Detecting Impersonation Attacks in Future Wireless and Mobile Networks*

Michel Barbeau, Jyanthi Hall, and Evangelos Kranakis

School of Computer Science, Carleton University, Ottawa, K1S 5B6, Canada

Abstract. Impersonation attacks in wireless and mobile networks by professional criminal groups are becoming more sophisticated. We confirm with simple risk analysis that impersonation attacks offer attractive incentives to malicious criminals and should therefore be given highest priority in research studies. We also survey our recent investigations on Radio Frequency Fingerprinting and User Mobility Profiles and discuss details of our methodologies for building enhanced intrusion detection systems for future wireless and mobile networks.

1 Introduction

As wireless systems are increasingly being used for critical communication it is becoming a challenge to keep electronic data transmissions secure. In general, it is difficult to implement effective security in small-footprint devices having low processing power, low memory capacity and using unreliable, low bandwidth. It is proving challenging to adapt wire-line technologies to the constrained mobile/wireless environment, enforce backward compatibility, and take account of heterogeneity.

Existing wire-line intrusion detection systems (IDSs) are classified either by the data collection mechanism (host-based, network-based), or by the detection technique (signature-based, anomaly-based, specification-based). No such simple classification is possible in wireless systems which are characterized by unavailability of key traffic concentration points, impossibility to rely on a centralized server, difficulty to secure signature distribution, and possible presence of *rogue* hosts.

Enabling wireless technologies like WTLS (Wireless Transport Layered Security) within WAP (Wireless Application Protocol), WEP (Wired Equivalent Privacy), TKIP (Temporal Key Integrity Protocol), Counter Mode CBC-MAC, Wireless PKI, Smart Cards, offer security with various degrees of success. Nevertheless, wireless devices (smart phones, PDAs, etc.) with Internet connectivity are becoming easy targets of malicious code (Cabir, Skulls, Mquito, Wince.Duts, Metal Gear, Lasco, Gavno, etc.) The question arising is *why can we not merely adapt methods from wire-line security?* We cannot, because wireless security is

* Research supported in part by NSERC (Natural Sciences and Engineering Research Council of Canada) and MITACS (Mathematics of Information Technology and Complex Systems) grants.

M. Burmester and A. Yasinsac (Eds.): MADNES 2005, LNCS 4074, pp. 80–95, 2006.

different from wire-line security. In fact wireless networks lack appropriate security infrastructure, and give potential attackers easy transport medium access. Rogue wireless access points deserve particular attention since they are not authorized for operation. They are usually installed either by employees (that do not understand security issues) or by hackers (to provide interface to a corporate network). Attention has been paid to finding rogues by using 1) wireless sniffing tools (e.g., AirMagnet or NetStumber), walking through facilities and looking for access points that have authorized Medium Access Control (MAC) addresses, vendor name, or security configurations, 2) a central console attached to the wired side of the network for monitoring (e.g., AirWave), 3) a free Transmission Control Protocol (TCP) port scanner (e.g., SuperScan 3.0), that identifies enabled TCP ports. However, are these techniques effective?

Attacks can be undertaken from an *armchair* or *war-walking* or even *war-driving*. Malicious attackers can be divided into two types. 1) *Focused attackers:* these are full time, dedicated professionals who have nothing better to do than target a specific enterprise. 2) *Opportunistic attackers:* that will attack a wireless network because it is there (a target of opportunity with no functional level of security that can be easily compromised). Although several attacks have been addressed including active/passive eavesdropping, man-in-the-middle, replay (including de-authentication and de-association), session hijacking, using traffic analysis, and masquerading, existing authentication schemes cannot fully protect hosts from well-known impersonation attacks.

1.1 Outline of the Paper

In this paper, first we confirm in Section 2 with simple risk analysis that impersonation attacks in wireless and mobile networks offer strong incentives to malicious criminal groups and should therefore be given highest priority in research studies. In Section 3, we survey our recent investigations on Radio Frequency Fingerprinting and User Mobility Profiling and discuss details of our methodologies for building enhanced intrusion detection systems that may prove more effective against impersonations attacks in future wireless and mobile networks.

2 Risk Analysis

An important aspect in the study of security is the understanding that not all threats are equally severe. Risk analysis enables the separation of the critical or major threats from the minor ones. Indeed, an attacker explicitly targets a wireless network only if there are valuable enough assets to pursue and payoffs are worthwhile. In understanding the risks, knowledge of the real threats helps place in context the complex landscape of security mechanisms. In this paper, we follow the risk assessment methodology by ETSI [8]. The evaluation is conducted according to three criteria: likelihood, impact and risk. The *likelihood* criterion ranks the possibility that a threat materializes as attacks. Two factors are taken into account: technical difficulties that have to be addressed by an attacker and motivation for an attacker to conduct an attack. The range of values for the

likelihood is low (1), possible (2) and likely (3) respectively corresponding to a level of difficulty which is high, moderate or low or a level of motivation which is low, reasonable or high. The *impact* criterion ranks the consequences of an attack materializing a threat. The range of values for the impact is low (1), medium (2) or high (3) respectively corresponding to a threat that results in annoyance with reversible consequences or limited scope outages; loss of service for a considerable amount of time or limited financial losses; and loss of service for a long period of time, several affected users, violations of law or substantial financial losses. The likelihood and impact criteria receive numerical values from one to three (indicated between the parentheses). For a given threat, the *risk* is defined as the product of the likelihood and impact. If the numerical value of the risk is one or two, then the threat is considered to be minor and there is no need for countermeasures. If the risk is three of four, then the threat is major and needs to be handled. If the risk is six or nine, then the threat is critical and needs to be addressed in priority. We analyze hereafter the risk of impersonation in wireless networks. The results are summarized in Table 1.

2.1 Risk of Impersonation

Impersonation takes the form of device cloning, address spoofing, unauthorized access, rogue base station (or rogue access point) and replay. Device cloning consists of reprogramming a device with the hardware address of another device. This can be done also for the duration of one frame, which is an operation termed MAC address spoofing. This is a known problem in unlicensed services such as WiFi/802.11. It is an enabler for unauthorized access and various attacks such as the de-association or de-authorization attack. The problem has been under control in cellular networks. Cell phone cloning has been made illegal in many countries. It is interesting to note that a recent case of CDMA phone cloning occurred in India [17]. In WiFi/802.11 networks, the identity of a device, i.e. its hardware address, can be easily stolen over the air by intercepting frames. Presently, no wireless access technology offers perfect identity concealment over the air. Device cloning (including MAC address spoofing) is likely to occur. Some of the aforementioned attacks can cause service disruptions for considerable amounts of time. It is a threat which has at least a medium impact. There is therefore a major risk associated with the device cloning threat.

Impersonation of a legitimate user can be done to obtain unauthorized access to a wireless network. Authorization at user level has been introduced in both WiFi/802.11 [30], [5] and WiMax/802.16 [23] to mitigate the threat. A detailed analysis is conducted for WiMax. The situation is similar for WiFi. In WiMax/802.16, authorization occurs after scanning, acquisition of channel description, ranging and capability negotiation. There are three options for authorization: device list-based, X.509-based or EAP-based. If device list-based authorization is used only, then the likelihood of a subscriber impersonation attack is likely. X.509-based authorization in WiMax/802.16 uses certificates installed in devices by their manufacturers. If X.509-based authorization is used, the likelihood for a subscriber to be the victim of impersonation is possible in

particular if certificates are hard coded and cannot be either renewed or revoked. The Extensible Authentication Protocol (EAP) is a generic authentication protocol [2]. EAP can be actualized with specific authentication methods such as EAP-TLS (X.509 certificate-based) [3] or EAP-SIM [14]. If EAP-based authorization is used, we believe that at this time it is safe to say that the likelihood of a subscriber impersonation attack is possible. Some of the EAP methods are being defined; security flaws are often uncovered in *unproven* mechanisms. Aboba maintains a Web page about security vulnerabilities in EAP methods [1]. It is a good idea to allow a second line of defense to play safe with EAP-based authentication. The impact of unauthorized access is medium, at least because, of the possible theft of network resources. Overall, the risk of unauthorized access in wireless networks is major or critical.

A *rogue base station* (or access point) is an attacker station that imitates a legitimate base station. The rogue base station confuses a set of subscribers (or clients) trying to get service through what they believe to be a legitimate base station. It may result in long disruptions of service. Attacks materializing this threat have high impact. The exact method of attack depends on the type of network. In a WiFi/802.11 network [29], which is carrier sense multiple access, the attacker has to capture the identity of a legitimate access point. Then it builds frames using the legitimate access point's identity. It then injects the crafted messages when the medium is available. In a WiMax/802.16 network [23], this is more difficult to do because WiMax/802.16 uses time division multiple access. The attacker must transmit while the impersonated base station is transmitting. The signal of the attacker, however, must arrive at targeted receiver subscribers with more strength and must put the signal of the impersonated base station in the background, relatively speaking. Again, the attacker has to capture the identity of a legitimate base station. Then it builds messages using the stolen identity. The attacker has to wait until time slots allocated to the impersonated base station start and transmit during these time slots. The attacker must transmit while achieving a *receive signal strength* higher than the one of the impersonated base station. The receiver subscribers reduce their gain and decode the signal of the attacker instead of the one from the impersonated base station. The rogue base station is likely to occur as there are no technical difficulties to resolve. EAP supports mutual authentication, i.e. the base station also authenticates itself to the subscriber. When EAP mutual authentication is used, the likelihood of the threat is mitigated, but not totally and remains possible for reasons similar to the ones aforementioned for EAP-based authorization. The rogue base station or access point attack is therefore a threat for which the risk is critical.

Replay protection insures that messages are freshly generated and are not retransmissions by attackers of previously intercepted messages. For the sake of efficiency, replay protection is often combined with message authentication. The first generation of WiFi/802.11 wireless networks adopted Wired Equivalent Privacy (WEP) for encryption [29]. WEP does not address either message authentication or replay protection. Recent developments, namely the WiFi

Protected Access (WPA) [5] and standard 802.11i [30], introduced much stronger confidentiality protection mechanisms in WiFi/802.11 networks. Firstly, encryption key establishment uses asymmetric key-based techniques. Secondly, WPA uses the Temporal Key Integrity Protocol (TKIP), which is RC4-based but with longer non reused keys. TKIP comprises a mechanism to insure message integrity and avoid replay, the Michael method. 802.11i supports both TKIP and Advanced Encryption Standard (AES). WiMax/802.16e uses the Data Encryption Standard (DES) or Advanced Encryption Standard (AES) to encrypt data traffic PDUs [23]. The AES includes a mechanism for the protection of integrity of data messages, their authentication and replay protection. DES does not. Replay protection of control traffic did not receive the same level of attention. In WiMax/802.16, management messages are never encrypted and not always authenticated. There are authentication mechanisms for layer management messages: the hashed message authentication code (HMAC) tuple and one-key message authentication code (OMAC) tuple. The OMAC is AES-based and includes replay protection, while to HMAC does not. The authentication mechanism for management messages to be used is negotiated at network entry. The scope of management messages to which authentication is applicable is limited in earlier versions of 802.16 (has been extended in version *e*). Hence, with earlier versions of 802.16 the management messages are not subject to integrity protection. Weaknesses in management messages authentication open the door to aggressions such as the man in the middle attack or rogue base station attack. The likelihood of replay attack is likely, possible or unlikely if no authentication, HMAC or OMAC is used respectively for management messages. In all cases, the impact of an attack of that type can be high because it might affect the operation of the communications. The risk is major or critical. It might be safe to allow a second line of defense against this type of attack in all the cases. Hence, it is a critical threat. The following table summarizes conclusions of our discussion.

Table 1. Risk of impersonation

Attack	Likelihood	Impact	Risk
Device cloning	Likely (3)	Medium (2)	Critical (6)
Unauthorized access			
with device list-based auth.	Likely (3)	Medium (2)	Critical (6)
with manufacturer certificate-based auth.	Possible (2)	Medium (2)	Major (4)
with EAP-based auth.	Possible (2)	Medium (2)	Major (4)
Rogue base station			
without mutual auth.	Likely (3)	High (3)	Critical (9)
with EAP-based mutual auth.	Possible (2)	High (3)	Critical (6)
Replay			
without message auth.	Likely (3)	High (3)	Critical (9)
with HMAC	Possible (2)	High (3)	Critical (6)
with OMAC	Unlikely (1)	High (3)	Major (3)

To sum up, the risk of impersonation in wireless networks is critical since the threat can be materialized into several forms of attack. Countermeasures are needed to address the threat.

3 Detecting Impersonation Attacks Using Device and User Profiles

One of the well known instantiations of identity theft, in WiFi/802.11 networks, is referred to as device cloning or Media Access Control (MAC) address spoofing. As aforementioned, this attack is carried out by obtaining the MAC address of a legitimate device, using tools that are readily available, e.g. NetStumbler [22]. This address is programmed into another device and subsequently used for obtaining unauthorized access to a Wireless Local Area Network (WLAN). Thus, the continued use of an access control list (ACL), based on MAC addresses, which are easily malleable, is no longer a viable strategy.

In order to address device cloning and MAC-address spoofing, authentication-based resolution strategies and intrusion detection-based countermeasures have been proposed. As far as resolution strategies are concerned, the use of public-key cryptography, although theoretically feasible, has some limitations. As the public/private key pair represents static data (unless it is changed periodically and that is unlikely), it can potentially be discovered using over the air and other mechanisms, especially since tamper-resistant hardware and software for hand held devices are still costly [32]. Another disadvantage [18] of this solution is the time required to manually type each MAC address and its associated public key into each access point. Unless the cost of administration is reduced via automation, this solution may not be suitable but for smaller networks. Finally, the level of resources required for public key cryptography is currently unavailable in wireless devices. Although this limitation will not persist for any length of time, as stated by Barbeau and Robert [6], even the use of elliptic key cryptography demands a level of resources that exceeds current availability.

Given these limitations and requirements, organizations may opt to address this problem using countermeasures, including intruder location by Adelstein et al. [4], commercial IDSs (e.g. AirDefense [16]) and user mobility patterns (UMPs) by Spencer [31]. Unlike the use of public-key cryptography, the use of intruder location or user mobility patterns, is less susceptible to forgery and impersonation attacks. For one thing, as intrusion detection mechanisms, both exploit behavioral characteristics or features, which are more difficult to forge or replicate. Whereas the intruder location mechanism examines the signal strength of WiFi/802.11 nodes, the use of UMPs is adopted in [31]. Second, both strategies require that an association, between a given MAC-address and its corresponding profile, be maintained for the purpose of detecting MAC-address spoofing. Essentially, it exemplifies the concept of using two or more pieces of identification for corroborating the identity of individuals. As far as commercial products are concerned, AirDefense does prevent MAC address spoofing by looking at the address prefix. However, this approach is limited in that the IDS makes a

distinction between devices based only on the manufacturer's identification. Hence, the need to identify devices, from the *same* manufacturer, remains unfulfilled.

In light of these circumstances, there is an opportunity to further explore the use of device-based and user-based features for addressing the aforementioned problem. The application of Radio Frequency Fingerprinting (RFF) and UMPs for Anomaly-Based Intrusion Detection (ABID) is presented next. Readers are encouraged to consult the work by Hall [10] for additional details.

3.1 Radio Frequency Fingerprinting

RFF is a technology, which has been designed to capture the unique characteristics of the radio frequency energy of a transceiver, in RF-based wireless devices. Pioneered by the military to track the movement of enemy troops, it has been subsequently implemented, as an authentication mechanism, by some cellular carriers (e.g. Bell Nynex), to combat cloning fraud [24].

The key benefit of employing this technique is the increased level of difficulty, associated with the replication of a transceiverprint, i.e. a set of features extracted from the transient of a signal. As illustrated in Figure 1, the transient of a signal is associated with the start-up period of a transceiver prior to transmission. Even more importantly, it reflects the unique hardware characteristics of a transceiver. Consequently, it cannot be easily forged, unless the entire circuitry of a transceiver can be accurately replicated (e.g. requiring the theft of an authorized device).

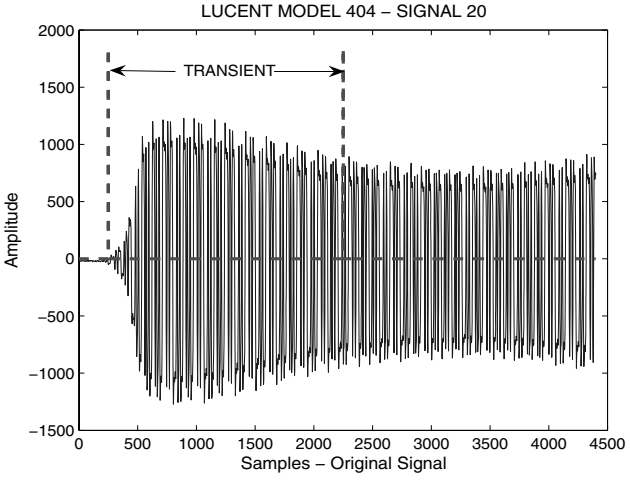

Fig. 1. Signal from a 802.11b transceiver

It is precisely this feature that has been exploited for the purpose of identifying RF-based transceivers. More specifically, a profile of each transceiver (using transceiverprints) is first created, followed by the classification of an

observed transceiverprint as normal or anomalous, i.e. it does not match the transceiver profile.

3.2 RFF - Related Work

Since 1995, the level of interest in RFF continues to rise, partly motivated by the need to identify malfunctioning or illegally operated radio transmitters, in support of radio spectrum management practices. In the paper by Ellis and Serinken [7], the authors examine the amplitude and phase components of signals, captured from various transceivers (some from the same manufacturer). The general conclusion is that all transceivers do possess some consistent features (derived from amplitude and phase components), although these features may not be necessarily unique.

As far as the detection of transients is concerned, several strategies have been explored. Proposed by Shaw and Kinsner in 1997, the Threshold detection approach [28] is based on the amplitude characteristics of the signal.

Another approach, which is also based on the variance of the amplitude, is the Bayesian Step Change Detector, proposed by Ureten and Serinken [35]. Unlike the previous approach, the detection of a transient does not require the use of thresholds, i.e. it is based exclusively on the characteristics of the amplitude data. However, as the performance is less than optimal for certain types of signals, e.g. WiFi/802.11 and Bluetooth, the authors have recently proposed an enhanced detection method, referred to as the Bayesian Ramp Change Detector [27].

Finally, Hall, Barbeau and Kranakis [11] have also experimented with the use of phase characteristics of signals for detecting the start of transients. This approach can be used with WiFi/802.11 and Bluetooth signals.

In terms of classification, the use of a pattern-based classifier, such as the PNN, is advocated by many research teams including Shaw [28], Hunter [15] and Tekbas *et al.* [33]. The use of genetic algorithm for classification purposes has also been explored by Toonstra and Kinsner [34]. Aside from obtaining an optimal solution, this approach is rather resource-intensive. Hence, the use of genetic algorithms may not be appropriate for resource-constrained devices.

3.3 RFF - Its Use in ABID

Unlike the use of RFF for identification purposes, another option is to incorporate it into an ABID system, as illustrated by Hall, Barbeau and Kranakis [12]. The idea is to associate a MAC-address of a device with the corresponding transceiver profile. Henceforth, if an observed transceiverprint from a claimed MAC-address, matches the corresponding transceiver profile, then the MAC-address has not been spoofed.

It is generally known that current IDSs render a decision, as to whether an observed behavior/event is normal or anomalous, based on a *single* observation. In an environment that is characterized by interference and noise, delaying the decision until *multiple* observations have been classified and combined reduces the level of uncertainty. Thus, the Bayesian filter, presented by Russell and Norvig in [25], can be used to achieve this goal.

In the past, the use of static profiles has generally been the norm. However, due to factors, such as transceiver aging, there is a need to periodically capture the altered characteristics of a transceiver. Therefore, this notion of concept drift (i.e. change in behavior over time) is addressed by continuously updating the profile of a transceiver.

3.4 RFF - Evaluation

The purpose of the evaluation is two-fold: 1) to primarily assess the composition of the transceiverprint, based on the false alarm and detection rates and 2) to determine the impact of profile updates on these metrics.

Evaluation results for each of the 30 profiled transceivers are depicted in Figure 2. The false alarm rate (FAR), for a given transceiver, is defined as the number of reported anomalous transceiverprints divided by the total number of transceiverprints, which belong to the transceiver. On the other hand, the detection rate is similarly defined, but using the transceiverprints from the remaining transceivers. These transceivers are used for simulating intrusions. In addition, a 95% confidence interval is used for rending a classification decision, i.e. normal or anomalous.

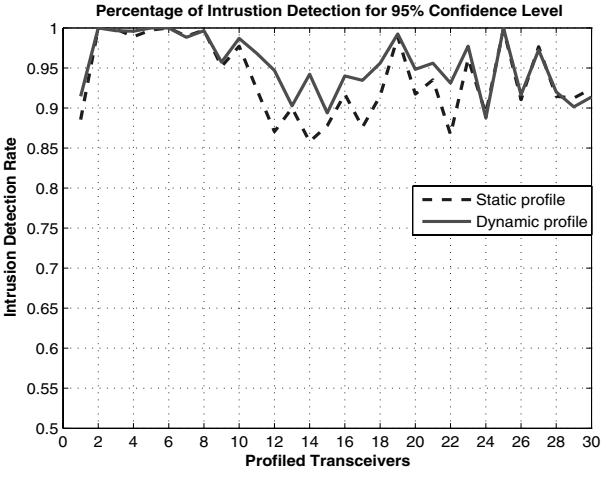

Fig. 2. Intrusion detection rate

False Alarm Rate

The FAR for this set of transceivers is 0%. Most importantly, this rate illustrates the feasibility of accurately characterizing the behavior of transceivers. Moreover, this rate is obtained when using both static and dynamic profiles (updated continuously). When a static profile is used, the FAR provides an indication as to the accuracy with which the set of transceiverprints has been selected for profiling purposes. In the case of a dynamic profile, the use of the upper/lower Euclidean distance thresholds and intra-transceiver variability

(i.e. the level of variability between signals from the same transceiver) permit the general characteristics of a transceiver to be preserved, without introducing abnormal behavior, e.g. outliers.

Detection Rate

The detection rate, associated with the use of static profiles, is typically lower (86-100%) for most of the transceivers, in particular transceivers 14 and 22, see Figure 2. Now, it is entirely possible that the underlying set of transceiverprints, used for profiling purposes, may not reflect the full range of variability of the corresponding transceiver. Consequently, a transceiverprint, from transceiver Y, could be mistakenly classified as belonging to transceiver X, resulting in a lower detection rate for X. This situation is remedied, to some extent, by continuously updating the profile. After a brief period of time, it begins to reflect the current behavior of the transceiver, a critical element for distinguishing between transceivers from the same manufacturer. The detection rate of 89-100% supports the use of dynamic profiles.

3.5 UMP - Related Work

In the past, UMPs have been used to address the inefficiencies of location-area based update schemes (e.g. by Wong [36] and Ma [20]) and to enhance routing in wireless mobile ad hoc networks (e.g. by Wu [37]). Their use in ABID has been investigated by Spencer [31]. Moreover, in the cellular network domain, the incorporation of user profiles into an ABID system has been evaluated by Samfat and Molva [26] as well as by Sun and Yu [32]. Samfat and Molva have also studied the use of usage patterns in anomaly detection. The novelty of their approach is that the detection procedure is carried out in *real-time*, i.e. within the duration of a typical call. Sun and Yu propose an *on-line* anomaly detection algorithm where the key distinguishing characteristic is the use of sequences of cell IDs traversed by a user. Both approaches do take into consideration the need for addressing concept drift. These solutions specifically target *phone* theft. It is not surprising that they leverage the existing infrastructure of cellular networks. A common characteristic of these solutions is the use of simulated data for both profiling and classification purposes. In our opinion, what would prove useful for addressing not only device cloning and MAC-address spoofing, but impersonation attacks in general is: *A generic user-based IDS mechanism.*

3.6 UMP - Its Use in ABID

We review hereafter our experience on the use of UMPs for ABID purposes. Our work considers a number of distinguishing features. Firstly, as far as the user profiles are concerned, our work is based on real mobility data collected as location broadcasts (LBs). The LBs contain latitude and longitude coordinates (LCs) and other related data. They were captured using the Automatic Position Reporting System (APRS). APRS is a packet radio-based system for tracking mobile objects. It captures and reports on locations, weather and other information for a geographical area, e.g. country or city. A detailed discussion of the APRS architecture is provided by Filjar and Desic [9].

With respect to classification, we use an Instance-Based Learning (IBL) classifier [19]. It compares an observed *set* of mobility sequences of a user to the training patterns in his/her profile. As with RFF, a set of mobility sequences, rather than a single sequence, is used to accommodate a moderate level of deviation in behavior. For a given user, if the Noise Suppressed Similarity Measure to Profile (NSMP) value, an average similarity measure formally defined in [19], falls within pre-established minimum and maximum thresholds (or acceptance region), then mobility sequences are considered normal. Otherwise, an alert is generated. The technical details of this approach are available in a companion paper [13].

3.7 UMPs - Evaluation

We discuss our evaluation of the use of UMPs and IBL for ABID. An objective is to determine the correlation between different precision levels (PLs) used for characterization and resulting false alarm and detection rates. A PL refers to a level of granularity for LCs, i.e. the number of decimals used to represent the latitude and longitude of every coordinate. PLs corresponding to one, two and three decimals are used in this study. The intra-user variability, an undesirable feature, increases with the PL.

It has been suggested by Markoulidakis [21] that nearly 50% of all mobile users of public transportation, e.g. buses, can be characterized. This statistic has been confirmed to some extent by Wu [37]. Users who took busses in the area of Los Angeles are the objects of our study. Los Angeles was selected because of the high density of APRS users. The top 50 users (those who had transmitted the highest number of LBs) were selected to participate in the study.

The evaluation was carried out for each of the 50 profiled users. For each user, the mobility sequences, which were created using the LBs, were divided into training, parameter and test data. The user-based thresholds were established by comparing the sequences in the parameter data to the patterns in the training data. In order to determine the percentage of false alarms (FAs), a comparison was made between the sequences in the test data of the user and his/her training patterns. The resulting NSMP values, which fell outside the acceptance region, were considered FAs. On the other hand, the detection rate or true detect (TDs) was obtained by comparing the test sequences of the remaining users to the training patterns of the user being evaluated. As with FAs, all NSMP values, outside the acceptance region, were considered TDs. Statistics, corresponding to these metrics, were obtained for all profiled users.

In order to simplify the analysis and subsequent discussion of results, three classes of users were defined. Class one (40% of the users) represents users who exhibit consistent Behavior. Class two (56%) and three (4%) are associated with users having progressively more chaotic behavior. We focus on the results obtained for representatives from each class, namely users that we number 19, 23 and 41 respectively in classes one, two and three.

False Alarm and Detection Rates

Figure 4 illustrates the percentage of FAs and TDs corresponding to each of three PLs used. We begin by analyzing the results for user 19. We observe that there

are no FAs for all three PLs. As illustrated in Figure 3, the minimum threshold, associated with a given PL, shifts towards the lower end of the spectrum, as the PL is increased, e.g. from PL 2 to PL 3. However, all three of them (e.g. 2, 5 and 16) are greater than the value of zero. It is an indication that the mobility sequences, in the parameter data, are similar to those in the training data. Furthermore, the mobility sequences of the test data are also similar to the parameter data, which had been used to establish the thresholds.

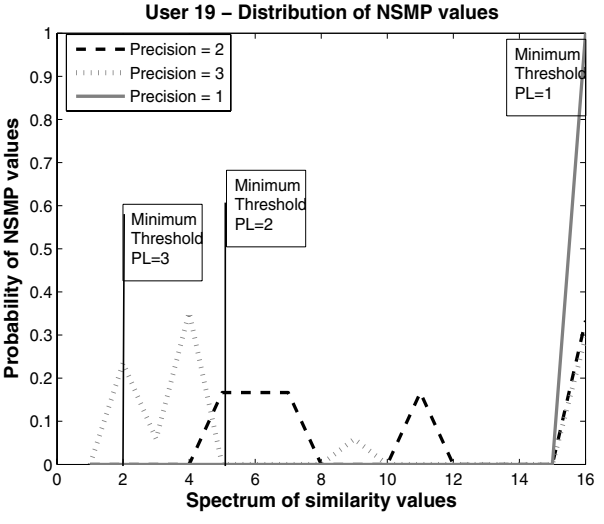

Fig. 3. Characterization using different precision levels

The TDs decrease as the PL is increased. Further scrutiny reveals that this behavior is also appropriate, given the impact of a PL on the NSMP distribution. Therefore, as the minimum thresholds shift towards the lower end, the probability of classifying intrusions as normal behavior becomes higher. This results in a decrease in the TD rate.

The characterization of user 23, on the other hand, is not as optimal. The minimum threshold of value zero is an indication that there are sequences in the parameter data, which are absent in the training data. Nevertheless, the test sequences are similar to those in the parameter set, resulting in zero FAs. In addition, the value of the minimum threshold, have also permitted all intrusions to remain undetected, resulting in a TD rate of zero. As the PL is increased to two and the maximum threshold becomes equivalent to the minimum threshold, it becomes more evident that the test sequences are dissimilar to those in the parameter data. However, they are similar to the training patterns. Consequently, the FA rate becomes 100%. The corresponding TD rate, at PL2, also increases due to the fact that the intrusions, which had fallen outside the minimum and maximum thresholds of zero, are now being detected at this level. Finally, as the PL is increased to three, the number of FAs decreases, as a result of the increase

in intra-user variability between the test sequences and the training patterns. As expected, the TD rate also decreases as the PL is increased. Simply stated, the increase in inter-user variability, in conjunction with the pre-established thresholds, has influenced the detection rate of intrusions.

Finally, results for user 41 are very interesting, although somewhat misleading. We observe that, as with user 19, there are zero FAs for all three PLs. However, unlike user 19, the minimum and maximum thresholds of zero and four respectively, for all PLs, have permitted the NSMP values of all test sequences to fall within the narrow acceptance region. Similarly, the minimum threshold of value zero has also prevented all intrusions from being detected, even when the test sequences of all other users are dissimilar to the training patterns of user 41.

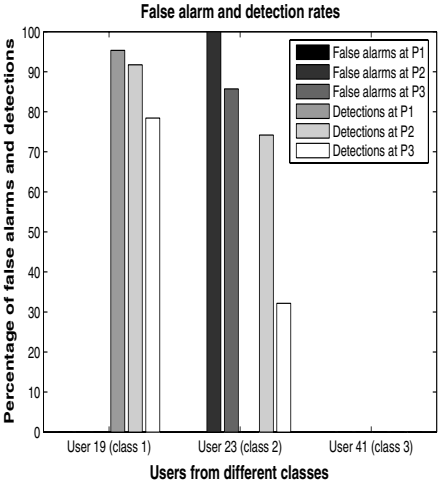

Fig. 4. False alarms and detections

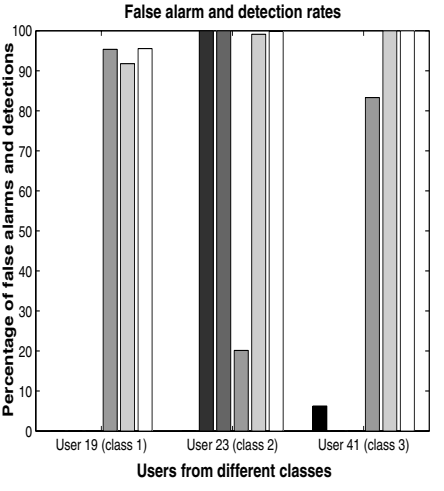

Fig. 5. Using enhanced characterization

Enhanced Characterization

What can be ascertained, from the previous evaluation exercise, is the need to improve characterization, i.e. shift the minimum threshold to a value greater than zero. One simple strategy is to incorporate the mobility sequences from the parameter data, which have a NSMP value of zero, into the training data.

Figure 5 demonstrates the application of this strategy and the resulting impact on FA and TD rates. With user 19, the FAs remain unchanged. The TD rates (for all PLs) have increased, as expected. Moreover, the largest increase of 19% is associated with PL 3, a desirable outcome. As far as user 23 is concerned, the three TD rates, associated with PL 1, PL 2 and PL 3 have increased by 20%, 33% and 23% respectively. However, the FAs for PL 3 has also increased due to the dissimilarity of some of the test sequences to those in the parameter set. Finally, the results for user 41 exemplify the potential benefit of this strategy. Although a 5% increase in the FAs (at PL 1) has been incurred, there is, nevertheless, a significant improvement in the TDs (85%, 100%, 100%), associated with the three PLs.

4 Conclusion

Using simple risk analysis, it can be demonstrated that existing authentication schemes cannot fully protect hosts in a wireless network from impersonation attacks. In our research investigations, we have considered two defense strategies 1) Radio Frequency Fingerprinting, and 2) User Mobility Profiling that look promising in providing defenses against impersonation attacks in wireless and mobile networks. Further research is needed that will test their effectiveness in real-time systems and eventually integrate them into future IDSs for wireless networks.

References

1. B. Aboba. The unofficial 802.11 security web page - security vulnerabilities in EAP methods. www.drizzle.com/ aboba/IEEE/, May 2005.
2. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible authentication protocol (EAP). The Internet Engineering Task Force - Request for Comments: 3748, June 2004.
3. B. Aboba and D. Simon. PPP EAP TLS authentication protocol. The Internet Engineering Task Force - Request for Comments: 2716, October 1999.
4. Frank Adelstein, Prasanth Alla, Rob Joyce, and Golden G. Richard III. Physically locating wireless intruders. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, pages 482–489, 2004.
5. WiFi Alliance. Wi-fi prottected access (WPA) enhanced security implementation based on ieee p802.11i standard, version 3.1, August 2004.
6. M. Barbeau and J-M. Robert. Perfect identity concealment in UMTS over radio access links. In *Proceedings of the Wireless and Mobile Computing, Networking and Communications*, Montreal, Canada, August 2005.
7. K.J. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints. *Radio Science*, 36:585–597, 2001.
8. ETSI. Telecommunications and internet protocol harmonization over networks TIPHON release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis. Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.
9. R. Filjar and S. Desic. Architecture of the automatic position reporting system (APRS). In *Proceedings of 46th International Symposium on Electronics in Marine (Elmar)*, page 331 335, 2004.
10. J. Hall. *Anomaly-based Intrusion Detection in Wireless Networks using Device and User-based Profiles.* PhD thesis, Carleton University, Fall 2005.
11. J. Hall, M. Barbeau, and E. Kranakis. Detection of Transient in Radio Frequency Fingerprinting using Signal Phase. In *proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications (WOC 2003)*, pages 13–18, Banff, Canada, July 2003. ACTA Press.
12. J. Hall, M. Barbeau, and E. Kranakis. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT)*, pages 201–206, St. Thomas, U.S. Virgin Islands, November 2004.

13. J. Hall, M. Barbeau, and E. Kranakis. Using mobility profiles for anomaly-based intrusion detection in mobile networks. In *Proceedings of the Wireless and Mobile Computing, Networking and Communications*, pages 22–24, Montreal, Canada, August 2005. Preliminary version in NDSS'05 Preconference Workshop on Wireless and Mobile Security.
14. H. Haverinen and J. Salowey. Extensible authentication protocol method for GSM subscriber identity modules (EAP-SIM). Work in progress, December 2004.
15. Andrew Hunter. Feature selection using probabilistic neural networks. *Neural Computing and Applications*, 9:124–132, 2000.
16. AirDefense Inc. http://www.airdefense.net. Accessed in February 2004.
17. Financial Times Information. Mobile cloning, March 2005.
18. Alicia Laing. The Security Mechanism for IEEE 802.11 Wireless Networks. http://rr.sans.org/wireless/IEEE80211.php, 2001.
19. Terran Lane and Carla E. Brodley. Temporal sequence learning and data reduction for anomaly detection. *ACM Transactions on Information and System Security*, 2(3):295–331, August 1999.
20. W. Ma and Y. Fang. A new location management strategy based on user mobility pattern for wireless networks. In *Proceedings of the 27th Annual Conference on Local Computer Networks*, 2002.
21. J. Markoulidakis, G. Lyberopoulos, D. Tsirkas, and E. Sykas. Evaluation of location area planning scenarios in future mobile telecommunication systems. *Wireless Networks*, 1, 1995.
22. Netstumbler. http://www.netstumbler.org. Accessed in February 2004.
23. LAN MAN Standards Committee of the IEEE Computer Society, the IEEE Microwave Theory, and Techniques Society. Local and metropolitan area networks - part 16: Air interface for fixed broadband wireless access systems - amendment for physical and medium access control layers for combined fixed and mobile operation in licensed bands. Draft IEEE Standard, IEEE P802.16e/D8-2005, May 2005.
24. Michael J. Riezenman. Cellular security: better, but foes still lurk. *IEEE Spectrum*, pages 39–42, June 2000.
25. S.J. Russell and P. Norvig. *Artificial Intelligence: A Modern Approach*. Prentice Hall, 2002.
26. D. Samfat and R. Molva. IDAMN: an intrusion detection architecture for mobile networks. *IEEE Journal on Selected Areas in Communications*, 15(7):1373–1380, Sept. 1997.
27. N. Serinken and O. Ureten. Bayesian detection of Wi-Fi transmitter RF fingerprints. *Electronic Letters*, 41(6):373–374, March 2005.
28. D. Shaw and W. Kinsner. Multifractal modelling of radio transmitter transients for classification. In *Communications Power and Computing*, pages 306–312, Winnipeg Manitoba, May 1997. IEEE.
29. IEEE Computer Society. ANSI/IEEE std 802.11 - wireless LAN medium access control (MAC) and physical layer PHY specifications, 1999.
30. IEEE Computer Society. IEEE Std 802.11i-2004 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 amendment 6: Medium access control (MAC) security enhancements. Standard Number IEEE Std 802.11i-2004, 2004.

31. Jared Spencer. Use of an artificial neural network to detect anomalies in wireless device location for the purpose of intrusion detection. In *Proceedings of the IEEE*, pages 686–691, SoutheastCon, April 2005.
32. B. Sun and F. Yu. Mobility-based anomaly detection in cellular mobile networks. In *International Conference on WiSe 04*, pages 61–69, Philadelphia, Pennsylvania, USA, 2004.
33. O.H. Tekbas, O. Ureten, and N. Serinken. Improvement of transmitter identification system for low SNR transients. *Electronic Letters*, 40(3):182–183, February 2004.
34. J. Toonstra and W. Kinsner. Transient analysis and genetic algorithms for classification. In *WESCAN*. IEEE, 1995.
35. Oktay Ureten and Nur Serinken. Detection of radio transmitter turn-on transients. *Electronic Letters*, 35:1996–1997, 1999.
36. V. Wong and V. Leung. Location management for next generation personal communications networks. *IEEE Network*, pages 18–24, Sept. 2000.
37. K. Wu, J. Harms, and E.S. Elmallah. Profile-based protocols in wireless mobile ad hoc networks. *Local Computer Networks*, pages 568–575, 2001.