SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2009; **2**:401–412
Published online 15 July 2009 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.128

Optimal WiMax planning with security considerations

Wassim El-Hajj[1]*, Hazem M. Hajj[2], Ezedin Barka[1], Zaher Dawy[2], Omar El Hmaissy[2], Dima Ghaddar[2] and Youssef Aitour[2]

[1] *College of Information Technology, UAE University, 17551 Al Ain, United Arab Emirates*
[2] *Department Electrical and Computer Engineering, American University of Beirut, Beirut, 1107-2020 Lebanon*

Summary

In the communication sector, the optimal objective is to equate quality and cost. The technologies that best serve these objectives are Wireless Access Technologies since they are easily deployed and capable of reaching and serving customers everywhere in a cost effective way. In this paper, we examine the communication options, and account for a country's geography to propose optimal WiMax planning keeping in mind the security concerns that are inherent in wireless communication. To perform WiMax radio network planning, we use a network simulation tool from ATDI called ICS Telecom. Our approach offers all users a minimum bandwidth of 1.4 Mbps as well as a coverage that exceeds 90% for all indoor users in the area under study. We optimize the network by iteratively minimizing the number of base stations required, and equivalently minimizing the cost, while maximizing the coverage for the subscribers. We also analyze the impact of security on the performance of WiMax. More specifically, we use well-known simulation software called Qualnet to simulate a WiMax environment under different security protocols and encryption scenarios. We then analyze the results to determine the impact of the added security features on the data rates between the base station(s) subscribers. The results of our proposed WiMax planning approach and the conducted security experiments showed that efficient deployment and coverage plans could be achieved for big cities as well as for rural areas. Copyright © 2009 John Wiley & Sons, Ltd.

KEY WORDS: WiMax planning; ICS telecom; WiMax security; IPSec; Qualnet

1. Introduction

As technology is advancing, and the Internet is becoming more vital, the need for faster, cheaper, and simpler means of communication became a necessity. When governments and industry realized that such a fast, cheap, and simple communication could be achieved through wireless technology, they started investing heavily in wireless communication. A big part of these investments went into developing and enhancing WiMax (Worldwide Interoperability for Microwave Access). A key factor in WiMax's success is in the ability to take advantage of the technology's capability to deliver the lowest possible data transfer cost per megabyte while achieving the expected quality of service goals. Minimizing investments is mandatory, but it is also important to maximize the next generation growth opportunity to open new data market segments. One of the most important aspects of WiMax technology is its flexibility in addressing different markets'

*Correspondence to: Wassim El-Hajj, College of Information Technology, UAE University, 17551 Al Ain, United Arab Emirates.
†E-mail: welhajj@uaeu.ac.ae

needs. The IEEE 802.16e version can be used to provide not only mobility, but also fixed and nomadic services, satisfying both highly sophisticated markets and underserved populations [1]. WiMax could also be used to connect enterprises and residential users in urban and suburban environments where access to copper plant is difficult. It will bridge the digital divide by delivering broadband in low-density areas.

In order to implement WiMax in any city or country, network planning is the first task that needs to be performed. This task involves planning both the radio and core network. In this paper, we propose an optimal deployment by minimizing the number of WiMax stations required, minimizing in-building signal losses, and minimizing the effect of mountains obstructions, while maximizing the coverage and number of users able to connect. This planning will be performed using the ICS Telecom planning tool from ATDI. But, building an efficient WiMax network will not be complete without addressing the security issues that it faces.

Security and threats against WiMax 802.16 physical (PHY) and MAC layers are due to the fact that there are no mechanisms provisioned to protect them. An attacker with a radio receiver can intercept messages sent over the air communication connection, fuzz the frames, replay or retransmit them as an authorized party. The attacker can simply prevent service by jamming the signal (denial of service). This will result in making the WiMax network unavailable and costly especially for users with critical applications such as medical or emergency professionals. An attacker can also flood a large number of messages at a higher rate than the base station can handle and thus making the service unavailable to legitimate users; this can be accomplished *via* rouge devices. Moreover, the attacker can potentially access valuable information about the mobile subscribers of a certain base station.

WiMax 802.16e improved on security and data integrity by offering both privacy and security for its L4 and higher layers. Several advanced IP-layer security standards such as IPSec were incorporated in WiMax to secure the access between a WiMax base station and a subscriber unit. Combining these mechanisms provides an end to end secure communication, but it also impacts the quality of service (e.g., throughput and jitter).

In addition to the WiMax network planning, our work analyzes the impact of such security measures and determines its impact on the throughput services provided by WiMax. More specifically, we simulate various WiMax environments under different encryption scenarios using Qualnet tool. We analyze the results to determine the impact of the added security features on the data rates between the subscribers of one or more base stations. We do this by first, presenting our simulation environment and describing the different scenarios on which our data will be based, and second, by collecting and analyzing the simulation results.

The rest of the paper is organized as follows. Section 2 discusses the important works that address optimal WiMax deployment. Section 3 gives a detailed description and analysis of our optimal WiMax planning approach. Section 4 analyzes the experiments we conducted to find the effect of WiMax security on the quality of service. Section 5 concludes the paper and introduces future work.

2. Related Work

Network planning problems have been well studied for different types of wired and wireless networks. But network planning for WiMax deployment has not been studied much. In Reference [2], the authors consider the design, analysis, and system performance of WiMax networks associated with point-to-multipoint topology. In their work, the authors took into account the noise ratio, carrier to interference ratio, and geographical information. The work in Reference [3] is closely related to the work presented in Reference [2], but the deployment was to be made in a very hilly region. The authors relied on the geographic information systems (GIS) tool to optimize some of their objectives such as optimizing the existence of line of sight coverage in the coverage area. The work in Reference [4] presents an analytical dimensioning approach for the planning of cellular WiMax networks within diverse multihop scenarios. One of the conclusions made in Reference [4] is that relays help to extend the range of the base station footprint coverage allowing for a cost-efficient deployment and service. In Reference [5], the authors discussed general guidelines on when to use multihop deployments and when to use single hop deployments. Although the above approaches present some important contributions, they do not offer a complete solution to the WiMax deployment problem, but our work does. Our work takes into account the optimization of both the backbone core network and the last mile radio network, while the other works only consider optimizing one of the previously mentioned networks.

3. Optimal WiMax Planning

In this section, we start by giving a brief introduction about WiMax technology and its challenges. We then

DOI: 10.1002/sec

discuss the approaches we used to obtain the optimal WiMax network (minimum cost and maximum coverage).

WiMax offers a high data rate and extended coverage. In fact, a maximum of 75 Mbps bandwidth is achievable with a 20 MHz channel under best channel conditions [6]. Also, the theoretical coverage radius is about 30 miles under optimal conditions and with a reduced data rate. At extremely long range, the data rate drops to 1.5 Mbps. The WiMax typical coverage with indoor Customer Premises Equipment (CPE) is about 5 km. This coverage increases to 15 km when the CPE is connected to an external antenna (LOS) [6].

WiMax signals encounter many challenges during propagation. Some are general to all types of topographies such as attenuation and Rayleigh fading. Others are evident in rural areas more than in cities such as signal losses due to mountain obstructions. Conversely, some difficulties facing signals are highly noticeable in cities such as in-building signal losses. The overall challenges facing WiMax signals can be categorized into: (1) Attenuation, (2) Rayleigh Fading, (3) Mountains as an Obstacle for Signals [7], (4) In-building Signals Loss, and (5) Interference. Challenges 1, 2, and 5 can be quantified using parameters and formulas suggested in literature. But challenges 3 and 4 depend highly on the WiMax deployment area and on the environment. For this reason, we conduct experiments to quantify the effect of in-building signal loss and the effect of mountain signal loss. All five challenges will be considered in our approach. The simulation tool that we used to plan our WiMax network is called ICS Telecom from ATDI [8]. It provides us with the ability to construct the optimal WiMax network.

3.1. WiMax Radio Planning through Simulation

We chose the city of Beirut, Lebanon as a case study. First, we set up *one base station* in an area in Beirut and conducted several tests and experiments on it. The first goal was to add indoor losses (*in-building losses*) and *mountain signal losses* into the coverage calculation conducted by the tool.

We used frequency equal to 2500 MHz, which is the frequency used for Mobile WiMax. We chose to use Time Division Duplexing (TDD), which is the duplexing method used for Mobile WiMax worldwide. The bandwidth for each channel was assigned to be 5 MHz. The Antenna Gain was assigned to be 16 dBi, which is a standard gain on an antenna. The antenna pattern was designed to have a uni-directional antenna for each sector, where we used a standard antenna rather than a MIMO antenna [9].

After specifying these important parameters, we generated 100 random subscribers (users) within a 2 km radius around the base station [10], so that we are able to see whether these users are able to connect to the base station. The users were randomly generated, with users placed indoors and outdoors in order to simulate real-life users. The subscribers were placed at a 1.5 m height in order to simulate users that are on the street, as well as indoor users at low altitude where there would be buildings obstructing the path of the signal, and the signal would undergo a lot of attenuation to reach the user at this low altitude.

Finally, we launched a coverage calculation in order to generate a 3D view of the coverage around the base station. The coverage calculation was done for Receivers at 1.5 m height. Also the coverage area spans for a 2 km radius around the base station, which is the maximum LOS coverage obtained from real-life experiments conducted by Imperatore *et al.*[10] on a WiMax network in a rural environment in Belgium.

A threshold of −100 dBm was chosen in order to supply the users with a minimum bit rate of 1.4 Mbps. As the received power increases, the achievable bit rate also increases.

3.1.1. Quantifying in-building signal losses

Based on the experiment discussed above, we were able to measure the losses due to the various building material. The result of this experiment was that the coverage of the base station was hugely decreased from almost 1.5 km to a maximum of 900 m in areas populated with buildings. This result was very different from our expectations since we had anticipated much better coverage when we incurred a linearly added loss of 25 dB.

Figure 1 shows the coverage of the base station with the extreme case of 0 dB loss. This simulates the ideal situation in which there is no signal loss. As can be seen, some areas are covered very well by the base station, while other areas where building density increases have less coverage. The gray areas represent no coverage. The subscribers are shown in the figure as white spots on top of the colored area.

Figure 2 shows a more realistic coverage, which is a 15 dB loss, which is around what signal propagation would undergo for a user close to the base station. This case takes into account signal loss in free space, buildings, walls penetration, as well as glass and wood. For

DOI: 10.1002/sec

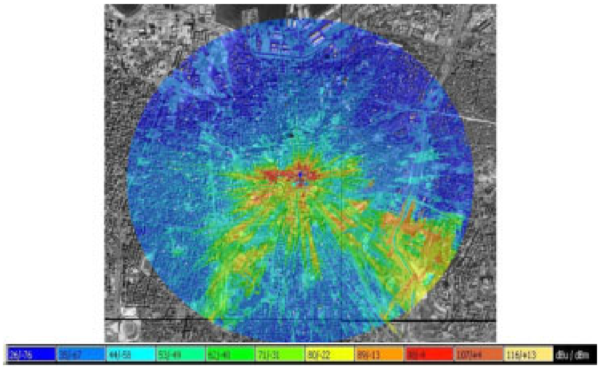

Fig. 1. Case where indoor loss parameters are not taken into account, 0 dB loss

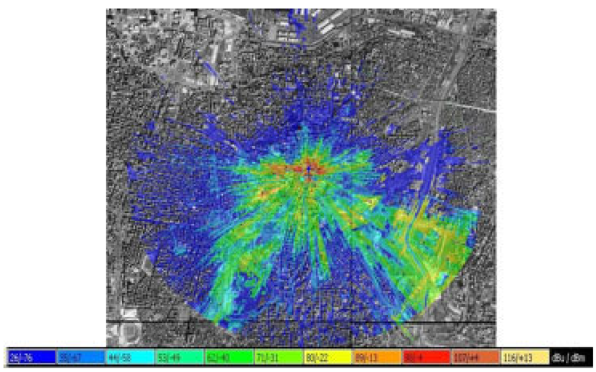

Fig. 2. Coverage at 15 dB loss.

the case of 15 dB loss, 54% of the users were able to connect to the base station.

Then, to complete the data collected from the experiments, we increased the loss from 0 dB until we got 0 connected subscribers at 80 dB, thus 0 users connected to the base station. Figure 3 shows the number of connected users *versus* loss in dB. This figure shows the loss that a typical signal would go through in an urban

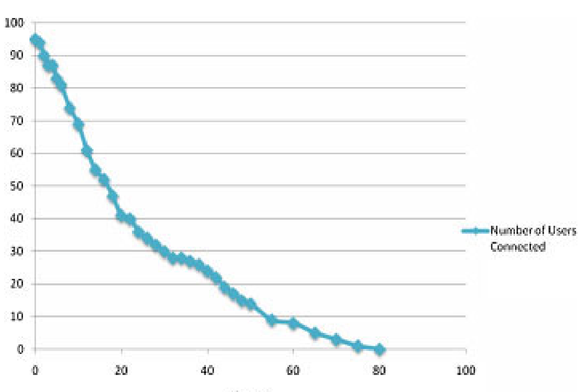

Fig. 3. Number of users connected *versus* dB Loss for the case of In-Building Loss.

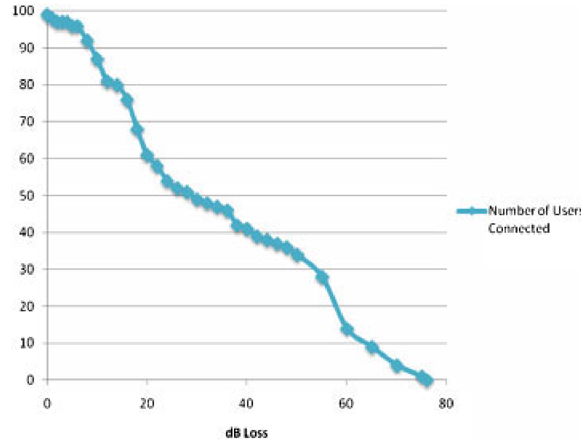

Fig. 4. Number of connected users *versus* loss in dB for the case of mountains signal loss.

environment. Initially, signal loss in free space, then signal attenuation due to window, then loss as the signal penetrates through the buildings' wall, i.e., cinderblock

3.1.2. Quantifying mountain signal losses

To quantify the effect due to mountain signal loss, we placed a base station on the base of a mountain and placed the users around the base station. Most of the users were placed on the mountains, while others were placed on the streets below the mountain. We conducted the same experiment we did in the previous section. We used the same parameters for the base stations and the subscribers, and only varied the loss. Figure 4 illustrates our results for the mountainous region.

3.1.3. Paving the way

Section 3.1 paved the way for us to tackle the optimal WiMax planning problem. The results acquired in this section (radio parameters) will be used as input in Section 3.2. The output of the experiments in Section 3.2 presents a complete coverage of the area under study where the number of base stations required is minimized, the cost is also minimized, and the coverage for subscribers is maximized. Note that we incorporated the losses due to buildings, walls, glass, building materials, and trees in the next step of our simulation.

3.2. Optimal WiMax Planning Approach

3.2.1. Area-based distribution

In order to optimize the Mobile WiMax network in Beirut, we started with a cellular structure and deployed our base stations in the center of these cells. From our study, we were able to see that the coverage in NLOS conditions was around a range of 900 m. Thus, we used cells of 900 m radius each to generate our cellular topology. The simulation tool we used, ICS Telecom, generated some base stations and placed them in the sea that we eliminated. The result of removing the base stations that were in the sea and keeping only those inland was an initial 46 Base Station cellular network.

3.2.2. Optimization based on local geography and building density

Step 1: Optimization of BS locations placed close to water edge.

Strategy: Move base stations inward orthogonal to the water edge so that the distance from BS to water edge = 900 m. This was repeated for all BS on the water edge, which resulted in having to shift all other BS in the same direction away from the water. An example of this process on one BS is shown in Figure 5.

Step 2: Optimization of BS locations close to other (inland) edge of map.

Strategy: Combine multiple base stations on the right edge of the map, two at a time and replace each pair by individual base stations located in between the original location of the pair. This process was done to all pairs of base stations on the right edge of the map. An example of this step can be seen in Figure 6.

Step 3: Optimization of BS locations located in open areas.

Fig. 5. Moving a base station from a location at the sea edge inland orthogonally to the sea edge. The small star shows the old BS location, whereas the big star shows the BS's new location.

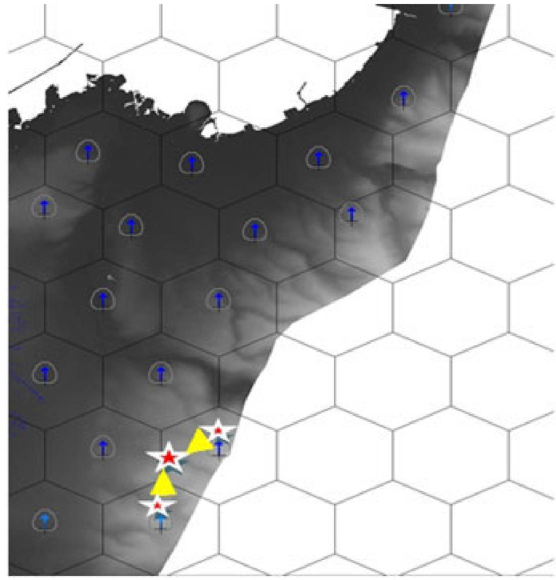

Fig. 6. Example of substituting every pair of base stations on the edge by a single BS.

In this case, we are considering base stations that are located in open space areas where there are fewer obstacles for the propagation of the signal. This results in an increased coverage area around the base station.

Strategy: Combine multiple base stations by attempting to have as few base stations possible to cover the open area. The choice is achieved by trial and error through multiple simulation attempts. A sample of this process is shown in Figure 7.

Step 4: Optimization of BS locations to increase surroundings coverage for all base stations.

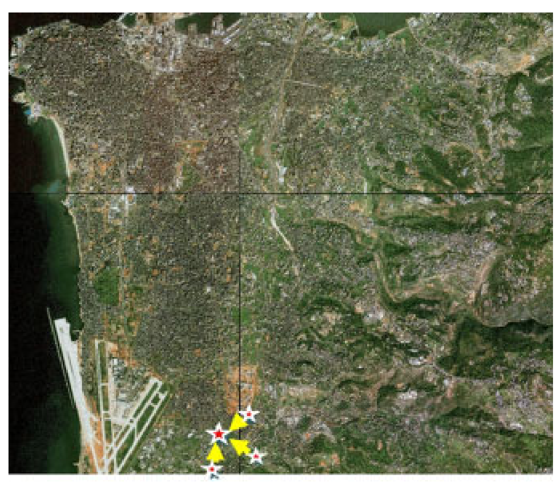

Fig. 7. Combining several base stations in open space areas into a single base station.

DOI: 10.1002/sec

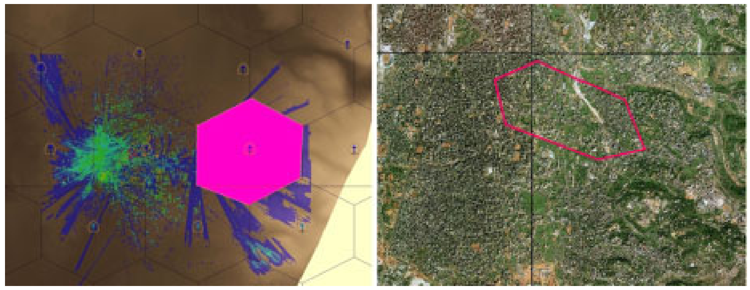

Fig. 8. Selection of a perfectly hexagonal area in pink (left) due to high building density. Selection of an extended area in pink (right) due to free space, thus an extended coverage capability by the BS.

Determine coverage strength for each base station separately given the surroundings of that base station. An observation that can be made is that in dense building locations, coverage area is reduced, while in open space regions, more area can be covered by the same base station.

Strategy: Based on the above observation, for each base station, draw a virtual area (not necessarily hexagonally shaped) surrounding the base station (according to the assessed coverage through the trial and error experiments) and have the simulation tool determine the best location for maximum coverage within the area selected. The tool tests the connectivity between 35 randomly placed base stations and 50 randomly placed users within the area selected to be studied. The simulation results in multiple candidate locations for best coverage, as well as other choices for lower coverage. A sample of this selection is shown in Figure 8. The selected area is shown in pink (ignore the other colors).

The test specifies the best area to place a base station with the highest percentage coverage. The best location possible for the base station is based on the ability to connect to the randomly placed users from the randomly placed base stations. Thus, it was not necessary to place the base station at the highest location in these simulations. A sample of this result is shown in Figure 9.

Based on these results, we examine base stations of neighboring areas. If all candidate locations can cause interference with neighboring BS, then we choose to place the base station in the next best coverage choice that would not cause interference with neighboring areas. Having these base stations close to each other would also result in the need to deploy a new base station that covers the areas that are not reachable by the neighboring base stations. Thus, we had to settle for placing these base stations in the 2nd or 3rd best locations that best fits the network topology and best covers the area under study and prevents interference with other base stations.

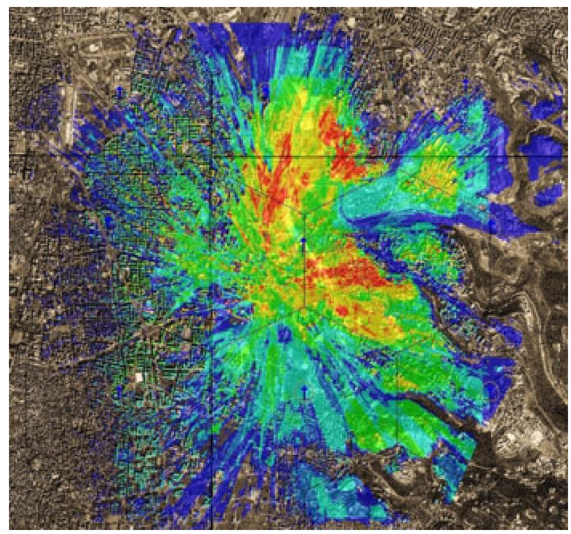

Fig. 9. Placing base stations in appropriate locations to get the highest percentage coverage.

This process of steps 1–4 was iteratively done on all the base station locations, and the initial 46 base stations were reduced to 37 base stations. From herein, the choice of base station locations became final, and the cellular structure of the network became invalid, as the network topology became an adaptive network structure that reduces the number of needed base stations.

Then, these base stations were made to be 3-sectored base stations each, and their parameters were specified as Table 1 shows.

3.2.3. Optimization of the number of BSs needed to cover neighboring area based on coverage strength

After finalizing the placement of the base stations in the best locations, it was critical to move to another

DOI: 10.1002/sec

Table 1. Base station parameters

Parameter	Value	Optimal
Operating frequency	2500 MHz	2.5 GHz
Channel bandwidth	5 MHz	Recommended by TRA: telecommunications regulation authority
Number of sectors at base station location	3	3 sectors is standard number, but can be changed to 4 in order to have more capacity (users and bandwidth). This is what is currently used by WiMax networks
Duplexing	Time division duplexing	Specified in 802.16e standard
Base station antenna gain	19 dBi	This provides us with a high gain antenna
Subscriber antenna gain	0 dBi	0 dBi
Antenna height	25 m	Standard height of antenna
Subscriber height	1.5 m	Subscribers outdoor are on street level. Indoor subscribers are inside but on street level
Antenna type	Standard	
Propagation model	ITU-R 525	Optimal Model for light urban areas
Threshold received power	−100 dBm	This provides each user with 1.4 Mbps bandwidth
Area around base station to be studied	2 km	Maximum LOS coverage radius

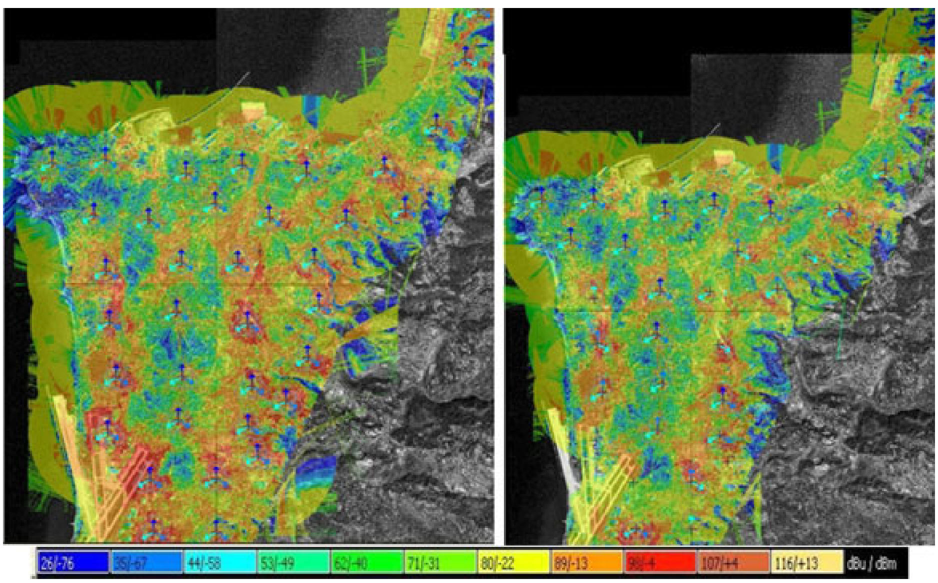

Fig. 10. Left side shows the coverage with 37 base stations, while the right side shows the coverage with 33 base stations.

step. This step constituted of optimizing the number of base stations needed to provide the desired coverage for indoor users.

Strategy: First, examine whole the complete coverage of the map. Then, examine the strength of overlapping coverage from neighboring base stations, and choose to remove one of the neighboring base stations and examine if the coverage is not substantially affected. If the coverage is not affected, then keep both base stations; otherwise, maintain the reduction. This strategy was conducted manually and resulted in the decrease of the number of base stations from 37 to 33. The result of this observation was selecting several stations and studying the effect of deactivating these stations on the total coverage. The left side of Figure 10 shows the coverage with 37 base stations, while the right side of the figure shows the coverage with 33 base stations.

3.2.4. Globally optimize the tradeoff between the number of base stations versus the total coverage

Our next step was to study the area covered, and minimize the number of base stations needed to cover that same area. As a result, 16.67 km^2 of the total 17.15 km^2 indoor area of Greater Beirut was covered, which amounts to 97.2% of indoor users coverage. Indoor

DOI: 10.1002/sec

Table 2. The various scenarios studied, each percentage coverage used with the corresponding needed number of BS and Sectors

	First scenario	95%	90%	85%	80%
Per cent coverage	97.2	95.02	90.2	85.12	80.13
Number of BS	33	31	25	21	18
Number of Sectors	99	71	46	32	25

area coverage was considered due to the difficulties of indoor signal loss and penetration, and the importance of providing WiMax service to indoor users.

ICS Telecom allows us to run a simulation in which we specify the percentage coverage required from the network deployed, and the tool will perform an iterative process which would produce the needed base stations and sectors to provide the percentage coverage requested. This is done by the tool switching off the unnecessary base stations in order to achieve the desired coverage. We used this process in order to generate the required base stations and sectors to a 95, 90, 85, and 80 per cent indoor coverage. The results can be summarized in Table 2. The inactive sectors were the areas where there was an overlapping coverage between two different base stations. Which means that the same area was covered by two sectors, thus having the two sectors covering the same area is redundant. As a result, the simulation turned off the sector covering less area than the other sectors covering the same area. Thus, many sectors were turned off and deemed unnecessary for covering a certain area.

3.2.5. Further optimization by observation for reaching desired coverage

In our study, we decided to focus on achieving more than 90% coverage for indoor users for Beirut, in order for the user to be able to have broadband access and an omnipresent coverage wherever he may be.

Thus, we used the 80% coverage map, which is the lowest coverage we studied, as a base for deciding the minimum number of additional base stations and sectors needed to achieve the desired coverage.

Strategy: First, we ranked the base station sectors that are provided by the previous simulation for each scenario of the percentage coverage we studied. The ranking was done based on coverage strength, where we began with the sectors and base stations at lower coverage. Thus, the sectors and base stations present in lower coverage plans have a higher rank since they are vital for the network. Then, we incrementally add the lower ranked sectors and check if the desired coverage is achieved.

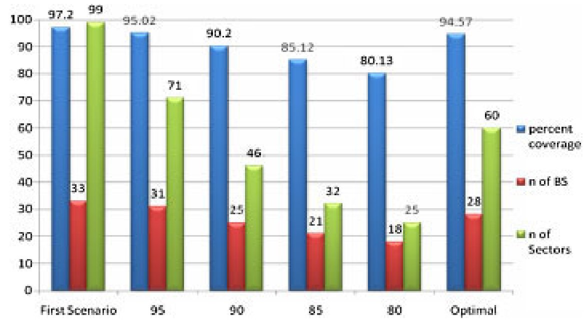

Fig. 11. Percentage coverage *versus* number of BS and sectors.

In reality, we started with the network of 80% coverage. We used all the sectors present in that network. Then, we compared the ranking of the base stations in the 85, 90, and 95% in order to properly assign the needed base stations in our network. We proceeded by sequentially examining each sector in the four scenarios and observing whether that area needs to be covered. The result of this careful examination was to decide which sectors are needed in the optimal Beirut Radio Network. We were able to specify 28 base station locations and 60 sectors that are needed. We then launched the coverage in order to observe how much area this scenario is able to cover. The result of this coverage was 94.57% coverage of Indoor users. This result, in comparison with the other simulations can be seen in Figure 11.

The optimal Beirut Radio WiMax network has 28 base station locations, with 10 base stations having three sectors, 12 base stations with two sectors, and 6 base stations with just one sector. Our Optimal Beirut Radio network is shown in Figure 12.

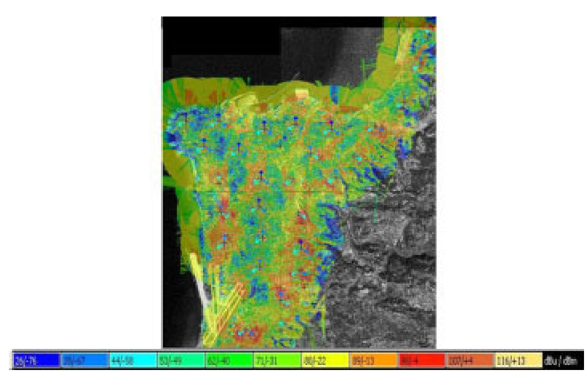

Fig. 12. Our optimal Beirut radio network with 28 base stations and 60 sectors.

DOI: 10.1002/sec

Table 3. Network properties after the optimization

Parameter	Value	Info
Maximum indoor coverage	900 m	In areas with buildings, maximum coverage radius was 900 m from base station
Initial number of base stations	46	
Final number of base stations	**28**	**Less base stations**
Initial Network Topology	Cellular	
Final network topology	**Random**	**Adaptive**
Number of sectors	10 have 3 sectors, 12 have 2 sectors, 6 have 1 sector (60 sectors)	Maximum
Capacity of each sector	70 Mbps	
Total expected bandwidth to be needed in Beirut	$60 \times 70 = 4200$ Mbps = 4.2 Gbps	

Finally, Table 3 gives details about the resultant optimal network. Note that we ended up with an adaptive network planning approach that produces optimal number of base stations. The number of base stations is minimal, the cost is minimal, and the coverage is maximum → Optimal WiMax Planning. Note that the map of Beirut can be replaced with any other map and the same procedure (discussed above) can be followed to obtain the optimal WiMax deployment. Recall that all the WiMax challenges (interference, attenuation, etc.) were incorporated in our approach.

It is extremely important to note that the above optimization was done through extensive simulation and not theoretically. In future work, we will be conducting the planning optimization in theory; the theoretical results we will be compared to the ones we obtained in this paper. Our intuition is that both results will be very close in terms of performance. It is also important to note that our method for optimizing the network is applicable to be used on other WiMax simulation tools, such as ProSite which is a tool for ProPhecy by ProVision Communications [11]. Both ICS Telecom and ProPhecy can provide highly accurate predictions for non-line-of-sight wireless propagation. ProPhecy has an optimization tool called “ProSite” which allows users to optimize their network based on several constraints, such as coverage percentage, total number of sites, total cost, projected revenue, etc. [12]. We believe that our work is parallel to the “ProSite” optimization engine which takes as input the coverage of the area as well as the base station locations and outputs the optimal network design according to the given constraints, which in our case are minimal number of base station with the maximal per cent coverage possible. Now we turn our attention to the security aspect of WiMax where we conduct an extensive study to show the effect of security on the performance of WiMax networks.

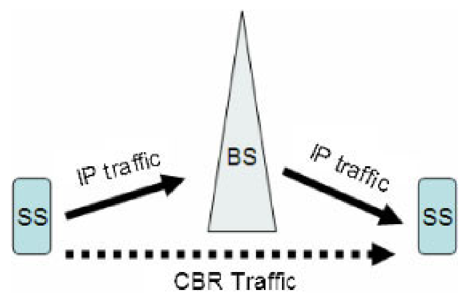

Fig. 13. Simple WiMax model architecture.

4. Consequences of WiMax Security

In order to establish a baseline to understand the impact of adding security to when two, or more subscriber station are communicating over a WiMax network, we simulated the environment and created scenarios to reflect this type of communication in Beirut. The security added is through the enabling of IPSec in different operational modes and with different packet sizes. In our simulation, we tried to reflect the situations where a subscriber station (SS) is sending CBR traffic to another subscriber station (SS), in both static and dynamic modes, and the CBR traffic traverses only one base station (BS), as shown in Figure 13.

4.1. Simulation Tool

To simulate a WiMax environment that uses IPSec to achieve, we used the MAC 802.16 model of QualNet 4.0, which has implemented features defined in both IEEE 802.16 and IEEE 802.16e [13,14]. To analyze the impact of security on the performance of WiMax, we have used two different scenarios. In the first scenario, the stress on the BS was minimal, which was caused by only two communicating SSs. In the second scenario, more stress was introduced to observe how the base

DOI: 10.1002/sec

station performs when more SS are communicating using IPSec and when more encryption computations are required. These encryption computations are impacted by the two transmission modes that IPSec operates in.

The first IPSec mode, transport mode, is used to encrypt and potentially authenticate the data carried by IP (e.g., a TCP segment). For this mode, the ESP header is inserted into the IP packet immediately prior to the transport-layer header (e.g., TCP, UDP, ICMP) and then an ESP trailer (Padding) is placed after the IP packet. In this mode, only the TCP segment, data, and the ESP trailer are encrypted.

The second IPSec mode, tunnel mode, is also used to encrypt the entire packet. For this mode, the ESP header is pre-fixed to the packet and then the packet, plus the ESP trailer are encrypted. This is used to counter traffic analysis. The following section describes the simulation scenarios.

4.1.1. Simulation scenarios

In order to analyze the impact of security on the communication between two subscribing stations using one base station, the following four different IPSec scenarios where used:

1. *Scenario 1*: IPSec One Tunnel- Transport Mode.In this scenario, a connection was established between two subscriber stations (SS) using one tunnel whose endpoints are the two SS and with IPSec being enabled in transport mode, as depicted in Figure 14.
2. *Scenario 2*: IPSec One Tunnel- Tunnel Mode.In this scenario, a connection was established between two subscriber stations (SS) using one tunnel whose endpoints are the two SS, but in this case, IPSec in tunnel mode was enabled to add security. Figure 15 depicts this scenario.
3. *Scenario 3*: IPSec Two-Tunnel Mode. In this scenario, a connection was established between two subscriber stations (SS) using two tunnels with IPSec in tunnel mode enabled. The two tunnels, where configured so that each is connecting one SS to the base station (BS), in IPSec tunnel mode. This is shown in Figure 16.
4. *Scenario 4*: Multiple Subscribers-One Tunnel Mode. In this scenario we used one tunnel whose endpoints being generated from many subscriber stations to one; IPSec in tunnel mode was enabled to add security. This scenario was simulated with the SS's being static and randomly placed within the WiMax cell coverage of the BS.

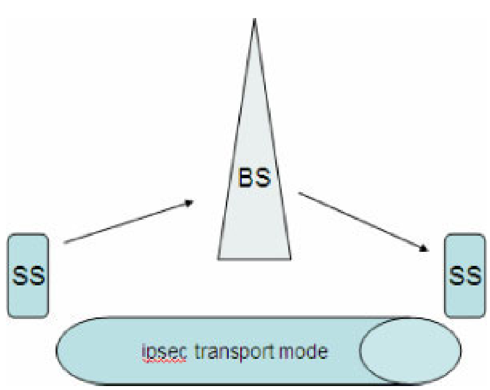

Fig. 14. Example of IPSec single-tunnel in transport mode.

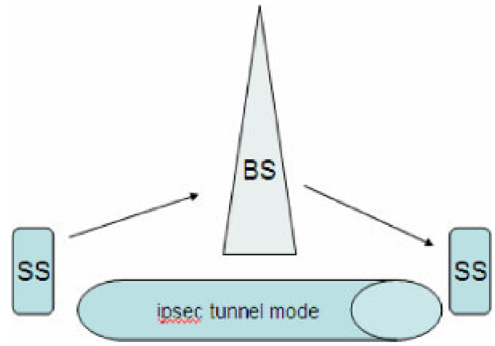

Fig. 15. Example of IPSec single-tunnel in a tunnel mode.

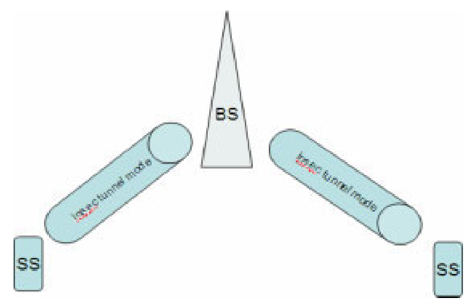

Fig. 16. Example of IPSec two-tunnel mode.

4.1.2. Experiment parameters

To ensure the consistency of our experiments, the parameters in table 4 were used:

4.2. Results and Analysis

Figure 17 represents the IPSec processing overhead in bits when only one SS is used in both transport (1TrM) and tunnel mode (1TuM). The traffic sent was a CBR

DOI: 10.1002/sec

Table 4. Experiment parameters

Simulation parameters	Encryption algorithm: DES-CBC Authorization algorithm: HMAC-MD5-96
Simulation variables	CBR inter-departure time: 0.001–0.032 seconds CBR packet size: 64–1024 bytes
Simulation metrics	CBR throughput in bits/second End-to-end delay in seconds Absolute jitter in seconds IPSec overhead in percentage of original data

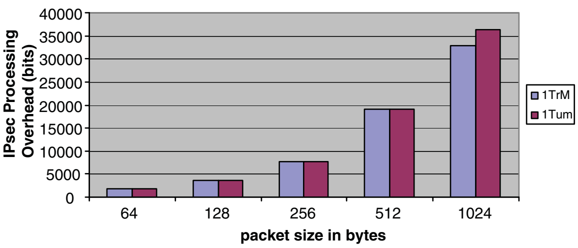

Fig. 17. IPSec processing overhead.

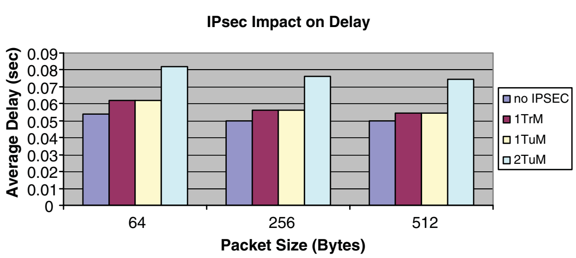

Fig. 18. IPSec impact on delay.

stream with an inter-departure time of 1 ms for various packet sizes. As shown in this figure the IPSec overhead is very similar for both modes for all packet sizes except for 1024 bytes where the over head due to the tunnel mode slightly exceeds the one for the transport mode.

Figure 18 shows how IPSec impacts the average delay when only one SS is used in transport (1TrM), one tunnel mode (1TuM) as well as in the two tunnel mode (2TuM). The traffic sent was a CBR stream with an inter-departure time of 2 ms for various packet sizes. The results show that, with a packet size of 64 bytes, and with IPSec not being enabled, the average packet delay is at minimum. However, with the same packet size and IPSec is enabled, the average delay showed slight increase, with relatively the same rate in both the transport and the tunnel modes. This delay is attributed to additional computational time introduced by the encryption in IPSec. In the transport mode, the bay station receives an encrypted packet from a sending SS, the bay station decrypts the packet to reveal the

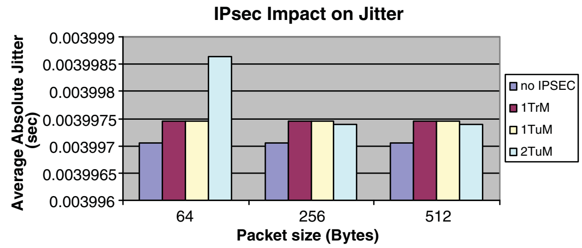

Fig. 19. IPSec impact on jitter.

address of the receiving SS, and then re-encrypts the packet before sending it to the intended destination. Further, when the packet size was increased to 256 and 512 respectively, the average delays slightly decreased for the 1TrM and 1 TuM modes, with more noticeable decrease when the 2TuM mode is used. This is due to the fact that encryption/decryption computations are done less frequently, because the number of transferred packets is less for the transfer of the same amount of information.

From these results, it is evident that performance of the IEEE 802.16, depicted in the average delay, is directly impacted by applying security through IPSec. These results show that enabling IPSec using the two tunnel modes has more impact on the average delay than when using the one tunnel mode. This is true due to the fact that in the two-tunnel modes encryption/decryption computations are done twice (once per tunnel).

Figure 19 shows the impact of IPSec on the average absolute jitter value for the same scenario as in Figure 18. The figure shows the variation in the jitter with respect to various packet sizes. Since the stream used is CBR i.e., the packet inter departure time is always fixed, the jitter here reflects the difference in the inter-arrival time of received packets.

The results show that the average absolute jitter value is almost constant when IPSec is not used; however, when IPSec is enabled, the jitter is slightly varying depending on the IPSec mode being used and the packet size with the exception of the case when the packet size is 64 bytes in the 2 TuM mode. In this case the jitter value is at its highest.

Figure 20 shows how IPSec impacts the average delay at the receiving SS when it is communicating with multiple (2, 4, 8) SS using the 1TuM mode. The traffic sent was a CBR stream with an inter-departure time of 8 ms for various packet sizes. As the results indicate, the impact was minimal until the number of SS exceeds 4, where it becomes exponentially higher. This is most probably due to the fact that the receiving

DOI: 10.1002/sec

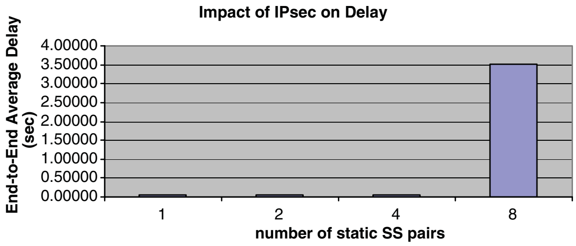

Fig. 20. IPSec impact on delay when many to 1 SS are connected for the 1TuM mode.

SS becomes overwhelmed by the number of packets that it needs to process simultaneously. We believe that this experiment is significant since it shows the impact on delay when *more than* one SS are involved in a secure communication using an IPSec enabled WiMax. Figure 20 shows that if one SS receives packets from more than four SS at the same time, then it will have a major impact on delay. This is because of the effort the receiving SS has to put in processing the IPSec packets.

5. Conclusion

In this paper, we proposed an optimal WiMax planning approach based on extensive simulation experiments using a tool called ICS Telecom. We also study the impact of security on the performance of WiMax networks. After making ourselves familiar with the details of the different parameters present in the tool, we designed experiments in order to quantify the effects of losses a WiMax signal is subject to as a function of the number of users able to connect to the base station. In particular we quantified the in-building signal loss and the loss due to mountains. The results were used in later experiments to obtain the optimal placement of base station such that the coverage is maximized and the number of base stations and therefore cost is minimized. The approach was a success and we were able to obtain the optimal WiMax configuration in a given geographical area. From the WiMax security perspective, it was evident that performance of the IEEE 802.16, depicted in the average delay, is directly impacted by applying security through IPSec. This result shows that enabling of IPSec using the two-tunnel mode has more impact on the average delay than when using the one tunnel mode. This is expected since in the two-tunnel mode encryption/decryption computations are done twice (once per tunnel). For future work, we will be studying the problems presented in this paper theoretically. We will also compare the effectiveness of our approach with other well-known approaches suggested in literature. We have high confidence that our suggested approaches will measure well against others.

References

1. José Luiz, Frauendorf N, Mehta T. Key Factors for IEEE 802.16e 2.5 GHz WiMax Deployments for Fixed Access Service Applications, WCA's Global Development Committee (GDC), São Paulo - Brazil & Reston – USA, Jan 2008.
2. Theodoros T, Kostantinos V. WiMax Network Planning and Systems Performance Evaluation, Wireless Communications and Networking Conference (WCNC), pp. 1948–1953, Hong Kong, 11–15 March 2007.
3. Velez FJ, Carvalho V, Santos D, *et al*. Aspects of cellular planning for emergency and safety services in mobile WiMax networks, Wireless Pervasive Computing 2006, Thailand, 16–18 Jan. 2006.
4. Hoymann C, Dittrich M, Göbbels S. Dimensioning Cellular WiMax Part II: Multihop Networks, *13th European Wireless Conference: Enabling Technologies for Wireless Multimedia Communications*, Paris, France, April 2007.
5. Hoymann C, Dittrich M, Göbbels S. Dimensioning cellular multihop WiMax networks, *IEEE Mobile WiMax Symposium*, Orlando, Florida, 25–29 March 2007.
6. Ahmed Y. WiMax - Broadband Wireless Access, Technical University of Munich, Germany, 16 April 2006.
7. Crozier E, Klein A. WiMax's Technology for LOS and NLOS Environments, *WiMax Forum White Paper*, August 2004.
8. Grenier E. Signal Propagation Modeling in Urban Environment, *ATDI White Paper*, June 2005.
9. A Practical Guide to WiMax Antennas: MIMO and Beam forming Technical Overview, *Motorola White Paper*, 2007.
10. Imperatore P, Salvadori E, Chlamtac I. Path Loss Measurements at 3.5 GHz: A Trial Test WiMax Based in Rural Environment, 2006-2007.
11. Base Station Optimizer Set To Generate Substantial Savings For Wireless Network Operators, 1 September 2006. [Online]. Available: www.WiMax-industry.com/ar/8u.htm. [Accessed: 5 June, 2009].
12. Planning Tool Improves Accuracy of WiMax Network Proposals, 5 May 2007. [Online]. Available: www.provision-comm.com/news/archive/ImprovedWiMax. [Accessed: 5 June 2009].
13. IEEE802.16e, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, 2005.
14. IEEE802.16, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 2004.

DOI: 10.1002/sec