Study of Timing Values in EAP Authenticated Wireless Hosts

Janaka Silva, Elankayer Sithirasenan, and
Vallipuram Muthukkumarasamy

School of Information and Communication Technology
Griffith University, Gold Coast, Australia
j.silva@griffith.edu.au e.sithirasenan@griffith.edu.au
v.muthu@griffith.edu.au

Abstract. Wireless Local Area Networks have exhibited significant growth within the last few years in both home and corporate environments because of low cost and improved quality. This growth has fueled new applications for wireless networks ranging from advanced warehouse inventory systems to wireless Voice Over Internet Protocol (VoIP) phones. Sometimes the deployment of wireless local area networks (WLANs) is even more economical than installing wired networks in a building. However, the level of security of wireless and wired networks remain a major concern. The IEEE 802.11i standard together with IEEE 802.1X standard provide enhanced encryption and authentication mechanism enabling rigid security for the wireless networks. However, increasing wireless network security breaches has proven the lack of protection mechanism for the WLANs. In this context we propose to investigate the possibility of using round trip timing values for studying the behavior of wireless hosts under different abnormal conditions. In order to test our concept we have analyzed large number of traces captured using EAP, PEAP, LEAP and TLS authenticated hosts from our experimental wireless network environment.

1 Introduction

Security and the behavioral nature of the wireless environment is much more complex than wired environment. Normal behavior of a wireless network can change dramatically due to a number of reasons, including the inherent qualities of the wireless environment. Much research has been carried out to model the actual changes of the wireless networks. Most of them focus on the security issues of the wireless networks. The latest standard IEEE 802.11i [9] is developed to enhanced the security capabilities of the WLAN.

IEEE 802.11i defines security and mutual authentication mechanisms at the Media Access Control (MAC) layer. This standard is designed to address the security deficiencies in the Wired Equivalent Privacy (WEP) mechanism. IEEE 802.11i scheme uses strong encryption and other enhancements to improve security of the WLANs addressing three main security areas. It provides mutual

authentication, key management and data transfer privacy. On the assumption of upgrading the hardware, 802.11i defines CCMP that provides strong confidentiality, integrity and reply protection. The 802.11i architecture contains the following components: IEEE 802.1X [10] for authentication (enabling the use of EAP and an authentication server), Robust Security Network (RSN) for tracking associations and Advanced Encryption Standard, based on CCMP to provide confidentiality, integrity and origin authentication.

Although the IEEE 802.11i provides effective measures to protect the wireless networks from confidentiality and integrity threats, their reliance on authenticity and availability are still of major concern. On the other hand Intrusion Detection Systems (IDS) are used for detecting security breaches in wired as well as wireless networks. Huge amount of wireless traces can be collected from today's wireless network environment. Analyzing them may reveal vital information about the behavior of wireless hosts. One of the major challenges in wireless networks is to identify and differentiate the legitimate and non-legitimate wireless hosts. In this study we discuss the use of round trip timing (RTT) values, to detect unusual behaviors of the wireless hosts. As such we have demonstrated the RTT variations of EAP [5] LEAP [11], PEAP [14] and TLS [1] authenticated wireless hosts during RSN association process.

This report is organized as follows: In section 2 we give a brief summery of the various studies carried out related to anomaly detection. Section 3 we discuss the IEEE 802.11i RSN association process. Details of the experimental setup and the software model used for calculating the timing values are discussed in section 4. Results and analysis of the RTT values for EAP LEAP, PEAP and TLS authenticated hosts during normal and abnormal conditions are presented in section 5. Finally, section 6 concludes our paper.

2 Related Work

Analysis of IEEE 802.11i by Sithirasenan et. al. [16] identifies a number of weaknesses in the standard together with some solutions from the software implementation perspectives. A similar analysis by He et. al [7] 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. [13] 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. [4]. 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.

Lim et al. [12] introduced a low cost solution for intrusion detection and response. Their system detects intrusions by various means such as MAC address filtering, tracking RTS/CTS to detect passive intruders and stateful monitoring to detect random responses by intruders. The prototype developed had several limitations in the processing power, hence the authors focused only on selected intrusions. They mainly considered DoS attacks and their system detected the NetStumbler without any false positives.

Gill et al. [6] proposed a passive technique for detecting session hijacking attacks. They use Received Signal Strength (RSS) and Round Trip Timings (RTT) to detect anomalies. Both cases require frequent re-tuning of threshold values for satisfactory performance. However, their system cannot be extended to detect other security threats in the wireless environment.

In addition to the above techniques there are several commercial products used for intrusion detection and preventions. AirDefence [2] and Air Magnet [3] claim to provide a complete hardware and software solution for intrusion detection and prevention in 802.11 wireless networks. AirDefence detects intruders and attacks and also analyzes vulnerabilities. Although the manufacturers claim their system provides active responses to every possible intrusion attempts there is no statistical evidence to justify it. Furthermore, WLANs with 802.1x authentication are yet to become popular and hence the credibility of the commercial systems still needs to be verified.

In a further study by Sithirasenan et al. [15] they discuss the use of different characteristics of the WLANs to substantiate between legitimate and illegitimate hosts. In their study they have proposed a system to monitor both timing and behavioral anomalies and the use a outlier based data association technique to substantiate the anomaly. They collected large amount of network traces, stored and analyzed them in order to detect and distinguish real time attacks on the wireless environment. For real time intrusion detection and prevention they have proposed a robust system called Early warning System (EWS). As an extension to the timing anomaly studies, in this paper we investigate the RTT values of EAP LEAP, PEAP and TLS authenticated hosts under both normal and abnormal conditions

3 Robust Security Network

The IEEE 802.11i standard 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 4-way handshake. If the 4-way handshake is not included in the authentication / association procedures, stations are said to use pre-RSNA.

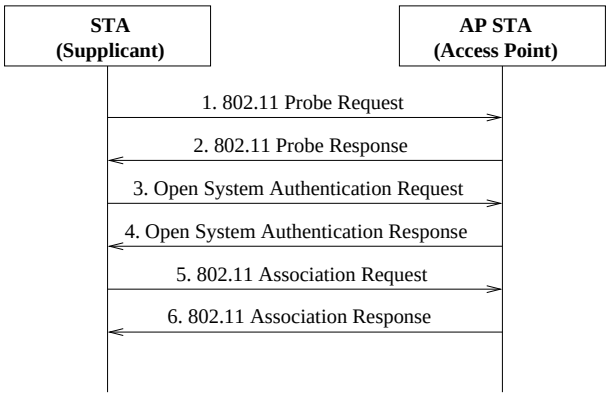

Fig. 1. RSN Discovery Phase

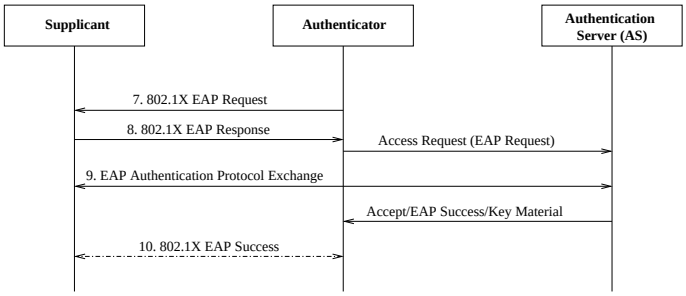

Fig. 2. RSN Authentication Phase

Figure 1 shows the first phase in RSNA - the discovery phase. During this phase both the STA and the AP agree on a common security policy. Flows 1-6 are the IEEE 802.11 [8] association process prior to attaching to the AP. During this process, security information and capabilities are negotiated using the RSN Information Element (IE). 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 [10] authentication as shown in Figure 2. If the STA and the authentication server authenticate each other successfully, both of them independently generate a Pairwise Master Key (PMK). Depending on the type of authentica-

tion mutually agreed between the STA and the authentication server, there could be several messages exchanged between them (flow 9) before the PMK is generated. The authentication server then transmits the PMK to the AP through a secure channel (for example, IPsec or TLS).

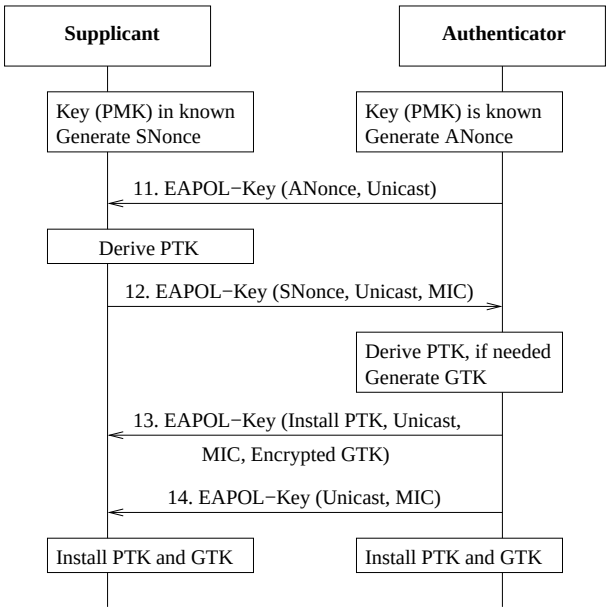

Fig. 3. RSN Key Establishment Phase

The next phase in the RSNA is the key distribution phase as illustrated in Figure 3. The PMK generated during the authentication phase is used 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 flows 11 - 14. Next, the group key handshake is initiated. 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 multi-cast messages are securely exchanged in the air.

Considering the RSN messages discussed above, in this paper we have analyzed the significance of RTT values for detecting anomalies. We have studied the RTT behavior of wireless hosts configured for EAP LEAP, PEAP and TLS authentication during their RSN association. In the next section we present the RTT values of the wireless hosts during normal conditions.

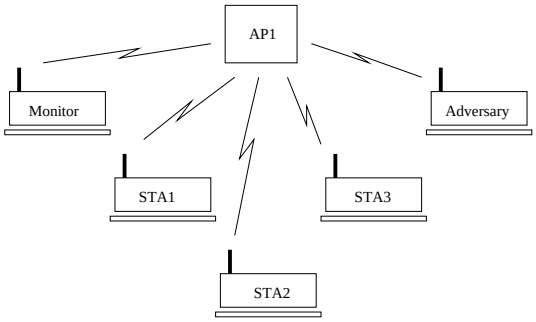

Fig. 4. Test Wireless Environment

4 Experiments

The experimental setup as shown in Figure 4 has a single Access Point (AP) and several wireless stations (STA) configured to authenticated with the AP using the different EAP authentication mechanisms. Here, STA1 and STA2 are both Linux machines and STA3 is a Windows XP machine. STA1 is configured for EAP-LEAP authentication, STA2 is configured for EAP-PEAP authentication and STA3 for EAP-TLS authentication. The Monitor is part of the data processing unit which captures wireless network traffic in promiscuous mode. The Adversary is capable of introducing various anomalies into the wireless network. When the experiments were carried out the test setup was exposed to the normal wireless environment of the university attracting traffic from various unspecified sources. Using this setup large number of wireless traces were collected and analyzed.

The software model for storing and calculating the timing values was built using PHP and MySQL. Basically the model takes the wireless traces as an input, processes it and stores them in a database table. Once the traces are stored in the database in a predefined format, the model queries the database and takes each of the EAP type traces separately and processes them and stores the RTT values together with various statistical information in another database table. One separate result table is used for one EAP Type method, for example if we want EAP TLS timing profile table we can generate it dynamically after the traces were stored in the database. The following pseudo code describes the derivation of the various statistical values from the database tables.

```
$result1 = query EAP specific Association Request Events from STA to AP
$result2 = query EAP specific Association Response Events from AP to STA
$rttsum = 0
$rttcount = 0

    while more rows in $result1
        fetch the next row in $result1 into $row1
        fetch the next row in $result2 into $row2

        while $row1 timing value > $row2 timing value
            fetch the next row in $result2 into $row2
        end while
```

```
            calculate current RTT value
            store current RTT value if it is the Maximum
            store current RTT value if it is the Minimum
            add current RTT value to $rttsum
            add one to $rttcount
        end while
calculate Average RTT
calculate Standard Deviation for RTT
```

The output RTT values table is defined based on each of the events associated with the respective EAP type. The timing profiles in these tables are the timing values to complete a particular round trip event during each of the EAP type specific authentication process. In this context a round trip event is considered to be the completion of two messages. The Request sent by the AP or STA and corresponding response received by the AP or STA. In order to present the values in a more functional manner the Mean, Maximum, Minimum, Standard deviation and the number of request and responses are calculated dynamically and stored. The Mean, Maximum and Minimum timing values together with the standard deviation gives the range of timings allowed for the round trip events during the normal operations.

5 Results and Analysis

Firstly, we present the measured RTT values of EAP LEAP, PEAP and TLS authenticated hosts during the RSN association process, under normal operations. In section 5.2, we present the RTT values of the these hosts under abnormal conditions from our experiments.

5.1 Normal behavior

Event	**Min (ms)**	**Max (ms)**	**Mean (ms)**	**StDev**
OPEN AUTHENTICATION	0.08	3.40	0.61	0.53
OPEN ASSOCIATION	0.51	2.65	0.65	0.29
EAP 1	0.05	2.57	0.79	0.43
EAP 2 (PEAP)	0.03	1.55	0.35	0.21
EAP 3 (LEAP)	0.42	1.30	0.48	0.13
EAP 4 (LEAP)	3.05	9.77	3.32	0.89
EAP Key Exchange	0.07	11.36	2.54	2.16
Overall	12.81	321.97	18.96	37.06

Table 1. EAP-LEAP Timing Profile

Table 1 shows the EAP-LEAP RTT values between AP1 and station STA1 obtained from a trace file consisting more than one hundred EAP-LEAP RSN associations, under normal conditions. The timing profile shows the allowable timing range required to complete a particular round trip event during normal EAP-LEAP authentication process. In this case, there are a total of seven

EAP-LEAP request/response messages. The maximum, minimum, mean and standard deviation values were calculated by the software model. This gives us an indication of the possible range of RTT values during the normal operations.

Event	**Min (ms)**	**Max (ms)**	**Mean (ms)**	**StDev**
OPEN AUTHENTICATION	0.37	0.61	0.44	0.05
OPEN ASSOCIATION	0.55	1.41	0.61	0.10
EAP 1	0.10	2.03	0.57	0.46
EAP 2 (PEAP)	0.23	4.24	2.05	0.80
EAP 3 (PEAP)	0.08	1.76	0.40	0.21
EAP 4 (PEAP)	0.02	1.49	0.83	0.41
EAP 5 (PEAP)	0.58	1.08	0.62	0.06
EAP 6 (PEAP)	0.36	0.59	0.45	0.03
EAP 7 (PEAP)	0.72	4.29	2.70	0.51
EAP 8 (PEAP)	0.08	2.50	0.60	0.44
EAP 9 (PEAP)	0.18	1.65	0.50	0.28
EAP Key Exchange	0.05	7.68	1.62	1.22
Overall	48.65	68.09	52.25	3.78

Table 2. EAP-PEAP Timing Profile

Table 2 shows the EAP-PEAP RTT values between AP1 and station STA2, obtained from a trace file consisting more than one hundred EAP-TLS RSN associations, under normal conditions. The timing profile shows the allowable timing range required to complete a particular round trip event during normal EAP-PEAP authentication process. Unlike for EAP-LEAP authentication, EAP-PEAP involves a total of twelve EAP-PEAP request/response messages.

Event	**Min (ms)**	**Max (ms)**	**Mean (ms)**	**StDev**
OPEN AUTHENTICATION	0.37	3.57	0.56	0.51
OPEN ASSOCIATION	0.11	9.07	0.85	0.85
EAP 1	36.25	106.13	53.91	8.24
EAP 2	10.89	89.74	25.69	11.11
EAP 3 (PEAP)	0.71	17.72	4.01	4.41
EAP 4 (TLS)	6.56	56.55	43.89	10.98
EAP 5 (TLS)	0.08	43.39	4.63	9.04
EAP 6 (TLS)	13.66	71.68	17.83	8.16
EAP 7 (TLS)	0.738	39.41	4.36	5.01
EAP Key Exchange	1.74	76.21	22.67	20.27
Overall	134.45	244.30	162.74	17.41

Table 3. EAP-TLS Timing Profile

Table 3 shows the EAP-TLS RTT values between AP1 and station STA3, obtained from a trace file consisting more than one hundred EAP-TLS RSN associations, under normal conditions. The timing profile shows the allowable timing range required to complete a particular round trip event during normal EAP-TLS authentication process. In this context a round trip event is considered to be the competition of two messages; a request and the corresponding response.

By approximating the RTT values to a standard normal distribution, we can specify an upper and a lower limit for RTT values (with one standard deviation above and below the mean value) of each EAP event. For example, in the case of EAP-TLS authentication, the lower limit of the overall RTT value would be 145.33 ms and the upper limit would be 180.15 ms. We can use these values as typical for timing anomaly detection.

5.2 Abnormal Conditions

Above discussed RTT profiles represent for normal behavior of EAP authenticated hosts. However when anomalies occur this behavior can change. There can be situations where the numbers of events are extraordinary high or low. There can also be situations where events can totally disappear from the respective range of the monitoring devices. Furthermore, abnormalities can be due to various wireless security attacks, such as, DoS, Man-in-the-Middle attack, Replay Attacks etc. Other reasons may be environmental disturbances. Since we are using IEEE 802.11 WLAN which operates on 2.4 GHz frequency band, it has higher probability of attracting noise and interferences. WLAN characteristics can vary widely, depending on device characteristics (e.g. antenna design and orientation) and environmental factors (e.g. floor plan). Following are some observations obtained during the abnormal conditions.

Event	**Time (ms)**
OPEN AUTHENTICATION	6.22
OPEN ASSOCIATION	4.28
EAP 1	6.11
EAP 2 (PEAP)	4.15
EAP 3 (LEAP)	3.27
EAP 4 (LEAP)	12.92
EAP Key Exchange	16.19
Overall	996.44

Table 4. Abnormal EAP-LEAP Timings

Table 4 is a good example of abnormal RTT values. These values are the average of more than ten experiments carried out by injecting abnormal management frames with EAP-LEAP authenticated hosts. According to these EAP-LEAP RTT values, almost every message exchange show significantly high RTT values resulting in high overall timing, compared with the normal values in Table 1. Also it can be seen that the timing values of every message exchange are highly unpredictable. Furthermore, statistically we can conclude that these timing values are abnormal since they do not fall within the 68% of the standard normal distribution. Figure 5 shows the mean and one standard deviation from mean values of EAP-LEAP RTT timings together with abnormal RTT values.

Table 5 shows another set of RTT values for EAP-PEAP authenticated hosts. These values are the average of more than ten experiments carried out by inject-

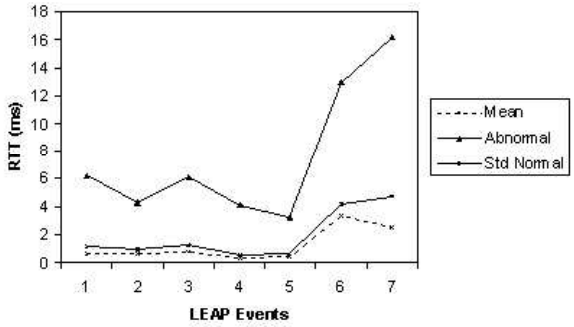

Fig. 5. EAP-LEAP Timings

Event	**Time (ms)**
OPEN AUTHENTICATION	8.26
OPEN ASSOCIATION	7.10
EAP 1	8.85
EAP 2 (PEAP)	6.07
EAP 3 (PEAP)	7.11
EAP 4 (PEAP)	12.47
EAP 5 (PEAP)	8.45
EAP 6 (PEAP)	11.99
EAP 7 (PEAP)	5.87
EAP 8 (PEAP)	9.64
EAP 9 (PEAP)	7.91
EAP Key Exchange	6.68
Overall	628.40

Table 5. Abnormal EAP-PEAP Timings

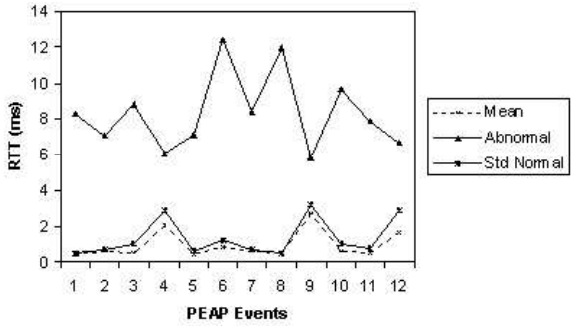

Fig. 6. EAP-PEAP Timings

ing abnormal management frames with EAP-PEAP authenticated hosts. Statistically, it is evident that most of the RTT values do not fall within the 68% of the standard normal distribution. Also, the first three RTT values are considerably high compared to the others. This is due to the unpredictable nature of the Open System association process, where hosts can be made to repeatedly deauthenticate and re-associate. The *zscore* (the number of standard deviations away from the mean) for the overall timing value is 150 in this case. Figure 6 shows the mean and one standard deviation from mean values of EAP-PEAP RTT timings together with abnormal RTT values.

Event	**Time (ms)**
OPEN AUTHENTICATION	3.07
OPEN ASSOCIATION	78.47
EAP 1	79.17
EAP 2	120.36
EAP 3 (PEAP)	16.11
EAP 4 (TLS)	89.24
EAP 5 (TLS)	25.26
EAP 6 (TLS)	33.21
EAP 7 (TLS)	44.75
EAP Key Exchange	35.69
Overall	1140.15

Table 6. Abnormal EAP-TLS Timings

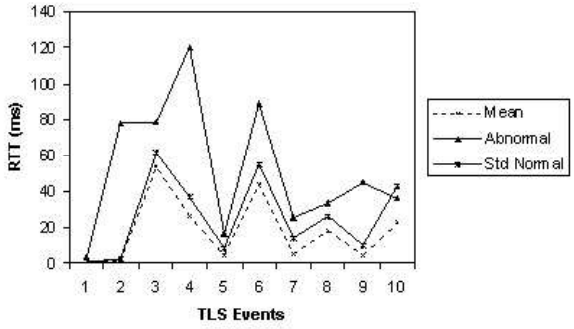

Fig. 7. EAP-TLS Timings

The RTT values shown in Table 6 can be considered as abnormal since the timing values for the EAP-TLS Request/Response messages are significantly high resulting in a high overall timing. These RTT values also do not fall within the 68% of the normal standard distribution. As we can see from Table 3 the normal RTT values, except for authentication and key exchange messages all

other messages do not lie within the acceptable deviation range and do not fall within standard normal distribution. In this case the *zscore* for the overall timing value is 56. Figure 7 shows the mean and one standard deviation from mean values of EAP-TLS RTT timings together with abnormal RTT values.

As seen in figures 5, 6 and 7 the mean RTT values for EAP-LEAP, PEAP, and TLS authenticated hosts are very much less than the abnormal RTT values. The three graphs can be used to visualize the significant differences between normal RTTs and abnormal RTTs for each event. Throughout our experiment we assumed that the calculated RTTs (using sample wireless traces) behave according to the normal distribution. Also RTT of a message exchange is a passive detection mechanism to detect unusual behaviors of the wireless as well as wired networks. Hence this technique may be used to detect intruders who can adversely affect the wireless network environment.

However this particular study does not address any specific type of wireless attacks. RTT measures can be used effectively in wireless networks if it is combined with appropriate statistical methods. In our future studies we will use two different statistical methods, namely t-test and Chi-square test to investigate the RTT values during different attack scenarios.

6 Conclusions

This study was conducted to investigate the characteristics of normal and abnormal RTT values of EAP-TLS, PEAP and LEAP authenticated wireless hosts. In this view we have presented a comparison between the normal and abnormal RTT values. The statistical timing values show that there is a significant variation between the values for normal and abnormal associations. This type of timing analysis may be useful to find out abnormalities in the wireless environment and may be helpful for wireless network intrusion detection and prevention.

In future work we will extend this research to find the best possible statistical representation for RTT values in various situations for a number of EAP type specific authentication methods. With more appropriate statistical representation we expect better intrusion detection and prevention capabilities.

References

1. B. Aboba and D. Simon. PPP EAP TLS Authentication Protocol. http://tools.ietf.org /wg/pppext/draft-ietf-pppext-eaptls/draft-ietf-pppext-eaptls-06.txt, August 1999.
2. AirDefence - intrusion protection and monitoring. http://www.airdefense.net/products/enterprise.php. Cited March 2006.
3. AirMagnet - wireless network management systems. http://www.airmagnet.com/products/enterprise.htm. Cited March 2006.
4. N. Asokan, V. Niemi, and K. Nyberg. Man-in-the-Middle in tunneled authentication protocols. Technical Report 2002/163, IACR ePrint archive, United Kingdom, October 2002.

5. L. Blunch and J. Vollbrecht. Extensible Authentication Protocol (EAP). http://www.ietf.org/rfc/rfc2284.txt, March 1998.
6. R. Gill, J. Smith, M. Looi, and A. Clark. Passive technique for detecting session hijacking attacks in ieee 802.11 wireless networks. In *AusCERT '05: Proceedings of the 4th Asia Pacific Information Technology Security Conference*, pages 26–38, May 2005.
7. 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.
8. IEEE Standard 802.11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, June 1999.
9. IEEE Standard 802.11i Part 11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements*, July 2004.
10. IEEE Standard 802.1X. *Local and Metropolitan Area Networks, Port-Based Network Access Control*, June 2001.
11. C. S. Inc. Cisco LEAP (LEAP). http://ietfreport.isoc.org/all-ids/draft-josefsson-pppext-eap-tls-eap-07.txt, October 2003.
12. Y. Lim, T. Schmoyer, J. Levine, and H. Owen. Wireless intrusion detection and response. In *Proceedings of the IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, volume 18, pages 68–75, June 2003.
13. M. Lynn and R. Baird. Advanced 802.11 attack., July 2002.
14. A. Palekar, D. Simon, G. Zorn, J. Salowey, H. Zhou, and S. Josefsson. Protected EAP Protocol (PEAP). http://ietfreport.isoc.org/all-ids/draft-josefsson-pppext-eap-tls-eap-07.txt, October 2003.
15. E. Sithirasenan and V. Muthukkumarasamy. Substantiating Security Threats Using Different Views of Wireless Network Traces. In *AusCERT'07: Proceedings of the 6th Asia Pacific Information Technology Security Conference*, pages 31–49, May 2007.
16. 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*, pages 181–190, April 2006.