On RSN-Oriented Wireless Intrusion Detection*

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
{atsak,gkamb,sgritz}@aegean.gr

Abstract. Robust Security Network (RSN) epitomised by IEEE 802.11i substandard is promising what it stands for; robust and effective protection for mission critical Wireless Local Area Networks (WLAN). However, despite the fact that 802.11i overhauls the IEEE's 802.11 security standard several weaknesses still remain. In this context, the complementary assistance of Wireless Intrusion Detection Systems (WIDS) to deal with existing and new threats is greatly appreciated. In this paper we focus on 802.11i intrusion detection, discuss what is missing, what the possibilities are, and experimentally explore ways to make them intertwine and co-work. Our experiments employing well known open source attack tools and custom made software reveal that most 802.11i specific attacks can be effectively recognised, either directly or indirectly. We also consider and discuss Distributed Wireless Intrusion Detection (DIDS), which seems to fit best in RSN networks.

Keywords: Robust Security Network, 802.11i, Intrusion Detection.

1 Introduction

802.11 family networks have received a lot of criticism concerning their ability to provide security equivalent to that we know from our experience with wired networks. Beyond doubt, security in wireless networks was considered to be problematic 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, 4] 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 for enhanced security, a subset of the IEEE 802.11i standard, namely WPA (Wi-Fi Protected Access), was created in order to mitigate WEP deficiencies. Currently, IEEE 802.11i [5] also known as WPA2, is the latest security substandard that promises enhanced security. IEEE 802.11i introduces the concept of Robust Security Network Association (RSNA) used for access control, and utilises

[*] This paper is part of the 03ED375 research project, implemented within the framework of the "Reinforcement Programme of Human Research Manpower" (PENED) and co-financed by National and Community Funds (25% from the Greek Ministry of Development-General Secretariat of Research and Technology and 75% from E.U.-European Social Fund).

R. Meersman and Z. Tari et al. (Eds.): OTM 2007, Part II, LNCS 4804, pp. 1601–1615, 2007.

the Counter–mode / CBC-MAC (CCMP) protocol for data confidentiality and data integrity. Hence, Robust Security Networks (RSNs) afford native per-user access control, strong authentication (e.g. token cards, certificates, and smart badges) and strong encryption. While 802.11i is considered better and more robust, in terms of security, than its forerunners, several flaws and weaknesses have been already identified [6-8].

In this context, as with wired networks, the employment of Wireless Intrusion Detection Systems (WIDS), either centralised or distributed, can be of great value towards shielding against existing and forthcoming more sophisticated threats. This can be seen as a second line of defence, where the WIDS co-exist and co-work with the network's native security protocols, thus assisting in enhancing the overall security.

Until now, several researchers have made a great contribution to WIDS technology, proposing numerous models, methods and mechanisms in an attempt to increase detection effectiveness and performance [10-16]. However, to the best of our knowledge little scrutiny has been done on blending 802.11i and WIDS. Contributing to this subject, the objective of our work is manifold. First of all, the major 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-oriented 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. Last but not least, we survey in short and investigate Distributed Intrusion Detection Systems (DIDS) mechanics and their intrusion detection logic focusing on 802.11i idiosyncrasies.

The rest of the paper is organised as follows. Next section categorises and provides a brief overview of the most common attacks triggered against 802.11 network domains. 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 section 3. Section 4 evaluates our 802.11i enabled WIDS components presenting the results derived from a properly designed test-bed that considers the majority of 802.11i specific attacks. Section 5 surveys works devoted to decentralised wireless intrusion detection paving the way towards effective 802.11i intrusion detection. Last section concludes the paper giving some pointers for future work.

2 Associating Wireless Attack Categories with 802.11i

Most common wireless network attacks can be classified into the following 6 distinct categories:

(a) Network discovery attacks.
(b) Eavesdropping/Traffic analysis.
(c) Masquerading/Impersonation attacks.
(d) Man-in-the-Middle (MITM) attacks.
(e) Denial-of-Service (DoS) attacks.
(f) IEEE 802.11i specific attacks.

Further down we shall examine briefly each of them in order to identify its impact and applicability to 802.11i.

2.1 Network Discovery

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 cannot be considered 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, it 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 native 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.

2.2 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).

2.3 Masquerading/Impersonation

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. An RSN provides mutual authentication as well as strong authentication credentials that normally an attacker would never be able to obtain.

2.4 Man-in-the-Middle

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/she 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 [17].

2.5 Denial-of-Service

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 e.g. 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 802.11 deployments. 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 employed by the EAP protocol. Apart from that, a DoS attack related to the Michael's mechanism "blackout" rule has been also highlighted. 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.

2.6 802.11i-Oriented 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 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 initialises a 4-way handshake during the authentication process, the attacker can at the same time initialise 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 initialised [6]. 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 [18]. However, this last cryptographic threat is out of the scope of this paper.

3 Intertwining 802.11i and WIDS Protection

Motivated by attacks categories described in the previously section, in the following we shall examine whether and by which specific means a WIDS could assist in combating them. Our primary concern is attacks that 802.11i cannot straightforwardly combat, such as DoS, while attacks that are eliminated by default when 802.11i is (compulsory) applied are not of first priority.

First of all, estimating 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. In any case, 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 utilise 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 organisationally 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.

```
Begin
Sniff for 802.11 frames;
Parse frames and extract MAC headers from the frames;
Check 802.11 frame type;
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;
                Log packet content;
                Send out an alarm;
Exit and Repeat
```

Fig. 1. Detection of Netstumbler (through static signatures)

As already mentioned, considering eavesdropping / traffic analysis the introduction of 802.11i has provided a strong encryption mechanism, namely AES, that at least to date is computationally infeasible 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 utilise 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.

On the other hand, 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 [6,7]. 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 utilisation 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/her wireless NIC card in order to launch an attack, the sequence number will start to increment as he/her 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. This situation is described in Figure 2.

```
Begin
Sniff for 802.11 frames;
If frame.getESSID = "AirJack" then Log Incident //possible AirJack attack
Sniff and Log next frames;
        Watch for DoS attack (e.g. dropped packets, etc);
        If DoS attack detected then Airjack detected //Airjack is launching a MITM attack
                Log AirJack attack;
                Send out an alarm;
Exit and Repeat
```

Fig. 2. Detection of AirJack (through both static signatures and anomaly detection)

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.

Indisputably, DoS attacks are of major concern 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 be proved 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 and accurate 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 3 it is demonstrated the idea behind the detection of a DoS attack that exploits de-authentication frames. The same detection strategy, i.e. anomaly-based, applies for Void11 and FataJack attack tools (see next section).

The last category of 802.11i-oriented attacks is really very motivating, 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.

```
Begin
Sniff for 802.11 frames;
If deauthentication frame then deauth_counter := deauth_counter + 1;
    If (deauth_counter > max_deauth_allowed) then
        If (time_btw_2_subsequent_frames < max_time_allowed) then
                Deauthtication Flood attack detected;
                Log attack;
                Send out an alarm;
                Block source IP;
Exit and Repeat
```

Fig. 3. Detection of de-authentication flood (anomaly-based detection)

New DoS attacks that rely on flooding the network with EAP messages can easily be detected, the exact same way a conventional DoS attack is 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. Also note that 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 this 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.

4 Evaluation

In the following, we elaborate on the performance of two real intrusion detection systems in practice. More specifically, properly designed tests are conducted, assessing 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 wireless IDSs, we selected the well known WIDZ (currently at version 1.8) and Wireless Snort (http://www.snort-wireless.org/). WIDZ is an open-source IDS designed to detect network discovery attacks, unauthorised APs as well as some basic DoS attacks, including association and authentication floods and FataJack.

Several amendments and code refinements were made to the WIDZ system core (denoted with the * symbol in Table 1, were applicable), 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 to detect unauthorised 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. Note that for conciseness purposes source code refinements and/or amendments are not included in the paper. All the source code used, both for WIDZ and custom tools, is available from the authors upon request.

Contrariwise to WIDZ, we did not make any changes or amendments to the source code of Snort Wireless. This tool is self-capable of identifying several attacks, which are: rogue AP, Ad-Hoc network connections, Netstumbler detection and some DoS, like authentication flood to AP, de-authentication flood to station. Nevertheless, its detection engine relies solely on the static signatures of the tools that trigger the corresponding attacks, rather on anomaly-based detection strategies. In a nutshell, Snort Wireless offers a set of detection rules that can be either parametrically altered or combined. However, to add an entirely new capability, one has to write a new module from scratch and combine it with the existing code, which in contrast to WIDZ, is practically very hard to manage. This situation, however, is expected to change in the oncoming next version of Snort Wireless.

The tests were conducted utilising 802.11i-capable equipment, while the attacks were simulated using the most widely open-source chosen tools. Table 1 depicts the WIDS and attack tools used, as well as the results derived from every category of attacks except for the 802.11i-oriented attacks. It is to be noted that masquerading / impersonation and MITM attacks were only possible in the pre-RSNA mode of 802.11i, as it was expected to.

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. The 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 realised 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.

Table 1. Test results

WIDS tool used	Attack	Tools Employed	Test Result
*WIDZ / Snort Wireless	Network Discovery	Netstumbler (Active network discovery)	Detected
-//-	-//-	Kismet (passive network surveillance)	Not detected (as expected)
WIDZ / Snort Wireless	Eavesdropping/ Traffic Analysis	Airopeek (passive network surveillance)	Not detected (as expected)
*WIDZ / Snort Wireless	Masquerading / Impersonation	AirJack	Detected
*WIDZ	-//-	MonkeyJack	Detected
Snort Wireless	-//-	MonkeyJack	Not detected
*WIDZ	DoS	Void11 / FataJack	Detected
Snort Wireless	-//-	-//-	Partially detected (Can only detect authentication and de-authentication flood attacks)

5 Distributed Wireless Intrusion Detection

5.1 Rationale: How and Why

Distributed Intrusion Detection Systems offer an alternative to traditional centralised intrusion detection. It is applicable to both wired networks as well as wireless ones. Especially in case of wireless networks where ad-hoc connections are often used, distributed intrusion detection promises greater coverage and improved likelihood of attack detection, thus increasing the overall security. Usually, in a DIDS there is no central director but individual IDS agents are installed in potentially every network node. Each one of the IDS agents is responsible for monitoring local activities, capturing data and collecting interesting information that may lead to the detection of an attack. Agents may collect and periodically send intrusion data and heartbeats towards a hierarchically superior entity and finally to the administrator’s console. If the information collected is not adequate or it shows evidence of wider or global problems, neighboring IDS agents can be asked to cooperatively participate in the intrusion detection process. Therefore, every node in the network can dynamically participate and collaborate with other agents in the intrusion detection system.

A DIDS seems to be the best way to accurately detect attacks and malicious events in a wireless network. Due to the inherent properties that wireless networks have, it is in some cases hard to distinguish between a normal malfunction of the network and an attack taking place. On the other hand, distributed intrusion detection systems seem the only way to overcome this problem with high probability of a correct guess. A DoS attack is often difficult to detect successfully as the effects of such an attack taking place are similar to a normal malfunction of the network. For instance, significant delays and high rate of dropped packets can be the result of either a DoS attack or a malfunction. Consequently, intrusion detection systems often show high rates of false positives, alerting for an attack that turns out to be harmless and true negatives, where what is identified as benign condition turns out to be harmful. Calibrating the required thresholds for both the aforementioned conditions correctly may lead to better results but this is often proved inadequate in practice.

To better understand DIDS detection logic we examine the scenario of a DoS attack against a specific node of the network. According to the scenario, an IDS agent is located at a legitimate network node which tries to send packets towards the node-victim. Also, suppose that the node-victim is suffering a DoS attack by another node (either insider or outsider). Due to the underlying attack the IDS agent on the victim will spot that almost every packet is not received correctly and being dropped. As a result, the agent in the transmitting node will detect frequent retransmissions of the packets, while the agent in the receiving node one will only witness more and more dropped packets. Meanwhile, agents residing on other nodes will not detect anything strange. A collaborative research of the incident by a big portion of the nodes participating in the network will lead to some interesting conclusions. Specifically, since the IDS agent in the transmitting entity is aware of which node is unable to receive the packets (through the header of the packets that contain the source and the target) it can communicate with the agent of the node-victim. Along with the information being sent by other IDS agents residing on adjacent nodes that do not detect any similar problems, it can be easily concluded that there is a DoS attack taking place against that specific node. Generally, in similar scenarios, a DIDS can detect the attack with greater probability of a correct guess compared to a congruent centralised one.

5.2 Related Works

Several studies have lately suggested that the future of intrusion detection systems lies on the use of distributed detection techniques. In the following we survey this literature in short.

In [19] the authors discuss the need for intrusion detection in wireless networks and argue that traditional intrusion detection techniques cannot provide adequate security. In this context, a DIDS is presented, where individual IDS agents are placed on every host of the network. Each agent is responsible for detecting signs of intrusion locally and independently. Also, adjacent nodes can collaboratively participate in the detection. The IDS should include six modules: (a) a data collection module responsible for gathering the required information, (b) the local detection engine which locally investigates for intrusions, (c) the cooperative detection engine that is utilised when several hosts participate in the detection process, (d) the local response module triggering actions concerning the local host and (e) a global response module responsible for the whole network. Finally, a communication module should provide secure communication among all IDS agents. For the intrusion detection mechanism the authors rely on the anomaly detection model. We shall mention that this work is one of the first and most complete studies regarding DIDS. The time the paper was written did not allow the authors to take into consideration the forthcoming 802.11i security protocol, thus no 802.11i specific issues are covered. Nevertheless the concepts mentioned in the paper provide a good and comprehensive background for any further efforts towards the joint utilisation of DIDS and 802.11i.

In [20], the authors propose an attack detection mechanism based on shared monitoring of the network by all nodes, which should be able to decide whether the network is experiencing a malfunctioning or is under attack. Monitors are placed on all nodes collecting data to be stored in lists, one for every node. The combination of different lists can lead to a better understanding of what happened in the network. An attack is detected by combining what two or more monitors logged and have stored in their lists. According to the authors, such a system can be useful for service providers to achieve the required Quality of Service (QoS) and for clients to be able to monitor it. The authors also claim that an IDS like the one they discuss can be misused by sending false attack reports. The list-based mechanism that the authors employ may seem promising, but in case of a real-life network where a big number of nodes will be present, it may prove unable to handle the processing demands for a real-time intrusion detection system.

Authors in [21] study the classic MITM attack and try to examine whether a cooperative detection mechanism can be used to improve the alarm confidence rate and safely uniquely distinguish an attack from others. Along with the detection model the authors also present the response strategies that should be triggered upon the detection of the attack. This effort relies on the concepts of the work presented in [1] adding some strategies to minimise the risk of false detection. A real MITM is implemented to assess the efficiency of the system as well.

In [22] the authors discuss the weaknesses of mobile ad-hoc networks and point out the need for intrusion detection. An agent-based distributed intrusion detection methodology is studied. A two-step intrusion detection mechanism is utilised that at first employs an anomaly detection model to detect abnormal behaviour and secondly uses identification models to identify the attack. The Support Vector Machine (SVM) is proposed for building both anomaly detection and intrusion identification models.

Last, in [23] a distributed intrusion detection system based on mobile agent technology is presented. By efficiently merging audit data from multiple network sensors, the entire network is analysed and the intrusion attempts are identified. The authors study the unique characteristics of ad-hoc networks and try to build a lightweight, low-overhead mechanism.

It is stressed that none of the works presented above cover any 802.11i specific topics or test its implementation against 802.11i protected networks. Moreover, excluding [21] the rest of the aforementioned works focus on wireless ad-hoc networks, although the same concepts are, to a certain degree, applicable to infrastructure networks too.

5.3 802.11i-Specific DIDS

According to the previous section, for the past few years there have been many efforts to utilise DIDS in order to enhance security mainly in 802.11 wireless networks. However, to the best of our knowledge no of them deals either partly or diametrically with 802.11i-enabled DIDS. As already mentioned, the 802.11i new security substandard promises advanced security and is certain to play an important role in tomorrow's wireless networks. However, due to its specific features and weaknesses, we believe that the combination of 802.11i security mechanisms along with an effective DIDS can offer unrivalled protection and security robustness.

As we already made clear the study of the 802.11i protocol ends up with the conclusion that though it offers satisfactory protection from most types of attacks, it does nothing to protect against DoS, which is often the first step to a series of other inroads. As DoS attacks become more and more often, dangerous and sophisticated an IDS seems the only way to combat them. Unfortunately, as we have previously pointed out from the laboratory tests employing small scale centralised IDS, it is often hard to distinguish a DoS attack from a normal malfunction of the network. Centralised IDSs are prone to a high number of false alarms when they face DoS attacks. On the other hand, as manifested in the introductive section of DIDS, cooperative distributed detection promises lesser false alarms, along with more precise detection guesses. To conclude with, we believe DoS attacks are the primary weakness of 802.11i and DIDSs seems the only solid way to deal with them efficiently.

A newly discovered weakness related to 802.11i refers to the ability to launch a reflection attack, when the network allows the creation of ad-hoc connections [6]. In general ad-hoc connections are regarded dangerous and are not desired in networks that require high level of security. The literature suggests that the safest and quickest way to discover ad-hoc connections in a wireless network is by utilising distributed intrusion detection mechanisms. Apart from this, DIDS mechanisms make feasible the detection of the physical location of the electronic device that connects to the network in ad-hoc mode as well. In a broader sense, the latest remark leads to another advantage that DIDSs offer as opposed to centralised ones. They allow for more precise detection of the location of the attacker, as he/her can be assumed to be located closely to the node whose intrusion agent has detected the attack (or somewhere in the neighbourhood in case of collaborating agents). This is of course closely related to the openness of the wireless medium that make the detection of the aggressor a hard issue to deal with.

Generally, the utilisation of a DIDS is expected to offer better response times, more efficient distributed real-time detection, lesser false positives and false alarms, more precise results, better understanding of the network behaviour and more robust and effective detection of all types of attacks. These qualities are highly appreciated when a high level of security is required, meaning that 802.11i mechanisms must be utilised as well. Having these two mechanisms acting jointly we can provide the highest security level for mission critical networks. Nevertheless, further analysis, studies and tests are required to evaluate their ability to cooperate and provide the required level of security.

6 Conclusions and Future Work

While intrusion detection systems have proved their effectiveness in wired networks, are still considered to be the new and promising approach to wireless security. Particularly, whereas wireless security protocols present security deficiencies and inroads become more frequent and sophisticated, intrusion detection can be proved a valuable ally. Without doubt, the flexible nature of intrusion detection systems provides us with the ability to combat new and most dangerous attacks and thus improve the overall network trustworthiness.

DoS attacks seem to be the most severe security problem that the newcomer IEEE 802.11i substandard has to cope with. A network whose primary security requirement is availability could use 802.11i in combination with a distributed IDS capable of detecting DoS. In that case, firm but flexible rules concerning what is identified as a DoS attack should be adopted. Regarding impersonation / masquerading and MITM attacks, which are considered very hazardous in wireless realms, a WIDS could prove really beneficial, since 802.11i is in many cases used in its pre-RSNA mode.

Regarding the new 802.11i-oriented attacks, we must mention that apart from DoS there is not yet a tool available of skilfully exploiting the corresponding vulnerabilities discovered. Likewise, there is no method yet to efficiently detect and repel these attacks. Even so, a WIDS capable of detecting ad-hoc connections as well as impersonation attacks could act proactively by preventing these new attacks from happening, though not specifically identifying them. As future work, we should like expanding this work by providing more robust decentralised intrusion detection methods as well as considering and implementing ideas towards heuristic detection of novel attacks.

References

1. Borsc, M., Shinde, H.: Wireless security & privacy. In: ICPWC 2005. proc. of IEEE International Conference on Personal Wireless Communications, pp. 424–428. IEEE press, Los Alamitos (2005)
2. 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)
3. 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)
4. Ioannidis, J.S., Rubin, A.D.: Using the Fluhrer, Mantin, and Shamir Attack to break WEP. In: Proc. of Network and Distributed System Security Symposium, San Diego, California (2002)
5. 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)
6. Changhua, H., Mitchell, J.C.: Security Analysis and Improvements for IEEE 802.11i. In: NDSS 2005. proc. of the 12th Annual Network and Distributed System Security Symposium, pp. 90–110 (2005)

7. Bellardo, J., Savage, S.: 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: Proc. of the USENIX Security Symposium, Washington D.C., USA, pp. 15–28 (2003)
8. 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)
9. 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, 55–64 (2006)
10. Lee, H.-W.: Lightweight wireless intrusion detection systems against DDoS attack. In: Gavrilova, M., Gervasi, O., Kumar, V., Tan, C.J.K., Taniar, D., Laganà, A., Mun, Y., Choo, H. (eds.) ICCSA 2006. LNCS, vol. 3984, pp. 294–302. Springer, Heidelberg (2006)
11. 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)
12. Zhong, S., Khoshgoftaar, T.M., Nath, S.V.: A clustering approach to wireless network intrusion detection. In: ICTAI 2005. proc. of the International Conference on Tools with Artificial Intelligence, pp. 190–196 (2005)
13. 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), 415–418 (2005)
14. 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)
15. Yang, H., Xie, L., Sun, J.: Intrusion detection for wireless local area network. In: Canadian Conference on Electrical and Computer Engineering, pp. 1949–1952 (2004)
16. Hsieh, W.-C., Lo, C.-C., Lee, J.-C., Huang, L.-T.: The implementation of a proactive wireless intrusion detection system. In: CIT 2004. proc. of the fourth International Conference on Computer and Information Technology, pp. 581–586 (2004)
17. Chen, J.-C., Wang, Y.-P.: Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience, Communications Magazine, IEEE Volume 43(12), (supl.26 - supl.32) (December 2005)
18. Junaid, M., Muid Mufti, Dr., Umar Ilyas, M.: 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
19. Zhang, Y., Lee, W.: Intrusion Detection in Wireless Ad-Hoc Networks. In: MobiCom'2000. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp. 275–283 (2000)
20. Aime, M.D., Calandriello, G., Lioy, A.: A wireless distributed intrusion detection system and a new attack model. In: Proceedings of the 11th IEEE Symposium on Computers and Communications (2006)
21. Schmoyer, T.R., Yu, X.L., Owen, H.L.: Wireless intrusion detection and response: a classic study using main-in-the-middle attack. In: Wireless Communications and Networking Conference, WCNC 2004, IEEE, Los Alamitos (2004)
22. Deng, H., Xu, R., Zhang, F., Kwan, C., Haynes, L.: Agent-based Distributed Intrusion Detection Methodology for MANETs, Security and Management, Nevada, USA (2006)
23. Kachirski, O., Guha, R.: Effective intrusion detection using multiple sensors in wireless ad hoc networks. In: System Sciences Proceedings of the 36th Annual Hawaii International Conference (2003)