An Integrated Scheme for Intrusion Detection in WLAN

Dong Phil Kim, Seok Joo Koh, and Sang Wook Kim

Department of Computer Science, Kyungpook National University
1370 Sankyuk-dong Buk-gu, Daegu, 702-701, Korea
{dpkim, sjkoh, swkim}@cs.knu.ac.kr

Abstract. Wireless Local Area Network (WLAN) is susceptible to security provisioning in spite of the solutions such as the Wired Equivalent Protocol (WEP) or IEEE 802.1x. This paper proposes an integrated scheme for intrusion detection in WLAN systems. The proposed scheme operates with one or more Gathering Agents (GAs) and a Master Server (MS). Each GA is used to get security information by collecting the frame packets in WLAN, whereas the MS is purposed to detect and prevent the various attacks by analyzing the packets in the WLAN systems. A detection engine contained in the MS employs OUI list matching for detection of MAC spoofing attacks, sequence number analysis for man-in-the-middle attacks, and Finite State Machine (FSM) analysis for Denial-of-Service (DoS) attacks. By experiments, it is shown that the proposed scheme could effectively detect and prevent the various attacks that could possibly be done in the WLAN systems.

1 Introduction

Wireless Local Area Network (WLAN) is one of the key wireless access technologies and has been rapidly spread out in the world-wide markets. One of the challenging issues on WLAN is the security problem. In particular, the security issue has so far been studied by many researchers, but the WLAN is still vulnerable to the promising attacks [1, 2, 3].

The WLAN basically has the broadcast nature in the radio transmissions, and thus anyone in the same network coverage may access to all the transmitted packets. It implies that the WLAN could be highly susceptible to security attacks. Furthermore, the security problem of WLAN has still been one of the key issues for commercial deployment, in spite of the existing solutions contained in the firewall or Enterprises Security Management (ESM). Some solutions have so far been proposed for the WLAN security management. Such security mechanisms include the Wired Equivalent Protocol (WEP) and IEEE 802.1x, and etc. The WEP and 802.1x cannot ensure to provide the complete detection/protection against a variety of promising attacks.

In this paper, we propose an integrated scheme for intrusion detection in the WLAN systems. We describe the architecture of the integrated mechanisms for intrusion detection in WLAN and show how the proposed scheme could

I. Chong and K. Kawahara (Eds.): ICOIN 2006, LNCS 3961, pp. 723–732, 2006.

detect the various promising attacks, and then discuss some experiments over the test networks. This paper is organized as follows. Section 2 describes the existing WLAN security solutions. In Section 3, we describe the proposed scheme for intrusion detection. Section 4 describes how to detect the various attacks by the proposed scheme. Section 5 discusses some experimental results for the proposed scheme over the test-bed networks. Finally, Section 6 concludes this paper.

2 Existing Security Solutions for WLAN

This section briefly reviews the security scheme defined in the 802.11 standard and the existing WLAN security solutions: Wired Equivalent Protocol (WEP) and IEEE 802.1x.

The open system authentication is the default authentication mechanism for 802.11. It operates in the simple two-step process. First, the station who wants to authenticate with another station sends an authentication management frame containing the identifier of the sending station. The receiving station then responds with a frame indicating whether it can recognize the identity of the sending station. The open system authentication is too much simple and thus rarely provides a high-level security [4]. That is, it is easier for an attacker to connect to the network and to launch the attacks.

On the other hand, it is assumed in the shared key authentication that each station has received a secret shared key through a secure channel, which is independent of the 802.11 networks. Stations perform the authentication based on the shared secret key. Use of the shared key here requires an implementation of the Wired Equivalent Privacy (WEP) algorithm [2, 6]. The WEP was designed to provide confidentiality for network traffic using 802.11. The details of the algorithm used for WEP are beyond the scope of this paper. Yet, the WEP has been reported that it is still vulnerable to security owing to the relatively short initial vectors and statically managed keys [2]. This leads to the attacker decrypting some portion of the 802.11 frames [7, 8].

The IEEE 802.1x [5] has been proposed for the port-based network access control, which is used to provide the network security for WLAN. It provides the centralized authentication of wireless clients with authentication servers such as RADIUS or DIAMETER. Since the 802.1x is used for denying unauthenticated network access, we can prevent the misuse of network resource from illegal users. However, 802.1x is still vulnerable to attacks, which take the availability of network resource, such as Denial-of-Service [7]. It cannot authenticate all the packets. Accordingly, it is possible for an attacker to place a hub between an 802.1x authenticating switch and a legitimate user for physical access to the wires [9].

To enhance the security of the WLAN, this paper proposes an integrated scheme for intrusion detection, which could be used to detect abnormal behaviors of the prospective malicious users by monitoring and analyzing all the wireless packets on the WLAN. The proposed detection scheme is designed to

characterize the various patterns of intrusions/attacks that could be done in the WLAN system.

3 The Proposed Scheme

In this section, we describe the proposed integrated scheme for intrusion detection. Figure 1 shows an overall architecture of the WLAN security system based on the proposed scheme. The system consists of gathering agent (GA) and master server (MS). The GA supports the real-time monitoring of the packets flowing in the WLAN system. It collects and analyzes the wireless packets for detecting the prospective attacks. In particular, the GA is used to monitor the current status on the stations by analyzing the 802.11 MAC frames.

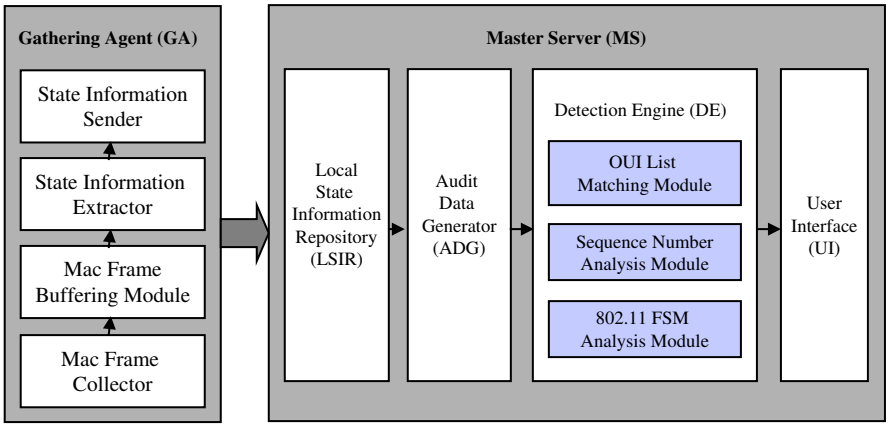

Fig. 1. Architecture of the proposed intrusion detection system for WLAN

With the analysis of those wireless packets, the MS will determine whether or not any attacks are intended in the WLAN systems. For this purpose, the MS provides the following four functions: Local State Information Repository (LSIR), Audit Data Generator (ADG), Detection Engine (DE), and User Interface (UI).

The LSIR stores the status information for the stations in the WLAN system by receiving the relevant frames from the GAs, and then forwards each data to the ADG. The ADG will analyze the packets to generate some audit data, and forward them to the DE. The DE consists of the following three detection modules: 1) OUI list matching, 2) sequence number analysis, and 3) 802.11 FSM analysis. Each module could be executed in the sequential order so as to detect the MAC spoofing, man-inthe- middle and Denial-of-Service attacks. As such, the intrusion detection will be performed in the integrated manner. If an attack is detected by the DE, it is informed to the UI, and further notified to the security officer.

The GA in the proposed scheme is used to support status monitoring between the wireless client terminals and an AP. The GA collects the MAC frames by using the MAC Frame Collector (with a wireless NIC) supporting RFMON mode, and then delivers the collected packets to the MAC Buffering Frame module. The MAC Buffering Frame module will take only the frames associated with management. It is noted that the management frames are purposed to establish communications between stations and AP, and thus to provide services for association establishment and authentication. Accordingly, a GA could extract the state information from those management frames.

The state information for AP is taken from Beacon and Association Response frames, the information for wireless client terminal could be taken from Probe Request, Authentication and Association Response frames. The state information for an AP includes the MAC address, SSID, available channels, transmission rates, and the number of the wireless client terminals associated with the AP. On the other hand, the state information for wireless client terminal includes the MAC address, SSID, available channel, encryption scheme, the delivered packet count and the current connection state. The GA will forward such state information to the MS.

3.1 Intrusion Detection

The master server (MS) determines whether or not any attack is being intended in the WLAN system. The received state information is stored in the Local State Information Repository (LSIR). Audit Data Generator (ADG) then generates the audit data for deciding whether or not the attack is being progressed. The ADG uses the MAC address and current connection state and transmitted packet counts from the state information for each station. Such the audit data will be forwarded into the Detection Engine (DE). The DE consists of the following three modules: OUI list matching, sequence number analysis, and 802.11 FSM analysis modules.

3.1.1 OUI List Matching

The OUI list matching module can be used to detect the conventional MAC spoofing attack. The stations on WLAN communicate each other by using the MAC addresses. It is noted that the MAC addresses could be used as a unique layer 2 identifier for the station in the WLAN. In the proposed scheme, the OUI list matching function uses such an OUI list so as to evaluate all source MAC addresses on the network. In the scheme, the detection of using a wrong prefix (which has not been allocated yet by the IEEE) can be reported as an anomalous activity.

3.1.2 Sequence Number Analysis

The sequence number analysis module is used to provide the protection against the man-in-the-middle attack, in which a rogue client may try to steal a real client MAC address and then to associates with the access point. The sequence number analysis module can be used to detect this kind of attack.

It is noted that the sequence number field in the MAC frame is a sequential counter that is incremented by one for each frame, starting at 0with a modulo of 4,096. Thus, it is unlikely that the MAC frames from the two different stations have the same sequence number [9]. By monitoring the sequence numbers in frames, we can detect the man-in-the-middle attack that is subject to the faked frames or illegally injected frames.

In the proposed scheme, the sequence number analysis function will compare the sequence numbers of the recently received audit data frames. If the gap of the sequence numbers between two consecutive frames is greater than two, the current audit data might be reported as an anomalous frame by the man-in-the-middle attack. Otherwise, the frame will be passed to the next step, the FSM analysis module, as described below.

3.1.3 FSM Analysis

The Finite State Machine (FSM) analysis is already employed to keep track of the status of a station in the 802.11 standard, in which the three states are defined for a station: listen, authentication, and association. In this paper, we design the FSM analysis module by extending the three states into the seven ones. The proposed FSM module can be used to provide the protection against the Denial-of-Service (DoS) attack, in which an attacker may try to exhaust most resources of the host or network, and thus render them unavailable to the legitimate users.

In general, an FSM progresses a system through a sequence of pre-defined states by transitions from one state to another. A transition occurs in response to events. In this paper, we redefine the FSM of 802.11 in terms of the connection states and generated events, as described in Table 1. As described in Table 1, we define the seven states for the proposed scheme. The LISTEN state is the starting point for the connection between AP and client terminals. Both AP and client terminals perform the authentication steps so as to verify each other. At this time, the states enter the AUTHENTICATION_REQUESTED and AUTHENTICATION_ESTABLISHED. They then try to establish an association by using the management frames. At this time, the states enter the ASSOCIATION_REQUESTED and ASSOCIATION_ESTABLISHED. If the connection is terminated gracefully, the state goes into CLOSED. Otherwise, the connection is abnormally terminated, the state will be in FAILUED.

The seven events used for transition of states in the FSM model are as follows:

P_0 : this event is generated when the AP broadcasts Beacon frames;
P_1 : this is generated when the station sends Probe Request frames, and receives Probe Responses from the AP;
P_2 : this is generated when the AP replies with Authentication frames for authentication;
P_3 : this is generated when the client terminal requests an association to the AP by sending an Association Request frame;
P_4 : this is generated when the AP agrees to open a connection for the terminal by sending an Association Response frame;

Table 1. Description of states for the proposed FSM analysis

Symbol	State	Description
L	LISTEN	All connections must start in a Listen state.
T1	AUTHENTICATION_REQUESTED	When the first Probe Request and Probe Response are sent, the connection is in the AUTHENTICATION_REQUESTED.
T2	AUTHENTICATION_ESTABLISHED	If the Authentication frame is sent and AP authenticates station,the connection is in the AUTHENTICATED_ ESTABLISHED.
H	ASSOCIATION_REQUESTED	When the Association Request is sent, the connection is in the ASSOCIATION_REQUESTED.
A	ASSOCIATION_ESTABLISED	When the Association Response is received, connection enters ASSOCIATION_ESTABLISED.
C	CLOSED	When the Deauthentication or Diassociation is sent, the connection is in CLOSED.
F	FAILED	When the Deauthentication/ Diassociation/Probe Request are sent more than Threshold, the connection is in FAILED.

P_5 : this is generated when the connection fails to authenticate by a Deau then authentication frame;
P_6 : this is generated when the connection enters the FAILURE state;
P_7 : this is generated when the number of frames transmitted is greater than the prespecified threshold in the fixed time interval;
P_8 : this is generated when the connection is terminated and goes into the LISTEN state.

Figure 2 illustrates the expected state transition diagram by the proposed FSM model, which is based on the states and events described above.

4 Detection of Attacks by the Proposed Scheme

This section describes how to detect any attacks with the help of the proposed schemes

4.1 MAC Address Spoofing

The OUI list matching module has already been equipped for some of the commercial products to detect the MAC spoofing attack. A malicious attacker may perform the MAC spoofing attacks by randomly generating the MAC addresses. The system may keep the OUI list for state monitoring, and the OUI list matching algorithm works well against the MAC spoofing attack.

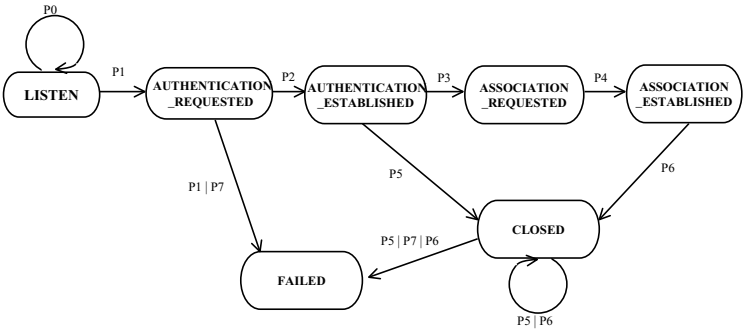

Fig. 2. Finite state transition for WLAN

4.2 Man-In-the-Middle Attacks

The man-in-the-middle attack will be done by a malicious user to inject invalid traffic during an association between an authenticated user and AP. To detect the man-inthe- middle attack, the sequence numbers of the MAC frames are analyzed. It is noted that the sequence number appears out of order when a man-in-the-middle attack is being made from injection of invalid traffic. For example, if an AP is assumed to start an association with a client station with 2,091. The next sequence number would be 2,092. The sequence number analysis module is invoked to detect the difference of the sequence numbers between the frames transmitted. Once an attack is initiated, the gap of the consecutive frame sequence numbers would be grater than two.

4.3 Denial-of-Service Attacks

A malicious node can deplete the resource of the network by transmitting a large of packets. The proposed system will detect this attack by measuring the total number of packets received from each node. If this count (total number) exceeds a pre-specified threshold, then an alert for the DoS attack is signaled. The threshold for the DoS attack may be configured from the experimentation. In the proposed FSM analysis, the FAILED state is considered as anomaly activity. For an example, the DoS attack based on the Disassociation or Deauthentication frames could be triggered by the P_6 or P_7 event for one station. For example, a system administrator might set the threshold for P_7 to be 40 frames per minute. In this case, if the number of the frames transmitted by the same source is more than 40 over one minute, then the P_7 event will be triggered.

5 Experimental Results

In this section, we describe some experimental results of the proposed scheme for intrusion detection. To perform the experimentation, we have implemented the gathering agent (GA) for frame monitoring and master server (MS) for detection of attacks.

5.1 Test Scenario

To experiment the proposed scheme for intrusion detection, we construct a small testbed, as shown in Figure 3, which consists of an AP and two mobile stations. For the test purpose, we have also employed GA, MS and three kinds of attackers on the testbed. For the attacker 1, Wellenreiter is used for MAC spoofing attack, and for the attacker 2 the WLAN-JACK is used for the man-in-the-middle attack, and the NetStumbler is used for the DoS attack.

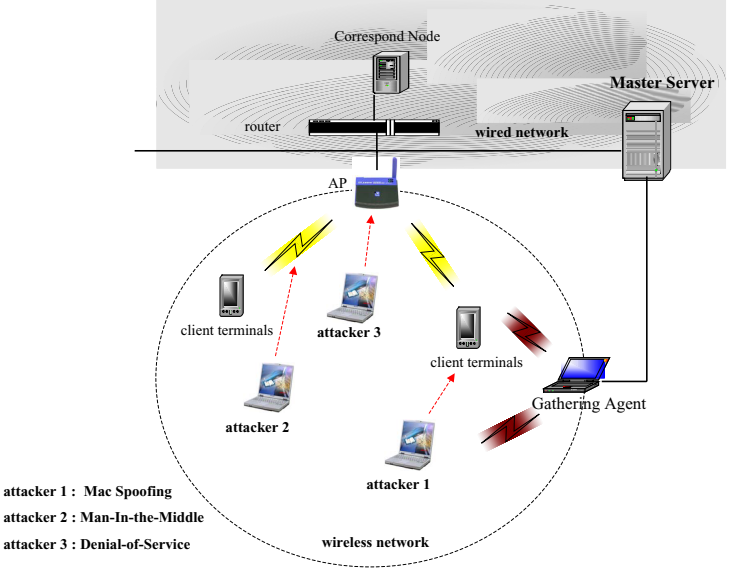

Fig. 3. Test environment for experiments

In Figure 3, the attacker 1 using Wellenreiter generates the random MAC address values ranged between 0x000000 and 0x00FFFF for the OUI portion (3bites) and then prepends a prefix value of 0x00 so as to avoid generating the MAC addresses conflicted with the reserved and multicast address space. In WLAN-JACK, it is assumed that attacker 2 monitors a pattern of legitimate sequence numbers. Attacker 2 identifies the Deauthenticate frames and then sends some spoofed Deauthetnicate frames over the broadcast address. Attacker 3 using NetStumbler sends Probe Request frames in order to identify AP, and then launches the DoS attacks.

5.2 Results and Discussion

To evaluate the proposed system, we measured the following performance metrics:

1) Hit Ratio (HR)

Hit Ratio is defined as the percentage of attacks correctly detected by the system over the total number of attacks down.

2) False Positive Ratio (FPR)

False Positive Ratio is defined as the percentage of the false positives (incorrectly) detected over the total number of attacks detected.

The HR can be used as a measure to see how effectively the proposed system could detect the various attacks. The FPR can be used to determine how much incorrectly the proposed system is performed.

Figure 4 and 5 show the results of HR and FPR, as the number of attacks taken increases for the three kinds of attacks, respectively. In the figures, the non-zero FPR is observed because the gathering agent cannot collect all the transmitted packets and thus the detection engine cannot process them. Overall, it is shown in the figures that the proposed system can effectively detect all kinds of attacks with a high Hit Ratio and a low False Positive Ratio.

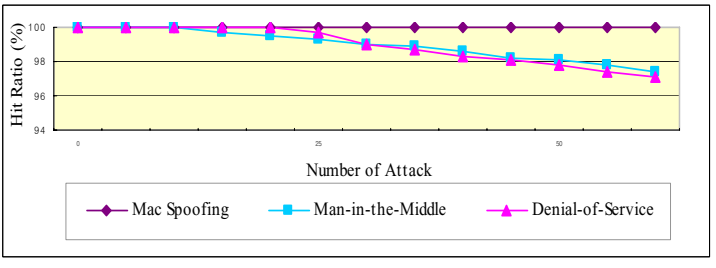

Fig. 4. Hit Ratio by the proposed scheme

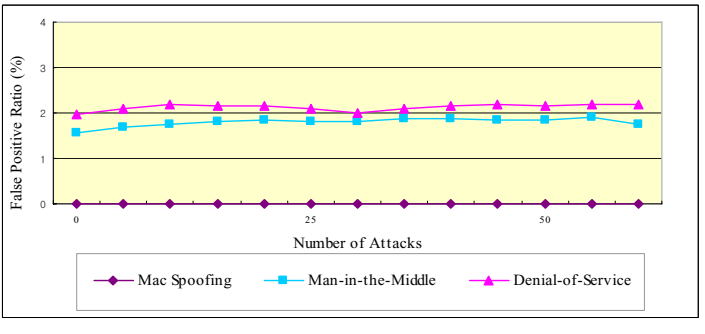

Fig. 5. False Positive Ratio by the proposed scheme

6 Conclusion

In this paper, we proposed a new integration scheme for intrusion detection for the WLAN system. The proposed scheme can be used to detect the various types of attacks such as the MAC spoofing, Man-In-the-Middle, and DoS attacks. From the experimental results, it is shown that the proposed scheme can effectively detect the promising attacks with high Hit Ratio and low False Positive Ratio.

Acknowledgment

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment).

References

1. IEEE 802.11 Standard, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, 1997.
2. Fluhrer, S., Mantin, I., and Shamir. A., Weakness in the Key scheduling Algorithm of RC4, Proceedings of the 8th Annual Workshop on Selected Areas in Cryptography, August 2001.
3. Lim, Y., Schmoyer, T., Levine, J., and Henry, L., Wireless Intrusion Detection an Response, Proceedings of the IEEE Workshop on Information Assurance, 2003.
4. IEEE Draft P802.1X/D11. Standards for Local and Metropolitan Area Networks: Standard for Port based Network Access Control, March 2001.
5. Arbaugh, W., Shankar, N., Y. Wan, An initial Security Analysis of the IEEE 802.1X Standard, Technical Report, Department of Computer Science, University of Maryland, 2002.
6. Wright, J., Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection, Available from http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf
7. IEEE OUI and Company_ID Assignments, Available from http://Stanard.ieee.org/regauth/oui/oui.txt
8. Wright, J., Detecting Wireless LAN MAC Address Spoofing, Available from http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf
9. Hennie, H., Finite-State Models for Logical Machines, John Wiley & Son.