

Detecting Security Threats in Wireless LANs Using Timing and Behavioral Anomalies

Elankayer Sithirasenan¹, Vallipuram Muthukkumarasamy²

¹Institute for Integrated and Intelligent Systems, ²School of Information and Communication Technology
Griffith University
Gold Coast Campus, Australia

¹e.sithirasenan@griffith.edu.au, ²v.muthu@griffith.edu.au

Abstract—With the increasing dependence on wireless LANs (WLANs), businesses and educational institutions are in need of a reliable security mechanism. The latest security protocol, the IEEE 802.11i assures rigid security for WLANs with the support of IEEE 802.1x protocol for authentication, authorization and key distribution. Nevertheless, fresh security threats are emerging often to oust these new defense mechanisms. Further, many organizations based on superficial vendor literature, believe their wireless security is sufficient enough to prevent any unauthorized access. Having wide ranging options for security configurations, users are camouflaged into deep uncertainty. This volatile state of affairs has prevented many organizations from fully deploying WLANs for their secure communication needs, though WLANs may be cost effective and flexible. In this paper, we present an anomaly based mechanism to detect both known and emerging security threats in WLANs. Our method uses both timing and behavioral anomalies. We first look for timing and/or behavior anomalies during the security association process and then use outlier based data association approaches to verify their legitimacy. The proposed concept was tested on our experimental setup and the results obtained from EAP-LEAP and EAP-PEAP authenticated hosts are presented here.

I. INTRODUCTION

The wireless network environment is exposed to a range of intrusion attacks. Unlike the wired networks the wireless networks face unique challenges due to their inherent nature. Although the newly introduced security standard, IEEE 802.11i [1] provide effective measures to protect the wireless networks from confidentiality and integrity threats, their reliance on authenticity and availability are still a major concern.

IEEE 802.11i provides mutual authentication, key management, and data confidentiality protocols that may execute concurrently over a network in which other protocols are also used. On the assumption of upgrading the hardware, 802.11i defines CCMP that provides strong confidentiality, integrity, and replay protection. In addition, an authentication process, combining the 802.1x port-based authentication and key management procedures, is performed to mutually authenticate the devices and generate a fresh session key for data transmission. Since 802.11i promises to be in the right direction for wireless security, it should be able to prevent an adversary from any attacks even if the adversary has powerful equipment and techniques for breaking into the system. In other words, an implementation of 802.11i protocol in a WLAN should

provide sufficient data confidentiality, integrity, and mutual authentication.

Although 802.11i guarantees extensive security for the wireless environment it is still premature to exclude potential future threats. Further, there are many wireless installations, where appropriate security mechanisms are neither used nor implemented effectively [2]. Hence in addition to improving the existing security mechanisms we also need other protection mechanisms to guard the wireless environment from novel security threats. Effective use of the wireless network will only be possible if security threats are detected in advance, preventing any potential catastrophe. In this respect, tracking wireless traces and properly analyzing them may reveal vital information about impending threats to the wireless environment. One such analysis considered in this paper is the round trip timings associated with the management frames. Unusual timing values exhibited by wireless stations could be the beginning of an intended security breach. Furthermore, legitimate wireless hosts attempting to connect to an authorized AP usually demonstrate a set of defined behavior. Tracking such behavior of all stations in the wireless environment would normally present useful information for detecting misbehaving stations. Therefore, tracking the management frames and properly analyzing them for timing and/or behavior anomalies will enhance the ability of the detection mechanism to discover security threats in advance.

This paper is organized as follows. Section II gives a brief overview of related work on intrusion and anomaly detection. Section III introduces the RSN framework. Details of our proposed anomaly detection system is given in Section IV. In Section V we present some of the experimental results. The results are discussed in Section VI. Finally, Section VII concludes the paper.

II. RELATED WORK

Analysis of IEEE 802.11i by Sithirasenan et. al. [3] identifies a number of weaknesses in the standard together with some solutions from the software implementation perspectives. A similar analysis by He et. al [4] on IEEE 802.11i wireless networking further highlights the weaknesses of the standard. They have discussed the possibilities of several attacks on poorly configured 802.11i networks. Further, they state that

although the new security standard offers sufficient protection to the wireless environment it is up to the implementer to ensure that all issues are addressed and the appropriate security measures are deployed. For instance, a single misconfigured station could lead the way for a cowardly attack and expose the organizational network. Lynn et. al. [5] discuss that if no authentication mechanisms are implemented an adversary could establish two separate connections to the supplicant and the authenticator to construct a Man-in-the-Middle (MitM) attack. Furthermore, if mutual authentication mechanism is not appropriately implemented an adversary will be able to launch a MitM attack and learn the Pairwise Master Key (PMK) as illustrated by Asokan et. al. [6]. Although these vulnerabilities are not directly connected with 802.11i, any implementer of 802.11i needs to consider these problems warily and keep monitoring the wireless hosts to guarantee proper integration of the security mechanisms.

The countermeasure proposed by Barbeau et. al. [7] includes the use of Radio Frequency Fingerprinting (RFF) and User Mobility Profiles (UMP) for Anomaly Based Intrusion Detection (ABID). At the same time the use of device and user profiles to detect anomalies has been studied by Hall et al. [8]. They discussed enhancing the capability of their system by supplementing existing user and device-based profiles, with those based on mobility. However, this system is more suitable for addressing the problem of stolen cell phones, given that the mobility behavior of the thief and the user are likely to be different. In the case of wireless networks the attacker needs to be in the same domain as the user to carry out an attack. Therefore the use of mobility profiles will not be suitable for intrusion detection in infrastructure WLANs.

Maxion et. al. [9] apply benchmarking to prove that differences in data regularities influence anomaly detector performance, and such differences are found in natural environments. All anomaly-detection algorithms operate on data captured from some kind of computing domain or environment. Embedded in each type of environment is a particular structuring of the data that is a function of the environment itself. The researchers provide quantitative results of running an anomaly detector on various data sets containing different structure. The results on different data regularities proved data consistency influences the anomaly detector performance. Hence they emphasize the need for anomaly detection systems that can handle differences in data regularities effectively.

III. ROBUST SECURITY NETWORK

The IEEE 802.11i standard [1] defines two classes of security framework for IEEE 802.11 WLANs: RSN (Robust Security Network) and pre-RSN. A station is called RSN capable equipment if it is capable of creating RSN Associations (RSNA), otherwise, it is a pre-RSN equipment. In an Extended Service Set (ESS), during the RSNA a number of messages are exchanged between the supplicant (STA) and the authenticator (AP). The network that only allows RSNA with RSN-capable equipments is called a RSN security framework. The major difference between RSNA and pre-RSNA is the

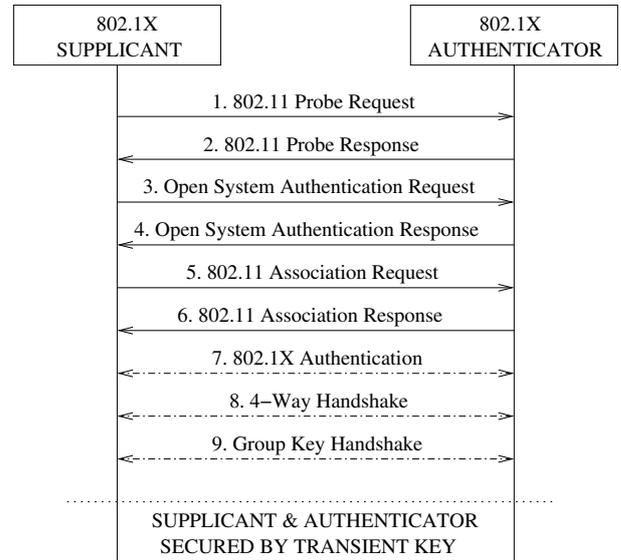


Fig. 1. RSN Association

4-way handshake. If the 4-way handshake is not included in the authentication / association procedures, stations are said to use pre-RSNA.

Figure 1 shows an example RSNA between a wireless station and the access point in an ESS. It assumes no use of pre-shared key. Flows 1-6 are the IEEE 802.11 [10] association and authentication process prior to attaching to the AP. During this process, security information and capabilities could be negotiated using the RSN Information Element (IE). This phase is called the discovery phase. The Authentication in Flows 3 and 4 refer to the IEEE 802.11 open system authentication. On successful completion of the discovery phase the AP initiates the authentication phase by starting the IEEE 802.1X [11] authentication shown by Flow 7. If the STA and the authentication server authenticate each other successfully, both of them independently generate a Pairwise Master Key (PMK). The authentication server then transmits the PMK to the AP through a secure channel (for example, IPsec or TLS).

The 4-way handshake then uses the PMK to derive and verify a Pairwise Transient Key (PTK), guaranteeing fresh session key between the STA and the AP. This is called the 4-way handshake phase as shown by Flow 8. Next, the group key handshake is initiated as shown by Flow 9. The group key handshake is used to generate and refresh the Groupwise Transient Key (GTK), which is shared between a group of STAs and APs. Using this key, broadcast and multicast messages are securely exchanged in the air.

The anomaly detection modules in our proposed Early Warning System (EWS) tracks all messages discussed above to make an assessment on the level and nature of an anomaly. The software model of the IEEE 802.11i security architecture, which was developed and analyzed by [3] is used as the base model for detecting behavioral anomalies. This model has been formally verified for consistency and completeness [12]. In the next section we introduce partial data cubes and the concept

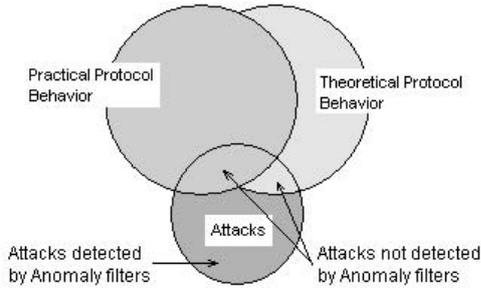


Fig. 2. Anomaly Filter

of surrogate views.

IV. THE EARLY WARNING SYSTEM (EWS)

Our EWS [13] includes a packet capturing module, an event engine, a timing anomaly detection module, a behavioral anomaly detection module, an intrusion prevention module and a data mining engine. The intrusion prevention module is the main component of our system with the ability of processing outlier based data association requests in real time. Our system has multiple levels of defense offering improved reliability for anomaly detection. The first level of defense is the detection of timing anomalies followed by the discovery of behavioral anomalies. If an event is detected with either one or both of the anomalies a third level of defense is triggered to validate the legitimacy of the event based on different views of data. Since our system needs to search enormous amounts of historical data (in real time) we use parallel processing techniques to query the database. In the following section we describe the process of anomaly detection in detail.

A. Anomaly Detection

As shown in Figure 2 anomaly filters detect anomalies that are outside the theoretical or practical behavior region of a protocol. Anomalies in these regions result in a large number of false positives. Most anomaly detection systems operate within this region and hence do not effectively detect anomalies that follow theoretical or practical behavior of the protocol. Anomalies outside the theoretical or practical behavior regions occur often and hence are usually easy to detect and substantiate. On the other hand, anomalies within the theoretical or practical behavior regions are rare and lead to false negative reporting. Detecting these anomalies is challenging and requires analyzing the protocol behavior from different perspectives. Our system detects such anomalies using timing inconsistencies and then substantiates the anomaly by analyzing its behavior from different view points. A wireless host which behaves normally from one view point can behave differently from another view point.

The first stage in our anomaly detection process is the examination of timing anomalies. This is achieved by maintaining a timing profile for every participating host in the wireless network. For example, we maintain the mean and the standard

deviation for each round trip message transfer i.e. the time taken to send a message and to receive the acknowledgment. A timing anomaly is triggered when a host exhibits an abnormal timing value (eg., deviation by one standard deviation) during a message exchange. The timing profiles are dynamically updated with new values for mean and standard deviation depending on the current operational nature of the wireless network.

The second stage is the behavioral anomaly detection. Here, the current behavior of the wireless host during the association phase is compared with that of a normally behaving host. A normally behaving host has to traverse all of the legitimate states of the RSNA process as shown in the RSN projection model [3]. If anomalies occur there can be situations where hosts fall into illegitimate states and fail to match the projection model. However, our system does not instantly classify such anomalies as illegitimate, instead, they trace such events and forward them to the intrusion prevention module for further processing.

The third stage of defense is the most important in our system and the module that executes this is called the intrusion prevention module. This module has to arrive at important decisions to verify the legitimacy of the anomalies discovered by the previous modules. Hence this module plays a vital role in maintaining the reliability and dependability of our system. In order to facilitate real time intrusion prevention, we adopt an efficient querying technique to search our database for outlier based data associations.

The intrusion prevention module executes a number of data association analysis to decide whether anomalies detected by the anomaly modules are legitimate or not. This is achieved by analyzing the detected anomaly from different view points. Wireless attacks such as "Session Hijack" or "Man-In-The-Middle" do exactly follow the protocol but can exhibit differences in timings. Hence, such attacks cannot be substantiated merely by looking at just one characteristic of the wireless environment. Instead, analyzing anomalies caused by these attacks from different view points can reveal better results. An anomaly can exhibit normal behavior from one characteristic, but behave abnormally on a different characteristic. Therefore, the more characteristics analyzed will deliver better detection results than merely analyzing single characteristic.

V. EXPERIMENTS

A number of experiments were carried out on our test environment to validate the proposed detection mechanism. Two different types of security threats; Denial-of-Service (DoS) attack and Replay attack were executed in order to verify the detection capabilities of Timing Anomaly and Behavior Anomaly modules.

A. Timing Anomaly

Table I and II show the timing profile between an access point (AP1) and a station (STA1). The timing profile shows the allowable timing range required to complete a particular

Event	Mean Time (ms)	Standard Deviation
802.11 AUTHENTICATION	0.90	0.88
802.11 ASSOCIATION	3.16	2.25
EAP I	1.16	1.73
EAP PEAP 2	4.51	6.41
EAP LEAP 3	2.75	1.37
EAP LEAP 4	15.67	4.05
EAP 4-Key Exchange	11.93	3.19
Overall	83.62	10.28

TABLE I
EAP-LEAP TIMING PROFILE

Event	Mean Time (ms)	Standard Deviation
802.11 AUTHENTICATION	0.46	0.17
802.11 ASSOCIATION	2.86	2.50
EAP I	0.49	0.74
EAP PEAP 2	3.77	2.16
EAP PEAP 3	3.38	7.08
EAP PEAP 4	5.51	5.20
EAP PEAP 5	6.21	5.10
EAP PEAP 6	5.25	7.14
EAP PEAP 7	6.52	5.12
EAP PEAP 8	1.19	2.31
EAP PEAP 9	2.96	5.66
EAP 4-Key Exchange	3.32	1.22
Overall	158.91	14.71

TABLE II
EAP-PEAP TIMING PROFILE

round trip event during EAP-LEAP and EAP-PEAP authentication processes respectively. In this context a round trip event is considered to be the completion of two messages; a request and the corresponding response. The Mean timing values together with the standard deviation gives the range of timings allowed for the round trip event during normal operation. Maintaining such profiles for every participating hosts may reveal any timing anomalies that could arise due to an abnormal condition.

B. Behavior Anomaly

The next stage in our anomaly detection process is the behavioral analysis of the participating hosts. The events shown in Table III represent the normal behavior of a station during an EAP-PEAP association process. Here the first three events represent 802.11 open system authentication. The next event initiate the 802.1x mutual authentication with the “EAP REQUEST IDENTITY 1” message. The 802.1x authentication begins with the access point requesting the wireless station to identify itself. The response from the wireless station is redirected to the authentication server which in turn initiates the EAP type specific authentication process. Depending on the security configuration appropriate EAP type specific authentication will commence. EAP-PEAP authentication consists of sixteen EAP type specific events (20, 22, 23, 25-27, 29-38).

Table IV lists the EAP-LEAP authentication events. It can be noticed that this list has event 21 - “EAP RESPONSE NAK 2”, which is sent by the station indicating that it not configured for EAP-PEAP authentication. In our experimental setup the RADIUS authentication server is configured for

ID	Event
0	{802.11 AUTHENTICATION}
3	{802.11 ASSOCIATION REQUEST}
4	{802.11 ASSOCIATION RESPONSE}
6	{EAP REQUEST IDENTITY 1}
7	{EAP RESPONSE IDENTITY 1}
20	{EAP REQUEST PEAP 2}
22	{EAP RESPONSE PEAP 2}
23	{EAP REQUEST PEAP 3}
25	{EAP RESPONSE PEAP 3}
26	{EAP REQUEST PEAP 4}
27	{EAP RESPONSE PEAP 4}
29	{EAP REQUEST PEAP 5}
30	{EAP RESPONSE PEAP 5}
31	{EAP REQUEST PEAP 6}
32	{EAP RESPONSE PEAP 6}
33	{EAP REQUEST PEAP 7}
34	{EAP RESPONSE PEAP 7}
35	{EAP REQUEST PEAP 8}
36	{EAP RESPONSE PEAP 8}
37	{EAP REQUEST PEAP 9}
38	{EAP RESPONSE PEAP 9}
39	{EAP SUCCESS 9}
52	{EAPOL KEY}

TABLE III
EAP PEAP EVENTS DURING NORMAL BEHAVIOR

ID	Event
0	{802.11 AUTHENTICATION}
3	{802.11 ASSOCIATION REQUEST}
4	{802.11 ASSOCIATION RESPONSE}
6	{EAP REQUEST IDENTITY 1}
7	{EAP RESPONSE IDENTITY 1}
20	{EAP REQUEST PEAP 2}
21	{EAP RESPONSE NAK 2}
11	{EAP REQUEST LEAP 3}
12	{EAP RESPONSE LEAP 3}
13	{EAP SUCCESS 4}
14	{EAP REQUEST LEAP 4}
18	{EAP RESPONSE LEAP 5}
52	{EAPOL KEY}

TABLE IV
EAP LEAP EVENTS DURING NORMAL BEHAVIOR

EAP-PEAP authentication by default. Therefore, when the EAP authentication is initiated the authentication server always requests for EAP-PEAP authentication, which the station can accept or deny. On both types of authentication processes the last four messages (52) represent the key distribution phase. EAP-LEAP authentication process consists of five events (11-14, 18) only.

Tables III and IV all list the EAP type specific events during normal behavior. However, when anomalies arise this behavior can change. There can be situations where the number of events are extraordinarily high or low. There can also be situations where events can totally disappear from the receptive range of the monitoring devices. Therefore tracking these events and analyzing appropriately can reveal vital information regarding any abnormality in the wireless environment. In the next section we discuss the results obtained from the various experiments carried out to study the behavior of these wireless hosts during DoS and Replay attacks.

Event	Time (ms)
802.11 AUTHENTICATION	0.06
802.11 ASSOCIATION	0.12
EAP 1	0.23
EAP PEAP 2	0.26
EAP LEAP 3	0.13
EAP LEAP 4	10.61
EAP 4-Key Exchange	0.42
Overall	171.21

TABLE V
EAP-LEAP ABNORMAL TIMING

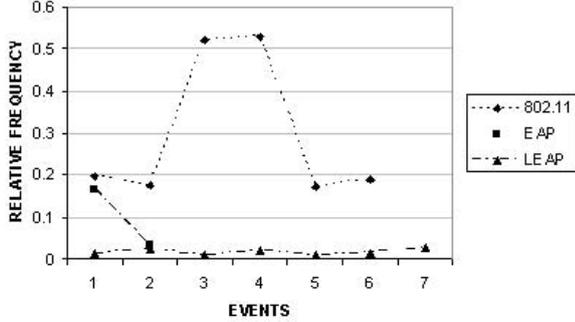


Fig. 3. DoS Attack during EAP-LEAP Authentication

VI. RESULTS AND DISCUSSION

In order to study the behavior of wireless hosts during different EAP type specific authentication process, we collected 802.11 management traces from two wireless hosts configured to authenticate using LEAP and PEAP authentication mechanisms. We also injected some abnormal management frames forcing the wireless hosts to deauthenticate and reassociate frequently. This was done by injecting “Deauthentication” and “Association Request” frames using the “airreplay” [14] tool. The analysis of the captured frames are discussed below.

The timings shown in Table V were obtained during a DoS attack. Here neither the access point nor the station was targeted. However we injected several “Deauthentication” frames with a fake MAC address flooding the channel. During this period we initiated a EAP-LEAP authentication process and the timings were noted. From the timing measurements in Table V it can be seen, that, although the values shown for “EAP Request/Response” messages are significantly less, the overall timing is however very high. Thus our Timing Anomaly module detects the abnormal condition. However, these kinds of abnormal timings can arise due to several reasons, some may be usual, others unusual. In this case, although the DoS attack did not affect the authentication process itself the timing anomaly detection module detected a time delay in the authentication process. Thus, to further investigate the legitimacy of this anomaly we pass this information to the third phase - the intrusion prevention module.

Figures 3 and 4 show the normalized relative frequencies of EAP type specific events on wireless stations configured for EAP-LEAP and EAP-PEAP authentication respectively, during a DoS attack. In both figures the relative frequencies

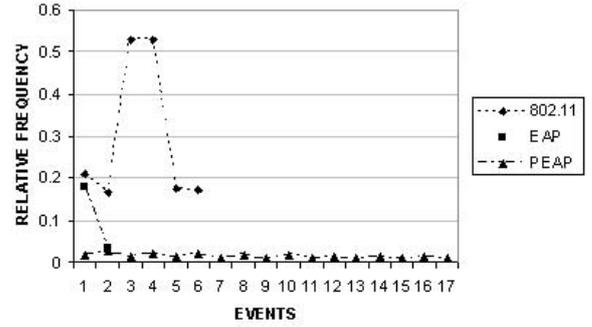


Fig. 4. DoS Attack during EAP-PEAP Authentication

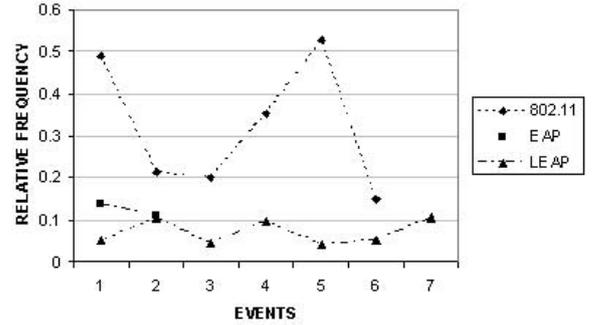


Fig. 5. Replay Attack during EAP-LEAP Authentication

of 802.11 events are considerably high compared to the EAP events. This is because of the “Deauthentication” frames injected. Consequently, this demonstrates the unreliable nature of 802.11 open system association. Here, the relative frequency is the ratio between the total number of a specific event to the total number of all EAP type specific events associated with that particular wireless host. During the DoS attack events “ASSOCIATION REQUEST” (5) and “ASSOCIATION RESPONSE” (6) have almost equal frequency. This is due to the reassociation after a deauthentication. Similarly, the “DEAUTHENTICATION” (3,4) and “AUTHENTICATION” (1,2) events also have equal frequencies. However, “DEAUTHENTICATION” events have high frequency because of the “Deauthentication” frames injected. It can be further noticed that the behavior of both EAP methods are almost similar during the DoS attack.

Figures 5 and 6 show the normalized relative frequencies of EAP type specific events on wireless stations configured for EAP-LEAP and EAP-PEAP authentication respectively, during a Replay attack. Here again, the relative frequencies of 802.11 events are considerably high. This is because of the “Authentication” and “Association Request” frames injected. Consequently, as in the case of DoS attack this demonstrates the unreliable nature of 802.11 open system association. In this case the events “AUTHENTICATION” (0) and “ASSOCIATION REQUEST” (5), both replayed messages, have very high frequency indicating the Replay attack. Hence, it is evident that the behavior of the EAP configured stations differ

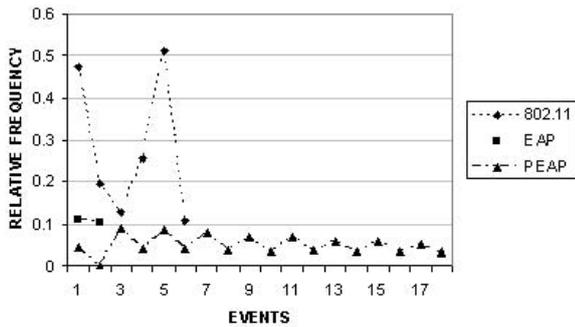


Fig. 6. Replay Attack during EAP-PEAP Authentication

depending on the type of attack they experience.

Further, it can be noticed that in both attack scenarios the relative frequency of “EAP REQUEST IDENTITY 1” event is high compared to other EAP events. This is because at this stage the authentication server has still not come into action. It is only after the authentication server issues the “EAP REQUEST PEAP 2” (since default EAP type is set to PEAP) message the EAP events become stable. In this study the “Replay” or the “DoS” attack executed do not interfere with the EAP encapsulated messages, however, a rogue access point can replay the first “EAP REQUEST IDENTITY 1” message.

Next, consider the EAP type specific events - the LEAP and PEAP. The relative frequencies of the type specific events are almost constant in both attack scenarios confirming the robustness of 802.1x authentication process. As soon as the EAP type specific authentication begins the association process becomes very reliable. Although, the DoS attack can jam the process delaying certain message exchange (as seen in Table V), the process itself is robust due to the effectiveness of the EAP.

The above examples demonstrate the effectiveness of using timing and/or behavioral analysis for detecting abnormal conditions. Although in our experiments we have not tested the vulnerabilities of the EAP authentication process itself, it is apparent that our concept is capable of detecting future exploits on the EAP process as well. Further, in most attack scenarios the attacker needs to inject many messages before he could actually compromise the credentials of a legitimate station. Therefore, as soon as we detect an abnormal condition we can continue to monitor the suspicious stations and once sufficient traces are collected we substantiate the abnormality using outlier based data association techniques. In this manner we can either raise an alarm that a security breach is on the verge or give an indication of the level of threat for the exposed station.

VII. CONCLUSIONS

In this paper, we have reported the use of timing and/or behavioral analysis for detecting abnormal conditions in the wireless environment. The experimental results obtained with the 802.11i based network are promising and confirming the concept of the proposed detection mechanism. Although, the

proposed system is not tested to detect all of the security threats, the main aim was to validate our methodology. In this view it is shown that analyzing the wireless environment with more than one characteristic can effectively substantiate the legitimacy of abnormal conditions created by unusual events.

The analysis of the test results demonstrate the effectiveness of our proposed system in detecting various security threats. However, we have not tested our system with abnormalities that can interfere with the EAP authentication process itself. As of to date EAP vulnerability on the wireless environment has not been reported. However, the results presented here proves that our concept is capable of detecting future exploits on EAP vulnerability. Although this technique is expected to provide very promising results in cooperate networks, their applicability on smaller networks may be limited due to resource requirements.

REFERENCES

- [1] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Standard 802.11i Part 11, July 2004.
- [2] A. Bittau, M. Handley, and J. Lackey, “The Final Nail in WEP’s Coffin,” in *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P’06)*, vol. 00, 2006, pp. 386–400.
- [3] E. Sithirasenan, V. Muthukkumarasamy, and D. Powell, “IEEE 802.11i WLAN Security Protocol - A Software Engineer’s Model,” in *AusCERT ’05: Proceedings of the 4th Asia Pacific Information Technology Security Conference*, May 2005, pp. 39–50.
- [4] C. He and J. C. Mitchell, “Security Analysis and Improvements for IEEE 802.11i,” in *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, February 2005. [Online]. Available: <http://www.isoc.org/isoc/conferences/ndss/05/proceedings/index.htm>
- [5] M. Lynn and R. Baird, “Advanced 802.11 attack.” Las Vegas, USA, July 2002.
- [6] N. Asokan, V. Niemi, and K. Nyberg, “Man-in-the-Middle in tunneled authentication protocols,” IACR ePrint archive, United Kingdom, Tech. Rep. 2002/163, Cotober 2002. [Online]. Available: <http://eprint.iacr.org/2002/163/>
- [7] M. Barbeau, J. Hall, and E. Kranakis, “Detecting impersonation attacks in future wireless and mobile networks,” in *Proceedings of the Workshop on Secure Mobile Ad-hoc Networks and Sensors*, September 2005.
- [8] J. Hall, M. Barbeau, and E. Kranakis, “Anomaly-based intrusion detection using mobility profiles of public transportation users,” in *Proceedings of the IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, vol. 2, August 2005, pp. 17–24.
- [9] R. A. Maxion and K. M. C. Tan, “Benchmarking anomaly-based detection systems,” in *Proceedings of the International Conference on Dependable Systems and Networks*, June 2000, pp. 623–630.
- [10] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11, June 1999.
- [11] *Local and Metropolitan Area Networks, Port-Based Network Access Control*, IEEE Standard 802.1X, June 2001.
- [12] E. Sithirasenan, S. Zafar, and V. Muthukkumarasamy, “Formal Verification of the IEEE 802.11i WLAN Security Protocol,” in *ASWEC’06: Proceedings of the 21st Australian Software Engineering Conference*, April 2006, pp. 181–190.
- [13] E. Sithirasenan and V. Muthukkumarasamy, “An Early Warning System for IEEE 802.11i Wireless Networks,” in *AusWireless’06: Proceedings the of 1st Australian Conference on Broadband Wireless and Ultra Wideband*, March 2006, pp. 25–30.
- [14] “Aircrack: WEP and WPA-PSK keys cracking program,” <http://www.aircrack-ng.org/doku.php>, July 2006.