Substantiating Security Threats Using Group Outlier Detection Techniques

Elankayer Sithirasenan
School of Information and
Communication Technology
Griffith University
Gold Coast, Australia
Email: e.sithirasenan@griffith.edu.au

Vallipuram Muthukkumarasamy
Institute for Intelligent and
Integrated Systems
Griffith University
Gold Coast, Australia
Email: v.muthu@griffith.edu.au

***Abstract*—With the increasing dependence on wireless LANs (WLANs), businesses, educational institutions and other organizations 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 profound 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 and substantiate both known and unknown security threats in WLANs. Our method exploits both timing and behavioral anomalies. We first observe for timing and/or behavior anomalies during the security association process and use outlier based data association approaches to substantiate their legitimacy. The proposed concept was tested on our experimental setup and the results obtained from EAP TLS 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], [2] provides effective measures to protect the wireless networks from confidentiality and integrity threats, their reliance on authenticity and availability are still a major concern. Further, the IEEE 802.11w standard (which is yet to be ratified), introduces protected management frames, guaranteeing more secure association process between wireless devices.

Although 802.11i and 802.11w 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 [3]. Hence in addition to improving the existing security mechanisms we also need other protection techniques to guard the wireless environment from new 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 analyzing them may reveal vital information about impending threats to the wireless environment.

It is realistic that in a wireless environment the behavior of access points (AP) vary from one vendor to another and depends on many factors. Hence, in order to analyze their behavior it is essential to maintain a behavioral profile for every participating wireless host (STA) - access point (AP) pair rather than having a generic profile for the environment. Throughput and resistance to one single node (STA) flooding depends on the actual implementation and operative system of the access point. A variation in timing during the association process for a given station depends on factors such as type of transversing traffic (number of packets and their sizes), UDP vs TCP traffic, number of traffic flows etc. Therefore, maintaining and analyzing dynamic profiles will be more effective than having static profiles. Hence, employing an adaptive technique to update the timing and behavioral profiles would be advantageous.

Trying to model what is "normal" in an AP is not an easy task, hidden nodes will trigger retransmissions and heavy real-time UDP traffic will have an impact in how packet queues are handled and hence the timing of management frames. Therefore, detecting a security threat merely based on timing and/or behavioral anomalies can lead to a large number of false positives. Hence, we explore the use of outlier based data association techniques to substantiate the security threats and thereby reducing the number of false positives.

This paper is organized as follows. Section II gives a brief overview of related work on intrusion and anomaly detection. Section III introduces the concept of OLAP and data views. The matrices used to substantiate the security threats are derived in Section IV. Details of experiments and their results are presented in Section V. In Section VI, we analyze the results and thereafter conclude the paper in Section VII.

II. Related Work

Analysis of IEEE 802.11i by He et al. [4] identifies a number of weaknesses in the standard and recommend some

978-1-4244-2324-8/08/$25.00 © 2008 IEEE.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.

solutions from the software/hardware implementation perspectives. A similar analysis by Sithirasenan et al. [5] 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 attack and expose the organizational network. Lynn et al. [6] 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. [7]. 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.

Barbeau et al. have analyzed impersonation attacks in future wireless and mobile networks [8]. They have performed a risk analysis on the possible types of impersonation attacks in wireless networks. Summing up their findings they stress that the risk of impersonation in wireless networks is critical since the threat can be materialized into several forms of attacks. Hence they highlight the need for effective countermeasures to address the threats.

The countermeasure proposed by Barbeau et al. [8] 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. [9]. They incorporate RFF into an ABID system to associate a MAC-address of a device with the corresponding transceiver profile. Hence, if an observed transceiver print from a claimed MAC-address matches the corresponding transceiver profile, then the MAC-address has not been spoofed. They make use of this idea to verify the credibility of their UMP based ABID system. 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.

Further enhancing their work, Gill et al. studied the anomaly detection response using correlation techniques in their later study [10]. Here, having detected an anomaly from either mechanism; Round Trip Timing (RTT) or Received Signal Strength (RSS), they wait for a confirmation from the other. For example, if the RSS detection algorithm registers an abrupt spike in RSS value for a particular MAC address, the correlation engine would register this and wait for the next RTS-CTS event for this MAC address and check the results of the RTT detection algorithm. If both algorithms register an alert for that MAC address, then an alarm would be raised. From a number of experiments performed they claim nil false negative and a low number of false positives. Hence they claim anomaly detection systems could not rely only on one observation and that multiple observations is necessary together with effective correlation techniques to verify the legitimacy of each alarms raised. However, this technique is not suitable in every situation since the legitimate user and the intruder can exhibit the same RSS and RTT.

Maxion et al. [11] 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.

Most data mining based intrusion detection systems detect unusual events or anomalous behavior in networks effectively [12]–[15]. However, the major problem is validating the legitimacy of abnormal events. Almost all of the work found in the literature present techniques to detect abnormal or rare events in networks. However, having found an anomalous or rare event how to validate it as legitimate or illegitimate is the major challenge yet to be addressed. In this view, discovery of outliers to extract a few data objects with abnormal behavior patterns, which are more imperative than common patterns in some cases, can be of practical significance in intrusion detection systems, credit fraud detection, etc [16]. Hence, in this study we investigate the use of outlier mining techniques to address the problem of validating the legitimacy of abnormal events.

III. OLAP and Data Views

A popular model for On-line Analytical Processing (OLAP) applications is the multidimensional database also known as the data cube [17]. A data cube consists of two kinds of attributes: dimensions and measures. The set of dimensions may consist of elements like IP addresses, port addresses, event identities etc. that together form a key. Measures are typically numeric elements like packet size, duration etc.

A data cube with five attributes will include a total of thirty two views. However, in an actual application although the number of attributes can be many, the required number of views may vary depending on the requirements. For example, if we assume that attribute “A” and “B” represent the identities of APs and STAs respectively, then for data association analysis between the APs and STAs we will consider only

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.

Reference	Attribute	Type
A	Source ID	Dimension
B	Destination ID	Dimension
C	Event ID	Dimension
D	Time of Day	Dimension
E	Channel ID	Dimension
F	Protocol ID	Dimension
G	Cipher ID	Dimension
-	Event count	Measure

TABLE I
DATA CUBE ATTRIBUTES

No.	Threat	Attributes
1	Replay attack	ABCDE, ABCE, ABCD, ABC, ACD, ACE, BCD, BCE, AC, BC
2	Message deletion	same as above
3	Masquerading and Malicious AP	BCDEFG, BCFG, BCDF, BCDG, BCEF, BCEG, BCD, BCE, BCF, BCG, BC, BD, BE, BF, BG
4	Session Hijack	ABCFG, ABCF, ABCG, ABC ABF, ABG, AB
5	Man-In-The-Middle (MitM)	same as above
6	Denial of Service (DoS)	ABC, AB

TABLE II
VIEWS ASSOCIATED WITH SECURITY THREATS

those views that consists of attributes "A" and "B", i.e. views "ABCD", "ABCE", "ABDE", "ABC", "ABD", "ABE" and "AB".

Table I presents the list of attributes that are stored in the data cube for our analysis. Since we are concerned with wireless traces in the association phase of the wireless devices, we store only those attributes that are necessary for this purpose. In this respect the identities (Source and Destination IDs) of the two communicating hosts, the current message (event) passed, the time during the message is passed, the channel on which the message is passed, the protocol used and the cipher used are stored in the data cube.

Table II shows the relationship between data cube views and some common security threats. This table was established considering each threat and identifying the attributes that are associated with the threat. Having identified the attributes, we then categorized the views that are vital for substantiating the security threat. For example in the case of Threat 1 - Replay Attack, we need to track the source and destination of every message in addition to the event identity. Hence, attributes A, B and C are important. However, attributes D (Time of Day) and F (Protocol ID) can be used to further refine the analysis. Therefore, to substantiate this threat we consider all views that include these attributes.

For Threat 6 - Denial-of-Service attack, we consider the events associated with the source and the destination. Hence, attributes A, B and C will be considered to substantiate this attack. In this manner we establish the necessary views that are useful for substantiating the various security threats.

The rationale for using data cube in our analysis is (i) we can readily utilize the advantages of OLAP, such as systematic storage of historical data and fast querying (ii) by linking the threat to the data cube views we can provide a suggestion about the type of threat and the possible solutions and (iii) the scaling of the entire system to meet the ever growing needs.

IV. QUANTIFYING SECURITY THREATS

In order to substantiate the security threats (using the data cube views) we established the notion of *group confidence*, extending the definitions discussed in [18]. The OLAP related definitions are obtained directly from OLAP with some minor changes [17], [19]. We then use the principles of information theory to derive mathematical expressions for *Group Confidence Level*.

Definition 1. Count

Function $count$ is defined in a natural way over the non-negative integers. $count(c)$ is the number of incidents that cell c contains. $count(c) = |content(c)|$.

Definition 2. Parent Cell

Cell $c' = (c'_1, c'_2, \ldots, c'_m)$ is the $parent\ \ cell$ of cell c on the kth attribute where $c'_k = *$ and $c'_j = c_j$, for $j \neq k$. Function $parent(c, k)$ returns $parent\ \ cell$ of cell c on the kth attribute.

Definition 3. Relative Frequency

$$R(c,k) = \frac{count(c)}{count(parent(c,k))} \tag{1}$$

We define $R(c, k)$ given by Equation 1 as *relative frequency* of cell c with respect to attribute k. We then define the *normalized support* for cell c as follows:

$$N(c,k) = -R(c,k)log(R(c,k)) \tag{2}$$

Higher values for *normalized support* indicate lower *relative frequencies*. Therefore, an event with very high *count* value will have lessor *normalized support* value compared to those events with less *count* values.

Definition 4. Uncertainty Function

Next, we define the *Uncertainty* function H to measure the uncertainty of a group of events. This uncertainty measure is defined in terms of the relative frequencies of n disjoint events associated with attribute k. One candidate uncertainty function that satisfies our requirements is the entropy: $H(X) = -\sum p_i \log(p_i)$. Thus, we have

$$H(c,k) = -\sum_{k \in 1 \ldots n} R(c,k) \log(R(c,k) \tag{3}$$

The uncertainty value provides an estimate as to how much abnormal a group of associated incidents is with respect to

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2008 proceedings.

normal events.

Definition 5. Group Confidence Level

Using the mathematical expression for *uncertainty* we establish the notion of *group confidence level* in relation to a group of associated events. This is defined as the ratio between the abnormal behavior and the normal behavior during a similar security association process. Hence, the group confidence level G is given by the following equation as a percentage.

$$G(c,k) = \left[\frac{H(c,k)}{log(n)}\right] * 100\% \quad (4)$$

The group confidence level G, thus obtained could be used as a scale to indicate the cohessiveness of a group of associated events.

V. Experiments and Results

In view of testing the above described concept, we proposed an Early Warning System (EWS) to detect and/or prevent intrusions in wireless networks. The EWS includes a packet capturing module, an event engine, a timing anomaly detection module, a behavioral anomaly detection module, an intrusion prevention module and the data mining engine. The data mining engine is the main component of our EWS with the ability of processing outlier based data association requests effectively, preventing intrusions in real time. The EWS have several levels of defense offering improved reliability for anomaly detection. The first level of defense is the discovery of timing anomalies followed by the discovery of behavioral anomalies. If an event is discovered with either or both anomalies a third level of defense is triggered to substantiate the legitimacy of the anomalies based on historical data. Since the EWS needs to search enormous amounts of historical data in real time we use parallel processing techniques to search the database. A more detailed description of the EWS can be found in [20].

The test setup used to perform the various experiments consists of several IEEE 802.11i configured access points and stations. Using this setup a number of experiments were carried out to validate the proposed substantiation mechanism. Two different types of security threats; Denial-of-Service (DoS) attack and Replay attack were executed in order to study the effectiveness of our substantiation technique in validating the timing and behavioral anomalies. Preliminary experimental results on timing and behavioral studies for EAP-LEAP and EAP-PEAP authenticated stations can be found in [21] and for EAP-TLS stations in [22]. Extending on this work, here, we present and analyze the substantiation of detected anomalies using *group confidence levels* on EAP-TLS configured stations.

Figure 1 shows the normalized support (Equation 2) for EAP-TLS events. These readings were obtained from our experimental setup during normal operations. Here, we use

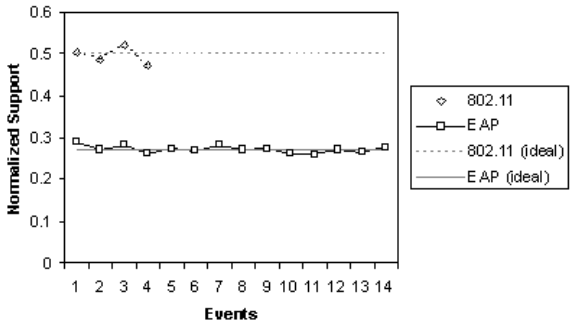

Fig. 1. Normal EAP-TLS Authentication

Parameter	$Ideal\ Norm.Supp$	$H(k)$	$G(k)$
802.11	0.50	1.98	99.25
EAP	0.27	3.80	99.96

TABLE III
EAP-TLS Measurements

the term normal operation meaning that there was no abnormal events introduced explicitly. However, the wireless environment was exposed to the regular campus wide wireless traffic. The diagram also indicates the ideal *normalized support value* (Table III) for both IEEE 802.11 and EAP events. The event numbers used in these diagrams are serial values that correspond to the various EAP-TLS events.

In Figure 1, the *normalized support values* for most events have *support values* close to the *ideal normalized support*. Although we can notice some deviation from the ideal support values, the overall confidence is high as shown in Table III. The table lists the *uncertainty* (Equation 3) and the *group confidence levels* (Equation 4) of IEEE 802.11 and EAP group events during EAP-TLS authentication.

From these results it is evident that EAP-TLS authentication scheme demonstrates high confidence levels (above 99.25%) during normal operations irrespective of those events deviating from *ideal support values*. This is due to the fact that all IEEE 802.11 and EAP events, as a group, behave in a moderately predictable manner under normal conditions. However, under abnormal conditions their group behavior cannot be guaranteed. To verify our claim we consider two abnormal situations in the wireless environment and discuss their results.

Figure 2 shows the normalized support for EAP type specific events on wireless stations configured for EAP-TLS authentication, during a DoS attack. In this case the *normalized support values* of IEEE 802.11 events deviate considerably from the ideal support values. For 802.11 association events support values deviate from 0.5 to about 0.02. In the case of EAP events the support value varies between 0.4 and 0.15. This is because of the "Deauthentication" frames injected. Consequently, this demonstrates the unreliable nature of 802.11 open system association.

During the DoS attack, events "ASSOCIATION REQUEST" (3) and "ASSOCIATION RESPONSE" (4) have

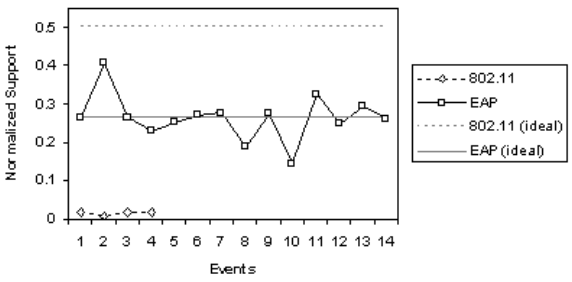

Fig. 2. DoS Attack during EAP-TLS Authentication

Parameter	EAP-TLS Authentication			
	DoS		Replay	
	802.11	EAP	802.11	EAP
$H(k)$	1.04	3.91	1.71	3.85
$G(k)$	40.36	90.53	73.60	94.29

TABLE IV
QUANTIFYING ATTACKS

almost equal *count*. This is due to the legitimate reassociation after a deauthentication. However, compared to the "DEAUTHENTICATION" (2) events the *count* for "AUTHENTICATION" (1) events is less because of the high number of injected "Deauthentication" frames. Similarly, the EAP events also have less count compared to the 802.11 "DEAUTHENTICATION" events. This is again because of the large number of "Deauthentication" frames injected and the reassociation does not take place at the same pace, since the channel is busy with "DEAUTHENTICATION" events.

On the other hand, if we look at the EAP events, except for some EAP events most of the events have support values close to ideal. Nevertheless, this demonstrates that the EAP-TLS authentication process could still be interrupted, resulting in fresh reassocation. In the next section we analyze a Replay attack comparing the results with that of the DoS attack.

VI. ANALYSIS

As discussed above, Figure 2 demonstrates the behavior of association events during the DoS attack. It shows that both 802.11 and EAP events are vulnerable to the attack. To further investigate this behavior we calculated the uncertainty and the confidence level for each case. As shown in Table IV, the confidence levels for IEEE 802.11 events (during DoS) are comparatively low (40.36%) indicating very poor resistance to DoS attack. In contrast, the confidence level for EAP events are not low as for 802.11 events. Hence, it is evident that EAP events are more consistent and hence more reliable than the 802.11 events.

Figure 3 shows the normalized support for EAP-TLS authentication events during, during a Replay attack. Here again, the *count* for 802.11 events were high because of the "Authentication" and "Association Request" frames injected. Consequently, as in the case of DoS attack this demonstrates

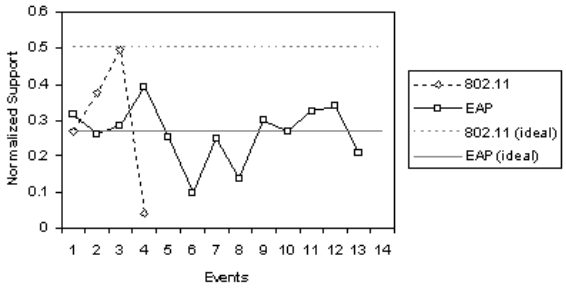

Fig. 3. Replay Attack during EAP-TLS Authentication

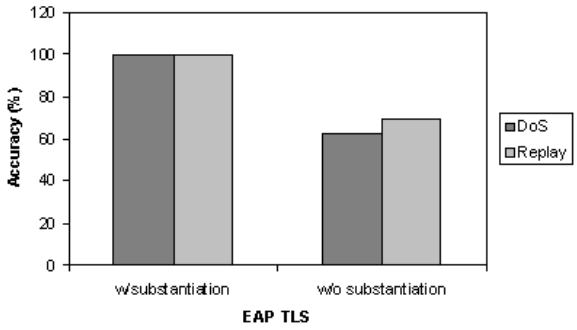

Fig. 4. EWS Accuracy with Substantiation

the unreliable nature of 802.11 open system association. In this case the events "AUTHENTICATION" (1) and "ASSOCIATION REQUEST" (3), both replayed messages, have very high *count* indicating the Replay attack.

Next, let us consider the EAP type specific events. As in the case of DoS attack some EAP events demonstrate close to ideal support and the others deviate considerably. To further investigate, we calculated the *uncertainty* and the *confidence level* for each case. As shown in Table IV the confidence level for 802.11 events is low (73.60) and is high (94.29) for EAP events.

Figure 4 shows the accuracy of our EWS with and without substantiation in a wireless environment with different number of abnormalities. Here the abnormalities were forced with some having an effect on the wireless hosts and the others being replications. The EWS without substantiation raised large number of false alarms and the EWS with substantiation demonstrated 99% accuracy. The large number of alarm values raised when substantiation was not effective was due to the fact that it was merely reporting all timing and/or behavior anomalies as security threats.

In the foregoing paragraphs we have discussed the vulnerabilities of the various protocols and how they affect the overall confidence of the security association. The results demonstrate the need for protected management frames to guarantee a reliable association process. However, in the case of RSN, it is important to note, that although IEEE 802.11 and EAP protocols may demonstrate low confidence levels, it is up

to the security policy maker to substantiate it appropriately, depending on user privileges. In the two attack scenarios discussed even though the behavior indicates that the RSN is unstable during the 802.11 and EAP protocol phases, it only affects the "availability" of the stations and does not compromise the "authenticity". Hence, when formulating the security threat levels one has to consider a range of factors, such as the user priorities, the required level of sensitivity etc. and set optimal thresholds to arrive at appropriate decisions.

VII. Conclusions

In this paper, we have discussed the use of group confidence level for substantiating anomalies. The proposed method is developed based on combining data mining methods with anomaly detection techniques. For this purpose we have considered both Replay and DoS attacks and demonstrated the use of confidence level as a measure of group cohesiveness. Any associated group of events under normal conditions demonstrate very high cohesiveness. In this context, the experimental results obtained with the 802.11i based network are promising and confirming the concept of the proposed method. Although, the confidence level approach does not detect all of the security threats, it is capable of detecting group abnormalities as shown in Replay and DoS attacks.

Further, we have also shown the effectiveness of our mechanism in terms of detection accuracy with and without substantiation. However, we have not compared our mechanism directly with other similar systems. Furthermore, we have not considered all of the possible security threats discussed in section III. However, the main contribution of this study is the novel substantiation mechanism. Our proposed concept may be extended to several fields including credit card security, health monitoring systems, Internet security, maritime border security, air traffic control and the like. The wireless environment considered in this paper is one such example where the number of anomalies and their nature can vary significantly. In the future work, we intend to extend on this concept to detect and categorize most of the other security threats.

Acknowledgment

We thank Prof. Frank Dehne of Carlton University in Ottawa, Canada for his advice on the use of data cubes on this work. We also thank Prof. Todd Eavis at Concordia University in Montreal, Canada for providing us with the software for generating and querying the data cube.

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] *IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2007, June 2007.

[3] 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.

[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] 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.

[6] M. Lynn and R. Baird, "Advanced 802.11 attack." Las Vegas, USA, July 2002.

[7] N. Asokan, V. Niemi, and K. Nyberg, "Man-in-the-Middle in tunneled authentication protocols," IACR ePrint archive, United Kingdom, Tech. Rep. 2002/163, October 2002. [Online]. Available: http://eprint.iacr.org/2002/163/

[8] 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.

[9] 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.

[10] R. Gill, J. Smith, and A. Clark, "Experiences in passively detecting session hijacking attacks in ieee 802.11 networks," in *AISW-NetSec '06: Proceedings of the 4th Australasian Information Workshop*, vol. 54, January 2006, pp. 26–38.

[11] 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.

[12] S. Manganaris, M. Christensen, D. Zerkle, and K. Hermiz, "A data mining analysis of rtid alarms," *Comput. Networks*, vol. 34, no. 4, pp. 571–577, 2000.

[13] C. Clifton and G. Gengo, "Developing custom intrusion detection filters using data mining," in *MILCOM 2000: Proceedings of the 21st Century Military Communications Conference*, vol. 1, October 2000, pp. 440–443.

[14] D. Barbar, N. Wu, and S. Jajodia, "Detecting novel network intrusions using bayes estimators," in *Proceedings of the First SIAM Conference on Data Mining*, April 2001, pp. 182–191.

[15] G. Florez, S. Bridges, and R. Vaughn, "An improved algorithm for fuzzy data mining for intrusion detection," in *NAFIPS 2002: Proceedings of the Annual Meeting of the North American Fuzzy Information Processing Society*, June 2002, pp. 457–462.

[16] E. Bloedorn, A. D. Christiansen, W. Hill, C. Skorupka, L. M. Talbot, and J. Tivel, "Data mining for network intrusion detection: How to get started," http:// www.mitre.org/work/tech_ papers/tech_ papers_01/bloedorn_ datamining/bloedorn_ datamining.pdf, August 2001.

[17] J. Gray, S. Chaudhuri, A. Bosworth, A. Layman, D. Reichart, M. Venkatrao, F. Pellow, and H. Pirahesh, "Data cube: A relational aggregation operator generalizing group-by, cross-tab, and sub-totals," *J. Data Mining and Knowledge Discovery*, vol. 1, no. 1, pp. 29–53, 1997. [Online]. Available: citeseer.ist.psu.edu/gray97data.html

[18] S. Lin and D. Brown, "An outlier-based data association method for linking criminal incidents," *Decision Support Systems*, vol. 41, no. 3, pp. 604–615, March 2006. [Online]. Available: http://www.sciencedirect.com/science/article/B6V8S-4DFT4HY-1/2/72b8c46bff2d3906934424feb82dab3b

[19] "Olap council," http://www.olapcouncil.org, cited March 2006.

[20] 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.

[21] ——, "Detecting Security Threats in Wireless LANs Using Timing and Behavioral Anomalies," in *ICON'07: Proceedings of the 15th IEEE International Conference on Networks*, November 2007, pp. 66–71.

[22] ——, "Substantiating Security Threats Using Different Views of Wireless Network Traces," in *AusCERT'07: Proceedings of the 6th Asia Pacific Information Technology Security Conference*, May 2007, pp. 31–49.