Towards effective Wireless Intrusion Detection in IEEE 802.11i

Alexandros Tsakountakis, Georgios Kambourakis and Stefanos Gritzalis

Laboratory of Information and Communication Systems Security
Department of Information and Communication Systems Engineering
University of the Aegean, Karlovassi, GR-83200 Samos, Greece
Tel: +30-22730-82246
Fax: +30-22730-82009
Email:{atsak, gkamb, sgritz}@aegean.gr

***Abstract*— The proliferation of wireless devices and the availability of wireless applications and services constantly raise new security concerns. Towards this direction, Wireless Intrusion Detection Systems (WIDS) can assist a great deal to proactively and reactively protect wireless networks, thus discouraging or repealing potential adversaries. In this paper we discuss the major wireless attack categories concerning IEEE 802.11 family networks and in particular the latest 802.11i security standard. We elaborate on 802.11i specific attacks and experimentally explore how these outbreaks can be effectively mitigated or thwarted by a properly designed WIDS. Among specially crafted software for both WIDS's modules as well as for attack generators, our test-bed embraces the majority of well known open source attack tools. Test results show that the proposed WIDS modules are able to effectively detect, either directly or indirectly, most attacks.**

***Index Terms*—** Wireless Intrusion Detection Systems; IEEE 802.11i; Wireless network attacks; Wireless security.

I. INTRODUCTION

Whereas IEEE 802.11 family networks [1] present security deficiencies, they manage to highly penetrate into the wireless market in a great degree due to their low cost, easy administration, great capacity, IP-oriented nature, etc. Specifically, as often happens with every new technology, WLANs have been criticized a lot concerning their ability to provide security equivalent to that we know from our experience with wired networks. To cope with the demand for security, IEEE focused on the creation of security protocols that would co-work with WLANs standards and provide the required level of security. In fact, security in wireless networks was considered to be deficient ever since its advent. Wired Equivalent Privacy (WEP) [2], as the first security protocol created by IEEE quickly proved to be insufficient. Several studies [3-5] have attested that none of the three security goals, data confidentiality, access control and data integrity, are achieved by WEP at least in the required level. Meeting urgent industry demands, a subset of the 802.11i standard, namely WPA (Wi-Fi Protected Access), was shaped in order to mitigate the flaws found in WEP. Currently, IEEE 802.11i [6] also known as WPA2, is the latest security standard that promises enhanced security. IEEE 802.11i introduces the concept of RSNA (Robust Security Network Association) used for access control, utilizes CCMP (Counter–mode / CBC-MAC) protocol for data confidentiality and data integrity. Although, 802.11i is considered better and more robust, in terms of security, than its predecessors, several flaws and weaknesses have been already exhibited [7-9].

Since the first line of defence for the wireless networks seems insufficient to meet current and future security demands, a second line of defence would be appreciated. This second line of defence refers to the utilization of Wireless Intrusion Detection Systems (WIDS). As with wired networks, WIDS will co-exist with the security protocols assisting in enhancing the total security.

Whilst much work has already been done on 802.11i as well as on wireless intrusion detection systems in general [10-17], to the best of our knowledge a little or no effort is targeting on 802.11i intrusion detection systems explicitly. In this context, the objective of our contribution is twofold. First of all, the cardinal wireless network attack categories are analysed focusing on 802.11i. In this part we also investigate the possibilities to design special WIDS modules to tackle 802.11i specific attacks. Secondly, we experimentally evaluate our 802.11i enabled WIDS modules, which have been embedded in a real word WIDS, namely WIDZ (http://www.loud-fat-bloke.co.uk). Tests were performed utilising the majority of well known open source attack tools and custom attack generators.

The rest of the paper is organized as follows. Section II classifies and gives a brief overview of the most common security attacks triggered against 802.11 realms. Attacks from every category will be studied according to the way 802.11i treats them. Possible solutions towards designing effective WIDS for 802.11i will be discussed in the next section. Section IV evaluates our 802.11i enabled WIDS components presenting the results derived from a properly designed test-bed that considers 802.11i specific attacks. Finally, section V offers concluding thoughts and future directions for this work.

II. WIRELESS NETWORK ATTACK CATEGORIES AND 802.11i

The In the following, we classify the most common wireless network attacks into 6 distinct categories: (a) Network discovery attacks, (b) Eavesdropping/Traffic analysis, (c) Masquerading/Impersonation attacks, (d) Man-in-

Third International Workshop on Security
Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007)
0-7695-2863-5/07 $25.00 © 2007 IEEE

the-Middle (MITM) attacks, (e) Denial-of-Service (DoS) attacks and (f) IEEE 802.11i specific attacks.

A. Network discovery attacks

Wireless LAN discovery tools such as NetStumbler (http://www.netstumbler.com) are designed to identify various network characteristics, i.e. the MAC address and Service Set Identifier (SSID) of the Access Point (AP) as well as its vendor, the communication channel and most importantly the security protocol used by the network. Although the use of these tools in not characterized as a real attack, it aims at discovering as much useful information about the network as possible. The derived information will be exploited later on for launching a real attack against the network. This technique is also well known as Wardriving. Tools such as Netstumbler rely on the utilisation of probe request frames to detect wireless networks. If an AP comes in range of a client, he responds to the probe request frame by a probe response frame making it visible. On the other hand, tools like Kismet (http://www.kismetwireless.net) employ passive network surveillance to detect wireless networks. Network discovery is actually a normal part of 802.11 protocols. It is meant to allow client devices to discover APs and available wireless networks in range. Since it is not regarded as an attack or a malicious activity, 802.11i does not include any mechanisms to combat network discovery tools.

B. Eavesdropping/Traffic analysis

Eavesdropping and traffic analysis attacks allow the aggressor to monitor, capture data and create statistical results from a wireless network. Since all 802.11 packet headers are not encrypted and travel through the network in cleartext format they can be easily read by potential eavesdroppers. Weak encryption mechanisms due to several protocol flaws (WEP) or poor secret key administration policies may disclose valuable parts of the rest of the 802.11 packets. Of course, the introduction of 802.11i has provided a strong encryption mechanism that is physically impossible to break. In systems protected by 802.11i, only limited information is available to eavesdroppers including the communication channel as well as the AP's and client's MAC address. The most widely used software in this category is Airopeek (http://www.wildpackets.com).

C. Masquerading/Impersonation attacks

This category of attacks considers aggressors trying to steal and after 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 (http://hostap.epitest.fi) that will enable him to act as a fully legitimate AP. The same attack is also known as Rogue AP aiming primarily at controlling the traffic inside the network, thus making eavesdropping easier for the aggressors. In the worst case scenario this kind of attack enables the attacker to gain authentication credentials simply by waiting for a user to authenticate himself to the Rogue AP. This attack can be also used as a part for launching a MITM attack. In this context, the AirJack (http://sourceforge.net/projects/airjack) and MonkeyJack (http://www.wikipedia.org/monkeyjack) software tools are most commonly used to launch a masquerading/ impersonation attack. However, this sort of attack should no longer be considered a real threat to wireless networks. A network protected by 802.11i using RSNA provides mutual authentication as well as strong authentication credentials that normally an attacker would never be able to obtain.

D. Man-in-the-Middle attacks

A successful MITM attack will place the attacker into the data-path between a user and an AP or between two users' devices in ad-hoc mode. As a result, the attacker can maliciously intercept, modify, add or even delete data, provided he has access to the encryption keys. Likewise to masquerading/impersonation attacks, this outbreak is considered infeasible to perform in a network protected by 802.11i, provided that the latter utilises RSNA and a proper implementation of EAP methods [18].

E. Denial-of-Service attacks

The main goal of Denial-of-Service (DoS) attacks is to inhibit or even worse prevent legitimate users from accessing network resources, services and information. 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. DoS attacks comprise a serious threat for any wireless network because the management and control frames employed by the network are not protected. This means for example that an attacker can flood an AP or a user's device with a large number of management frames trying to paralyse it. Among management frames, de-authentication and disassociation ones are the most widely used. On the other hand, Clear-to-Send (CTS) and Request-to-Send (RTS) are the most common control frames used in 802.11deployments,

In this context, 802.11i does not seem capable to prevent DoS attacks. Furthermore, new DoS attacks, targeting specifically to 802.11i implementations, have very recently appeared. These attacks involve the exploitation of EAPOL-Start, EAPOL-Success, EAPOL-Logoff and EAPOL-Failure used by the EAP protocol. Apart from that, a DoS attack related to the Michael's mechanism "blackout" rule has been also highlighted [19]. In our opinion, DoS attacks should be the greatest concern for wireless network administrators. Currently, the protection against DoS attacks offered by current security protocols is by no means adequate, resulting in an urgent need for adopting new security and retaliatory mechanisms.

F. IEEE 802.11i specific attacks

Apart from the new specialised 802.11i DoS attacks, several other new threats have been also identified. The 802.11i standard allows RSNA and pre-RSNA (i.e. WEP and the original 802.11 authentication) to co-exist in what is referred to as a Transitional Security Network (TSN). This means that a user's device may be configured to connect to both RSNA and pre-RSNA networks. In this case, a security rollback attack may be employed by an adversary to trick the

0-7695-2863-5/07 $25.00 © 2007 IEEE

user's device into using pre-RSNA by impersonating association frames from an RSNA-configured AP.

Another problem that exists in networks protected by IEEE 802.11i makes possible a reflection attack. When 802.11i ad–hoc mode is employed, every network device is able to act as a supplicant and an authenticator at the same time. When a legitimate user initializes a 4-way handshake during the authentication process, the attacker can initialize another 4-way handshake with the same parameters but with the victim device acting as the intended supplicant. The victim's device will be fooled into computing messages as a supplicant and the attacker can use these messages as valid responses to the 4-way handshake, the victim has initialized [7].

Finally, a weakness regarding the CCMP protocol has been identified. Thought considered hard to create a realistic attack based on this weakness, it is wise for network administrators to keep that weakness in mind [20]. However, this last cryptographic threat is out of the scope of this paper.

III. BLENDING 802.11i AND WIDS PROTECTION AGAINST WIRELESS NETWORK ATTACKS

Based on the previously discussed attacks categories, in this section we shall examine whether and by which specific means a WIDS could assist in combating them. We shall concentrate on attacks that 802.11i cannot straightforwardly combat, such as DoS attacks, while attacks that are eliminated by default when 802.11i is (compulsory) applied are not of first priority.

A. Network discovery attacks

Judging the need to detect network discovery attacks or not, we come to the conclusion that though not of top priority it is in many cases desirable to be able to detect them if applicable. After all, a network that remains hidden or gives out only limited information about itself decreases its chances to attract attackers. We should mention that WIDS can partly detect these attacks. In fact, current WIDS are only able to detect attacks that utilize active network scanning. This is because in that case, an increase in the number of probe request frames as well as probe response frames takes place. A WIDS can scan the network for these frames and in case the number of these frames exceeds a threshold, a network discovery attack is most likely taking place.

The best approach towards detecting these attacks is the detection of the tools used for launching them. The most widely utilised tool, namely Netstumbler, can be easily detected via its unique signature pattern. This unique pattern, which can be found in the 802.11 probe request frames, includes several distinct features. For instance, LLC encapsulated frames used by Netstumbler contain the value 0x00601d for organizationally unique identifier (OID) and 0x0001 for protocol identifier (PID), while the payload data is 58 bytes. The ASCII string, attached to the payload is either *Flurble gronk bloopit, bnip Frundletrune!* for version 3.2.0 or *All your 802.11b are belong to us* for version 3.2.3 or *intentionally left blank 1* for version 3.3.0. Other strings with suspicious content may also generate an alert. The pseudocode depicted in Figure 1 explains the idea behind the detection of Netstumbler.

1. Begin
2. Sniff for 802.11 frames
3. Parse frames and extract MAC headers from the frames
4. Check 802.11 frame type.
5. If probe request frame
If (wlan.fc.type_subtype = 0x08 and llc.oui = 0x00601d and llc.pid = 0x0001) and (data[14:4] = 69:6e:74:65 and data[18:4] = 6E:74:69:6f and data[22:4] = 6e:61:6c:6c and data[26:4] = 79:20:62:6c and data[30:4] = 61:6e:6b:20) then Netstumbler detected
6. Log packet content
7. Send out an alarm.
8. Exit and Repeat

Fig. 1 Detection of Netstumbler

B. Eavesdropping / Traffic analysis

As already mentioned in section II.C, the introduction of 802.11i has provided a strong encryption mechanism, namely AES, that at least to date is physically impossible to break. Therefore, these attacks are considered harmless to a wireless network protected by IEEE 802.11i. The data sent, cannot be decrypted and the information about the network a malevolent user has access to, cannot lead in severe security problems. Examining the ability to detect these attacks using a WIDS we must keep in mind that the tools exploited to launch such attacks utilize passive network surveillance, thus the detection is difficult. Summarising, we believe there is no need to take these attacks into serious consideration when we deploy 802.11i WIDSs.

C. Masquerading / Impersonation attacks

Masquerading/Impersonation attacks pose no threat when IEEE 802.11i RSNA mode is enabled. On the downside, when pre-RSNA security is used these attacks can cause serious problems. Apart from that, several studies have shown that there are some potential implementation oversights that could cause problems even when RSNA is used. Taking into consideration the damage these attacks can provoke, we stress that a 802.11i WIDS must be able to successfully detect these attacks and inform network administrators.

The use of MAC address or SSID filtering using black/white lists cannot be longer regarded as a safe way to detect these attacks. A more efficient way to detect them involves the analysis of the sequence numbers. The 802.11 standard has set aside 2 bytes for sequence control. 802.11 frames have a 12-bit sequence number and a 4-bit fragment number in the sequence control field. 802.11 framework uses sequence number for error detection and recovery. We can also use this sequence number to detect these attacks. The 12-bit sequence number ranges from 0 to 4095 and again resets to 0. The sender NIC (Network Adapter) increments the sequence number with every frame it places on the physical layer. Whenever a malevolent user tries to spoof his wireless NIC card in order to launch an attack, the sequence number will start to increment as he sends packets. A WIDS can examine the packets and discover that the sequence number of a specific packet is not the expected one. The attacker is by no means able to get the appropriate sequence number, thus this

detection method can be proved very efficient. Additionally, tools used to launch these attacks, such as AirJack do have a specific signature that could be used for detecting them. That should be a complementary way of detecting these attacks, since it is rather easy to modify the signature and fool the WIDS.

D. Man-in-the-Middle attacks

Likewise to masquerading/impersonation attacks, MITM attacks must also be taken into consideration although IEEE 802.11i promises protection against them. Generally, a MITM attack is generally difficult to detect. Nevertheless, several side-effects take place when the attack unfolds making its detection possible. For instance, there will be a surge of spoofed de-authentication frames directed against the targeted host, a very brief time interval where the connectivity between the host and the AP is lost, and the targeted host will soon begin to send probe request frames trying to find an AP to associate with. In fact, a MITM attack includes an impersonation attack as well as a DoS attack. As a result, a WIDS capable of efficiently detecting these attacks can assist to protect the network from a MITM attack too. However, to be able to fully detect and counter fight MITM attacks requires complicated detection methods that include discovering rogue APs and keeping a record of all active connections between the APs and clients.

E. Denial-of-Service attacks

Without doubt DoS attacks are of major importance in 802.11i. They are easy to launch and 802.11i is unable to efficiently combat them. As a result, a WIDS able to detect this sort of attacks can prove very valuable. The detection of DoS attacks relies on network surveillance. Several distinctive events can be identified while a DoS attack is taking place. Among these events we can record: high frequency of certain management or control frames, noticeable large number of different source addresses, destination address set to broadcast address when it should not, use of invalid source addresses or unrealistic number of unique network names (SSID) on a single channel. Upon capturing these events, a WIDS uses already defined threshold values comparing them to the obtained ones. The actual difficulty here is to find suitable threshold values. Setting them too low would cause many false alarms, while setting them too high could mean that we probably miss less aggressive attacks. In Figure 2 we demonstrate the idea behind the detection of a DoS attack that exploits de-authentication frames.

```
1. Begin.
2. Sniff for 802.11 frames.
3. If deauthentication frame deauth_counter + 1
If (deauth_counter > max_deauth_allowed)
If time_btw_2following_frames < max_time_allowed
then Deauthtication Flood detected.
4. Log attack.
5. Send out an alarm ; block source IP
6. Exit and Repeat.
```

Fig. 2 Detection of De-authentication flood

F. IEEE 802.11i specific attacks

This category of network attacks is really very interesting, as it refers to new vulnerabilities discovered in 802.11i. These vulnerabilities are not yet actual attacks and there are no tools available, capable of exploiting them. Nevertheless, network administrators should be aware of these vulnerabilities. This is where a WIDS can prove itself valuable, as it can provide detection, thus protecting the network.

New DoS attacks that rely on flooding the network with EAP messages can easily be detected, the exact same way traditional DoS attacks are detected. The WIDS searches the network for specific EAP messages (EAPOL-Start, EAPOL-Success, EAPOL-Logoff and EAPOL-Failure), and decides if there is an undergoing DoS attack. This is achieved by comparing the obtained values to a given threshold. Moreover, the DoS attack related to the Michael mechanism can be also identified, when e.g. repeated initiations of the 4-way handshake between an AP and one or more user stations are detected. On the other hand considering the security rollback attack, it requires an impersonation attack to happen at the same time. Most WIDSs are already configured to identify impersonation attacks, thus the security rollback attack can be adjacently combated, even though the attack will not be specifically identified.

Last, a WIDS can also assist in combating the reflection attack that can be launched against 802.11i networks. This attack is only feasible if the network allows ad-hoc connections. A WIDS can easily be configured to detect ad-hoc connections. In fact, most contemporary WIDSs already incorporate that feature, as the ad-hoc connections are generally undesirable. Moreover, this attack mandates the use of an impersonation attack simultaneously, which a WIDS can detect and alert the network administrators.

IV. 802.11i-ENABLED WIDS EVALUATION

In this section, we study the performance of a real intrusion detection system in practice. Towards this direction, properly designed tests are conducted, evaluating the ability to detect the aforementioned categories of network attacks. We were mostly concerned about the 802.11i specific attacks, while 802.11i was used both in RSNA and Pre-RSNA mode.

As a wireless IDS, we select the well known WIDZ (currently at version 1.8). WIDZ is an open-source IDS designed to detect network discovery attacks, unauthorized APs as well as some basic DoS attacks, including association and authentication floods, and fataJack.

Several amendments and code refinements[1] were made to the WIDZ system core, so that we could test all types of attacks including the new 802.11i attacks, where possible. Specifically, we added the Netstumbler and Ministumbler signatures, as an alternative way to detect Wardriving tools. Furthermore, ASCII strings attached to the payload were examined for containing other suspicious text. The component responsible for detecting DoS attacks was upgraded in order to detect new attacks based on EAPOL-Start, EAPOL-Success, EAPOL-Logoff and EAPOL-Failure frames. WIDZ was able

[1] For conciseness purposes we decide not to include source code refinements and/or amendments in the paper. However, all the source code used, both for WIDZ and custom tools, is available upon request.

Third International Workshop on Security
Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007)
0-7695-2863-5/07 $25.00 © 2007 IEEE

to detect unauthorized clients and APs through the employment of the MAC address technique. To deal with impersonation and MITM attacks more precisely we had to add the AirJack and MonkeyJack signatures. Although the use of static signatures cannot provide complete detection of these attacks - as signatures can be altered by the attacker - it comprises the first line of defence. Finally, in order to defend against reflection attacks we added a module capable of detecting ad-hoc connections.

The test was conducted utilising 802.11i-capable equipment, while the attacks were simulated using the most widely open-source chosen tools. Figure 3 depicts the tools used, as well as the results derived from every category of attacks except for the specific 802.11i attacks. It is to be noted that masquerading / impersonation and MITM attacks were only possible in the pre-RSNA mode of 802.11i, as we expected.

Attack	Tools used	Test result
Network discovery	Netstumbler (active network surveillance)	Detected
	Kismet (passive network surveillance)	Not detected (as expected)
Eavesdropping / Traffic Analysis	Airopeek (passive network surveillance)	Not detected (as expected)
Masquerading / Impersonation	AirJack MonkeyJack	Detected (through signatures and history records)
Denial of Service	Void11 FataJack	Detected

Fig. 3 Test results

Considering 802.11i specific attacks, we first created a custom tool to act as an EAP frames-based DoS tool. It is designed to repeatedly send EAPOL-Start or EAPOL-Logoff messages to a target. Although that tool could not stand as a fully functional DoS tool in the real world, it allowed us to test the performance of our WIDS on the detection of the new DoS attacks. Our IDS managed to successfully detect the attack, identifying it accordingly as an EAPOL-Start or EAPOL-Logoff flood attempt. In addition, Michael's related DoS attack was also exposed by the corresponding custom WIDS module. This is due to the repeated 4-way handshakes that this attack provokes in situations where: (a) there is a Message Integrity Code (MIC) failure on a multicast/unicast message at the wireless device or (b) there is a MIC failure associated to group/pairwise keys at a given AP.

Trying to evaluate the WIDS concerning its ability to directly detect the security rollback and reflection attacks, we quickly realized it is almost impossible to perform that task. While these two attacks are theoretically feasible they proved very difficult, if not unfeasible, to practically implement. On the contrary, we are convinced that our WIDS could assist in preventing these two attacks. This is because it features the ability to detect ad-hoc connections and impersonation / masquerading incidents. Therefore, it would proactively alert network administrators of these occurrences, thus preventing the corresponding attack in the egg. Consequently, the attacks would not be identified but could be prevented, which is actually the main goal.

V. Conclusions and Future Work

The use of intrusion detection systems in wireless networks is considered to be the new and promising approach to wireless security. As security protocols present security deficiencies, intrusion detection can be proved valuable. In a nutshell, the flexible nature of intrusion detection systems provides us with the ability to combat new attacks and improve the overall network trustworthiness.

The security evaluation of 802.11i shows that the major concern lies on DoS attacks. A network whose primary security requirement is availability could use 802.11i in combination with an intrusion detection system capable of detecting DoS attacks. In that case, strict rules concerning what is identified as a DoS attack should be adopted. Regarding impersonation / masquerading and MITM attacks, which are considered very dangerous in wireless realms, a WIDS could prove really beneficial, since 802.11i is in many cases used in its pre-RSNA mode.

Considering the new 802.11i specific attacks, we must mention that apart from the new DoS attacks there is not yet a tool available with the ability to exploit the corresponding vulnerabilities discovered. Similarly, there is no method yet to efficiently detect those attacks. Nevertheless, a WIDS capable of detecting ad-hoc connections as well as impersonation attacks could assist in preventing those new attacks from happening, though not specifically identifying them.

As a statement of direction, we are working towards expanding this work by providing more robust intrusion detection methods as well as considering and implementing ideas towards heuristic detection of new attacks.

VI. References

[1] IEEE Standards Association, IEEE 802.11 Standard, http://standards.ieee.org/getieee802/download/802.11a-1999.pdf.

[2] Borsc, M. & Shinde, H., "Wireless security & privacy", in proc. of IEEE International Conference on Personal Wireless Communications (ICPWC '05), pp. 424-428, 2005, IEEE press.

[3] Borisov, N., Goldberg, I. & Wagner, D., "Intercepting mobile communications: The Insecurity of 802.11", in proc. of the seventh annual international conference on Mobile computing and networking, pp. 180-189, 2001.

[4] Fluhrer, S., Mantin, I., Shamir, A., "Weakness in the key scheduling algorithm of RC4", In Eigth Annual Workshop on selected Areas in Cryptography, Toronto, Canada, 2001.

[5] Stubblefield, J. Ioannidis, A.D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to break WEP", in proc. of Network and Distributed System Security Symposium, San Diego, California, 2002.

[6] IEEE P802.11i/D10.0. Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for

Information Technology –Telecommunications and information exchange between systems, April 2004.
[7] Changhua He, Mitchell, J. C., "Security Analysis and Improvements for IEEE 802.11i", in proc. of the 12th Annual Network and Distributed System Security Symposium (NDSS'05), pp. 90-110, 2005.
[8] Bellardo, J. & Savage, S., "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions", in proc. of the USENIX Security Symposium, pp. 15-28, Washington D.C., USA, 2003.
[9] Mishra, A. & Arbaugh, W. A., "An Initial Security Analysis of the IEEE 802.1X Standard", Technical report, CS-TR-4328, UMIACS-TR-2002-10, 2002.
[10] Zhou, W., Marshall, A., Gu, Q., "A sliding window based Management Traffic Clustering Algorithm for 802.11 WLAN intrusion detection", IFIP International Federation for Information Processing 213, pp. 55-64, 2006.
[11] Lee, H.-W., "Lightweight wireless intrusion detection systems against DDoS attack", Lecture Notes in Computer Science 3984 LNCS, pp. 294-302, 2006.
[12] Khoshgoftaar, T.M., Nath, S.V., Zhong, S., Seliya, N, "Intrusion detection in wireless networks using clustering techniques with expert analysis", in proc. of the ICMLA 2005: Fourth International Conference on Machine Learning and Applications, pp. 120-125, 2005.
[13] Zhong, S., Khoshgoftaar, T.M., Nath, S.V., "A clustering approach to wireless network intrusion detection", in proc. of the International Conference on Tools with Artificial Intelligence, ICTAI 2005, pp. 190-196, 2005.
[14] Feng, L.-P., Liu, M.-Y., Liu, X.-N., "Intrusion detection for Wardriving in wireless network", Beijing Ligong Daxue Xuebao/Transaction of Beijing Institute of Technology 25 (5), pp. 415-418, 2005.
[15] Yang, H., Xie, L., Sun, J., "Intrusion detection solution to WLANs", in proc. of the IEEE 6th Circuits and Systems Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication, pp. 553-556, 2005.
[16] Yang, H., Xie, L., Sun, J., "Intrusion detection for wireless local area network", Canadian Conference on Electrical and Computer Engineering, pp. 1949-1952, 2004.
[17] Hsieh, W.-C., Lo, C.-C., Lee, J.-C., Huang, L.-T., "The implementation of a proactive wireless intrusion detection system", in proc. of the fourth International Conference on Computer and Information Technology (CIT 2004), pp. 581-586, 2004.
[18] Jyh-Cheng Chen; Yu-Ping Wang, "Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience", Communications Magazine, IEEE Volume 43, Issue 12, supl.26 - supl.32, Dec. 2005.
[19] Ferguson, N., "Michael: An Improved MIC for 802.11 WEP, IEEE TGi doc 802.11-02/020r0, January 2002.
[20] Junaid, M., Dr Muid Mufti, M.Umar Ilyas, "Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol", White Paper, electronically available at: http://whitepapers.techrepublic .com.com/whitepaper.aspx?&tags=attack&docid=268394.