Annals of Telecommunications, Vol. 61, No 11-12, November-December 2006, pp. 1300-1313.

Rogue-Base Station Detection in WiMax/802.16 Wireless Access Networks

La détection de fausses stations de base dans les réseaux d'accès sans fil WiMax/802.16

Michel Barbeau
School of Computer Science, Carleton University,
1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6

Jean-Marc Robert[1]
Alcatel, CTO Security Research and Competence Center,
600 March Rd., Ottawa, ON, Canada K2K 2E6

ABSTRACT

We address the problem of detecting a rogue base station (BS) in WiMax/802.16 wireless access networks. A rogue BS is a malicious station that impersonates a legitimate access point (AP). The rogue BS attack represents a major denial-of-service threat against wireless networks. Our approach is based on the observation that inconsistencies in the signal strength reports received by the mobile stations (MSs) can be seen if a rogue BS is present in a network. These reports can be assessed by the legitimate base stations, for instance, when a mobile station undertakes a handover towards another BS. Novel algorithms for detecting violations of received signal strength reports consistency are described in this paper. These algorithms can be used by an intrusion detection system localized on the legitimate BSs or on a global network management system operating the BSs.

RESUME

Nous abordons le problème de la détection de fausses stations de base dans les réseaux d'accès sans fil WiMax/802.16. Une fausse station de base est une station qui usurpe l'identité d'une vraie station à des fins malicieuses. Ce type d'attaque représente une menace majeure. Notre approche à ce problème est fondée sur l'observation que la présence d'une fausse station de base se manifeste par des incohérences dans les rapports de puissance des signaux reçus. Ces rapports peuvent être en autre vérifiés lorsqu'une station mobile procède à un changement de station de base. De nouveaux algorithmes pour détecter des incohérences de rapports de puissance de signaux reçus sont décrits dans cet article. Ces algorithmes peuvent être intègrés à des systèmes de détection d'intrusions installés sur les stations de base réelles ou à un système de gestion de réseau veillant au fonctionnement des stations de base.

[1] Current address: Département de Génie Logiciel et TI, École de technologie supérieure, 1100, rue Notre-Dame Ouest, Montréal (Québec), CANADA, H3C 1K3 – jean-marc.robert@etsmtl.ca.

I. Introduction

A wireless access network consists of access points (APs) and mobile stations (MSs). The APs provide network attachment to the MSs. As a serving AP selection strategy, a MS may choose the one that offers the strongest signal. A *rogue AP* is a malicious station that impersonates a legitimate AP. The rogue AP confuses a set of MSs trying to obtain network attachment through what they believe a legitimate AP. The exact method of attack depends on the type of network and state of associations between an impersonated AP and the victim MSs. For instance, in a WiFi/802.11 network, which uses the carrier sense multiple access (CSMA) scheme, a rogue AP attack may be conducted as follows. An attacker captures the identity, i.e. the medium access control (MAC) address, of a legitimate AP by listening to the traffic. The attacker builds a frame using the legitimate AP's MAC address. Then, it follows the CSMA scheme to send the frame.

In a WiMax/802.16 network, the attack is more difficult to do because of the time division multiple access (TDMA) scheme. To succeed, the attacker must use the MAC address as well as a time slot allocated to the impersonated base station (BS), the access point element providing attachment in a WiMax/802.16 network. Moreover, the attacker must transmit while the impersonated BS may be transmitting as well. The signal of the attacker, however, must arrive at the targeted receiver MSs stronger than the legitimate signal of the impersonated BS. In such a case, the legitimate signal would be seen as background noise. Therefore, the rogue BS attack may be conducted as follows. An attacker captures the MAC address of a legitimate BS by listening to the traffic. The attacker waits until a time slot allocated to the impersonated BS starts. Then, the attacker transmits his rogue signal and makes sure it arrives at a MS with *received signal strength* (RSS) higher than the one of the impersonated BS. The receiver MSs reduce their gain and decode the signal of the attacker instead of the original impersonated BS. This can happen because receivers are designed to operate over a wide range of signal levels, e.g. a 120 dB wide range [16]. They cannot, however, decode multiple signals spread over that wide range at the same time. This is because the demodulator inside a receiver must be fed with a relatively constant signal level, independently of the levels of the input signals. A mechanism called *automatic gain control* reduces the gain of the amplifier inside the receiver in presence of a strong signal to achieve the constant signal level required by the demodulator. A received signal may be strong enough to reduce the gain to a point where another received signal is relatively too weak to be interpreted by the demodulator and it just appears as background noise. The exact minimal difference α in strength between the two signals depends on the design of the receiver. A malicious higher RSS signal can be achieved in several ways. More power or a higher gain antenna can be used or the distance to the receivers can be shortened.

In this paper, we study the problem of detecting and preventing the rogue BS attack, using as examples WiMax/802.16 networks [10, 11]. WiMax/802.16 is a next generation wireless access network technology which is faster, offers better quality of service and is more secure than previous technologies. The rogue BS attack represents, however, a major denial-of-service threat against wireless networks [3]. Firstly, mutual authentication (a possible mitigator) is optional. Secondly, it occurs late in the network entry process. Finally, security at the physical layer is absent. Hence, a rogue BS attack can take place at several points during the dialog between a MS and a BS. For example, authentication occurs only when a MS is undertaking a handover to a target BS. If the targeted BS is rogue, then the transition fails and the MS experiences a service disruption.

Our approach is based on the following observation: inconsistencies in RSS reports from a MS can be seen if a rogue BS uses the identity of a legitimate BS. These reports can be assessed by the serving BS when a MS undertakes a handover, for instance. Novel algorithms for detecting violations of RSS report consistency are described in this paper. The detection techniques can be used by an intrusion detection system based on the legitimate BSs or on a global network management system operating the BSs.

The related work is reviewed in Section II. Background knowledge required by the algorithms is reviewed in Section III. The algorithms are described in detail in Section IV. An extension to our algorithms is discussed in Section V. We conclude with Section VI.

II. Related Work

The rogue BS/AP attack is also known as the false BS/AP attack or the active attack. The existence of the problem has been documented for GSM networks by Niemi and Nyberg [12] and for IEEE 802.16 networks by Johnston and Walker [8]. The problem is also well known for WiFi/802.11 networks and intrusion detection systems implementing counter measures have been proposed [1, 6, 9, 15].

An enabler for this attack is the absence of AP authentication or AP data unit authentication. The problem has been addressed by the introduction of AP authentication in third generation wireless access networks such as UMTS [12] and WiMax/802.16 Amendment E [11].

Assuming it contains no vulnerabilities, WiMax/802.16 BS authentication is, however, optional, occurs late in the network entry process and is not present in all protocol aspects. WiMax/802.16 supports two models of authentication at network entry: unilateral (MS only) and mutual (BS and MS). Mutual authentication in WiMax/802.16, when available, occurs after scanning, acquisition of channel description, ranging and capability negotiation. Furthermore, WiMax/802.16 does not have any security mechanism at the frame layer (i.e. at the physical layer). Thus, a second line of defense is required, as a protection against rogue BS attacks, because there are several doors left open.

Work in this direction has been done only for WiFi/802.11 networks. Beyah et al. [4] propose an approach based on the analysis of the temporal characteristics of network traffic. It is based on the assumption that wireless traffic is more random than wired traffic. Note that the discovery of rogue APs is done by visual inspection of traffic plots and is not automated. Chirumamilla and Ramamurthy [5] propose to check MAC addresses extracted from beacons of APs for membership in a list of registered APs.

Failure to resolve a MAC address in this list is interpreted as a rogue AP attack. This verification is performed by agents located in APs or installed as independent sensors in locations where there is no AP. This approach is vulnerable to MAC address spoofing. Moreover, due to directional antennas, it is possible to hide rogue APs in regions not covered by any agent.

The problem of rogue BS detection has never been addressed in the context of WiMax/802.16 access networks. In this work, we propose a mechanism for early detection of a rogue BS when a handover is being planned by a MS in a WiMax/802.16 network. There is no assumption about traffic models in our solutions.

Another novel aspect of our work is to use the MSs as mobile sensors. Therefore, there is no possibility to hide rogue APs in uncovered areas. As the numerous MSs are roaming in the network cells, they would eventually catch any rogue BS.

III. Background

The definition of the rogue BS detection algorithm is based on the architecture of a WiMax/802.16 access network, the concept of scanning-interval and the log-normal shadowing model of signal loss in free space. This work is based on a draft revision of the IEEE 802.16 standard [10] and an amendment for combined fixed and mobile operation [11].

A WiMax/802.16 access network consists of a number of BSs providing attachment to roaming wireless MSs. By design, every MS tries to get attachment through the BS that presents the strongest RSS. It eventually becomes the serving BS. The RSS value for a BS is relative to the position of every MS.

The BSs are connected together on a separate backbone network, which is used to exchange topology information. Every BS should know the location, the effective isotropic radiated power (EIRP) (i.e. transmission power) and other control information of any legitimate BS in its neighborhood. In the sequel, we assume that this information can be trusted.

A handover can be initiated by a MS when the RSS from the serving BS falls below a certain threshold. As a prelude to a handover, a MS can explore the neighborhood and discover other available BSs. To conduct that exploration, the MS can make a demand to its serving BS for a time interval during which the MS scans the frequencies and assesses the RSS of available BSs. The process is termed a scanning interval and is depicted in Figure 1. The scanning interval allocation request (MOB-SCN-REQ) message is sent by a MS to its serving BS. The BS replies with a scanning interval allocation response (MOB-SCN-RSP) message. The response contains IDs (i.e. MAC addresses) of recommended BSs. During the allocated scanning interval, the MS may perform association tests with the recommended BSs. The MS may conclude by sending a scanning result report (MOB-SCAN-REPORT) message to the serving BS. The MS reports the RSSs of the recommended BSs. The report consists of a list of pairs. Each pair consists of a BS ID and a corresponding RSS. The RSS is obtained by averaging measures of the strength of the signal taken during the preamble of a frame.

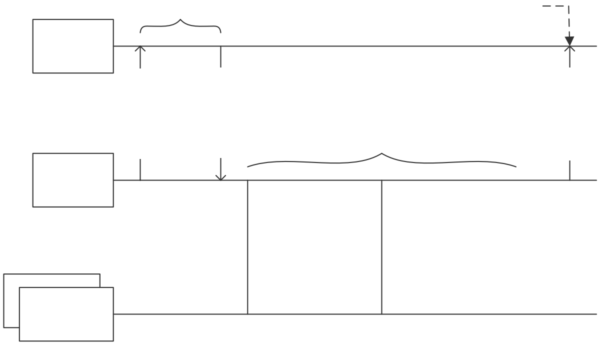

Figure 1: The scanning interval procedure.
La procédure de balayage des fréquences.

According to Rappaport and Rappaport [14], the theoretical path loss $L(d)$ in dB, as a function of the distance *d* in meters, is a random variable following a normal distribution:

$$L(d) = \overline{L}(d_o) + 10\upsilon\log({}^{d}\!/_{d_o}) + X_\sigma \qquad (1)$$

The term d_0 represents a reference distance close to the transmitter i.e. $d_0 \leq d$. The average loss measured at that distance is $\overline{L}(d_0)$. The value of υ ranges from 1.5 to 6. It is termed the path loss exponent. It captures the rate at which the strength of the signal is fading. It is determined using sampling. The term X_σ is a Gaussian distributed random variable (in dB) with zero-mean and standard deviation σ (in dB). Finally, the average theoretical path loss at distance *d* is given by

$$\overline{L}(d) = \overline{L}(d_o) + 10\upsilon\log({}^{d}\!/_{d_o}) \qquad (2)$$

An example is plotted in Figure 2. We assume a 3 km path length at a frequency of 2.1 Giga Hertz, which are possible parameters of operation for WiMax/802.16 [7]. We use a path loss exponent $\upsilon = 2.7$ and standard deviation $\sigma = 12$ dB, which are consistent with the results of Rappaport and Rappaport [14]. Let μ denote the theoretical average loss $\overline{L}(3km) = 94dB$. Then, more than 95% of the area under the curve is concentrated in the interval $\mu - 2\sigma$ and $\mu + 2\sigma$. It means that 95% of the time the loss will be in the 70 dB to 118 dB range, for the given distance. The model is documented in a book of Rappaport and Rappaport [14]. The model described in that book has been validated experimentally by a number of authors, for example see the work of Seidel et al. [17] and Sarkar et al. [18] and numerous additional references on that topic.

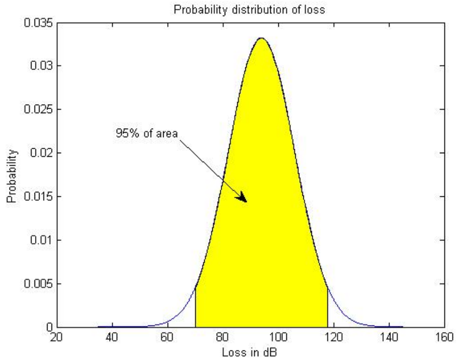

Figure 2: The log-normal shadowing model.
Le modèle d'atténuation log-normal.

IV. Detection Algorithm

Using the attack method outlined in the introduction, a malicious BS can impersonate a legitimate BS during a scanning interval. The MS performing the scanning interval mistakes the malicious BS for the legitimate impersonated BS.

As discussed in the introduction, one major denial-of-service threat occurs when the MS initiates a handover with the malicious rogue BS. By nature, the RSS of the rogue BS will be substantially higher than the RSS of the impersonnated BS. Based on this observation, we present solutions for detecting a rogue BS while a handover is being performed and hence avoiding a transition to a malicious BS. Firstly, we assume that the locations of the MS and legitimate BSs are known. We solve the problem under this assumption in Subsection IV.1. Secondly, we assume that the locations of the legitimate BSs are known, but the location of the MS is unknown. We present a different solution working under this assumption in Subsection IV.2 which has estimated the distances between the MS and the legitimate BSs.

Table 1 summarizes the assumptions on which our detection algorithms are based.

Common assumptions
1. Attacker transmits while achieving a received signal strength (RSS) stronger than the impersonated one. 2. Every BS knows the location and the effective isotropic radiated power (EIRP) (i.e. transmission power) of every legitimate BS in its neighborhood. 3. Log-normal shadowing model of signal loss in free space.
First scenario specific assumption
1. Location of a MS can be obtained (e.g. GPS).
Second scenario specific assumption
1. Impossible to obtain the location of a MS. 2. If sectorized antennas are used, every BS knows the azimuth and the beam width of any legitimate BS in its neighborhood.

Table 1: Assumptions used in this paper.
Hypothèses utilisées dans ce travail.

IV.1 Locations of MS and BS are known

As we have mentioned earlier, our main objective is to detect a rogue BS during the handover phase. The serving BS has to play a crucial role during this step. Based on the information provided by the MS, the serving BS has to determine whether an available BS is a legitimate or not.

To achieve this goal, each BS builds a database containing the following information, for each legitimate BS in the neighborhood: its geographic location coordinates, its effective isotropic radiated power (EIRP), its azimuth and beam width (if a sectorized antenna is used), and, finally, its estimates of the average short distance loss $\overline{L}(d_0)$, the path loss exponent υ and the standard deviation σ as defined in Equation 2 (obtained through a calibration phase). This information must be acquired securely through a backbone network protocol or by configuration. The reliability of our solution relies on the accuracy of these data.

Following the reception of a MOB-SCAN-REPORT message from a MS, the serving BS examines the RSS received by the MS for every available BS (see Figure 1) and it determines the effective path loss associated to the candidate BS as follows:

$$E = EIRP - RSS - G_r \tag{3}$$

where G_r is the gain of the MS's receiver antenna.

Assuming that the MS can provide also its location (note that GPS equipped cell phones are already available on the market), the serving BS can compute the distance *d* between the MS and a candidate BS and determine the associated theoretical path loss with Equation 2. The following fact gives the relationship between the effective and the theoretical path losses.

Fact 1 The gap between the theoretical path loss $\overline{L}(d)$ defined in Equation 2 and the effective path loss *E* defined in Equation 3 is less than or equal to 2σ with a probability 95%.

This fact follows from the standard table of the normal distribution [19].

Based on this fact, we can design the following test to validate every signal received by the MS. First, compute the effective path loss using the EIRP, of the legitimate BS, and RSS, received by the MS (see Equation 3). Then, calculate the average theoretical path loss between the BS and MS using Equation 2. Test the following condition:

$$|\overline{L}(d) - E| \le 2\sigma. \tag{4}$$

For a legitimate BS, failure to pass this test is very unlikely and is considered anomalous. With this technique, the theoretical *false-positive rate* (i.e. a legitimate BS recognized as a rogue one) corresponds to the tails of the distribution delimited by $\mu \pm 2\sigma$ where μ corresponds to the theoretical average path loss $\overline{L}(d)$ associated to the given position of the MS. Thus, the probability is equal to 5%. Furthermore, if the BS uses sectorized antennas, then the azimuth reported by the MS must be within the sector of the BS. If these tests fail, then the signal report for this BS should be considered anomalous and eliminated from the list of candidate BSs for the handover phase.

The *false-negative rate* (i.e. a rogue BS recognized as a legitimate one) depends on the attacker strategy as well as the sensitiveness of the MS. For a rogue BS, the objective is to have a signal strong enough to overwrite the legitimate signal of the impersonated BS without going outside the expected window defined by Equation 2. As mentioned in the introduction, the actual difference between the rogue signal and impersonated signal should be at least α (in dB), depending of the MS design. Therefore, if an attacker would like to succeed with probability 50%, it should aim to produce a signal with RSS at least $EIRP – \mu + \alpha$. Since the legitimate signal is below μ with probability 50% according to the log-normal shadowing model described in Section III, the rogue signal would overwrite the legitimate one at least in these cases. Therefore, if this α (10 dB is chosen as an example) is lower than or equal to 2σ, the false-negative rate corresponds to the area delimited by $\mu - 2\sigma$ on the left and $\mu - \alpha$ on the right. Otherwise, the rogue signal would be outside the legitimate window and an alarm would be raised. Figure 3 summarizes the rates of false alarms associated with this method in the worst case for the given attacker scenario.

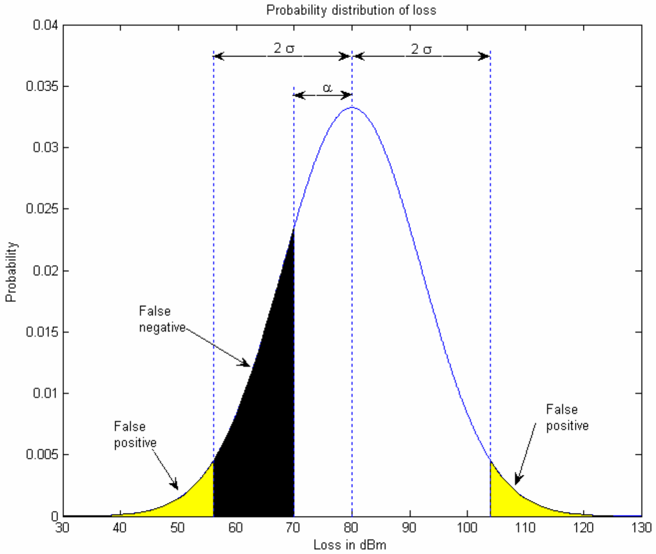

Figure 3: Rates of false alarms.
Taux des fausses alarmes.

IV.2 MS' location is unknown and BSs' locations are known

In this section , we relax the hypothesis that the MSs are equipped with specialized hardware (e.g. GPS) reporting their locations. Therefore, our solution must rely solely on the information that the BSs kept about their neighbor BSs, as defined in the previous section.

In this context, given a loss *L*, the log-normal shadowing model can be used to estimate the distance *d* separating a MS of a given BS as follows:

$$d = d_0 10^{\frac{L-\bar{L}(d_0)}{10\nu}} \qquad (5)$$

The loss *L* is a random variable, so is the variable *d*.

Lemma 1 Let *E* be the effective path loss calculated using Equation 3 from a BS to a MS. Let *d* be the corresponding distance calculated using Equation 5, with *L*=*E*. The real distance from MS to BS is within the interval delimited by the minimum value $d_{\min} = d_0 10^{\frac{L-\bar{L}(d_0)-2\sigma}{10\nu}}$ and maximum value $d_{\max} = d_0 10^{\frac{L-\bar{L}(d_0)+2\sigma}{10\nu}}$ with a probability greater than or equal to 95%.

Proof. The conclusion follows from the fact that, 95% of the time, the maximum difference from the measured path loss and average theoretical path loss is 2σ dB.

Corollary 1 Let (*x*, *y*) be the geographic location coordinates of a BS. Let $d_{\min}$ and $d_{\max}$ be defined as in Lemma 1. The MS is located in a region, with a probability of 95%, defined by an annulus centered at the geographic location coordinates (*x*, *y*) and with radii $d_{\min}$ and $d_{\max}$.

Following the reception of a MOB-SCAN-REPORT message, the RSS_i received for each BS_i is examined, for $i = 1,\ldots,k$. The effective loss *E* is determined using Equation 3. The distance between MS and BS_i is estimated as in Lemma 1. Each BS_i defines an annulus A_i centered at location (x_i, y_i) with radii $d_{i,\min}$ and $d_{i,\max}$. If the annuli $\{A_i,\ldots,A_k\}$ have a non empty intersection, then we conclude that the signal reports are consistent with the legitimate locations of the BSs. Therefore, there is an area where it is plausible for the MS to be located. Otherwise, we conclude the RSS reports are not consistent and assume the presence of a rogue BS impersonating a neighbor BS.

Note that even if the attacker BS can succeed only by achieving a RSS higher than the RSS of the legitimate BS (as required by WiMax/802.16), it is important to approximate the distances with annuli. The following example shows that it is not sufficient to consider only the disks defined by the radius $d_{i,\max}$.

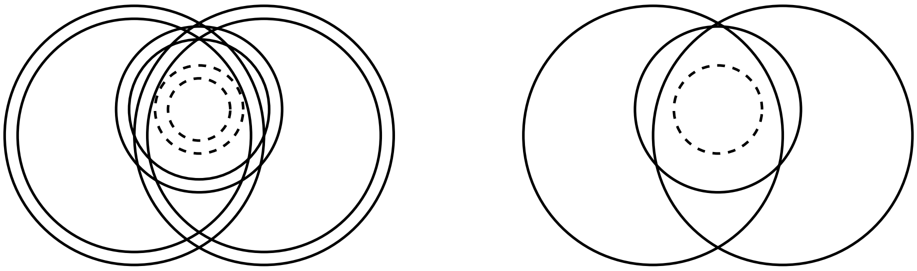

Figure 4: Annuli approximation (left) and disk approximation (right).
Approximation par des anneaux (gauche) et approximation par des disques (droite).

In the annulus case, the three solid-line annuli have a common intersection. However, if the smaller solid-line annulus is replaced by the dash-line one (i.e. the rogue BS has a stronger signal than the legitimate one), the intersection is now empty. This case should raise an alarm.

In the disk case, if the smaller solid-line disk is replaced by the dash-line one, the intersection is still now empty. Therefore, the malicious rogue BS would not be detected.

IV.3 Annuli Intersection Verification

Let MS be a mobile station. Let n be the total number of access points. Let $BS = \{BS_1, BS_2, \ldots, BS_k\}$ be a set of access points for which the MS has returned signal reports, $k \le n$. For $i = 1, \ldots, k$, let $d_{i,\min}$ and $d_{i,\max}$ be the most likely minimum and maximum distance (estimated using Lemma 1) from MS to BS_i, respectively. Let A_i be the annulus centered at BS_i's location (x_i, y_i) with radii $d_{i,\min}$ and $d_{i,\max}$. The signal reports are said to be consistent if the annuli have a common non-empty intersection. This problem can be formulated as follows:

Problem 1 Is there a solution (x, y) to the set of equations

$$(x - x_i)^2 + (y - y_i)^2 \le d_{i,\max}^2 \quad (6)$$

$$(x - x_i)^2 + (y - y_i)^2 \ge d_{i,\min}^2 \quad (7)$$

for $i = 1, \ldots, k$?

This annuli intersection problem can be transformed into a problem of intersecting $2k$ halfspaces and a paraboloid, for which a simpler solution already exists.

Equations 6 and 7 can be re-written as

$$x^2 + y^2 - 2x_i x - 2y_i y \le d_{i,\max}^2 - x_i^2 - y_i^2 \quad (8)$$

$$x^2 + y^2 - 2x_i x - 2y_i y \ge d_{i,\min}^2 - x_i^2 - y_i^2 \quad (9)$$

Thus, the problem can be reduced to the following set of equations

$$z = x^2 + y^2 \tag{10}$$

$$z - 2x_i x - 2y_i y \le d_{i,\max}^2 - x_i^2 - y_i^2 \tag{11}$$

$$z - 2x_i x - 2y_i y \ge d_{i,\min}^2 - x_i^2 - y_i^2 \tag{12}$$

for $i = 1, \ldots, k$.

The problem therefore consists in finding a solution (x, y, z) to these equations. Equation 10 defines a paraboloid and each instance of Equations 11 and 12 defines a halfspace in the three dimensional space. According to Preparata and Shamos [13], the intersection of $2k$ halfspaces can be computed in time complexity $O(k \log k)$ and corresponds to a convex polyhedron. The polyhedron has a complexity of $O(k)$, i.e. the number of faces, edges and vertices is $O(k)$. The intersection of a paraboloid and a polyhedron can be done in time complexity $O(k)$ by intersecting each face of the polyhedron with the paraboloid.

IV.4 Sector Intersection Verification

Let $B_1, \ldots, B_k$ be a set of sectors of annuli. The signal reports are said to be consistent if the sectors have a non empty intersection. For every access point BS_i, the edges of the sectors are modeled as two linear inequalities:

$$y \le a_{i,u} x + b_{i,u} \tag{13}$$

$$y \ge a_{i,l} x + b_{i,l} \tag{14}$$

The equation of annulus (Equations 6 and 7) is added to model entirely the sector. The problem can be formulated as follows:

Problem 2 Is there a solution (x, y) to the Equations 6, 7, 13 and 14, for $i = 1, \ldots, k$?

The solution consists of a transformation of Problem 1 to a problem of intersecting $4k$ halfspaces and a paraboloid. This is similar to the problem solved in the previous section.

IV.5 Fast Approximation for Annuli Intersection

It is possible to develop a faster test, if we accept a higher rate of false-negative . This solution requires some pre-processing of the information.

A Voronoi diagram [2] is defined as the partitioning of a plane into convex polygons determined by *n* generating points. Each polygon contains exactly one generating point. Every other point in the polygon is closer to the polygon's generating point than to any other generating point. The locations of the BSs are used as generating points. The corresponding Voronoi diagram is invariant while the network topology is fixed and can be pre-computed in time complexity $O(n \log n)$.

Then, we compute the minimum distance $Min_{i,j}$ and maximum distance $Max_{i,j}$ between the location of BS_j and a point in the Voronoi polygon P_i associated to BS_i, for each $i = 1,\ldots,n$, $i \neq j$, The time complexity for this calculation is proportional to the number of generating points times the number of vertices in a Voronoi polygon, which is proportional to the number of generating points. Hence, the time complexity for this last pre-processing step is $O(n^2)$.

Once the Voronoi diagram and the minimum and maximum distances have been computed, the validation test during the handover phase goes as follows. First compute the distances $d_1,\ldots,d_k$ to the neighbor BSs, according to Lemma 1. Then, determine the closest access point BS_j to the served MS. We can then assume that MS is in the associated Voronoi polygon P_j. Therefore, the test determines whether $Min_{i,j} \leq d_i \leq Max_{i,j}$, for each $i = 1,\ldots,k$, $i \neq j$. This has time complexity $O(k)$.

V. Extension

The methods described in the previous section can also be used in a broader context. The MSs can be seen as mobile sensors trying to detect rogue base stations in the access networks. The MS simply collects the RSS from all the BSs encountered whilst roaming and reports this information to the serving BS. Those reports can be sent either at the connection phase, periodically or when requested by the serving BS.

For each data set reported by an MS, the serving BS determines if the reported RSS are consistent (as described in Section IV) with its knowledge of the legitimate BSs in the respective area. If the signals are not consistent, then the serving BS can raise an alarm to the network management system. The potential identities of the rogue BSs can be determined by determining the maximal cardinality subset of the geometric representations which are consistent i.e. which have a non empty intersection.

Each legitimate BS can use this method to monitor the access network. If a given BS is reported too often and, eventually, by too many base stations, the central network management acts accordingly and asks to all legitimate base stations in the access network to identify the corresponding BS as at risk. Finally, the network management systems through the legitimate BSs can download a black list of the BS identifiers at risk in the MSs.

VI. Conclusion

Algorithms for detecting a rogue BS in a WiMax/802.16 access network have been presented. When authentication of BS is not enabled, it is a first line of defense. It is a second line of defense when authentication is enabled. These solutions represent some prevention mechanisms against denial of service attacks, since resources are not lost in attempts to establish connections with a rogue BS.

The main limitations of our approach are (i) it works only when an MS is performing the scanning interval and (ii) the approach is probabilistic and has inherently a level of uncertainty.

For the second scenario where the MS' location are approximated, the work is based on the log-normal shadowing model of signal loss in free space (whose validity has been demonstrated experimentally). We have established the logical correctness of the approach. The results are, however, of solely of analytic nature. More research is required to obtain experimental results and conduct comparisons with analytic results.

Finally, under the realistic assumption that the number of available or recommended BS will be rather small (e.g. three to five), the scanning interval (during which the MS performs association tests with the recommended BSs) is expected to be very small (in the order of few seconds). At pedestrian or vehicular speed, mobility has a little impact on the accuracy of our solutions. However, if the number of BSs to test is relatively large, scanning interval will last longer and the estimation of the accuracy of locations will suffer. The exact characterization of this accuracy taking into account the mobility factor has not been completed and is an issue that needs to be explored in the future.

References

[1] AIR DEFENSE, Best Practices for Rogue Wireless LAN Detection, White Paper, 2005.

[2] AURENHAMMER (F.), KLEIN (R.), Voronoi Diagrams In *Handbook on Computational Geometry*, Sacks (J.R.) and Urrutia (J.) eds, pp. 201-290, North-Holland, Amsterdam, Netherlands, 2000.

[3] BARBEAU (M.), WiMax/802.16 Threat Analysis, In *1st ACM Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet),* pp. 8-15, 2005.

[4] BEYAH (R.), KANGUDE (S.), YU (G.), STRICKLAND (B.), COPELAND (J.), Rogue Access Point Detection Using Temporal Traffic Characteristics, In *IEEE Global Telecommunications Conference (GLOBECOM)*, **4**, pp. 2271-2275, 2004.

[5] CHIRUMAMILLA (M.K.), RAMAMURTHY (B.), Agent Based Intrusion Detection and Response System for Wireless LAN, In *IEEE International Conference on Communications (ICC)*, **1**, pp. 492-496, 2003.

[6] ERNST AND YOUNG, The Necessity of Rogue Wireless Device Detection, White Paper, 2004.

[7] GHOSH (A.), WOLTER (D.R.), ANDREWS (J.G.), CHEN (R.), Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential, *IEEE Communications Magazine*, **43**, no. 2, pp. 129-136, February 2005.

[8] JOHNSTON (D.), WALKER (J.), Overview of IEEE 802.16 Security, *IEEE Security and Privacy Magazine*, **2**, no. 3, pp. 40-48, May-June 2004.

[9] PHIFER (L.), Best Practices for Rogue Detection and Annihilation, AirMagnet Technical White Paper, 2004.

[10] LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Draft IEEE Standard, IEEE P802.16-REVd/D5-2004, 2004, Draft revision of IEEE Std. 802.16-2001.

[11] LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, Local and Metropolitan area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in licensed bands, Draft IEEE Standard, IEEE P802.16e/D7-2005, 2005.

[12] NIEMI (V.), NYBERG (K.), *UMTS Security*, Wiley, 2003.

[13] PREPARATA (F.P.), SHAMOS (M.I.), *Computational Geometry, An Introduction*, Springer-Verlag, New York, 1985.

[14] RAPPAPORT (S.), RAPPAPORT (T.), *Wireless Communications: Principles and Practice*, 2nd Edition. Prentice Hall, 2001.

[15] RED-M, Red-Detect, Datasheet, 2005.

[16] ROHDE (U.), WHITAKER (J.), *Communications Receivers*, McGraw-Hill Telecommunications, 2000.

[17] SEIDEL (S.Y.), RAPPAPORT (T.S.), Jain (S.), Lord (M.L.), Singh (R.), Path Loss, Scattering and Multipath Delay Statistics in Four European Cities for Digital Cellular and Microcellular Radiotelephone, *IEEE Transactions on Vehicular Technology*, **40**, no. 4, pp. 721-730, November 1991.

[18] SARKAR (T.K.), ZHONG (J.). KYUNGJUNG (K.), MEDOURI (A.), SALAZAR-PALMA (M.), A Survey of Various Propagation Models for Mobile Communication, IEEE Antennas and Propagation Magazine, **45**, no. 3, pp. 51- 82, June 2003.

[19] ZWILLINGER (D.), *CRC Standard Mathematical Tables and Formulae*, 30th Edition, CRC-Press, 1996.