauthorized entrance, activity, or file modification. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack such as a denial of service attack [1]. There are two basic types of intrusion detection depending on the data collection mechanism - Host-based and Network-based. Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages. In short, host-based IDSs examine data held on individual computers that serve as hosts, while network-based IDSs examine data exchanged between computers. In addition, IDS may be classified based on the detection technique as described below [2, 3, 5].

There are generally two types of approaches based on the detection technique taken toward network intrusion detection: Misuse Detection also referred to as Signature based Intrusion Detection (SID) and Anomaly based Intrusion Detection (AID). In misuse detection, each network traffic record is identified as either normal or one of many predefined intrusion types. A classifier is typically then trained to discriminate one category from another, based on network traffic data. On the other hand, anomaly detection amounts to training models for learning normal traffic behavior and then classifying, as intrusions, any network behavior that significantly deviates from the known normal network traffic patterns. Therefore, anomaly detection techniques rely on a norm profile and consider a deviation of the subject's behavior from its norm profile as a symptom of an intrusion. Signature recognition techniques utilize intrusion

signatures profiles of intrusion characteristics and consider the presence of an intrusion signature as evidence of an intrusion. Anomaly detection techniques use only data of normal activities in information systems for training and building a norm profile. Signature recognition techniques rely on data of both normal and intrusive activities for learning intrusion signatures either manually or automatically through data mining.

However, signature recognition techniques have a limitation in that they cannot detect novel intrusions whose signatures are unknown. Anomaly detection techniques capture both known intrusions and unknown intrusions if intrusions demonstrate a significant deviation from a norm profile. Several types of anomaly detection techniques exist: string-based, specification-based, and statistical-based.

These model errors are called the inaccuracy in the behavior models. For example, a part of intrusive behavior model falls into normal behavior space. In addition, the intrusive behavior model cannot cover all intrusive behavior space, and the normal behavior model cannot cover all normal behavior space either. This is referred to as the incompleteness in the behavior models. In summary, there are two quality factors in every behavior models, namely inaccuracy and incompleteness. To build a practical intrusion detection system, it is critical to know the precise influence of these two quality factors on its performance [4].

Model Generalization and Its Implications on Intrusion Detection

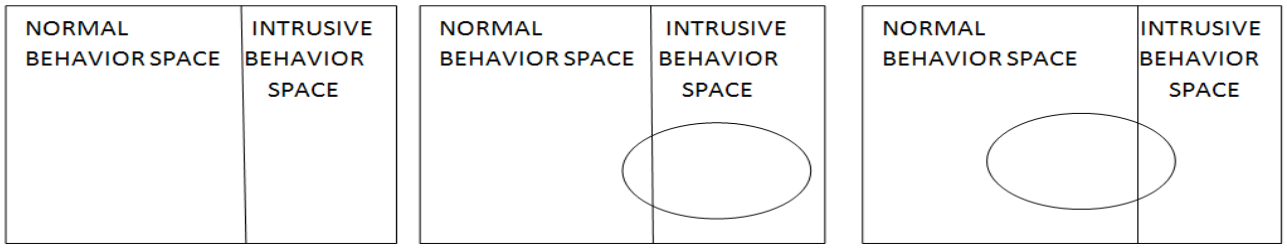

Fig.1 (a) Behavior spaces. (b) Intrusive behavior model. (c) Normal behavior model.

Conceptually, SID is only based on the knowledge of the intrusive behavior space, and AID is only based on the knowledge of the normal behavior space. Perfect detection of intrusions can be achieved only if we have a complete behavior model of any one of the two behavior spaces, because what is not bad is good and vice versa ideally.

Most of past research only credited the overall efficiency of an intrusion detection technique to such model generalization, and there is hardly any evaluation of

It is difficult to model such behavior spaces completely and correctly in reality. Figures 1(b) and 1(c) illustrate real behavior models for signature-based (i.e., intrusive behavior model) and for anomaly-based intrusion detection (i.e., normal behavior model). As the figures indicate, there exist model errors in the behavior models for SID techniques as well as AID ones.

Intrusion Signature

Intrusion signatures have been characterized as strings, event sequences, activity graphs, and intrusion scenarios (consisting of event sequences, their preconditions, and target compromised states). Finite state machines, colored Petri Nets, associate rules and production rules of expert systems have been used to represent and recognize intrusion signatures. Intrusion signatures are either manually encoded or automatically learned through data mining. However, signature recognition techniques have a limitation in that they cannot detect novel intrusions whose signatures are unknown.

III. SECURITY THREATS IN WIRELESS NETWORKS

A great deal has been published about previous research on specific security threats in wireless networks from different perspectives. In general, those threats fall into six basic categories [3, 7] as discussed below.

3.1 Interception *and unauthorized monitoring of wireless*

Traffic takes advantages of the open nature of wireless network in several different approaches.

• *War Drivers* [8] are attackers that drive around in a car with a specially configured laptop computer that has software such as Netstumbler [9] to identify wireless network characteristics, e.g. physical location, SSID and security mechanism. We can assume that it is still possible to identify a stumbler by looking for clients that constantly probe for networks but never join. It is also possible, however, to use a completely passive variant of Netstumbler. Use of Netstumbler alone may not be a danger that warrants any action from a wireless intrusion detection system.

• *Sniffing software*, e.g. Kismet [10], enables a war driver or other intruder to eavesdrop on all traffic data of wireless networks. An attacker could capture all the management data that are in plaintext in frame header and use them for further attacks. Even the encrypted data can be accumulated to crack WEP encryption. Detection of passive sniffing is almost impossible.

3.2 Encryption *attacks*

Encryption attacks in 802.11 networks are an extension of interception attacks and have been well-known almost ever since the beginning of the deployment of in 802.11 LAN's. Lots of early research has elaborated on the weakness of the algorithms used in WEP and its successor, WPA.

3.3 Jamming *an access point*

This a type of Denial-Of- Service attacks. Current research has shown that, not only do the Denial-of-Service attacks developed for conventional networks still work in a wireless network, but 802.11 networks themselves are extremely vulnerable to Denial-Of-Service [11]:

• *Radio Frequency interference*: An 802.11 network operates in the unlicensed 2.4 GHz and 5GHz bands and although the technology used was originally developed for the military to prevent jamming by an opponent, the current implementation is not immune to radio interference. A strong radio signal may still render an access points useless. To detect these kind of attacks it is necessary to monitor signal to noise ratios on a wireless network. Most network cards will allow you to collect information on signal strength and signal-to noise ratios.

• *Power saving attack*: Another misuse of a management frame, a Traffic Indication Map (TIM) message, can be used by the attacker to fool the client to enter a sleep state which was designed for power saving. This attack can be detected by similar sensor architecture as used in the previous attack.

• *Virtual carrier-sense attack*: An attacker could periodically claim a large duration field in a forged transmission frame to prevent other clients from gaining access to the channel.

• *Fake SSIDs*: Attacker deluges the air with beacons with fake SSIDs to make all access point busy on processing faked SSIDs. It is easy to detect but difficult to protect these types of attacks.

3.4 Insertion *attacks*

Insertion attack involves any attempts to make use of wireless network resource without prior permission. One typical example would be Internet bandwidth theft. Detection of unauthorized clients is complicated because it is easy to fake the address of a frame: the Media Access Control or MAC address. While authorization at a higher level can make the attacks more difficult, it is still possible to insert an unauthorized client by attacking an existing authorized connection (see: client to client attacks).

3.5 *Client-to-Client attacks*

These are effective attacks in wireless networks and are often ignored by designers of a wireless intrusion detection system. They seem to concentrate on protecting the internal information systems of the organization and ignore the enormous amount of sensitive information available on the clients.

An attacker can also spoof clients by pretending to be a legitimate access point after the connection with that access point has been established. Or it can spoof the access point by sending a De-authentication & Disassociation message to a client it wants to replace and hijack the session from this client. These are the most dangerous attacks that a wireless intrusion detection system will need to be able to detect with high accuracy to be an effective intrusion detection system.

3.6 Misconfiguration

This category of attack very often reduces the effectiveness of security mechanism of wireless networks. This is where Intrusion Prevention Systems are useful tools. In order to have the best usability most of wireless access points and routers disable all security mechanism by default. Unless administrators configure the security mechanisms correctly, wireless networks will be subject to attacks by almost anyone who is looking for free Internet access or who tries to hide his/her trail in any attempt at an e-crime. As many vendors provide web interface to administrate access points and usually set the common password by default, an intruder who has identified the vendor of an access point has a good chance to take control of that access point as well.

IV. MODULAR APPROACH FOR INTRUSION DETECTION SYSTEM

Although different taxonomy structures for WLAN attacks exist, it is usually acknowledged that taxonomy should be comprehensible to both security experts and personnel who are less familiar with security. One must strive to make it complete so that every observed attack fits somewhere in the taxonomy structure. In the existing approaches, attack categories must be mutually exclusive, i.e., the categories should not overlap, which facilitates better classification and prediction of future attacks.

Wireless Network Metrics are the measurable parameters or features that an intrusion detection system can use to model the various wireless attacks on the network as well as normal traffic. These features can add a strong layer of security to a WLAN. In addition to threat detection, merely letting people know that an IDS is in operation can add an element of deterrence and therefore, enhance security.

In our approach, we cluster wireless traffic data and use heuristic to label each instance as intrusive or normal. The heuristic used is the execution of modules for individual features in intrusion detection system in which we search for the specific features collectively defined an activity (i.e. pattern) followed by an attack. Then, we put these results of features in a table consist list of features with respect to MAC or IP address of a node (i.e. we maintain a check list for individual node), so we can calculate the intrusive behavior of a node rather than a particular attack.

Technique adopted for the detection of features is tabular in which we create a list of features vertically (as shown below in table no.1) and on the basis of detected features the alarm can be generate for the respective attacks (as shown below in table no.2). It is a reverse approach than the usual Intrusion Detection Systems in which they detect specific attacks. In the earlier, IDS two checks were needed for the same feature in two different attacks but in the

TABLE 1. POSSIBLE RELEVANT METRICS FOR CHARACTERIZING WIRELESS NETWORK ATTACKS

Loops/alternate routes	MAC Address	Class1frames RTS/CTS/ACK/POLL
Timeout for RTS	ARP/IP pair changes	NIC Vendor
3DES or RC4	packet leash	Deauth msg + spoofed msg
Frag headers	OUI	Reason Code
MAC list in AP	Broadcast SSID	Static/Dynamic IP
NIC in promiscues mode	IP address	SSL/Encryption in use/WEP
CCM Mode	Change of MAC allowed in	Antenna type
Switch/hub	NIC	VPN in use
TKIP	Sequence number of Client	Retry bit in control frame
M4C address overload	Sequence number of 4 P	spoofed disassociate msg
Signal/noise ratio	2-bit state (Unauth &	802.1x extensions in use
Adhoc Network	Associated)	Authentication attempts
PPP enabled	Buffer overflows allowed	

TABLE 2. POSSIBLE ATTACKS IN WIRELESS NETWORKS.

ATTACK TYPE	***ATTACK NAME***
Passive	War Driving Man-in-the-Middle Attack High Power amplifiers Dictionary attack- WPA
Masquerade	By passing Access control lists Disassociation ARP Poisoning MAC Based inference of -4CL Virtual carrier sense attack Authenticated user impersonation Invalid State Deauthentication
Replay	Packet Re-routing
Modify	Packet Alteration Packet Insertion
Denial of Service	Denial of Service RTS/CTS Flood Fragmentation Attacks Wormhole Attacks Network Injection Attacks Multiple virtual Access points

proposed modular approach there is only single check required to detect same feature in both attacks.

V. EXPECTED DELIVERABLES

Using modular approach an IDS can detect known attacks (i.e. signature of the attacks we know) by detecting the features of those attacks, also it can generate alarm for the unknown attacks which uses the same terminology as in the database because in this approach we are checking for the particular features so if a intruder changes its technique we can detect it by checking the feature list detected. Because we are using the network traffic analysis by placing sensors at access points and servers, we can detect the physical location of the intruder also by using some physical detection algorithm. The scheme proposed needs to be verified on real world wireless network traffic dataset.

VI. CONCLUSION

Since both SID and AID have problems of higher false alarm rate due to inappropriate threshold value to generate alarm for intrusion, an approach is needed that uses the combination of both of these techniques. In the modular approach, we are using the signature based detection approach by detecting the feature listed for known attacks as well as we are checking for the abnormal behavior through the table of features detected so the unknown attacks can be detected. Our study demonstrates the usefulness and promise of the proposed approach, laying the groundwork for a modular based framework for intrusion detection system.

REFERENCES

[1]. V.Gupta and S. Gupta.,"Experiments in Wireless Internet Security", Wireless Communications and Networking Conference, (WCNC 2002), IEEE Volume 2, pp.860 - 864 , 2002.

[2]. P.Brutch and C.Ko, "Challenges in intrusion detection for wireless ad-hoc networks," IEEE Proceedings on Workshop on Security and Assurance in Ad hoc Networks, 2003, pp368 - 373, Jan. 2003.

[3]. Tsakountakis, G.Kambourakis, S.Gritzalis, "Towards effective Wireless Intrusion Detection in IEEE 802.11i," in: Security, Privacy and Trust in Pervasive and Ubiquitous Computing, (SECPerU 2007), Third International Workshop, pp. 37-42, 2007.

[4]. Z. Li, A.Das and J.Zhou, "Theoretical basis for intrusion detection," Information Assurance Workshop, (IAW 2005), Proceedings from the Sixth Annual IEEE SMC, pp. 184 - 192, 2005.

[5]. N.Ye, SM.Emran, Q. Chen and S.Vilbert, "Multivariate statistical analysis of audit trails for host-based intrusion detection", Computers, IEEE Transactions on Volume 51, Issue 7, pp. 810 – 820, July 2002

[6]. M.Kiani, A.Clark and G.Mohay," Evaluation of Anomaly Based Character Distribution Models in the Detection of SQL Injection Attacks", in Availability, Reliability and Security, (ARES 2008), Third International Conference on Publication, pp. 47-55, 2008

[7]. Internet Security System technical paper, "Wireless LAN Security:802.11b and Corporate Networks," Oct. 23, 2001. [Online]. Available: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf. [Accessed: Sep. 15, 2008].

[8]. J. Duntmann's, "Wardriving FAQ- Jeff Duntemann's", April 2003. [Online]. Available: http://faq.wardrive.net/, [Accessed: Oct. 24, 2008].

[9]. NetStumbler.org WiFi Forums, [0nline]. Available: http://www.netstumbler.org/, [Accessed: SEP. 5, 2008]

[10]. Kismet, [Online]. Available: http://www.kismetwireless.net, [Accessed: SEP. 15, 2008].

[11]. C. Wullems, A. J. Clark and M. Looi, "A Trivial Denial of Service Attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANS", in proceedings of Second Wireless Telecommunications Symposium (WTS 2004), pp. 129-136., May 2004, IEEE Press.

[12]. S. Zhong, T. M. Khoshgoftaar and S. V. Nath, "A Clustering Approach to Wireless Network Intrusion Detection", in proceedings of the 17th IEEE International Conference on Tools with Artificial Intelligence (ICTAL'O5), PP. 54- 60, 2005.