Anomaly-based Intrusion Detection Using Mobility Profiles of Public Transportation Users

Jeyanthi Hall, Michel Barbeau, Evangelos Kranakis
Carleton University, School of Computer Science
Ottawa, Ontario, Canada K1S 5B6
Telephone: 1-613-520-4333
Email: jeyanthihall@rogers.com, {barbeau,kranakis}@scs.carleton.ca

***Abstract*— For the purpose of anomaly-based intrusion detection in mobile networks, the utilization of profiles, based on hardware signatures, calling patterns, service usage, and mobility patterns, have been explored by various research teams and commercial systems, namely the Fraud Management System by Hewlett-Packard and Compaq. This paper examines the feasibility of using profiles, which are based on the mobility patterns of mobile users, who make use of public transportation, e.g. bus. More specifically, a novel framework, which makes use of an instance based learning technique, for classification purposes, is presented. In addition, an empirical analysis is conducted in order to assess the impact of two key parameters, the sequence length and precision level, on the false alarm and detection rates. Moreover, a strategy for enhancing the characterization of users is also proposed. Based on simulation results, it is feasible to use mobility profiles for anomaly-based intrusion detection in mobile wireless networks.**

Keywords: Mobile Networking, Security, Intrusion Detection, IBL, and Mobility Profiles.

I. Introduction

Mobile wireless networks continue to be plagued by theft of identity and intrusion. Both problems can be addressed in two different ways, either by misuse detection or anomaly-based detection. Misuse detection is carried out by recognizing instances of well known patterns of attacks. The main limitation of this approach is that the system fails to uncover new kinds of attacks, unless it has been instructed to do so. Anomaly-based intrusion detection (ABID) consists of observing and recognizing deviations from normal behavior, which has been captured and maintained in electronic profiles. It is generally acknowledged that the main limitation of the anomaly-based detection approach is that it generates a higher rate of false alarms than the misuse detection approach.

The limitation imposed by anomaly-based detection approach can be minimized by combining observations across time and across domains. When intrusion detection is carried out using a given profile, multiple observations can be correlated in time using a state-probabilistic model such as Bayes filters [1]. This strategy accommodates a moderate degree of variability in normal behavior, as indicated by Morin and Debar in [2], and consequently reduces the rate of false alarms. Furthermore, using a statistical tool, such as multivariate analysis [3], the detection results, associated with multiple profiles from different domains, can also be combined to further reduce the rate of false alarms. Examples of intrusion detection systems (IDSs), which make use of multi-sensor data for enhanced detection, include AAFID by Balasubramaniyan [4] and EMERALD by Porras and Neumann [5].

The use of different profiles for ABID has been investigated by various groups. Node/device profiles are created by exploiting the unique hardware signature of their wireless interface [6] and [7], operating system (proposed by Taleck [8]), and other characteristics of a wireless device. In terms of user-based profiling, the use of calling patterns for fraud detection in cellular networks is explored by Boukerche *et al.* [9]. Calls are classified into the normal category or anomalous category based on whether or not the time and location of the calls match the profile of the user. If the probability of fraud is high, then a warning message is sent to the client who owns the phone.

Commercial systems, namely the Fraud Management System by Hewlett-Packard (FMS-HP) [10] and Compaq (FMS-C) [11] also employ service usage profiles, which are built using calling patterns, call frequency, call times and duration, wireless home/roaming behavior, and other call-related information.

In this paper, we examine the feasibility of using profiles, which are based on the mobility patterns of users, for ABID at the application layer. In particular, a novel framework that makes use of a statistical classifier is presented. The instance based learning (IBL) classification system [12] used is a general class of machine learning techniques. In addition, we focus on the analysis of two key system parameters, the sequence length (SL) and precision level (PL), in order to determine their impact on the false alarm and detection rates. A strategy for enhancing the characterization of users is also proposed. Finally, results of simulations, conducted using location broadcasts (LBs) from users, who make use of public transportation, e.g. bus, in the area of Los Angeles, are discussed.

Our primary objective is to supplement existing user and device-based profiles, with those based on mobility, in order

The authors graciously acknowledge the financial support received from the following organizations: Alcatel, Mathematics of Information Technology and Complex Systems (MITACS) and Natural Sciences and Engineering Research Council of Canada (NSERC).

0-7803-9182-9/05/$20.00 ©2005 IEEE.

to further enhance ABID in mobile wireless networks. In fact, the use of mobility profiles is particularly applicable for addressing the problem of stolen cell phones, given that the mobility behavior of the thief and the authorized user are likely to be different. Lastly, we believe that the underlying framework can be applied, with minimal translation, e.g. use of cells instead of geographical coordinates, to the mobile wireless network.

The remaining sections of the paper are organized as follows. Section 2 presents the framework for the application of mobility profiles to ABID. Whereas Section 3 discusses the analysis of the two key system parameters, simulation results are presented in Section 4. Other related work are identified in Section 5, followed by the conclusions and future research initiatives in Section 6.

II. ABID USING MOBILITY PROFILES

This section provides an overview of the ABID system. As with most IDSs, the two primary objectives are to define user mobility profiles (UMPs) and to design an appropriate classification system.

A. Framework

Details of the framework, which is used for the implementation of the ABID system, are provided in this subsection. It is important to note that the detection process, as described in the sequel, is repeated for each user. Moreover, during the profiling phase, the subset of activities, from data collection to the definition of the UMP, is typically carried out on a one-time basis and prior to classification.

The intrusion detection process begins with the data collection exercise. Once the LBs, which contain geographical/location coordinates (LCs) and other data, have been captured for a period of approximately 3-6 months, a high-level mapping (HLM) is applied. The purpose of using the HLM is to decrease the granularity of the LCs in order to accommodate minor deviations or intra-user variability. Upon completion of this phase, the LCs (feature) are extracted from each broadcast during feature extraction. A set (defined by SL) of these chronologically ordered LCs are subsequently concatenated to define a mobility sequence. This process continues until all the mobility sequences (data set) have been created. The unique sequences (training patterns), from the first four out of six equal partitions of the data set, is stored in the UMP, along with other user-related information. During the classification phase, a set of mobility sequences of user A is compared to the training patterns in his/her profile. If the noise-suppressed similarity measure to profile (NSMP) value falls within the pre-established thresholds (also stored in profile), this set of mobility sequences is considered normal (belonging to User A), otherwise an intrusion is suspected.

B. High-Level Mapping

The term *intra-user* variability refers to the difference between the LCs (j represents the latitude and i represents the longitude) that are transmitted by user A as he/she travels using routes one (solid line) and two (dashed line), see Fig. 1. Let us assume that the full sequence of LCs, associated with route one, has been captured and stored in the profile (training patterns) of user A. If the sequence of LCs, associated with route two, is compared to those in the training patterns, it would result in a similarity value of zero, and would be interpreted as an intrusion. Thus, the HLM converts LCs, based on one of three precision levels, in order to change the degree of similarity between corresponding LCs in two sequences.

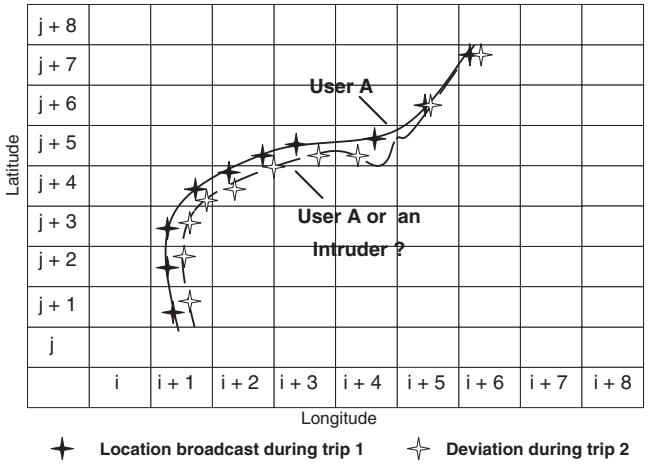

Fig. 1. Intra-user and inter-user variability

This mapping process, which is applied to a LC in each LB, is carried out as follows. The original format of the LC is (###.#####) and (###.#####), where the first and second terms represent the latitude and longitude respectively. Based on the precision level (PL), the LC is truncated and rounded to the specified number of digits after the decimal point. With level three (highest precision), the specified digit of the first and second terms (###.##) is rounded to 0 if it is within 0-4, and to 5 if it is within 5-9 range. Thus, for example, the LC 33.14623,114.26874 is mapped to 33.10,114.25. Similarly, the HLM for levels two and one are (###.#) and (###.0) respectively. The choice of PL is explored in Section 3.

Caution must nevertheless be exercised since minimizing intra-user variability will also minimize *inter-user* variability. That is, it will increase the similarity between LCs of User A and an intruder, making it more difficult to distinguish between the two users.

C. Feature Extraction

The extraction of LCs (feature) from the HLM data is required in order to create mobility sequences. The selection of the appropriate SL is also addressed in Section 3.

The feature extraction process begins by concatenating the first set (e.g. ten) of chronologically ordered LCs into a single sequence, where $k = 1$ and $m = 10$ represent the first and last LC respectively. Each subsequent sequence of equal length is obtained by shifting k and m by one, as suggested by Lane and

Brodlay [13]. The purpose of using an overlapping window, which is continuously shifted by one, is to accommodate different sequences that begin with different LCs. This process is repeated until all the LCs in the HLM data stream have been exhausted. The resulting set of sequences (data set) are used for profiling and classification purposes.

D. Profile Definition

Once the mobility sequences have been obtained, the next step is to create the UMP. A detailed description of each component in the UMP ensues.

Identifier represents the unique identification of the user, which has been issued by Industry Canada. It is transmitted with all LBs. *Training Patterns* characterize the mobility behavior of a user. Due to factors, such as traffic and weather, a mobility sequence of a user may deviate from the norm. This deviation is referred to as noise, which must be minimized. The term *window size* refers to the number of mobility sequences to be used for obtaining the NSMP value. If the NSMP value falls within the pre-established *minimum* and *maximum* thresholds, the mobility sequences are considered normal. The values of the thresholds are determined by obtaining a distribution of the NSMP values, using the training patterns and parameter sequences (5^{th} partition of the data set), and by applying the desired false alarm rate (application-dependent) to the distribution.

As aforementioned, a mobility profile of each user is created prior to classification. However, in order to address the issue of concept drift (change in mobility patterns), it is essential that these profiles be updated periodically. One approach is to maintain a window of training patterns that is continuously shifted in time, as new sequences are added (analogous to the use of exponentially weighted moving average). As the window is shifted, some of the components, e.g. thresholds, in the UMP are updated accordingly. This should not only reduce the rate of false alarms and increase the detection rate, but also maintain a given level of performance (currently being investigated).

E. Classification

The final step, in the intrusion detection process, is the classification of a set of mobility sequences, as normal or anomalous, using the NSMP value. The following subsection provides a brief overview of the key concepts defined in IBL. Readers are encouraged to consult the paper by Lane and Brodlay [13] for a more detailed discussion of the IBL framework.

Similarity Measure

As you may recall, a mobility sequence is composed of a chronologically ordered sequence of LCs and that these sequences are used for training, establishment of parameters and test/simulation (6^{th} and final partition of the data set) purposes. Therefore, the *similarity measure (SM)* of two sequences X (e.g. test sequence) and Y (e.g. training pattern) of equal length l is defined as follows:

$$sim(X,Y) = \sum_{i=0}^{l-1} w(X,Y,i)$$

with:

$$w(X,Y,i) = \begin{cases} 0 & \text{if } i < 0 \text{ or } x_i \neq y_i \\ 1 + w(X,Y,i-1) & \text{if } x_i = y_i \end{cases}$$

where i represents the index of the sequence of LCs. Thus $w(X,Y,i)$ equals zero if the LCs of the X and Y sequences at index i are not identical. Otherwise, a value of one is added to the outcome of $w(X,Y,i)$ at $i-1$. The maximum SM value for a given l is $\frac{l(l+1)}{2}$.

Similarity Measure to Profile

Whereas the SM is determined based on a one to one comparison of the LCs of a test sequence and training pattern, the similarity measure to profile (SMP) is calculated by performing a one to many comparison of a test sequence X with *all* the training patterns in a profile D. It is defined as:

$$sim_D(X) = max_{Y \in D} sim(Y,X).$$

Hence, the SMP is the maximum of the SM values.

Noise Suppression

As with all chaotic systems, noise is inherent and reflects the deviation of an observed behavior (test sequence) from the training patterns stored in the profile. A degree of *intra-user* variability is to be expected, since it is a function of many factors including traffic conditions and weather. Nevertheless, noise can be suppressed, to some extent, by calculating the average SMP of a *set* of W test sequences according to:

$$v_D(p) = \frac{1}{W} \sum_{q=p-W+1}^{p} sim_D(q).$$

The term $v_D(p)$ is referred to as the NSMP value of the sequence starting at position p.

Decision Rule

Whether or not a set of mobility sequences is associated with a given user, can be determined by comparing the resulting NSMP value to the pre-established minimum t_{min} and maximum t_{max} thresholds. While t_{min} is used for detecting sequences, which have low NSMP values, t_{max} proves beneficial in detecting sequences that have unusually high similarity to the profiled behavior, perhaps an indication of an impersonation attack.

The calculation of t_{min} and t_{max}, for each user, is carried out by applying an acceptable false alarm rate r (application-specific) to a normalized probability distribution (NPD) of NSMP values. Thus, t_{min} and t_{max} are dependent on r and NPD.

The parameter r dictates the width of the acceptance region (between t_{min} and t_{max}) on the x-axis, see Fig. 2. It also

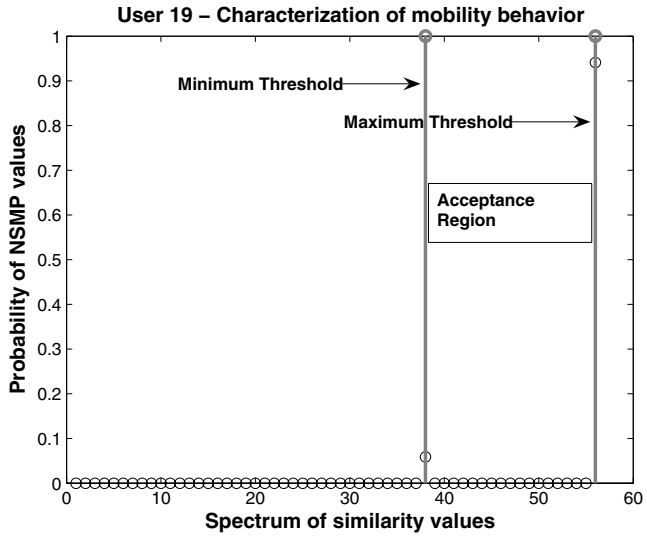

Fig. 2. Minimum and maximum thresholds

represents a trade-off between false alarm and intrusion rates. For example, a smaller value of r corresponds to a wider acceptance region, with t_{min} being shifted to the left. As a result, the rate of false alarms would be decreased. However, the expanded region would also accommodate more intrusions, and therefore, cause the corresponding detection rate to decrease.

As far as the NPD is concerned, it is generated by using the parameter sequences (5^{th} partition of the data set) and the training patterns (first four partitions), obtaining a distribution/histogram of NSMP values (in the range of $0, \ldots, l(l+1)/2$), and normalizing this distribution based on the probability of each NSMP value. The actual set of sequences from the data set, used for training and parameter specification, is an important factor to be considered. By allocating the first four partitions to training, the probability of accurately characterizing the mobility behavior of a user is increased. This is, of course, based on the assumption that the mobility patterns of a user is typically established within a given timeframe. In any event, new mobility patterns can be incorporated into the training patterns, by addressing the issue of concept drift, as aforementioned in the subsection on profile definition.

Finally, t_{max} and t_{min} are established using $r/2$ quantiles (upper and lower) of the NPD, as proposed by Lane and Brodlay [13].

Fig. 2 illustrates the application of $r = 0.05$ to the NPD of user 19, who was selected at random. In this figure, the x-axis represents the spectrum $(0, \ldots, 55)$ of the similarity values that are possible for a sequence of LCs of length 10. Please note that the actual values are in the range of $(1, \ldots, 56)$ for improved graphical representation. The y-axis represents the probability of each NSMP value in the NPD. Both the minimum and the maximum thresholds are indicated using vertical lines. What is illustrated in the figure is the width of the acceptance region (from the minimum threshold to the maximum threshold), which is a function of the NPD and the false alarm rate r. The narrow acceptance region, defined by high NSMP values of 38 and 56, reflects the consistency of the mobility behavior, as characterized by the parameter sequences, with respect to the training patterns. As a result, the detection rate should be high, since the probability of intruders having high NSMP values, which fall within the thresholds, is fairly low.

III. Empirical Analysis of System Parameters

In the previous sections on HLM and feature extraction, we had indicated that the PL and SL are of significance and that an appropriate value had to be selected.

Aside from stating the obvious, our first objective is to determine the impact of these parameters on the characterization of users (distribution of the NSMP values) and intrusions (successful impersonation attempts against a user). We address the impact of these parameters on false alarm and detection rates in the section on simulation.

Given that the mobility behavior of the 50 users does differ to some extent, and that this variability is likely to influence the analysis of both parameters, we have categorized these users based on the precision with which the training patterns are being followed (repetitions). The three classes are defined as follows. Whereas class one represents users with the highest level of similarity (consistent behavior), class two and three are associated with those with progressively lower levels of similarity (more chaotic behavior). Due to space constraints, we focus on the results obtained for user 19 (class 1 with 40% of users) as they illustrate the expected behavior, associated with an adequate level of characterization. Nevertheless, we briefly comment on results (figures not shown) obtained for user 23 (class 2 with 56%) and user 41 (class 3 with 4%).

A. Sequence Length

Fig. 3 illustrates the use of three different lengths (5,10,15) for sequences and the impact on the characterization of user 19. Values of NSMP, which are located at the lower-end of the SM spectrum are vulnerable to the choice of r. Since r dictates the width of the acceptance region, in particular the minimum threshold, all values of NSMP that are less than the threshold are treated as false alarms.

Other parameters used include the window size of 100, precision level of one (PL1), and minimum threshold of two. The maximum threshold, however, was based on the SL being used.

In Fig. 3, the x-axis represents the spectrum of similarity values for all three SLs. Since the results, associated with each length, have been incorporated into one plot, the range of the x-axis is actually from 1-121 (for SL15). In other words, results obtained for SL5 (length of five) are localized towards the lower end of the spectrum. NSMP values, which have been normalized, are indicated by the y-axis.

What is being illustrated is as follows: as the SL is increased, the percentage of NSMP values, located at the higher-end of the SM spectrum starts to decrease. In this case, the

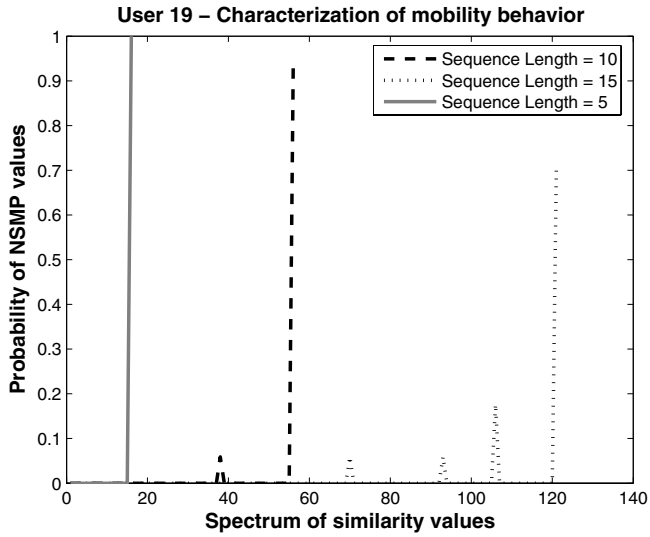

Fig. 3. Characterization using different sequence lengths

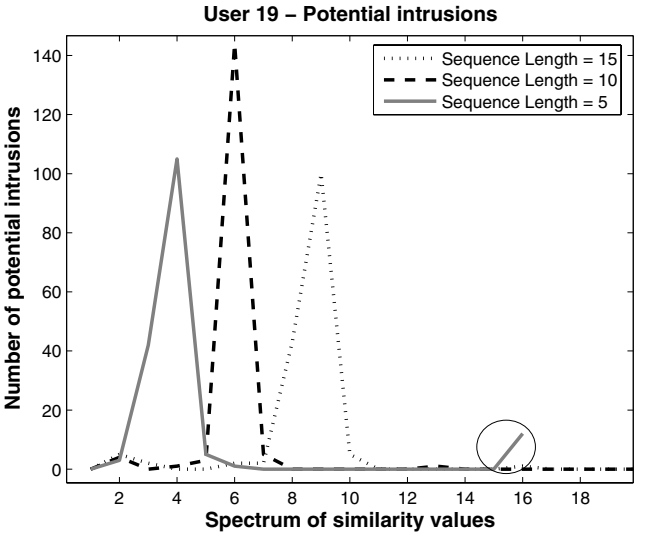

Fig. 4. Intrusions at different sequence lengths

NSMP values are located precisely at 15, 55 and 120 on the x-axis. Furthermore, as the percentage of these values decreases, they are distributed towards the lower end of the spectrum. This behavior is logical since the probability of achieving a high NSMP value decreases as the SL is increased. Therefore, should the NPD of a user be localized at the higher end of the spectrum, selecting a larger SL would be not be advisable since it shifts the NPD further towards the left. However, if the NPD is located at the lower end of the spectrum (user 41), it is advantageous to use a larger SL, since this results in the NPD being shifted towards the higher end of the spectrum. On the other hand, when the NPD is distributed between the lowest and highest similarity values (user 23), a larger sequence length is also desirable for shifting the NPD towards the center of the spectrum, and away from the lower end.

We continue our analysis of the impact of SL on the distribution of potential intrusions. All parameters, which were used in the previous test, remain the same, with one exception. The NSMP values of potential intrusions, are calculated using the training patterns of user 19 and test sequences from the remaining 49 users.

Fig. 4 depicts the distribution of intrusions associated with each of the three SLs used. It is important to note that we have zoomed in on the range of SM values between 1-16, since most of the intrusions are located in this range. The original x-axis does cover the range of 1-121. This figure demonstrates the fact that, as the SL is increased, the distribution shifts towards the higher end of the SM spectrum. This behavior is justified since there is a higher probability of achieving a high NSMP value when the SL is longer. The key difference between user 19 and users 23 and 41 is the magnitude of the distribution. Due to the more chaotic behavior, the magnitude is higher for user 23 and even more so for user 41.

The last detail to note is the small number of intrusions at location 16 on the x-axis. It is an indication that one or more of the 49 users have mobility sequences that are identical (based on PL1) to user 19. In fact, most of these intrusions are caused by user 13. Increasing the PL in order to increase the granularity of the LCs, discussed next, addresses this problem.

B. Precision Level

We proceed with the analysis of the PL and its impact on the characterization of users and number of potential intrusions. Given that our goal is to minimize the number of intrusions first and then address the problem of characterization, we have used a SL of five.

Fig. 5 indicates that the distribution of NSMP, associated with a given PL, shifts towards the lower end of the spectrum as the PL is increased, e.g. from PL2 to PL3. This behavior is consistent with all three classes of users. Therefore, a lower PL can be used for HLM in order to improve characterization. Doing so, increases the similarity between corresponding LCs. Thus, the probability of a match between a training pattern and a parameter sequence is higher, resulting in a higher NSMP value.

Although the use of a lower PL is desirable for characterization purposes, it becomes problematic where intrusions are concerned, see Fig. 6. What is evident, in this figure and applicable to all classes of users, is that the distribution shifts towards the higher end of the spectrum as the PL is decreased. On the other hand, the intrusions at SM value of 16 are eliminated when PL2 and PL3 are used. This should not come as a surprise since increasing the PL also decreases the similarity between two LCs. As a result, the probability of obtaining a high NSMP value is reduced, as indicated by the distribution of intrusions for PL3. Thus, the use of a higher PL would reduce the number of intrusions and improve the detection rate.

In summary, the selection of values for both the SL and PL is a challenging task since all of the possible permutations produce results that are negatively correlated. Nevertheless, an

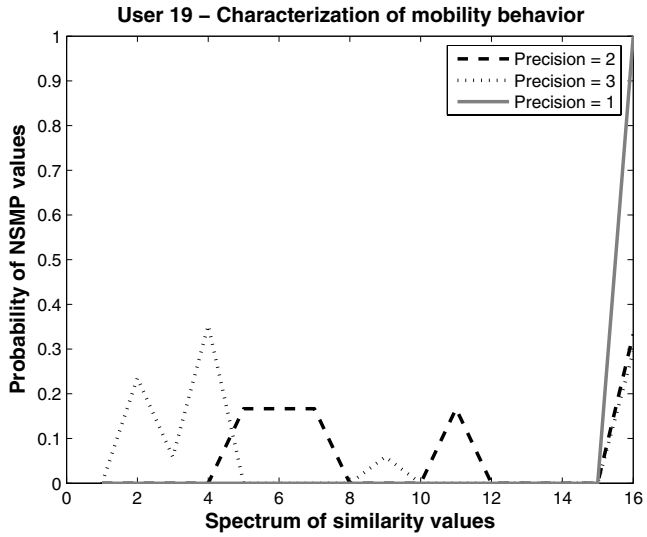

Fig. 5. Characterization using different precision levels

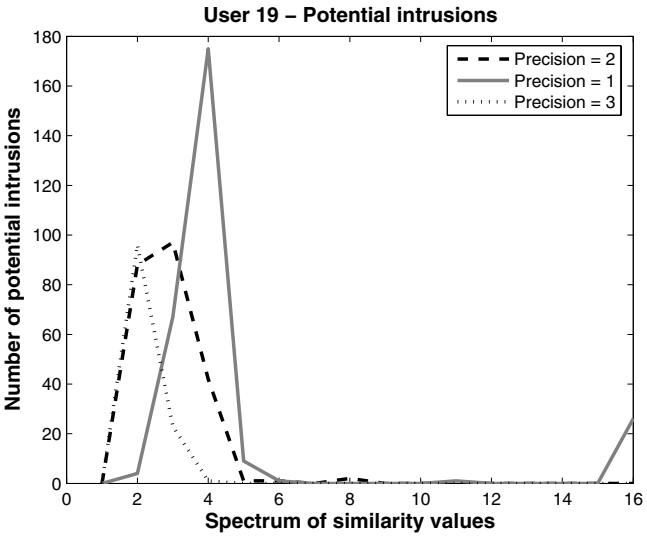

Fig. 6. Intrusions at different precision levels

optimal strategy would produce results in which the NSMP values, associated with characterization, are localized towards the higher end of the spectrum, while those related to intrusions are located at the lower end. This would produce low false alarm and high detection rates.

IV. Simulation

Our primary objective, in carrying out the following simulation exercise, was to determine the impact of PL on the false alarm and detection rates (metrics). We relaxed the use of various SLs for the time being, given that a smaller SL is preferable for improving the detection rate. We were also interested in the correlation between the quality of characterization, attainable using IBL, and the resulting false alarm and detection rates.

A. Simulation Infrastructure

Details of the simulation infrastructure are as follows. The acquisition of the LBs was carried out using the Automatic Position Reporting System (APRS) and appropriate hardware (e.g. receiver and antenna). The APRS is an internet-based system (open-source) that tracks objects and users using amateur radio.

It has been specified by Markoulidakis in [14] (follow-up on the Universal Mobile Telecommunications System RACE specification) that nearly 50% of all mobile users use public transportation, e.g. bus, and that they can be characterized. Furthermore, this statistic has been confirmed to some extent by Wu in [15]. Hence, we targeted users who took the bus in the area of Los Angeles. This city was selected due to the high density of APRS users, an ideal environment that promotes a high probability of intrusions. Finally, the top 50 users (those who had transmitted the highest number of LBs) were selected to participate in the simulation.

The captured LBs (approx. 2 million) were transferred from the APRS to a MySQL database for further processing. All subsequent analysis and simulations were carried out using an HP laptop and Matlab software.

B. Details of Simulation

The simulation exercise was carried out for each of the 50 profiled users. In order to determine the percentage of false alarms, a comparison or classification was made between the test sequences of user A and his/her training patterns. The resulting NSMP values, which were outside the minimum and maximum thresholds (r=0.05), were considered false alarms (FAs). Similarly, the percentage of true detect (TD) (detection) was obtained by comparing the test sequences of the remaining 49 users to the training patterns of user A. The resulting NSMP values, which fell outside the thresholds (r=0.05), were considered TDs. Statistics, corresponding to the metrics, were obtained for all profiled users.

C. Simulation Results

We limit the discussion and focus on the results obtained for the representatives of each class, namely users 19, 23, and 41. Although an attempt was made to generalize the results for each class, it proved challenging due to the moderate level of intra-class variability.

False Alarm and Detection Rates

Fig. 7 illustrates the percentage of FAs and TDs corresponding to the three PLs.

We begin with the discussion of user 19 (class 1) and observe that there are no FAs for all three PLs. It is due to the fact that all NSMP values, related to the test data, fell within the pre-established thresholds. This is an indication that the mobility sequences in the test data are similar to those in the parameter data, which had been used to establish the thresholds. In terms of TDs, the percentage of TDs decreases as the PL is increased. Further scrutiny reveals that this behavior is appropriate in light of the fact that the distribution of NSMP

values shifts to the lower end of the SM spectrum, see Fig. 5. Therefore, as the minimum thresholds shift towards the lower end of the SM spectrum, the probability of intrusions, within the acceptance range, is higher, see Fig. 6. This results in an increase in the rate of intrusions and a corresponding decrease in the TD rate.

The characterization of user 23 (class 2), on the other hand, is not as optimal. In fact, the NSMP values are distributed between the SM values of 1 and 16 (figure not shown) for PL1. The wide acceptance region and the fact that the minimum threshold has a value of *one* (actual value is zero) reflects the absence of sequences (parameter data) in the training data. Although the test sequences may or may not be similar to those in the parameter data, all of them have fallen within the thresholds, resulting in zero FAs. These two factors (wide region and value of minimum threshold) have also permitted all intrusions to fall within the thresholds 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, but are nevertheless similar to the training patterns. As a result, all NSMP values, associated with the test sequences, fall outside the thresholds causing the FA rate to become 100%. The corresponding TD rate at PL2 also increases due to the fact that the intrusions, which fell outside the minimum and maximum threshold of one, 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 training patterns. As expected, the TD rate also decreases as the PL is increased, since most of the intrusions fall within the thresholds, and hence, are not detected.

Results for user 41 (class 3) 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 threshold of *one*, for all three PLs, has permitted all NSMP values of test sequences and intrusions to fall within the narrow acceptance region (maximum threshold of four). The end result (e.g. zero detection rate) is misleading since test sequences of all other users are dissimilar, to some extent, to the training patterns of user 41, yet are being considered normal simply because of the minimum threshold.

Enhanced Characterization

What is evident, from the previous simulation exercise, is the need to shift the minimum threshold towards the higher end of the spectrum, such that it is greater than one. One simple strategy is to add the parameter sequences, which have a NSMP value of one, to the training patterns. This strategy reduces the width of the acceptance region and shifts the NPD, especially the minimum threshold, towards the higher-end of the spectrum.

Fig. 8 demonstrates the application of this strategy and the resulting impact on the FA and TD rates. With user 19 (class 1), the FA rates remain unchanged whereas the TD rate for PL3 has increased by 19%. As far as user 23 (class 2) is concerned, the three TD rates, associated with PL1,PL2, and PL3 are increased by 20%, 33%, and 233% respectively. However, the FA rate for PL3 is also increased due to the dissimilarity between some of the test sequences and parameter sequences. Finally, the results for user 41 (class 3) exemplify the effectiveness of this strategy. Although a 5% increase in the FA rate (at PL1) is incurred, there is, nevertheless, a significant improvement in the TDs (85%, 100%, 100%), associated with the three PLs.

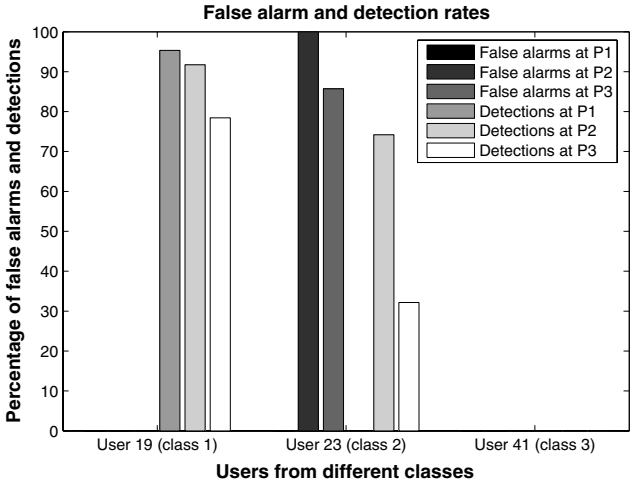

Fig. 7. False alarms and detections for different precision levels

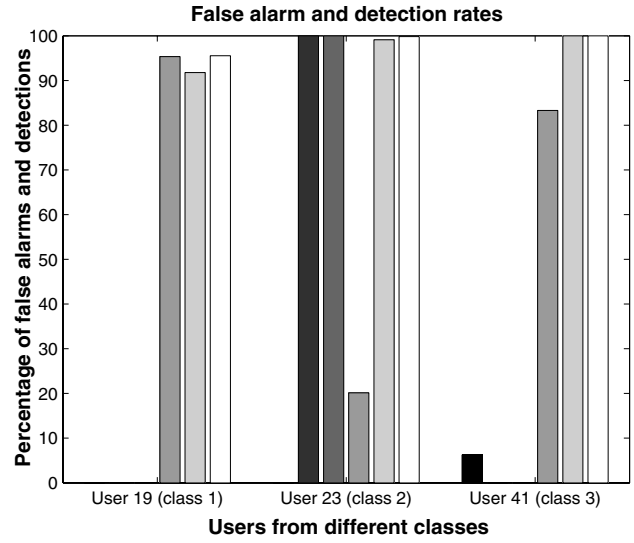

Fig. 8. False alarms and detections using enhanced characterization

V. Related Work

The use of UMPs for ABID in mobile networks has not been researched extensively. However, research initiatives, which have been undertaken by researchers include Buschkes, Kesdogan, and Reichl [16], Samfat and Molva [17], and Sun and Yu [18]. The work conducted by Buschkes makes use of sequences of cells, traversed by users, as a feature

of the profile. Intrusion detection of users, who use cloned phones, is carried out by analyzing major deviations from the route. Similarly, Samfat and Molva model the behavior of users using the telephony activity and migration patterns. The implementation of multi-level intrusion detection at the visitor location, and use of multiple profiles, differentiates their work from the others. Finally, the most recent work by Sun and Yu also employs sequences of cells to represent a feature. However, the characterization is accomplished via a high order Markov model [19]. Furthermore, the sequences, which are stored in a mobility trie (an acceptable solution given that the size of the alphabet is small) is updated using the technique of exponentially weighted moving average.

Of course, user mobility profiles have also been used to address the inefficiencies of location-area based update schemes. Details can be found in the work by Wong [20] and Ma [21]. Finally, the use of profile-based protocols for enhanced routing in wireless Mobile Ad Hoc Networks is addressed by Wu in [15].

VI. Conclusions and Future Research Initiatives

Based on simulation results, it is feasible to use mobility profiles for ABID in mobile wireless networks. The challenge is to accurately characterize the mobility behavior of users. One simply strategy, which enhances the characterization of users and increases the detection rate at a minimal cost (low percentage of FAs), is to incorporate the missing parameter sequences into the training patterns. Furthermore, the issue of concept drift (accommodating variability in mobility behavior over time) can also be addressed by continuously monitoring the false alarm rate and selectively incorporating newly observed mobility sequences into the training patterns, using a window that is shifted in time (analogous to exponentially weighted moving average). The selection criteria can be based on pre-established thresholds, such as the frequency of all new sequences encountered over a period of time.

Once the characterization of users has been adequately addressed, the selection of specific values for SL and PL should be based on the level of intra-user variability. These values could then be incorporated into a user's profile. Categorizing users into different classes, based on the level of variability, represents an alternate strategy.

Finally, the adoption of the IBL classification technique is suitable since the definition of the similarity measure is comparable to that of the euclidian distance. Supplemented by the high level mapping exercise, which reduces the intra-user variability between mobility sequences and training patterns, this technique performs well, as indicated by the false alarm and detection rates obtained for all three classes of users.

As far as future research initiatives are concerned, the following issues will be explored in the near future: user privacy; concept drift; the expansion of the feature set (e.g. time frame and other relevant features) for improving detection rate; a comprehensive analysis of the system performance for comparison purposes; and the use of different parameter values, which reflect the mobility behavior of users.

Acknowledgment

The authors wish to thank Andrew Robison and Frederic Gariador, from Alcatel Canada, for fruitful discussions.

References

[1] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*. Prentice Hall PTR, 2002.

[2] B. Morin and H. Debar, "Correlation of intrusion symptoms: an application of chronicles," in *Proceedings of the International Conference on Recent Advances in Intrusion Detection*, Berlin Heidelberg, 2003, pp. 94–112.

[3] J. Joseph, F. Hair, E. Anderson, W. Black, and R. Tatham, *Multivariate Data Analysis*. Prentice Hall PTR, 1998.

[4] J. Balasubramaniyan, J. Garcia-Fernandez, D. Isacoff, E. Spafford, and D. Zamboni, "An architechture for intrusion detection using autonomous agents," COAST Laboratory Purdue University, Tech. Rep., 1998.

[5] P. Porras and P. Neumann, "EMERALD: Event monitoring enabling responses to anomalous live disturbances," in *Proceedings of the Twentieth National Information Systems Security Conference*, 1997, pp. 353–365.

[6] M. Riezenman, "Cellular security: better, but foes still lurk," *IEEE Spectrum*, pp. 39–42, June 2000.

[7] 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)*, St. Thomas, U.S. Virgin Islands, November 2004, pp. 201–206.

[8] G. Taleck, "Ambiguity resolution via passive os fingerprinting," in *Proceedings of the International Conference on Recent Advances in Intrusion Detection*, Springer-Verlag Heidelberg, 2003, pp. 192–206.

[9] A. Boukerche, *Security and fraud detection in mobile and wireless networks*. John Wiley and Sons, Inc., 2002, ch. 27.

[10] (2003) Hp - fraud management system. Hewlett Packard. [Online]. Available: http://www.hp.com

[11] (2001) Compaq - fraud management system. Compaq. [Online]. Available: http://www.hp.com/hps/nsp/

[12] D. Aha, D. Kibler, and M. Albert, "Instance-based learning algorithms," *Machine Learning*, vol. 6, pp. 37–66, 1991.

[13] T. Lane and C. Brodlay, "Temporal sequence learning and data reduction for anomaly detection," *ACM Transactions on Information and System Security*, vol. 2, pp. 295–331, August 1999.

[14] J. Markoulidakis, G. Lyberopoulos, D. Tsirkas, and E. Sykas, "Evaluation of location area planning scenarios in future mobile telecommunication systems," *Wireless Networks*, vol. 1, 1995.

[15] K. Wu, J. Harms, and E. Elmallah, "Profile-based protocols in wireless mobile ad hoc networks," *Local Computer Networks*, pp. 568–575, 2001.

[16] R. Buschkes, D. Kesdogan, and P. Reichl, "How to increase security in mobile networks by anomaly detection," in *Proceedings of the Computer Security Applications Conference*, Phoenix, AZ, USA, Dec. 1998, pp. 3–12.

[17] D. Samfat and R. Molva, "IDAMN: an intrusion detection architecture for mobile networks," *IEEE Journal on Selected Areas in Communications*, vol. 15, pp. 1373–1380, Sept. 1997.

[18] B. Sun and F. Yu, "Mobility-based anomaly detection in cellular mobile networks," in *International Conference on WiSe 04*, Philadelphia, Pennsylvania, USA, 2004, pp. 61–69.

[19] L. Rabiner and B. Juang, *An introduction to hidden markov models*. Prentice Hall PTR, 1986.

[20] V. Wong and V. Leung, "Location management for next generation personal communications networks," *IEEE Network*, pp. 18–24, Sept. 2000.

[21] 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.