EWIDS: An Extended Wireless IDS for Metropolitan Wireless Networks Based on Kinematical Analysis

Luci Pirmez†, Nilson Rocha Vianna††, Reinaldo de Barros Correia†, Luiz Fernando Rust da Costa Carmo†††/††, Claudio Miceli de Farias† and Helio Mendes Salmon††

† NCE/IM, Federal University of Rio de Janeiro, Postal Code 2324, Rio de Janeiro, RJ, 20001-970 – Brazil
†† Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), Rio de Janeiro, RJ – 20.010-000 - Brazil
††† Inmetro, Duque de Caxias, RJ -25250-020 - Brazil

Summary
Wireless metropolitan area networks (WMANs) are well known to subject users or applications and to a vast gamma of security risks, hindering security critical distributed applications from employing this type of network as a communication infrastructure. Most existing approaches for addressing WMAN security issues use cryptography-based mechanisms or ad-hoc adapted versions of traditional Intrusion Detection Systems (IDS) for wired networks. While the first approach may lead to unfeasible computation costs for mobile hand-held devices, the second exhibits a high dependency on the freshness of their attack-signature databases, besides not considering any inherent characteristic of wireless networks, such as mobility. Thus, we present EWIDS (Extended Wireless IDS); a lightweight IDS specially designed for WMANs, which detects anomalous wireless device transmissions by employing kinematical analysis on the motion of users' mobile devices. EWIDS also takes into account the decision information generated by transmitter fingerprint mechanisms used to identify wireless device. Both information is integrated through a fuzzy logic engine in order to increase the system performance. Realistic simulations based on WMAN scenarios revealed that our approach is very promising, since worst-case results have shown high correct alarm rates associated with low false positive rates.

Key words:
Intrusion Detection Systems, Wireless Intrusion Detection Systems, Security in Wireless

1. Introduction

The growing importance of ubiquitous computing has been driving the colossal growth of wireless market in the last few years. Despite this huge acceptance on the part of market, wireless technology has not fulfill addressed several challenging issues that still refrain from deploying QoS-constrained and secure applications. Wireless signals can be intercepted by anyone within range, enabling any device or station, being them authorized or not, to capture transmitted data. Attacks [1] like MAC spoofing, Man-in-the-middle (MiTM), and Session Hijack are very common in wireless networks and allow the attacker to obtain personal information from other users or to make malicious activities using a third party's identity. These threats become even more critical when attackers can actuate in wireless network that are able to cover wide geographical areas such as IEEE-802.16 networks [2, 3], enclosing several organizations / enterprises within its coverage area. The IEEE 802.16e standard enhances the original one with mobility so that Mobile Subscriber Stations (MSSs) can move during services across multiple base stations. Regarding boundaries of the organization, an attack can be classified according to its origin: external or internal. External attacks are the ones launched from outside the organization. Internal attacks are accomplished from inside the organization, by people with access privileges to the information system, such as evil-minded, unhappy employees, or by infiltrated people making use of social engineering techniques. Beyond the security requirement, wireless networks must also deal with mobility and QoS requirements. Mobility is a fundamental aspect of ubiquitous computing. On the other hand, QoS requirements are becoming more and more important as long as some special demanding applications, such as multimedia, have grown considerably. Thus, mobility, QoS requirements and security are the most relevant requirements of current metropolitan wireless networks and, due to cross-dependencies and conflicting goals, must be treated together or at least be kept into account together whenever one is to be considered separately. This paper proposes an Extended Wireless Intrusion Detection System (EWIDS) to enhance security in wireless metropolitan networks without any interference on mobility and QoS issues. EWIDS does not restrict the movement of mobile devices and does not infer future devices positions within the coverage area of wireless metropolitan networks. Actually, EWIDS assures a high degree of mobility for users since it is not based on any users' itinerary. Therefore, in order to preserve processing capacity, our proposal does not use any user's resource to verify the legitimacy of users who are trying to make a connection to the network, or to log in. Additionally, EWIDS architectural

Manuscript received July 5, 2011
Manuscript revised July 20, 2011

components were built with fuzzy logic, a technique known by its ability to achieve low-complexity solutions in many problem domains. Taking these issues as a guideline, EWIDS have been designed to work independently from any underlying standardized security mechanism or protocol, including cryptographic or traditional authentication algorithms. EWIDS uses a novel scheme for detecting malicious transmissions based on kinematical analysis of users' mobility. The main contributions of EWIDS are: (i) the possibility of detecting intrusion regardless of database updates of attacks/anomalies signatures, turning this approach scalable for an environment with potentially thousands or millions of users; (ii) EWIDS allows detecting zero-day attacks, those with an unknown signature; (iii) minimal interference on mobility and QoS issues is achieved, making it appropriated to scenarios in which user devices have limited processing and storage capacities; (iv) EWIDS reduces significantly the frequency of false positives (FP) and false negatives (FN) since our proposal correlates information of different nature (kinematical analysis and transmission signature) in its decision process; (v) the kinematical analysis approach of EWIDS reduces the amount of per-user-device information required in comparison with the itineraries-based approach, initially used for cellular, enhancing system scalability; and (vi) EWIDS largely restricts the effectible positioning of the attackers (almost the same of wired-networks), providing protection against different attacks. To validate our proposal, we performed several simulations under various scenarios, representing the metropolitan wireless network environment. The remainder of this paper is structured as follows. In second section, the basic concepts related to the paper are presented. The proposed EWIDS architecture is described in the third section. The next section describes the EWIDS Deployment Issues. In the fifth section, test platform and simulation results are presented. In the next section, related papers are discussed. Finally, conclusions and possible further works are discussed in the last section.

2. Kinematical Analysis and Transmission Signature

Kinematical Analysis and Transmission Signatures are present in this section as EWIDS foundations for detecting suspicious or malicious activities in wireless metropolitan networks. In the context of this work, the kinematical analysis may be divided in two different approaches: users' itineraries-based approach and users' motion dynamics-based approach. The itineraries-based approach, initially used for cellular networks [4], builds dynamically route patterns based on usual itineraries of cellular network users. This approach generates an enormous amount of sensitive information, which is previously processed and stored for each user, in a periodic basis. To verify if a transmitting device is cloned or not, the itinerary of its supposed user is dynamically computed and compared with the user's route patterns previously stored in a database. The more the computed itinerary and the route pattern mismatch, the more abnormal is the device. The roaming between cells determines the users' itineraries and their route pattern. In [5], the authors explore an itineraries-based analogous approach to track users in mobile wireless networks. The users' route patterns, which are named User Mobility Profiles – UMPs, are determined after a three-to-six observation period. In a periodic basis, UMPs are established for each registered user. In the motion dynamics-based approach, adopted by EWIDS, the coherence among the users' positions, elapsed time and estimated speeds is verified. Users' speeds are dynamically calculated as a function of the current and past values of position and time. The estimated speeds are then analyzed according to speed profiles: vehicle-speed and foot-speed profiles, for example. In this way, we can infer that a user's current position is coherent whenever this user is located within an imaginary circle around the last users' position. The radius of this circle is given by a function of the users' estimated speeds and of the elapsed time interval between two consecutive positions. In wireless networks, this approach can be enhanced significantly as proposed by EWIDS. In our proposal, the motion dynamics-based approach may also include a relative-motion analysis, establishing a maximum distance among devices associated to the same user. It is worth to note that a user can simultaneously operate several mobile devices. The adoption of the motion dynamics-based approach in WIDSs such as EWIDS addresses several issues of great concern in mobile wireless networks. The first issue is the scalability. Of this point of view, this motion dynamics-based approach is better than the itineraries-based approach since the first one does not generate a huge amount of sensitive information as the itineraries-based approach. The second issue is related with the limited applicability of the itineraries-based approach since this approach is only effective for users with predictable patterns of movement. In case of this approach be indiscriminately applied to all users, the number of FP alarms will increase considerably. In brief, the motion dynamics-based approach gives more freedom of movement to users, without increasing the risks of their wireless devices being cloned. The third issue is focused on the users' location privacy. Unlike the itineraries-based approach, the motion dynamics-based approach can be defined making use only of the last two positions and of a set of statistical parameters, which reveal little about the behavior of users' movement. This characteristic tends to preserve better the privacy of users' locations. In addition, motion dynamics-based approach works fine in conjunction with schemes for hiding users' real locations,

as described in Section 5. Finally, the motion dynamics-based approach restricts considerably the attackers' freedom, since this approach confines the attackers within a small circular area (in our case of 100 meters radius for worst-case scenario). This area is significantly smaller than the coverage area of the wireless metropolitan network (may reach 50 km) and of the cellular network that users regularly move around (10km).
The presence of illegal or unauthorized users inside a metropolitan wireless network can be achieved through a motion analysis of the mobile devices whenever the following premises are considered: (i) users can not be in two different places at the same time; (ii) users may log in the network with one or more mobile devices; (iii) the locations of the devices indirectly determine the positions of the users; (iv) logged-in devices associated to the same user must be close to each other; (v) the movement of the devices must respect the kinematical evolution of the users' motion; and (vi) devices are checked if they are located in a position known by the user or within a probable area for its location. Kinematical analysis refers to both absolute and relative mobility investigations. Absolute mobility analysis establishes an area for a user's transmitter based on the previous movements of permanently logged devices - predictable area - or, of previously disconnected ones (or in idle mode) - probable area. Both areas are calculated from the profile of movement of the device, which includes the last registered position (Datum), the current position, the last registered user's speed profile, the current speed (and its variation), the past average speed, the total covered distance, the number of transmissions, and the transmission timestamp. Both the probable and the predictable areas are, in fact, circles centered at the last known users' location (Datum). Relative mobility analysis considers the whole set of devices belonging to the same user and establishes an inclusion circle (centered at the user's current position) within which legal devices must be located, based on the assumption that users usually hold their mobile devices while in movement. An alternative approach (and sometimes complementary) to verify the relative position is to consider the relative speeds of the devices. Based on the same principle that the devices are attached to their users, the absolute speeds of the devices (belonging to a same user) must be similar, that is, their relative speeds must have value near to zero. In case of any discrepancy among the absolute speed of a device and the absolute speeds of the set of the other devices belonging to the same user, this device can be considered illegitimate. The electromagnetic signal transmitted over an open communication medium can be monitored, captured, and analyzed for detection mechanism in an effort to trace and identify users of wireless devices [7]. This uniqueness arises from the differences found in the circuitry of wireless interface of different manufacturers, and in the electrical parameters of circuit from device to device of the same manufacturer. Cellular companies were the first to use these mechanisms aiming to combat fraud as cell phone cloning. More recently, this technique is being introduced in wireless networks to guarantee users' anonymity and privacy [7] and to identify transmissions from unauthorized devices. It is important to note that there are few proposals in the literature dealing with the identification of wireless devices through their transmission signature. The mechanism proposed in [8] specifically for 802.11 devices establishes a set of 10 statistical parameters conveyed from the transient portion of the radio-frequency signal that uniquely identify the transceiver of a device. Upon isolating the transient, the amplitude, phase and frequency components of that transient are subsequently extracted. In turn, these components are used for the extraction of specific features that define a transceiverprint. Therefore, all this information is combined to determine each device's electromagnetic characteristic (transmission signature), which is stored in a signature database. Once the transmission signatures of all authorized devices have been stored in the signature database, the mechanism can dynamically analyze a transmission. For such task, a classifier is then used to determine the probability of a match between a transceiverprint (electromagnetic characteristic of the current transmission) and each of the transceiver profiles (signatures) stored in the database. Finally, a Bayesian filter is applied to the classification result in order to decide if the current transmission originates from an authorized or unauthorized (cloned) device. A detailed description is found in [8]. As far as we are concerned, there is no other published work about transmission signatures based detection mechanisms for wireless 802.16e devices. It is worth noting that any transmission signature-based detection methodology is applicable to EWIDS. In fact, EWIDS performance depends on transmission signature-based detection mechanisms performance, especially in scenarios where attacks originate from unregistered or external user's devices. In this paper, results of the transmission signature obtained in [8] were incorporated in EWIDS and integrated with the results of the kinematical analysis.

3. EWIDS Description

EWIDS identifies anomalous behavior (intrusion) occurrences by means of an integrated and hybrid approach, joining the detection of non-authorized devices (transmission signature) and incoherent locations of users (kinematical analysis). EWIDS is reactive in the sense that a notification is generated and sent to classical IDS whenever the detection of an anomaly or attack is accomplished, allowing an immediate reaction before that an attack can succeed to compromise the system. Four

important directives were accomplished during the design phase. The first directive concerns the use of two different correlation levels of information; each one being carried out by a different component of EWIDS architecture. This decision turns the task of correlation of each level more manageable since variables set in each component is reduced, facilitating the configuration process of the FP and FN alarm rates. The second directive is related to the nature of the information being correlated. Different than the first level, in which two similar types of information have been considered (results from both absolute and relative mobility analyses), the second level takes into account two different types (not similar) of information: (i) device identification based on the transmission signature of the radio transceiver and (ii) kinematical analysis based on motion dynamics of users' device motion (to identify illegal or unauthorized users inside a metropolitan network). This approach is fundamental to improve efficacy of EWIDS since, in boundary condition situations, decisions based solely on one type of information may be misleading or dubious. A decision process with two different types of information shrinks the boundary condition problem, reducing the FN and FP rate as well as the crossover error rate. The equilibrium point (crossover point) is reached when the ratio between FP and FN rates equals to 1. The Crossover Error Rate is the error rate at which the FP frequency equals the frequency of FN. It is worth to note that the higher a sensibility of the IDS is, the lower the FN rate is (few attacks are not detected), but the higher the FP rate is (increase the number of false alarms). The third directive concerns the choice of the most suitable mechanisms for implement both levels of information correlation. The mechanism used for the first level of information correlation relies on adopting the classical logic algebra due to: (i) a low computational complexity and (ii) a reduced number of inputs dealing with similar information. Moreover, the second level of correlation deals with different information types and a higher number of vague or imprecise inputs, and so it is much more easily handled by a logical fuzzy. Motivations include the results achieved with the use of artificial intelligence techniques in IDS domain [10, 11, 12]. The fourth directive is related to the input variables of the fuzzy system. It considers historical and real-time information on mobility and signature transmission of the current device as the input vary. The use of historical data allows the fuzzy system to reduce FP and FN alarms rates, due to fluctuations of short-term values, turning EWIDS decisions accurate. EWIDS architecture is composed by three components**: the Device-Identifier Component (DIC), the Mobility-Analyzer Component (MAC) and the Judge Component (JGC).** These components interact internally and with external entities (Location System, Transmission Signature Database and Classical IDS). The first component – Device-Identifier Component (DIC) – is responsible for performing the simulation procedure of device identification based on the device's transmission signature of the radio transceiver used in the wireless connection [8]. DIC works exclusively in the physical layer, distinguishing authorized devices from intruder ones. A signature collection, covering the whole set of authorized devices, is used to infer about the current transmission. DIC component is especially important when an attacker tries to act as a legitimate user, using a non-authorized device. DIC is able to avoid MAC-spoofing or more sophisticated attacks such as man-in-the-middle or hijacking [1] once data are transmitted during their attacking procedures. After finishing the transmission signature analysis, DIC sends to the JUDGE a legitimacy verdict about a user, a timestamp, and the device's identification. The second component – **Mobility Analyzer Component** (MAC) – relies on kinematical analysis, i.e. motion dynamics-based approach of users' device, to identify illegal or unauthorized users inside a metropolitan network. EWIDS assumes that a location system [13], possibly located in a Ubiquitous Computing Middleware, is able to track devices' positions and report them to the MAC component. With the locations of users' devices, MAC keeps track of devices' motions by examining the devices' kinematical behaviors from both absolute and relative motion perspective. To accomplish this task, MAC uses three different components: Absolute Motion Analyzer, Relative Motion Analyzers, and Evaluator. Figure 1 describes MAC architecture and the data needed for its processing. **Tracklogger database** stores recent data about past motion of all users' mobile devices registered in the wireless metropolitan network. Absolute and Relative Motion Analyzers rely on Tracklogger's information and Location System's information to, in conjunction with Evaluator component, make a decision about the legitimacy of a device. **Absolute Motion Analyzer** (AMA) analyses the validity of the current device's position. AMA verifies whether a device's position is within the respective **probable or expected circle** (PEC), by checking if the Euclidian distance between the current and previous positions (Datum) is shorter or larger than the PEC radius (distance variable in Figure 4). Together with the analysis decision (Ds_AMA variable in Figure 4), AMA generates an abnormality degree (AD_AMA variable in Figure 1), which reflects how much the device is apart from its expected location. The AMA abnormality degree is defined as a function of the number of times that the distance between the two previous positions overcomes the PEC radius. **Relative Motion Analyzer** (RMA) checks if the distances between the device under analysis and each one of the other devices belonging to the same user are shorter than the radius of the inclusion circle. Then, RMA sends to the Evaluator its decision-making about the **abnormality of the device** (Ds_RMA in Figure 1) and the

abnormality degree (AD_RMA variable in Figure 1). The RMA abnormality degrees is defined as the ratio between the average value of the distances previously calculated (distance between device under analysis and each one of the other devices belong to the same user) and the radius of the inclusion circle.

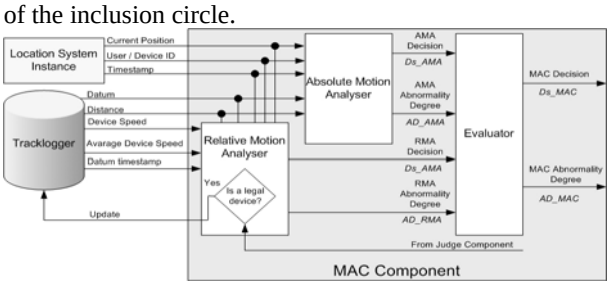


Figure 1. MAC Architecture

The decision-making criterion determinates that a device is abnormal when more than 50% of all distances previously calculated are larger than the radius of the inclusion circle. **Evaluator** is responsible for performing the first level of correlation making use of the results of AMA and RMA. For that, Evaluator uses a logic algebra engine with the true table 1. MAC generates two outputs: its decision (Ds_MAC variable in Figure 1) and the abnormality degree value (AD_MAC variables in Figure 1). In general terms, the true table states that if at least one of the two previous analyses signs an abnormal situation, Evaluator assumes that the current transmission is issued by an illegal device. Concerning the values of the MAC Abnormality Degree, if AMA and RMA diverge in their decisions, then Evaluator chooses the average value of the AMA and RMA abnormality degrees else Evaluator picks the maximum or the minimum value, depending on its final decision. These degree values are taken into account by Judge Component in its decisions. **Judge Component** performs the second level of correlation. The decision about legitimacy of a user's device is done by correlating information of the two different approaches (transmission signature and kinematical analyses) which were generated by DIC and MAC components. To correlate these different approaches, Judge makes uses of fuzzy logic. Pre-Processor block formats historical data to the FIM and formats real time data to be stored in the Historical Information Database. Table 2 describes the seven input variables of the FIM.

Table 1. Evaluator - True Table

AMA Decision	RMA Decision	MAC Decision	MAC Abnormality Degree
legal	legal	legal	minimum
illegal	legal	illegal	average
legal	illegal	illegal	average
illegal	illegal	illegal	maximum

Both AR_MAC and AR_DIC values are defined as the ratio between the amount of generated alarms and the amount of transmissions performed by the device under analysis.

Table 2. Input Variables of the Fuzzy Inference Machine

Input Variables	Description	Data Type
Ds_MAC	MAC decision	Real-Time
AD_MAC	Abnormality Degree of MAC	
Ds_DIC	DIC decision	
AR_MAC	Alarm rate of MAC	Historical
AR_DIC	Alarm rate of DIC	
AD_MAC_{avg}	Average of MAC abnormality degrees issued recently	
NT_DEV	Number of transmissions of the device under analysis	

These values symbolize the robustness of MAC and DIC decisions. For example, whenever AR_MAC value is high and MAC decision is illegal, the FIM generates an alarm with a high abnormality degree value. Conversely, low AR_MAC value and illegal MAC decision produce low abnormality degree value, indicating a possible spurious decision. By considering AR_MAC values, the FIM can filter the uncertainty of certain boundary situations, reducing the FPs and FNs rates. The AD_MACavg expresses the average of the more recent abnormality degree values and reflects the severity of current alarms signaled by MAC (freshness avoids reducing excessively the impact of the current abnormality degree). Fuzzy Machine treats this average as a correction factor of AD_EWIDS Abnormality degree value, assigning high or low for final abnormality degree values. NT_DEV variable states the amount of transmissions of the device under analysis, which statistically denotes the sample size of our approach: lower NT_DEV values imply higher degree of uncertainty, meaning higher FN and FP alarm rates. Fuzzy Machine takes into account the size of the samples (NT_DEV value), aiming to reduce the impact of statistical uncertainty of the historical values, especially those related to recently tracked devices. The output variables - Ds_EWIDS and AD_EWIDS - provide, respectively, the EWIDS decision and its abnormality degree value and are calculated through a set of fuzzy rules, constituting the EWIDS Fuzzy System. It is located within the FIM of Judge Component (JGC). The knowledge base of EWIDS fuzzy system comprises a semantic base and a set of fuzzy rules. We assumed that linguistic variables are defined [16] through a quintuple (X, L, U, G, M), where X is the variable symbolic name; L is the set of labels assumed by X; U is the universe of discourse that contains all possible values assumed by X; G is the syntactic rule, usually defined in the form of a grammar; and M are the semantic rules that define the meaning of each label L (also known as membership

function). In EWIDS system, both variables and fuzzy sets were established after a refinement process of EWIDS system itself. This refinement process focused improving the numbers of FP and FNs. Note that the most worth fuzzy input variables are, such as those related to the DIC and MAC decisions, the higher will be the numbers of labels. The sizes of the universes of discourse were set according to the algorithms adopted by the DIC and MAC components, and the scheme for calculating the historical data. For the EWIDS fuzzy system, nine linguistic variables were defined, seven input and two output, representing the MAC Decision, DIC Decision, Alarm Rate of MAC, Alarm Rate of DIC, Abnormality Degree of MAC, Average Abnormality Degree of MAC, Number of Device's Transmission, EWIDS Decision and Abnormality Degree of EWIDS. They were labeled as Ds_MAC, Ds_DIC, AR_MAC, AR_DIC, AD_MAC, AD_MACAVG, NT_DEV, Ds_EWIDS and AD_EWIDS, respectively. These variables match the linguistic variables of the FIM of the Judge Component. For DS_MAC and DS_DIC, the grammar G is given by GDs_MAC =GDs_DIC ={s0=True, s1= False} and two labels were defined as True (T) and False(F) in order to represent, respectively, the two type of decision of the MAC and DIC components. For AR_MAC and AR_DIC, the grammar G is given by GAR_MAC =GAR_DIC ={s0= Normal, s1= Abnormal, s2= Very Abnormal} and three labels were defined as Normal (N), Abnormal (A) and Very Abnormal (VA) in order to represent, respectively, the three type of alarm rate of the MAC and DIC components. For AD_MAC and AD_MACAVG , the grammar G is given by GAD_MAC =GAD_MACavg ={s0= Normal, s1= Low, s2= Medium, s4= High} and four labels were defined as Normal (L), Low (L), Medium (M), High (H) in order to represent the four type of abnormality degree and the four type of average abnormality degree of the MAC component. For NT_DEV, the grammar G is given by GNT_DEV ={s0=Low, s1= Not Low} and two labels were defined as Low (L) and Not Low(NL) in order to represent the two type of sample size in relation to number of device's transmission. For DS_EWIDS, the grammar G is given by GDS_EWIDS ={s0=Normal, s1= Abnormal} and two labels were defined as Normal (N) and Abnormal (A) in order to represent, respectively, the two type of decision of EWIDS system. For AD_EWIDS, the grammar G is given by GAD_EWIDS ={s0= Normal, s1= Low, s2= Medium, s4= High} and four labels were defined as Normal (L), Low (L), Medium (M), High (H) in order to represent respectively the four type of abnormality degree of EWIDS system. The universes of discourse for Ds_MAC and Ds_DIC were defined considering the closed interval of real numbers between – 0.5 and 1.5. The universes of discourse for AR_MAC and AR_DIC were defined considering the closed interval of real numbers between 0 (zero) and 1. The universes of discourse for AD_MAC and AD_MACAVG were defined considering the closed interval of real numbers between -5 and 50. The universe of discourse for NT_DEV was defined considering the closed interval of real numbers between 0 (zero) and 30. The universe of discourse for Ds_EWIDS was defined considering the closed interval of real numbers between -2 and 2. The universe of discourse for AD_EWIDS was defined considering the closed interval of real numbers between -10 and 40. The second step for building the semantic base is the definition of fuzzy inference rules. Semantic rules determine the shapes that represent each fuzzy set. We adopted the triangular and trapezoidal shapes for linguistic variables. The mapping between labels and scalar values were done in such a way that all values within a universe of discourse were maps at least one label. The boundaries of the polygonal (fuzzy set) are defined as follows: the smallest scalar value on the left side whose membership degree in the previous fuzzy set is equal to 1 (lower boundary) and the highest scalar value whose membership degree in the next fuzzy set is equal to 1, on the right side (upper boundary). For a given linguistic variable, each fuzzy set must have an intersection with its previous and next fuzzy set. So, a given value belonging to its Universe of Discourse will be contained in, at least, one of its fuzzy sets. The next stage in generating the knowledge base consists of building the fuzzy rules relating the linguistic values of the fuzzy variables. Fuzzy sets of the linguistic variables are related through logic operators, as in the statement: "If (Ds_DIC is T) and (Ds_MAC is F) and (AD_MAC is L) and (AR_DIC is N) and (AR_MAC is A) and (AD_MAMavg is L) and (NT_DEV is NL) then (AD_EWIDS is L) (DS_EWIDS is A)". The last step for building the semantic base is the configuration of the system parameters. To evaluate the rules a Mamdani fuzzy system was used with the following methods: (i) And method - min; (ii) Or method - max; (iii) Implication method - min; and (iv) Aggregation method - max. The mom defuzzification method (average of the maximums) was used to generate the scalar output. The fuzzy system version with the best trade-off between complexity and accuracy was the one with nine fuzzy variables presented in this paper.

4. EWIDS Deployment Issues

The deployment of EWIDS System on a WMAN causes three important issues: (i) social aspects in tracking the users' location; (ii) management; and (iii) dissemination of devices' transmission signatures through WMAN. Concerning social aspects, EWIDS has three characteristics that distinguish it from other systems. The first one, EWIDS, in contrast to location-based systems that require a large amount of potentially sensitive information, requires only the most recent users' locations

to decide about the consistency in kinematical movement of the users' mobile devices. This characteristic allows to reduce the amount of sensitive information that might be exposed, or, in case of exposition, it may reveal little information about the user. The second one, EWIDS does not need the current locations of the users. By using kinematical analysis, EWIDS makes use of the relative positions among devices with respect to its user. It is possible to employ axis rotation techniques in order to change the reference point of the location system, hiding the real users' locations. The last characteristics, EWIDS does need the real user's identity. It only knows the relationship between the users and their respective mobile devices. In short, EWIDS delivers a location-aware security system that allows the use of pseudonyms associated with information-hiding tools, a class of service defined in [18]. According to the dissemination of the devices' transmission signatures through the WMAN, EWIDS allows to verify the device's transmissions disregarding their locations and the base station's coverage area from where they transmit. So, the Device-Identifier Component (DIC) may be deployed in a distributed manner as dedicated detection stations located close to all the base stations of the wireless network. These stations comprise a transmission signature analyzer and a transmission signature database. In order to successful verify a transmission signature, the transmission signature databases located in all the dedicated detection stations must be updated periodically. For that, it is needed the exchange of information about transmission signature among these dedicated stations. This information exchange may be performed through a backbone infrastructure connecting all base stations, which is out of the scope of our work. Although the backbone infrastructure is not available to the users, it could generate breaches of security that can be exploited by attackers. One future countermeasure is to configure with strong cryptographic the backbone links that will be used for exchange of information about transmission signatures. It is important to note that information about transmission signatures do not transit through the channels used by the users. To collect the devices transmissions, the DIC only monitors the users' channels most close to each base station. According to the management of the devices' transmission signature, some difficulty in deploying EWIDS system in WMANs due to a huge number of users potentially entering and exiting the network, is posed. This task may be carried out using delegation. The boundaries of cable networks are well defined, making it easy to distinguish internal from external users. However, in WMANS, all users are internal since many organizations are located inside of a coverage area of this network. Thus, the concept of internal and external users must be thought in terms of logical domains. A WMAN infrastructure is shared among many organizations. Each organization constitutes a different logical domain. Internal users from one logical domain (organization) are external in relation to others. Therefore, the WMAN service provider can delegate registration and management of transmission signatures to these logical domains. Although the registration of transmission signature of unaffiliated or roaming users must still be undertook by the service provider, this scheme reduces considerably the burden of managing and registering.

5. Test Platform and Simulation Results

MATLAB 7.0 has been used in the simulation process as it includes a large set of specific resources for fuzzy based systems. In particular, we have used the following set of fuzzy enabling tools: the Fuzzy Engine, the Rule Viewer, the editors FIS Editor, Membership Function Editor and Rule Editor and the native scripts. The implementation has encompassed the EWIDS Prototype, the Generator of Scenarios, the Positioning Error Injector and the Simulation Controller. The EWIDS Prototype comprises three different modules, which correspond to the three new components of the EWIDS Architecture – Mobility-Analyzer (MAC), Device-Identifier (DIC) and Judge (JGC). The MAC and DIC modules have been implemented as Simulink / Matlab models while the JGC module uses the embedded FIM of the Fuzzy Logic Toolbox. The Generator of Scenarios creates simulation scenarios according to a set of parameters - number of users, number of devices per user, coverage area (range), speed profiles (foot-motion or vehicle-motion) and victim-attacker distance. The algorithm randomly chooses the initial positions of users and attackers, and generates their movement within the coverage area. The Positioning Error Injector introduces randomly errors to the positions generated by the Generator of Scenarios. This represents the positioning errors associated to the precision rendered by the positioning applications. This allows measuring, in the simulation phase and according to a set of chosen metrics, the accuracy of EWIDS under scenarios very similar to real world. The Simulation Controller is responsible for managing the simulations, instantiating EWIDS Prototype, triggering Generator of Scenarios, Positioning Error Injector, and FIM (JGC module) properly. It also generates statistical reports according to the number of simulation rounds, among other parameters. Several scenarios have been simulated to validate the components of the EWIDS architecture. To represent situations as close as possible to the real world, these scenarios are related to IEEE 802.16e wireless broadband metropolitan mobile networks (full mobility) with PMP topology. Therefore, these scenarios encompassed several base stations spread out on the metropolitan coverage area and a set of subscribing mobile stations (actors). In addition, each scenario intended to be used by two types of

actors: legitimate users and attackers. Such actors, as already mentioning, may be static or mobile. The mobile ones may move without restraint within the coverage area, according to two types of speed profile: foot-motion or vehicle-motion. Legitimate users may register in the wireless network using one or more mobile devices. The attackers may be internal or external in relation to the service provider of the wireless network. Considering the attackers, each one chooses a different victim (a legitimate user's device) according to two distance patterns: Short (1 to 100 m) or Medium (500 to 1000 m). The attacks are started at randomly instants during the simulation period. Simulations encompassed eight scenario types according to five parameters: (i) metropolitan coverage area; (ii) attacker-legitimate user distance (Short and Medium); (iii) speed profile (foot-motion – 1 to 3m/s or urban vehicle-motion – 7 to 17m/s); (iv) attacker type (only internal), and (v) number of devices per user (1 or 2). For each scenario, fifty simulations rounds were run to generate the mean values, standard deviations and confidence intervals of 95%. We have evaluated the efficacy of EWIDS architecture using six different metrics [17]: (i) **Correct Alarms** – number of correct alarms divided by the total of illegitimate transmissions; (ii) **False Positives** – number of false alarms divided by the total number of alarms; (iii) **Detected Attackers** – number of detected attackers divided by the total number of attackers configured in a specific scenario; (iv) **High-valued Abnormality Degree** – number of correct alarms with high abnormality degree values divided by the total of alarms; (v) **Medium-valued Abnormality Degree** – number of correct alarms with medium abnormality degree values divided by the total of alarms; (vi)**Low-valued Abnormality Degree** – number of correct alarms with low abnormality degree values divided by the total of alarms. Figures 3 and 4 present the simulation results. At some points, these intervals are intermingled with the curve marks due to their small size. In both figures, the vertical axis indicates the metric values while the horizontal axis the scenarios in an increasing distance order. Considering scenarios with short distances between the attacker and the victim, and 1 or 2 devices per user, the FN (Figure 2) are higher for urban vehicle-motion than for foot-motion speed profile, indicating that EWIDS fails in detecting a higher number of attackers for higher speeds. As speed increases, the predictable/probable circle (PPC) radius increases, enlarging the area within which EWIDS assumes that transmitting devices are legitimate. Despite the larger PPC areas produced by higher speeds, FN are almost unaffected for medium distances between the attacker and the victim because most of attackers are still outside the PPC circle. Figure 3 shows the plots of the FP metric using the same scenarios of Figure 2. These two curves correspond to the lowest and highest precision positioning errors considered in simulations: 1 and 15 meters, respectively. The FP are higher for urban vehicle-motion profile than for foot-motion, mainly for scenarios with short distances between the attacker and the victim and 2 devices per user. In fact, the influence of positioning errors is amplified whenever using higher speeds. This effect arises from the increase of the ring area, which is equal to the difference between the PDC areas computed with and without the positioning errors.

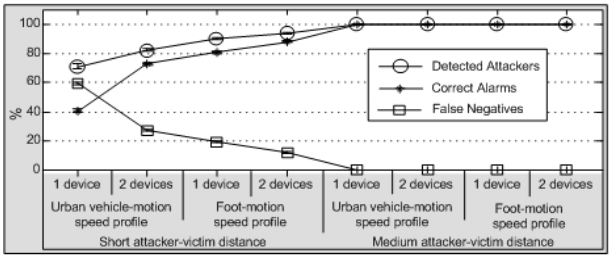


Figure 2. Detected Attackers, Correct Alarms and False Negatives

The larger the ring area, the higher is the number of legitimate devices, located inside it, which are wrongly classified as illegitimate. For scenarios with 2 devices per user, the Relative Mobility Profile (RMP) sub-module also contributes to the final analysis of the Mobility-Analyzer Component (MAC). RMP enhances the efficacy of MAC component for detecting attackers but at the cost of increasing slightly the FP. The abnormality degree value, stored in the AD_EWIDS output variable of the Judge module, indicates the EWIDS confidence in classifying a device transmission as abnormal (DS_EWIDS output variable of Judge Module). Thus, it is important to investigate the behavior of the associated metrics described previously. Figure 4 depicts the behavior of these three metrics for the same scenarios of Figure 2 but considering positioning errors of 1 and 15m.

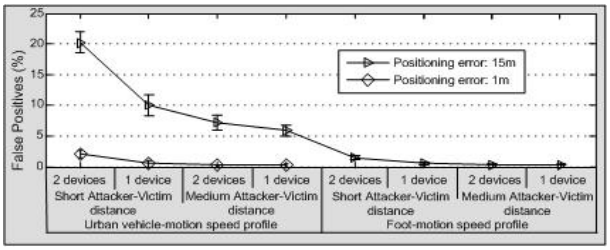


Figure 3. Behavior of False Positives Metric

In Figures 2 and 4, the plots show that the AD_EWIDS abnormality degree is high whenever the detected attacker and correct alarms are high. Therefore, alarms with high abnormality degree values are more trustful than alarms with low values. These plots also show that low abnormality degree values and low correct alarms are always associated to the same scenarios. By issuing low

abnormality degree values, EWIDS reveals that its decision process must still be refined due to the lack of sufficient information associated to the device in the historical database or due to device locations inside the border regions of the predictable/probable circle, making the results of the analysis dubious.

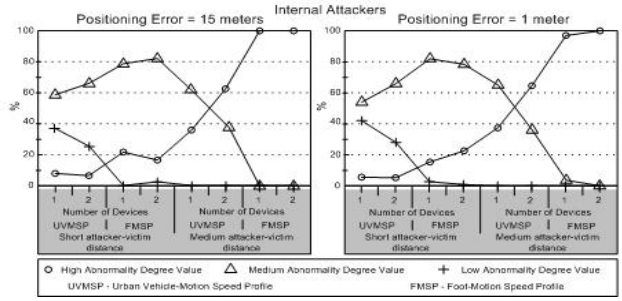


Figure 4. Behavior of AD_EWIDS Metric

6. Related Work

A number of researches have been addressing IDS for the last few years. Zhang et al [15] used software agents for conceiving IDS that detects anomalies in wireless networks. It allows every node to take part in the detection process. Each node is responsible for monitoring its neighborhood to detect anomalies in the routing protocol traffic. Potter [5] introduced a component in Zhang-like IDS that is in charge of setting off counter-measures actions. He also tested his adapted IDS under main-in-middle attacks. Komninos [6] established a procedure that detects unauthorized and compromised nodes in wireless ad-hoc networks. This procedure stems on agents running in the network nodes, which initially monitor the traditional authentication process and afterwards keep looking into nodes behavior according to its standard profile. All previous proposed intrusion detection systems use node resources such as battery energy and nodes' CPU cycles to run the agents, which degrade the performance of real-time applications, especially when the nodes are mobile handheld devices with limited processing and low energy storage capacities.
The distributed agent-based IDS developed by Dasgupta et al [14], which employs anomaly-detection methodology, is not suitable for mobile devices with limited resources for the reasons already pointed out. A hybrid IDS architecture [9], which integrates anomaly and misuse detections through a rule-based system, must still be subjected to a thorough test procedure, including main-in-the-middle attacks, which are the most concerning treats in wireless environments. Hall et al. [12] have recently proposed IDS based on Users' mobility profiles (routes commonly taken by users) for cellular networks. These systems establish users' profiles and monitor users' motions by registering and consulting their roaming between cells. Hall's IDS runs in wireless networks and builds users' mobility profile by capturing and storing in a database the users' locations for a period between 3 and 6 months. These locations include geographical information timely stored. These IDS works fine once users have regular moving behavior. In addition, if an attacker succeeds in grabbing the users' profile, it can set off attacks easily. Dickerson [10] adopted fuzzy logic techniques and a mobile-agent infrastructure. The FIM integrates the information generated by the mobile agents. The IDS proposed by Gomez [11] searches for attack patterns in a database of events using a fuzzy classification algorithm. The attack patterns must be stored in a database that must be updated as soon as a new attack pattern appears. More recently, several lightweight IDS have been designed to address the constraints of mobile wireless networks. Following the trend of designing lightweight wireless IDS, EWIDS does not overwhelm mobile devices because its components may run on dedicated stations, preserving network resources and not degrading QoS-critical applications. In addition, EWIDS does not affect the mobility of devices since it does not make use of users' pre-stored mobility profiles, which require that users should present a regular moving behavior. Another feature of EWIDS is to detect malicious activities using kinematical analysis of mobility, which is a technique computationally less complex than the ones based on itinerary profiles. This feature becomes vital to WMAN networks because they may potentially encompass thousands of devices, making scalability a major concern. An additional EWIDS feature, rarely observed in intrusion detection systems, is the integration of two different techniques, the transmitter fingerprint [8] and Mobility kinematical analysis, which enhance the overall IDS performance. Besides, differently from traditional IDS proposals, EWIDS does not aim at specific attacks, making it a general-purpose type of IDS.

7. Conclusions and Future Work

In this paper, we have addressed one of the most challenging problems in wireless metropolitan networks: better performance of Intrusion Detection Systems. The proposed Extended Wireless IDS bases its decisions on integrating through a fuzzy logic engine the proposed mobility kinematical analysis with a radio transmission signature-based mechanism. EWIDS architectural components may use dedicated stations in PMP topologies, next to the concentration-traffic network devices, minimizing any influence on the intrinsic network QoS and mobility issues. EWIDS evaluations were carried out through simulations over a dedicated test platform, which is composed by a detailed implementation of core components and behavioral models of test environment. The chosen scenarios were as close as possible of IEEE 802.16e and PMP networks. Results have demonstrated

that the proposed algorithms are specifically suitable for wireless IDS, as long as they have succeeded in boosting attackers detection without increasing significantly FP and FN. Another important EWIDS characteristic is a hard positioning constraint for successful attacks: attackers must be close to their victims. According to the results, EWIDS restricts attackers within a maximal circular area of 100 meters radius for worst-case scenario (internal attackers), which is significantly smaller than Wireless-MAN network areas (may reach 50 km). Regarding future work, it is important to investigate EWIDS improvements to short attacker-victim distances circumstances, and to reduce FP in vehicle-motion profiles. Robustness is also a major aspect to be investigated. To represent wireless environments more realistically, next simulation scenarios need to consider transient faults on nodes and on positioning systems. Another research direction considers EWIDS instantiation to mesh topology networks. In this case, EWIDS components must be able to accomplish their tasks in a distributed manner and to control malicious nodes considering information from their neighborhood.

References

[01] BOOB, S. and Jadhav, P., Wireless Intrusion Detection System, International Journal of Computer Applications, volume 5, number 8, p. 9-13, 2010.

[02] Chin-Tser Huang; Chang, J.M., "Responding to Security Issues in WiMAX Networks," IT Professional , vol.10, no.5, pp.15-21, Sept.-Oct., 2008.

[03] Boom, Derrick D., Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks, Master Thesis - Naval Postgraduate School, California, 2004.

[04] SUN, B. and F Yu. Mobility-based anomaly detection in cellular mobile networks. International Conference on WiSe 04, P., Pennsylvania, USA, pp.61-69., 2004.

[05] HALL, J., M.B. 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. August, 2005.

[06] Komnimos, Nikos, D.V.a.C.D., Detecting Unauthorized Nodes in Mobile Ad Hoc Networks and I.P. Ad Hoc Networks, Corrected Proof, Available online 12/27/2005.

[07] K.A. Remley, C.A. Grosvenor, R.T. Johnk, D.R. Novotny, P.D. Hale, M.D. McKinley, Electromagnetic Signatures of WLAN Cards and Network Security, IEEE International Symposium on Signal Processing and Information Technology, 2005.

[08] Hall, Jeyanthi, Michel Barbeau, Evangelos Kranakis, Enhancing Intrusion Detection In Wireless Networks Using Radio Frequency Fingerprinting, Proceeding (433) Communications, Internet, and Information Technology, 2004.

[09] Depren, Ozgur, M.T., Emin Anarim, M. Kemal Ciliz, An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks, Experts Systems with Applications 29-4, 2005.

[10] Dickerson, J.E., J. Juslin, O. Koukousoula, J.A. Dickerson, Fuzzy intrusion detection, IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conference 03, pp. 1506-1510, 2001.

[11] Gomez, Jonatan, Dipankar Dasgupta, Evolving fuzzy Classifiers for Intrusion Detection, Proceedings of the 2002 IEEE Workshop on Information Assurance, 2001.

[12] Hall, J., M.B., E. Kranakis, Using Mobility Profiles for Anomaly-based Intrusion Detection in Mobile Networks, In proceedings of the Wireless and Mobile Computing, Networking and Communications, 2005.

[13] Gwon, Youngjune, Ravi Jain, Toshiro Kawahara, Robust Indoor Location Estimation of Stationary and Mobile Users, IEEE INFOCOM, 2004.

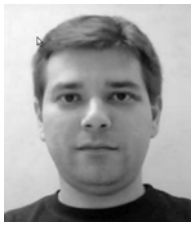
[14] Dasgupta, D., F.G., K. Yallapu, J. Gomez, R. Yarramsettii, CIDS: An Agent-based Intrusion Detection System, Computers & Security 24-5, pp. 387-398, 2005.

[15] Zhang, Yongguang, Wenke Lee, Yi-an Huang, Intrusion Detection Techniques for Mobile Wireless Networks, Wireless Networks 9, pp. 545–556, 2003. [16] PORTER, B., Wireless Intrusion Detection, Wireless Security, 2004.

[17] Crothers, T., Implementing Intrusion Detection Systems: A Hands-on Guide for Securing the Network, Wiley, 2002.

[18] Beresford A. R., Stajano F., Location Privacy in Pervasive Computing, IEEE Pervasive Computing Magazine, Jan/Mar, 2003.

Luci Pirmez is a professor at the Institute of Informatics of the Federal University of Rio de Janeiro (UFRJ), Brazil. She received her Ph.D degree in computer science from the Federal University of Rio de Janeiro, Brazil in 1996. She is a member of research staff of the Computer Center of Federal University of Rio de Janeiro. Her research interests include wireless networks, wireless sensor networks, network management and security.



Helio M. Salmon received a M.Sc. degree on Computer Science in 2011 from the Federal University of Rio de Janeiro, Brazil. He is enrolled in the Brazilian Navy's Engineering Corps as a Lieutenant in 2000. His research interests are in wireless networks, wireless sensor networks, network security and intrusion detection systems.

Luiz Fernando Rust da Costa Carmo received a Ph.D. degree on Computer Science in 1994, from the Laboratory for Analysis and Architecture of Systems of the French National Organization for Scientific Research (LAAS/CNRS). He is a Senior Specialist in Computer Sciences of the Brazilian Institute of Metrology and Quality (INMETRO). His research interests include formal description techniques, communication networks, embedded systems and information security.

Nilson Rocha Vianna received a M.Sc. degree on computer science in 2006 from the Federal University of Rio de Janeiro, Brazil. He is a member of research staff of the Brazilian Navy. His research interests include wireless networks, information and network security, fuzzy logic and Cyberwar.

Reinaldo de Barros Correia took his M.Sc. degree from the Electronic Computation Center (NCE), in 2003. As a research collaborator, he develops research on information security and network management areas.

Claudio Miceli de Farias is a PhD. Student at the Federal University of Rio de Janeiro (UFRJ), Brazil. His research interests include Smart Grids, Wireless sensor networks and Network Security.