T.C.

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

PERFORMANCE COMPARISON AND ANALYSIS BETWEEN GRP AND LANMAR ROUTING PROTOCOLS IN WIMAX TECHNOLOGY

Ammar Naser Obaid OBAID

Master of Science

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

Istanbul, 2021

PERFORMANCE COMPARISON AND ANALYSIS BETWEEN GRP AND LANMAR ROUTING PROTOCOLS IN WIMAX TECHNOLOGY

By

Ammar Naser Obaid OBAID

Electrical and Computer Engineering

Submitted to the Graduate School of Science and Engineering

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2021

The thesis titled “PERFORMANCE COMPARISON AND ANALYSIS BETWEEN GRP AND LANMAR ROUTING PROTOCOLS IN WIMAX TECHNOLOGY” prepared and presented by Ammar Naser Obaid OBAID was accepted as a Select Degree Thesis in Electrical and Computer Engineering.

Asst. Prof. Dr. Sefer KURNAZ

Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Sefer KURNAZ	School of Engineering and Natural Sciences, Altınbaş University	_____
Prof. Dr. Osman Nuri Uçan	School of Engineering and Natural Sciences, Altınbaş University	_____
Prof. Dr. Ahmet Mesut RAZBONYALI	Faculty of Engineering and Natural Sciences, Maltepe University	_____

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Approval Date of Institute of Graduate Studies: ____/____/____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Ammar Naser Obaid OBAID

Signature

DEDICATION

First, I would like God Almighty to give me strength of mind, health, strength, guidance, knowledge and skills to complete this study. This thesis is devoted sincerely to my beloved father, may God Almighty have mercy on him, who was my source of inspiration and who is the reason I reached this stage of my educational life; He always told me before his death, "Every success in your life will be my best gift." To my mother, who supported me with love and kindness, to my brothers, my sister and my wife.

ACKNOWLEDGEMENT

I would like to thank my supervisor professor Asst. Prof. Dr. Sefer Kurnaz for all support during my study. It is great pleasure to express my deepest gratitude to my friends who have shared with me best moments during my study for the master's degree.

ABSTRACT

PERFORMANCE COMPARISON AND ANALYSIS BETWEEN GRP AND LANMAR ROUTING PROTOCOLS IN WIMAX TECHNOLOGY

OBAID, Ammar Naser Obaid,

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Sefer Kurnaz

Date: 03/2021

Pages: (58)

Mobile WiMAX is a technology that bridges the gap between mobile access and fixed. Also, this technology supports fast-growing broadband access with inexpensive mobile applications. WiMAX technology depends on IEEE 802.16 standard and is provide integration Multiple-Input and Multiple-Output (MIMO) and Orthogonal Frequency-Division Multiple Access (OFDMA) frameworks. The choice of an appropriate routing protocol is a key issue system scalable and effective wireless network. Therefore, the problems occur in message sending for dynamic WiMAX. In this work, the Mobile WiMAX performance has been analyzed in various cases utilizing the NS-2 simulator for two routing protocols are Geographic Routing Protocol (GRP) and Landmark Routing (LANMAR). The results show that the GRP routing protocol has better performance than the LANMAR routing protocol in a different quality of service (QoS).

Keywords: NS-2, WiMAX, GRP, LANMAR, Routing protocols

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF ABBREVIATIONS

EHealth	:	Electronic Health
GRP	:	Geographic Routing Protocol
WiMAX	:	Worldwide Interoperability for Microwave Access
CMS	:	Cloud Management Software
SaaS	:	Software as a Service
IaaS	:	Infrastructure as a Service
PaaS	:	Platform as a Service
iHealth	:	Intelligence Health
EHR	:	Electronic Health Recode
DSL	:	Digital Subscriber Line
NLOS	:	Non- Line Of Sight Propagation
TCL	:	Tool Command Language
TCP	:	Transmission Control Protocol
UDP	:	User Datagram Protocol
OFDM	:	Orthogonal Frequency Division Multiple Access

1 INTRODUCTION

Wireless networks have a significant role in transmitting data with high speed and low overhead. These technologies have become significant due to the mobility nodes concept. WiMAX (Worldwide Interoperability for Microwave Access) is one of these technologies that has been used to provide 1 Gbit/s for fixed stations. Also, it supporting the delivery of last-mile wireless broadband access as a substitute to DSL and cable with provides about 15 Mbps of channel capacity of a particular cell [1]. WiMAX is named the next generation broadband wireless, which indicates to IEEE 802.16 family of wireless networks. Also, this network offered wide specifications for the Physical (PHY) and Media Access Control (MAC) layers. Also, it is designed to operate in the licensed frequency range of 10-66 GHz and unlicensed frequency range of 2-11 GHz [2]. Besides, WiMAX faces various challenges in meeting additional demands to enable mobility WiMAX. It consists of high-speed Internet access that provides multimedia data and different information. In the last years, many researchers focus on improving efficient approaches for wireless networks. These networks have promising areas of research due to their different applications and flexibility [3]. But, they are still facing several defy that are under evaluation and study in utilize of routing protocols for wireless networks such as Ad hoc On-Demand Distance Vector (AODV), Optimized Ad-hoc On-demand Multipath Distance Vector (AOMDV), Destination-Sequenced Distance Vector (DSDV), Zone Routing Protocol (ZRP), Optimized Link State Routing Protocol (OLSR), Dynamic Source Routing (DSR), Dynamic MANET On-demand Routing Protocol (DYMO), and Temporally-Ordered Routing Algorithm (TORA). The authors of [4] analyzed AODV, AOMDV, and DSDV routing protocols for IEEE 802.16 WiMAX network using NS-2 simulator. These protocols were run to measuring throughput by varying the number of subscriber stations. They observed that the throughput varying over a range and decreased as the number of subscriber stations communicating with the wired sink node over the base station, increments. They also observed that the throughput is the highest for DSDV protocol than AOMDV protocol. The authors of [5] evaluated AODV, ZRP, OLSR, and DSR routing protocols based on different node density that includes 25, 50, 75, and 100 nodes using QualNet simulator in WiMAX technology. The results show that throughput is best given by OLSR protocol. The authors also show comparing Variable Bit Rate (VBR) and Constant Bit Rate (CBR) to an OLSR protocol at 100 nodes as CBR has less jitter, less delay, and higher throughput compared to VBR. Then, the authors have analyzed OLSR, DSDV, and DSR routing protocols in WiMAX technology

to a specific routing approach [6]. The simulation results show OLSR protocol which refers to Link state table-driven protocol with some optimizations performs better than the DSDV and DSR protocols.

The authors of [7] compared analysis of three routing protocols include ZRP, DYMO, and AODV under a mobility model with varying transmission range for important performance metrics. From results that have been obtained by authors, it is concluded that DYMO and AODV perform well with respect to jitter and End to End delay while ZRP gives high throughput in varying transmission range scenario. While other authors have demonstrated DYMO and OLSR routing protocols in WiMAX technology in terms of End-To-End delay using QualNet simulator. As they demonstrated DYMO has achieved better than OLSR with outperforms 79.5% [8]. As shown above, several routing protocols were analyzed in WiMAX networks such as DSDV, OLSR, AODV, TORA, DSR, and ZRP routing protocols but trying to analyze and study other routing protocols have some merits to improve the routing process in the network. In this paper, we compare and analyze the performance of routing protocols GRP and LANMAR by a node intensity of 50 nodes using an NS-2 simulator in WiMAX technology. Two scenarios have been used under usual and dropping packet conditions based on different QoS metrics, which include throughput, normalized routing load, and packet delivery fraction.

2 LITERATURE REVIEW AND BACKGROUND

2.1 ANALYSIS OF THE WIMAX 802.16E STANDARD

Although WiMAX was not designed as a mobile system from the beginning, its features and demand for applications led to the specification of support for the mobility of subscriber stations. For the optimal function of this technology in a mobile environment, it is necessary to analyze many problems that hinder the required mobility. It is mainly a matter of selecting the appropriate frequency band and specifying the transmission path.

Most wireless systems assume that they do not have direct visibility between the receiving and transmitting station (NLOS). During propagation, the radio signal has in the way of the building and other terrain obstacles. Other problems are the movement of the receiving station relative to the transmitter, delays in signal propagation, interference from other signals, noise, or distortion that cannot be precisely determined in advance and changes over time[9].

2.1.1 Fluctuation of the received signal

In mobile communications, in addition to receiving a direct signal, many reflections are also received (multipath propagation). This phenomenon results in fluctuations in the power of the received signal by up to tens of dB, even at relatively small distances between the receiver and transmitter.

2.1.2 Power losses

In the NLOS environment, the received power is more dependent on the propagation distance than in LOS systems. In addition to distance, other factors are added here, such as the location of the antenna. Losses also increase with the square of the frequency.

2.1.3 Direct signal propagation

In the case of large obstacles, such as buildings, the direct propagation signal is very attenuated or completely suppressed. The receiving station then mainly receives reflections of the transmitted signal.

2.1.4 Inter symbol interference

In a multipath environment, a phenomenon occurs during one symbol period that the current and reflection-delayed data symbol (ISI) arrives at the receiver input at the same time. At higher bit rates, the symbol period is relatively small, increasing the possibility of ISI. To eliminate this phenomenon, the equalization method is used, which selects the strongest of the received delayed signals. The OFI modulation technique implemented in WiMAX technology helps to reduce the consequences of ISI.

2.1.5 Doppler shift

The relative movement between the transmitter and the receiver causes a frequency scatter called the Doppler shift. The Doppler shift is directly proportional to the speed of the moving user station and the carrier frequency. In broadband systems, Doppler shift causes a reduction in signal-to-noise ratio (SNR), complicating carrier synchronization and recovery. This phenomenon also affects OFDM systems, as it can disrupt the orthogonally of individual subcarriers.

2.1.6 Noise

In communication systems, the white noise channel (AWGN) is most often considered. The thermal noise of the receiver is given by the bandwidth, and therefore its level is greater in broadband systems than in narrowband and leads to a reduction in coverage area.

2.1.7 Interference

Every data transmission system has a limited bandwidth that must be shared by many users. As a result, one user's transmission affects all others. In systems focused on maximum transmission capacity, interference has a greater effect than the noise level.

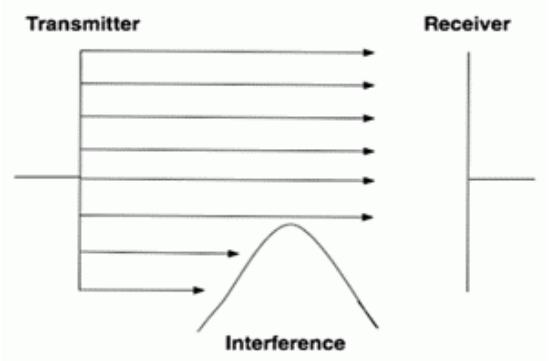

Figure 2.1: Transmission interference.

The causes can be different, eg another transmission on the same frequency. WiMAX has several techniques for suppressing the effects of interference:

- OFDM technology
- adaptive antenna system
- dynamic frequency selection

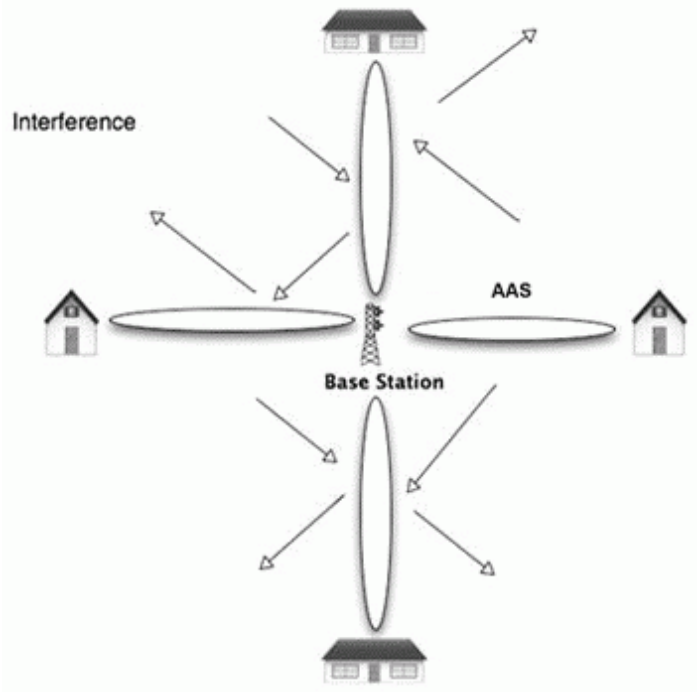

Figure 2.2: Transmission interference.

2.2 FREQUENCY BANDS FOR BROADBAND WIRELESS SYSTEMS

Selecting the appropriate frequency band plays one of the key roles in designing wireless networks. Some bands have been used to develop WiMAX technology, in the future, however; only selected bands divided by country are expected to be used, The choice of frequency band and its width results in limitations in the form of transmission speeds and coverage areas.

Table 2.1: Frequency bands usable for WiMAX

Zone	Band allocation	Bandwidth	Description
3,5GHz	3,4-3,6GHz 3,3-3,4GHz 3,6-3,8GHz	Total 200MHz; ranges from 2x5MHz to 2x56MHz	Licensed band. Bands accessible by country. Suitable for Europe.
2,5GHz	2,495-2,690GHz	Total 194MHz	America and Asia
2,3GHz	2,305-2,320GHz 2,345-2,360GHz	2x5MHz	United States, Australia
2,4GHz	2,405-2,4835GHz	80MHz	Free. zone. Highly used, guaranteed, performance limitations
5GHz	5,250-5,350GHz 5,725-5,825GHz	200MHz	Performance restrictions
UHF	television band	30-48MHz	

Most bands carry restrictions either in bandwidth, unavailability in our region, or possibly performance restrictions. The 2.4 GHz and 5 GHz bands are unlicensed, but this results in a high level of interference for many users of various other services, such as WiFi, Bluetooth, industrial equipment, radars, etc. From the above overview, it is currently possible to count on a licensed band 3, 5 GHz, which is intended for wireless broadband services in many countries around the world. The available bandwidth is up to 200 MHz, which results in the possibility of relatively high transmission speeds.

It is necessary to place an ever-growing number of users who want to use more demanding applications in a relatively narrow band. The basic method for more efficient use of spectrum is the use of cell architecture, where individual cells are covered by access points with lower performance. The cells are then further divided into several sectors using directional antennas. The frequency used in one cell is repeated in another cell that is at a distance where there is no longer any risk of interference. On the other hand, high utilization of the available frequencies is necessary to achieve the highest possible system capacity. This leads to the design of systems enabling the transmission and reception of a signal with a low SINR (signal / interference + noise ratio).

2.2.1 Adaptive modulation and coding

The choice of modulation and coding rate may vary depending on the number of users or the amount of data transmitted. In both cases, the result is mainly affected by the SINR ratio.

2.2.2 Spatial multiplex

When using multiple antennas, it is possible to transmit multiple independent signals in parallel, and the signal can be processed at the receiver in a similar manner. Spatial multiplexing allows an increase in data rate in proportion to the number of antennas used.

2.3 IMPORTANT FEATURES OF THE WIMAX STANDARD

Physical layer with OFDM: OFDM provides advantages in terms of better resistance to multipath propagation and enables transmission in NLOS environments. OFDM modulation technology is nowadays implemented, for example, in WiFi or digital television systems. The OFDM principle consists in the use of several hundreds to thousands of carrier frequencies (256 frequencies are used for WiMAX). The carriers are further modulated as required by various robust modulations

from BPSK to 64-QAM. The individual carriers are orthogonal to each other, so the maximum of each carrier should overlap with the minima of the others. The data stream of the entire channel is thus divided into 256 partial data streams of individual carriers.

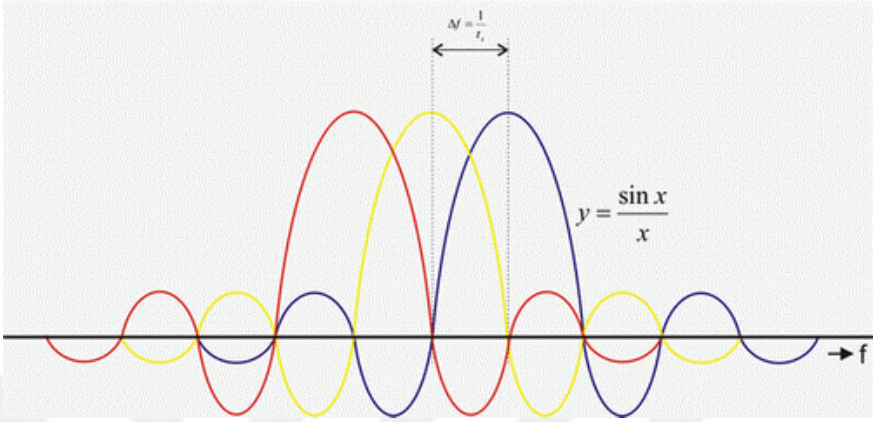

Figure 2.3: Partial overlap of carrier frequencies.

- Baud rate: usable data rates up to 75Mbps (for 20MHz bandwidth). In real conditions, using a downlink to uplink ratio of 3: 1, a speed of 25Mb / s can be achieved downlink and 6.7Mbps for uplink. The transmission speed can also be increased by using more antennas and spatial multiplexing.

- Bandwidth and bit rate: The physical layer architecture supports streaming changes according to the available bandwidth. This option is supported by the OFDMA method, which allows you to change the length of the FFT. WiMAX can change the length of the FFT in the range from 128 to 1024 points depending on the band 1.25MHz, 5MHz and 10MHz. This also facilitates roaming options in areas of transition between networks with different bandwidths.

- Adaptive modulation and coding: WiMAX supports several modulation techniques and correction codes. These techniques can be suitably applied to transmission channels with different degrees of noise and interference, and thus it is always possible to achieve maximum channel utilization with minimum error rate.

- TDD and FDD support: time division duplex is preferred today for several reasons. The main reason is the possibility of choosing a suitable ratio between uplink and downlink data flows. FDD is used only for some types of Fixed WiMAX in the 3.5GHz band.

- OFDMA: this technique allows multiple access to the transmission medium, so that users divide the OFDM band according to their immediate needs. This creates the possibility of better use of system capacity.

- Quality of service: WiMAX supports a wide range of applications including voice and multimedia services. Related to this is the support of a constant or variable data flow, data transfer in "real time".

- Security: WiMAX offers a high level of transmission security (encryption, passwords, and authentication protocols).

- Mobility support: the mechanisms implemented in WiMAX allow a certain degree of user station mobility. OFDM technology with a suitable spacing of subcarrier frequencies allows movement depending on the band used, but according to the 802.16e standard, up to a maximum of 150 km / h.

- IP protocol support: the entire WiMAX network uses IP protocol technology, so there is no problem with connecting to surrounding systems.

2.4 WIMAX SYSTEM THROUGHPUT

Figure 2.5 shows how many users can be connected to the network at the selected guaranteed speed for the 3.5 MHz bandwidth. Four guaranteed speeds (marked as BR in Fig. 8) were considered in the calculation. If the capacity of the system is greater than the required capacity, the user can be served. Otherwise, it is necessary to reduce the guaranteed speed to ensure the service of other users. When using 0.5 Mbit / s, up to 12 end users can be served, while only 3 users can use the available transmission capacity at a guaranteed speed of 3 Mbit / s. When using a 20 MHz radio channel (Fig. 2), the system can serve up to 30 users at a guaranteed speed of 0.5 Mbit / s and 5 users at a speed of 3 Mbit / s.

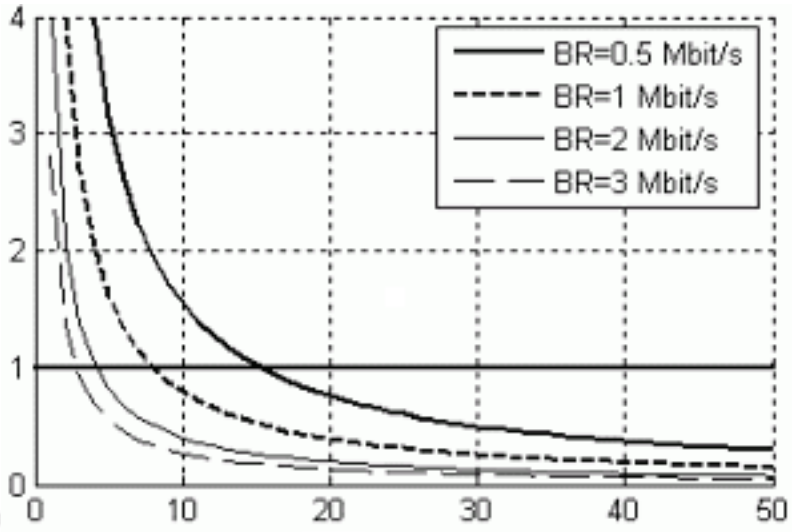

Figure 2.4: System bandwidth for 3.5 MHz bandwidth.

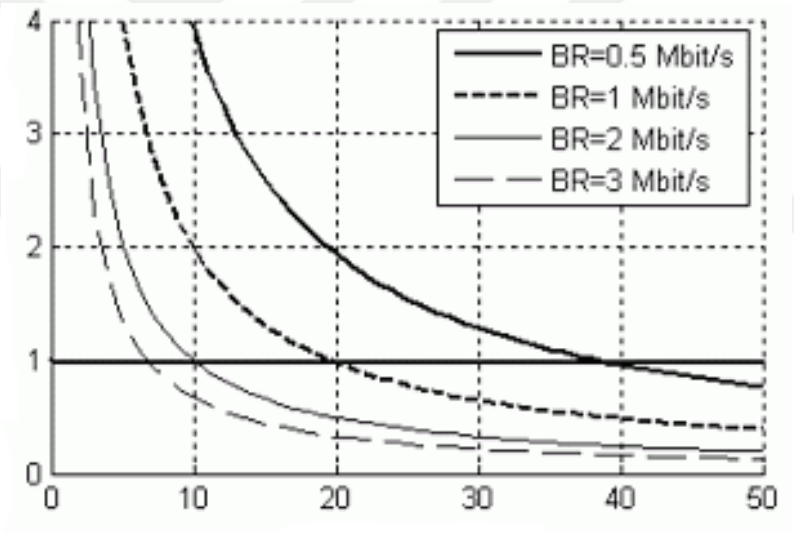

Figure 2.5: System bandwidth for 20 MHz bandwidth.

2.5 TYPES OF NETWORK TOPOLOGY

According to the IEEE 802.16 or IEEE 802.16e standard, two possible network topologies can be defined: point-to-multipoint (PMP) and mesh topology. The PMP topology must be mandatory, while the implementation of a mesh topology is optional.

The PMP architecture is based on the classic cellular structure of the network, where individual user stations connect directly to the base station.

With a mesh topology compared to PMP, direct communication between stations is also possible. They count on the use of fixed stations as retransmission points. This makes it possible to increase the range of one base station without having to increase the transmission power.

2.6 TRANSMISSION CONTROL

WiMAX supports flexible bandwidth allocation of radio channels and channel reuse to increase cell capacity as the network grows. It also specifies transmit power control (TPC) and channel quality measurements, as additional tools for cell planning and efficient spectrum utilization. Dynamic Frequency Selection (DFS) is mandatory for work in unlicensed bands4.

Metropolitan networks according to 802.16, like all radio networks, have to cope with changing environmental conditions, because especially rain can have a negative effect on the quality of signal reception. The specification therefore includes radio link control (RLC) to set the initial parameters of the radio link and to change them when conditions change. The 802.16 device monitors the quality of the connection after its initialization and adjusts the transmission parameters accordingly.

2.6.1 Transceivers and antennas

The structure of WiMAX stations is very simple. It is built on two elements, namely a transceiver (combination of transmitter and receiver) and an antenna.

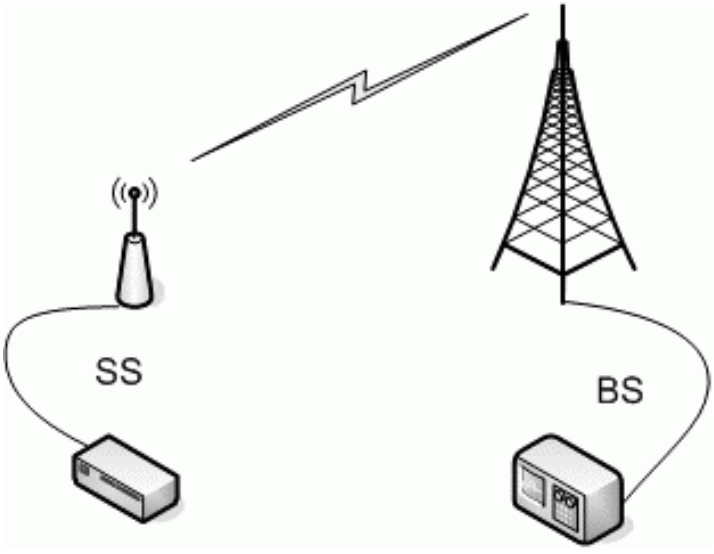

Figure 2.6: Radios and antennas.

2.6.2 Transceiver

The core of WiMAX are transceivers, which contain both a receiver and a transmitter. It generates carrier frequencies (for WiMAX 2 - 11GHz). The transceiver contains circuits with complex sets of processors.

Most base stations are designed to have a separate antenna from the transceiver. In contrast, client stations have two solutions, either with an external antenna installed, eg outside the building, or with an antenna located inside the building.

The main advantage of such a BS solution is that the transceiver is protected from extreme weather conditions. In addition, an antenna located outdoors has better signal reception than an antenna located indoors, especially if direct visibility is required.

The antenna with the radio station is connected by a cable, the so-called "pigtail". It is advisable to always have this cable as short as possible in order to avoid as little signal attenuation as possible. For example, the widely used LMR-400 cable attenuates 1 dB every 3 m. So if we have an antenna on the roof of a 20-storey building and a radio on the ground floor, then it may happen to us that we will have no signal[4].

Quarter When placing a radio station in a protective box, we must consider what the atmospheric influences (especially temperature) are in the given locality, or how to ensure sufficient safety of the box. We ensure a suitable temperature by insulating and venting the box. The base units can withstand temperatures in the range of -30 to 50 ° C.

2.6.3 WiMAX antennas

WiMAX antennas are multiple types optimized for different applications. The figure illustrates three main types of antennas.

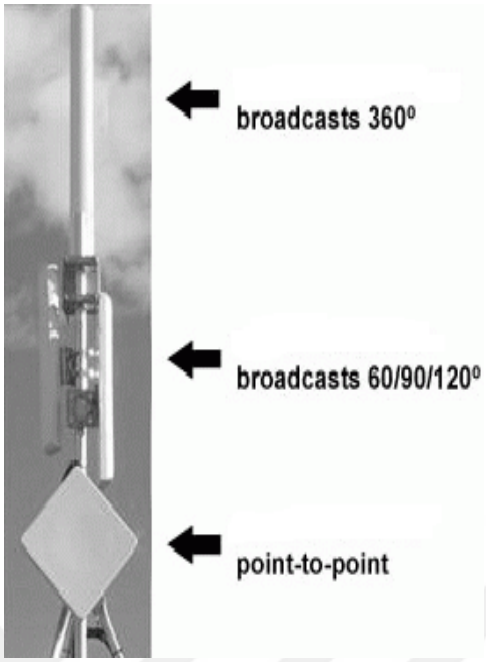

Figure 2.7: Antenna types.

2.6.4 Omnidirectional antennas

Omnidirectional antennas are suitable for PMP network topology. Their disadvantage is that the transmission power is spread in the area of 360 ° around the antenna, which reduces its range and signal power in the selected direction. It is advisable to deploy these antennas in areas with a high concentration of users.

2.6.5 Sector antennas

Sector antennas concentrate the transmission signal in a certain area (sector). They offer greater range and performance with less power than omnidirectional antennas. For these features, many operators tend to choose more sector antennas rather than one omnidirectional antenna to cover 360 °.

2.6.6 Panel antennas

Panel antennas are usually flat, square with a side length of about 30 cm. They can be used for both P2P and PMP connections. In some cases, they are therefore also used as sector antennas, but with a limited beam angle (20 ° / 60 °). With P2P connections, their range is greater and the signal is better.

2.7 CUSTOMER STATIONS

Wimax offers two versions of client stations. The first solution is with the antenna located outside the outdoor building, while the second has an antenna located inside the indoor building.

2.7.1 Outdoor user station

Outdoor stations are very simple and offer better parameters compared to Indoor stations. This is mainly due to the fact that the signal does not have to pass through, for example, concrete walls and steel structures. In addition, there is often a requirement for direct visibility, to maximize the connection, and then the Outdoor solution is ideal. On the contrary, the indoor design should be a bit cheaper, because, for example, protection against atmospheric influences does not have to be addressed.

2.7.2 Indoor User Station

The biggest advantage of the internal design of user stations is the fact that the customer can install the device himself, because it is practically without installation. The customer can use the device almost immediately and does not have to wait for a professional installation. The advantage is that the antenna is not exposed to atmospheric influences and does not have to work in extreme conditions.

The following figure illustrates the WiMAX transmission and reception kits.

Figure 2.8: Example of an assembly from Alvarion6.

So far, the technology is mostly used in the commercial sector. The price of base stations is around CZK 150,000 per base unit and approximately CZK 60,000 for each antenna unit, which, when using three antennas, is based on approximately CZK 350,000 for 360 ° coverage. Another investment is, of course, the necessary construction work and a license permit (for one channel, the price of the license is around CZK 30,000 per year) 7.

Even so, the costs are surprisingly low, given the potential of such a network. The reason is also the fact that all the necessary logic is concentrated in the base station and a standard IP network already works above it.

While the theoretical assumed baud rates achievable with WiMAX technology are around 75 Mbit / s per transmission channel using the PMP topology, the results of the tests performed speak much more pessimistically. The speeds actually achieved are around 20 Mbit / s for the 20 MHz channel and 7 to 8 Mbit / s for the 3.5 MHz channel. The difference between theoretical and actual values is mainly the transmission overhead[10].

2.8 FIXED VERSUS MOBILE WIMAX

The IEEE 802.16 Group was established in 1998 to standardize a wireless broadband data interface. The original intention was to standardize a system with direct visibility of stations (LOS) in the 10-66GHz band. The resulting standard was defined in 2001 and included a physical layer with a single carrier frequency and time division multiplexing (TDM). Subsequently, an amendment to this standard was developed implementing the radio path without direct line visibility (NLOS) in the band 2 - 11 GHz and using the physical layer with OFDM technology. The OFDMA technique is then applied at the MAC layer.

In 2005, another 802.16e addendum was developed to support user station mobility. The standard is often referred to as 802.16e-2005 or mobile WiMAX.

The table only provides an overview of communication profiles for the 3.4GHz to 3.8GHz band, which is currently being considered for Europe. Only the first of these profiles uses frequency division duplex (FDD), the other profiles use time division duplex (TDD).

- FDD, or frequency duplex, uses different frequencies to transmit and receive. It is therefore necessary to reserve two frequency bands of the same width for operation. This allows

simultaneous reception and transmission (Full Duplex). There is also a variant where we only receive or only transmit (Half Duplex).

- TDD uses only one frequency band for reception and transmission. It can therefore only be transmitted or received. A great advantage over Half Duplex is the possibility of asymmetry of communication in the forward direction "downstream" and in the reverse direction "upstream". With a suitable setting, the maximum utilization of the frequency band can be achieved.

Table 2.2: Comparison of 802.16 and 802.16e standards parameters

	802.16	802.16e
Current status	created at v r. 2001	Created at v r. 2005
Frequency band	10GHz – 66GHz	2GHz – 11 GHz (fixed) 2GHz – 6 GHz (mobile)
Environment	LOS	LOS pro fixed NLOS pro mobile
Transmission technique	Only one carrier frequency	One carrier ; OFDM s 128, 256, 512, 1024 a 2048 subcarriers
Modulation	QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM
Baud rate	32Mb/s – 134,4Mb/s	1Mb/s – 75Mb/s
Multiplex	Burst TDM, TDMA	Burst TDM, TDMA, OFDMA

Bandwidth	20MHz, 25MHz, 28MHz	1,75MHz, 3,5MHz, 7MHz, 10MHz, 14MHz, 15MHz
Implementation	---	Mobile WiMAX

Table 2.3: Examples of basic parameters of the WiMAX system in the 3.5GHz band

Zone	Bandwidth	FFT OFDM size	Duplex
Fixed WiMAX			
3,5GHz	3,5 MHz	256	FDD
	3,5 MHz	256	TDD
	7 MHz	256	FDD
	7 MHz	256	TDD
Mobile WiMAX			
3,4- 3,8 GHz	5 MHz	512	TDD
3,4-3,6 GHz	7 MHz	1024	TDD
3,6-3,8 GHz	10 MHz	1024	TDD

2.8.1 Fixed WiMAX

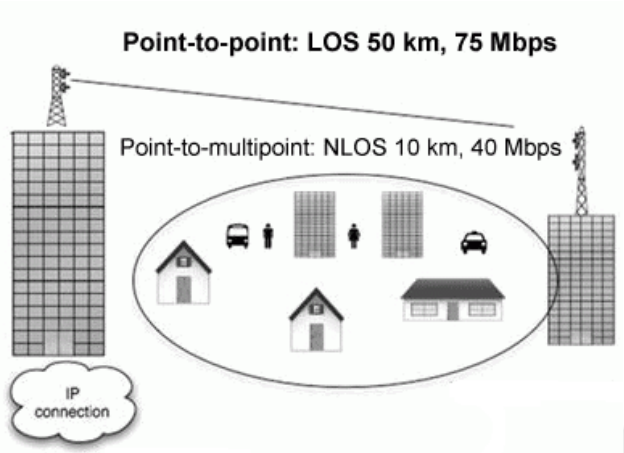

Figure 2.9: Demonstration of station interconnection.

The form of fixed WiMAX is regulated by the IEEE 802.16-2004 standard. It works in both licensed and unlicensed bands in the range of 2 - 11GHz, even without the requirement for direct visibility8.

The theoretical range in open space is up to 50 km and in densely built-up areas up to 10 km. The transmission speed is theoretically up to 75 Mbps, which, however, is shared by all users connected to the base station. The stated real values are (for transmission over a distance of about 20 km outside the city and in the city from 3 to 10 km depending on the density of the installation) throughput of up to 40 Mbps without direct visibility.

One base station is able to serve hundreds of companies with high demands on the quality, reliability and robustness of the connection and up to thousands of users with a connection comparable to DSL. Fixed WiMAX is ideally suited for building a backbone network in urban areas. A high-quality Internet connection with quality control support is suitable for real-time data, voice and video transmission.

2.8.2 Mobile WiMAX

Mobility in WiMAX networks is ensured by the 802.16e-2005 standard. It is an extension of the 802.16-2004 standard and had to solve three major problems. Changes in signal modulation during fast movement, handover of end stations between cells and connection management between individual providers (roaming). Now mobile WiMAX should operate at 2 - 6 GHz with a maximum

transmission speed of 15 Mbps (real 2 - 3 Mbps) and a latency of about 50 ms. Thanks to its technical parameters, it can be used for mobile TV services or online games.

2.8.3 Introduction of mobility support to WiMAX technology

For the purpose of creating a mobile data transmission network, it is now possible to consider only the 802.16e standard, which describes WiMAX technology supporting a certain mobility of user stations. However, it is still to some extent a transitional step towards higher generation mobile networks. The interconnection of WiMAX systems from various manufacturers and the implementation of this issue directly into the standards then becomes more important with the support of mobility. Today's application of WiMAX technology is mainly in wireless broadband access, in outdoor networks, private networks, as well as the extension of public WLAN access and other applications requiring wireless connection without direct visibility.

2.8.4 802.16e mobile metropolitan wireless network

This technology implements mobility into a wireless metropolitan network, specifically combining fixed and mobile support in the licensed frequency bands 2 - 5 GHz. A mobile link is a link where the transmitting antenna is fixed while the receiving antenna is freely movable. The most difficult case for mobile connection planning is the propagation of waves in urban areas. The signal propagating in the installation between the fixed and mobile antenna is affected by a number of different physical mechanisms. These are reflection, bending, wave scattering and diffraction at the edges of roofs. These individual mechanisms of wave propagation are determined mainly by the type of environment and the position of both antennas of the mobile link. The addition of 802.16 is therefore intended to ensure that the base station supports both fixed and mobile broadband wireless access. The importance of 802.16e lies between fast wireless communication with short range (WLAN) and highly mobile communication in large cellular networks. The specification is based on 802.16d technical principles, but must include support for handover of station communication between cells (based on the received base station signal, which the mobile station detects based on regular messages from base stations) and roaming. 802.16e will offer less capacity than 802.16d because it projects mobility overhead.

2.8.5 Quality of service

The quality of voice or video telephony service is defined as the perceived quality of voice or video. Better services mean less bit error rate of the received signal. In a radio network, the user ideally receives the full bit rate, but in the event of a deterioration in transmission conditions, with a greater distance from the base station or interference, the rate will decrease accordingly. In this situation, packets can also be lost, which in turn means their retransmission and, in connection with this, a lower transmission speed.

2.9 WIMAX VERSUS WIFI

These are not interchangeable technologies, but complement each other. WiFi technology is designed for local wireless networks, while WiMAX is for metropolitan networks. Their characteristics also differ accordingly. In the past, none of these technologies focused on mobility to a greater extent than within the area covered by a single access point. The first standard involving user station mobility is 802.16e.

Table 2.4: Comparison of WiMAX and Wi-Fi parameters

Feature	Wi-Fi	WiMAX
Standard	802.11a/b/g/n	802.16d/e
Data rate (MAX)	300 Mbps	70 Mbps
Transmission distance (MAX)	300m	50Km
Operating Frequency	2.4 GHz and 5 GHz	2-11 GHz
Channel Bandwidth	20 to 25 MHz	Ranging from 1.25 to 20 MHz
Encryption	RC4 and Advanced Encryption Standard (AES)	Triple Data Encryption Algorithm (3 DES) and Advanced Encryption Standards (AES)

Wi-Fi is a technology for short-distance use. The range of access points is several tens of meters inside buildings and several hundred meters outside. It operates in the unlicensed band, which

causes mutual interference in densely populated areas when transmitted on the same frequency. In addition, Wi-Fi does not have quality service support implemented. Wi-Fi technology is suitable for use of wireless local area networks, so-called WLANs, for which it was also originally designed.

Unlike the older Wi-Fi standard, WiMAX is designed exclusively for outdoor environments, where it can achieve higher transmission speeds, has a higher range, offers the possibility of connection even without direct visibility. In addition, a licensed band is used, which eliminates mutual interference. Supports quality of service (QoS) management. In particular, the last advantage is very welcome, because thanks to QoS, the end customer can be guaranteed high speed and stable responses, which is suitable for modern services such as IP telephony or real-time video transmission. It is intended primarily for providers (operators, providers) who, thanks to QoS, have the means to guarantee services to users. Also, security is at a much higher level than Wi-Fi.

3 ROUTING PROTOCOLS

This is a common property of many well-known WSN routings protocols. It is partially caused by the fact that, when initially proposed, performance of sensor devices was low and users were often willing to sacrifice security for increased network lifetime.

In last few years, the number of WSN applications has been in- creasing. They are deployed in fields that have high security demands, like military or healthcare. This implies the need to secure the communication. Sensors use a wireless radio which makes it easy to capture or create false traffic and may be distributed in a large area without physical security. This creates an opportunity for attackers to steal them, extract data including cryptographic keys or reprogram them. They possess low resources so the traditional security mechanisms are useless or at least ineffective in WSNs. Designing a secure routing protocol for this type of network is relatively new and difficult challenge that requires trade-offs between the cost and the achieved security.

Overview of attacks on common WSN routing protocols is given in [11]. It demonstrates that almost all protocols that were not designed with security in mind are subject to multiple kinds of attacks and shows the need for the secure ones. It also proposes basic threat model and security goals for WSN routing protocols.

To prevent these attacks, secure routing protocols were proposed, most of which are derivatives of existing insecure routing protocols, mostly those focused on efficiency. Some of the secure routing protocols are described in following sections. These should give a general overview of the current state of secure routing in WSNs. Many other protocols exist but are not included in this work due to nature and scope of this thesis or their unavailability in university information sources or other free channels (e.g. Secure-CTP).

3.1 DATA-CENTRIC

Data-centric routing protocols are the most intuitive type. Sensors collect data and route them to single or multiple sinks/base stations (BS). Data can be queried (e.g. by BS) or sent automatically after a thresh old is reached or a timer goes off. Sensors can be queried by their attributes instead of IDs. To increase reliability, data might be sent through multiple paths. Sensors also serve as

routers for the data from other sensors. One of the well-known examples is directed diffusion. In this case, BS sends a query to the network and a node fulfilling the condition replies with data.

3.1.1 ESDDP [12]

Directed diffusion works in a query-response manner. BS queries the network with interest packet for the data by sensors or data attributes and nodes respond with the actual data.

Energy-efficient secure directed diffusion is a protocol based on directed diffusion that aims to provide authentication, data integrity, freshness and confidentiality while also being energy efficient. It utilizes LEAP protocol for key management and distribution but only uses 3 out of 4 keys:

- Pairwise key shared with a BS.
- Pairwise key shared with neighbor.
- Global key shared between all the nodes in the network.

The pairwise key shared with the BS and a global key are redistributed before the deployment. Pairwise keys shared with neighbors are established after the deployment.

Interest messages from the BS are encrypted by the global key. Interest packet integrity is achieved by using MAC with the global key, data packet integrity by using MAC with the pairwise key for each pair of nodes. A timestamp is used to achieve message freshness. Sensor nodes are meant to be cheap and therefore not tamper-proof.

In case of physical key extraction, interest packets can be easily forged by an attacker. Authors did not take this scenario into account.

In general, timestamp is not a good idea in sensor networks, as they might easily get desynchronized.

3.1.2 SeRINS

Unlike majority of secure routing protocols for WSN, SeRINS focuses on insider attacks. It makes assumptions that attacker is able to capture a small amount of nodes and extract keys but it takes

longer to extract keys than for a node to complete neighbor discovery phase. SeRINS uses key management and distribution scheme to establish keys between neighboring nodes. There are multiple to pick from two keys are pre-shared with BS; one serves to establish a secure channel between neighboring nodes and is erased after some time period.

SeRINS works in rounds, a new topology is established for every round. Topology update is initiated by BS. Hash chain is used to prove that the update originates in BS. The routing tree is established similarly to CTP protocol. Each node records a first parent node and few or none alternative normal parent nodes. Normal parent nodes are those that advertised themselves after the node advertised itself. When sending the message, the node selects one of the parents in a round-robin manner to avoid attacker with some probability.

To protect from bogus routing information broadcasted when establishing the routing tree, SeRINS employs its neighbor report system: if the node receives suspicious hop count (distance from BS), it reports it to the BS. BS then asks every neighbor node of the suspicious node to report suspicious node's hop count to prevent blackmail attack. If they all agree on the suspicious value, BS broadcasts message to the whole network to revoke suspicious node's key ring.

To authenticate routing advertisement messages, ARMS [34] is used. These messages are locally broadcasted and need immediate authentication (so µTESLA is not an option) to prevent DoS attacks. ARMS utilizes hash function to create a relation between consecutive broadcasts that can be verified.

Most of the WSN routing protocols do not handle insider attacks. SeRINS is designed with an assumption that it is easy to extract data including cryptographic material from a node and therefore the proto- col needs to work even if a number of nodes are compromised. It can prevent all the investigated attacks, most of them directly and relay attack indirectly by employing packet leashes.

3.1.3 **SPINS** [13]

While not being its primary target, SPINS proposes authenticated routing protocol as an application of its two building blocks: SNEP and µTESLA.

SNEP (Sensor Network Encryption Protocol) is intended to provide data confidentiality, authentication, integrity and freshness. It reuses a block cipher for all cryptographic primitives (encryption, MAC, hash, random number generator) to save space. It is not itself a routing protocol, though. It only serves as a building block for more complex protocols. SNEP can provide a secure channel between two parties within the WSN.

µTESLA is another building block for WSN protocols that is widely used in many different secure routing protocols for WSNs. It proposes efficient method for authenticated broadcast. Most of the other solutions rely on asymmetric cryptography or cause high packet overhead. As mentioned earlier, this is not suitable for sensor networks as they are made of battery-powered devices with low performance. µTESLA, however, uses only a hash function to create a hash chain and a symmetric cipher. It works in rounds with different key used for each round. First, a random secret is chosen and the hash function is ap- plied multiple times, depending on the number of rounds. The last output of this function is pre-distributed to all the nodes. When the BS broadcasts a message, it includes the MAC computed with preceding element of the hash chain. After a round passes, BS broadcasts the key. All the nodes can now verify the key by computing its hash. If the result matches the previous key, it indeed is the correct one. This protocol is not suitable when immediate authentication of messages is required due to nature of usage scenario.

3.1.4 Authenticated routing

One of the usages for SNEP and µTESLA protocols is authenticated routing that is proposed by their authors. Unlike most of the protocols designed for WSNs, it is not meant to be energy-efficient which renders it unusable in battery-powered networks.

This protocol works in rounds. In each round, nodes form a routing tree. This is useful when the nodes are likely to fail or move. First, BS broadcasts a beacon for the new round. When the node receives it, it registers its originator as a parent node and sends it further. This approach is very similar to CPT but the beacon is protected by MAC. This protocol seems to be vulnerable to sinkhole attack achieved by executing a relay attack. Sinkhole attack allows execution of selective forwarding and therefore also black hole attack.

3.1.5 Conclusion

Three data-centric protocols were presented in this section. They vary in purpose and quality. ESDDP relies on tamper-proof nodes and SPINS focuses on protocol building blocks, while it proposes a routing protocol only as a usage scenario. Overall, SeRINS seem to be the best option out of these protocols, defending even against insider at- tacks. Outsider attacks were only executable on SPINS protocol. These attacks include sinkhole attack, relay attack and selective forwarding as well as black hole attack.

3.2 CLUSTER-BASED PROTOCOLS

Cluster-based protocols were introduced to decrease delay and in- crease throughput and network lifetime by aggregating data from sensors. The most cited cluster-based routing protocol for WSN is LEACH. Most of the other cluster-based protocols are either based on LEACH or are at least inspired by it. The same holds for the majority of secure hierarchical routing protocols for WSN. This section discusses some LEACH-based protocols and also 3 hierarchical protocols that are not directly based on LEACH but still share some similarities with it.

LEACH is a cluster-based protocol that aims to provide high efficiency. The main assumption of this protocol is that every node is within radio range of every other node but the power used to communicate rises with the distance. Like every other pioneering routing protocol for WSN, it lacks security features. Many authors try to fix this by modifying this protocol to provide at least integrity and authenticity. Some of these protocols are presented in this section.

LEACH protocol is vulnerable to a number of possible attacks, such as selective forwarding, HELLO flood, replay attack, etc. LEACH- based secure routing protocols improve the overall security but most of them achieve this only under certain circumstances. Majority of them assume that the sensors are tamper-resistant or do not consider physical key extraction at all. However, sensors in WSN are meant to be cheap so they can be deployed in hundreds, possibly thousands. Protecting them against this type of attack would be expensive, which makes this assumption unreasonable. None of the LEACH-based protocols maintains the security of the rest of the network in case of physical key extraction from a compromised node. In some of the protocols, this does not compromise the whole network but the significant part of the network is still affected. This proves that secure protocol must be designed with security in mind right from the beginning,

rather than adding some degree of security to already existing protocols, This is the case of the cluster-based protocol described which is indeed designed as secure routing protocol from scratch.

There were many attempts to secure LEACH protocol that vary in design quality considerably.

The main goal of this section is to describe most cited or interesting protocols that aim to improve security aspects of hierarchical protocols that standard LEACH protocol does not handle.

Various protocols with different approaches were chosen to give a general overview of possible solutions and their advantages or disadvantages.

This section, however, does not describe all the LEACH modifications that aim to increase security. Protocols that do not seem to increase security or are not properly described (e.g. RLEACH[14]) are also omitted.

3.2.1 SLEACH [15]

SLEACH uses symmetric cryptography and TESLA-based protocol to improve the security of LEACH.

Advertisement phase is modified to authenticate broadcast from cluster-head (CH) using the base station. Apart from the fact, that all the communication is a broadcast on the physical layer, CH does not broadcast its advertisement message directly. Instead, it sends encrypted message to a BS, which subsequently uses TESLA-based[16] protocol to broadcast the message in an authenticated way.

After the sensor chooses its CH for the next round, it, again, does not immediately communicate directly with the CH. It sends the information to the sink instead. Let me remind that basic assumption in LEACH is that all the nodes are able to communicate directly with the sink but it costs more energy. The sink computes the key for the sensor from the secret that is shared by both sensor and the BS and sends it to CH. Therefore, sensor already possesses this key and can authenticate the CH by having it. When both of them share the same key, they can communicate in a secure way.

To protect against laptop-class attackers, sensor node does not choose the CH based on the signal strength only but rather uses probabilistic way to avoid having the same CH for all the rounds.

This decreases the probability of attacker capturing the data if he does not compromise too many nodes.

In case of failure, sensor node chooses other CH to protect against DoS attack by initiating communication with all the nodes.

This protocol is secure against most of the attacks. Relay attack could be possible but randomized way of choosing CH significantly decreases the probability of success. Even in case of successful relay attack, data confidentiality is still maintained so packet modification is not possible.

This protocol does not consider physical attacks. In case that attacker captures the node and extracts the secrets, he is able to decrypt all the data that were and will be sent from/to this node. He can also become a CH, which means he can alter the data and send it to the sink.

3.2.2 SecLEACH [17]

Authors claim that SecLEACH provides authenticity, integrity, confidentiality, and freshness.

SecLEACH is based on F-LEACH [18], an attempt to secure LEACH protocol that is based on a hash chain. It supports authenticated broad- cast from both BS and also CH. CH broadcast is done by sending the message protected by a pairwise key shared with BS to BS and BS broadcast. F-LEACH does not provide message authentication from nodes to CHs. It is also vulnerable to physical attacks.

SecLEACH secures F-LEACH by using modified random key pre- distribution proposed in [19]. The pool of random keys with their IDs is generated in the same way as in the original solution. Each node is then assigned fixed number of keys. When a node becomes a CH candidate, nodes can compute the list of keys it possesses. Nodes choose closest CH candidate with which they share a key. The communication with CH is then protected by the key they share. At the end of cluster formation, number of regular nodes are paired with CH. The rest of the nodes do not belong to any CH. These can be treated in multiple ways but authors do not describe any. The clusters may be different from those in regular LEACH protocol due to nodes not sharing a key. Because of that, efficiency may be affected and is dependent on chosen protocol parameters - number of all nodes, number of cluster heads, number of keys, and number of keys possessed by each node.

In this protocol, a node chooses closest CH candidate with common key for its CH. If this is attacker's node, even without knowledge of any key, it can pretend to be part of the network and will make the closest nodes join it. A node joining the cluster does not verify whether CH candidate is legitimate which could lead to DoS attack. Although authors do not describe this situation, it can be solved.

Security against physical attacks is not described in the paper. The fact that keys are predistributed randomly means that to ensure high probability of nodes sharing the key, each sensor must possess multiple keys. If the attacker manages to obtain keys from one node, he can immediately communicate with multiple nodes in the network. The trade-off must be set to balance security and connectivity.

3.2.3 S-LEACH (SLEACH) [20]

S-LEACH (also dubbed SLEACH) is the first attempt to secure the LEACH protocol, It was proposed the same year as SLEACH.

S-LEACH, like few other protocols, uses symmetric cryptography and µTESLA protocol. In pre-deployment phase, nodes are given master key shared with BS and the last element of µTesla hash chain. Each node generates its own key for MAC computation from the master key. In advertisement phase, CH candidate advertises its ID together with MAC of the ID. When BS receives all of them, it broadcasts the list of all legitimate CHs authenticated by µTesla. A node can now authenticate the message and choose its CH in an ordinary way. Schedule for each cluster can be authenticated in a similar way if required. Data from nodes are authenticated by MAC using key shared with BS. CH cannot verify it but BS does when it reaches it.

The big disadvantage of this protocol is that, if an attacker sends arbitrary data to a CH, it is forwarded to BS without verification and when it reaches BS, it is already aggregated so the BS must discard it. The intruder is then reported to CH. This approach is vulnerable to DoS attack. DoS can be also achieved by generating a big amount of requests to join a cluster. Authors claim that reported malicious node will be excluded from the network but an attacker can choose any ID (Sybil attack) so he either will not be excluded or may cause exclusion of every node in the network by stealing identity (blackmail attack).

I agree with authors that S-LEACH secures the network against selective forwarding, sinkhole attack and HELLO flood attack unless there are insider attackers. However, it seems to be vulnerable to identity replication of end nodes and either Sybil or blackmail attack.

3.2.4 MS-LEACH [21]

MS-LEACH aims to improve S-LEACH in terms of data confidentiality and node-to-CH authentication. It also moves the data authentication from BS to CH, which prevents discarding all the data in case that some bogus data were sent by an attacker.

It introduces a new pairwise key between a node and a CH. How- ever, this key is generated from the initial hash chain value and node's ID only. This means that if the attacker learns this value, he can gener- ate all the keys used for MAC computation for all the nodes. CH will accept the data because the MAC will be correct. That means that it will also be accepted by the BS. If the attacker learns the initial hash value, confidentiality in the whole network is discarded too And because sensors in WSN are meant to be cheap and not tamperresistant, this may even degrade the level of security in original S-LEACH instead of improving it.

3.2.5 SS-LEACH

SS-LEACH [20] also improves S-LEACH but in a different, more rea- sonable way. It uses self-localization of the nodes and a key redistribution. It forms dynamic stochastic multi-paths cluster-heads chains. It aims to improve both security and energy efficiency.

The key redistribution works similarly to S-LEACH. The difference is that after the nodes are deployed, they broadcast their keys' IDs. This way, each node can find neighbors it can communicate with. Nodes determine their relative position to other nodes in the network. After this, periodicity phase starts, when the clusters are formed and data are being sent and aggregated.

To form a cluster, each node sends its remaining energy to the BS together with the longest distance it can transmit to. BS chooses the first CH based on this information. This CH chooses the second-level CH in a similar way. CH broadcasts that it becomes the CH and all the nodes choose their CH based on the shared keys and signal strength, The communication between nodes is secured by pre-shared keys.

Physical tampering issue with pre-deployed keys from the S-LEACH was not improved. However, the overall security of the protocol is definitely better.

3.2.6 LS-LEACH [22]

LS-LEACH is the last LEACH-based protocol listed here. It uses a symmetric key with two pre-shared keys on each node. One of them is a pairwise key shared with the BS; the second one is shared between all the nodes in the network. Authors name the key shared with the BS a private key. However, the content of the paper suggests this is a symmetric key. They also claim to use this key to encrypt a message with MAC algorithm. In this protocol, BS sends new shared password after each round to be used in the next one. According to the protocol, if the number of attempts to communicate with any node reaches a defined threshold, this node will inform its CH which will then inform BS that will perform necessary actions. However, these actions are not defined in the paper. It is also not clear who tries to communicate with the node if CH is the one to be informed and sensors do not communicate with each other.

After physically extracting keys for a current round from a node, key for the next round is obtained in accordance with the protocol so the security of the whole network is compromised. Keys for communication with BS can be also used to forge data.

3.2.7 ESRP [23]

In contrast with the majority of LEACH-based protocols, ESRP is in- tended for networks with deterministic node location and the clusters are formed by BS.

After deployment, nodes report their positions and energy levels to a BS. Authors did not describe the process to secure this information. After position and energy have been reported, BS chooses the node with the highest amount of energy as CH1. The farthest node from CH1 with highest amount of energy is selected as CH2. Authors did not describe the situation when the farthest node from CH1 is close to BS. This could mean that the node next to a BS sends information through CH2 and CH1. Ordinary cluster members are assigned to clusters based on their number and position. BS distributes information about clusters and CHs to all nodes. It also generates and distributes a secret key to a CH and a public key to all nodes. The process of doing this is yet again not described. TDMA and intra-cluster routing work in the same way as ordinary LEACH protocol, When a CH wants to send a packet to its upstream CH, they will perform Prover -Verifier

protocol. Prover (downstream CH) will prove its identity to the verifier (upstream CH) through a zero-knowledge protocol. It will then hear in promiscuous mode whether the upstream CH sends it further. I suspect this verification only proves knowledge of the secret in time of the verification.

According to original protocol proposal [24], keys are only 8-bit long and they last through the whole protocol run so they can be easily brute-forced. The data is not encrypted and the authenticity within intra-cluster routing is not guaranteed. The intrusion detection system does not consider that attacker can forge arbitrary nodes IDs.

3.2.8 SCMRP [25]

SCMRP is one of the few WSN routing protocols that use public key cryptography. Even though this design choice allows creating simpler protocols, it is not suitable for WSN due to its high CPU demands. In pre-deployment phase, every node receives its ID, a secret key shared with BS, a certificate signed by BS and a public key.

Nodes broadcast their ID together with their certificate. They also listen for others' IDs and verify certificates. When it is done, they all send their neighbors table to the BS, encrypted and protected by MAC with the key shared with BS.

BS creates network topology based on the neighbor information from nodes and calculates paths. It generates a pairwise key for all neighboring pairs of nodes based on their IDs and a secret. It then sends the pairwise key to a node and also the same key, encrypted with the key that the neighbor shares with the BS, encrypted and authenticated by MAC, together with the BS certificate. When the node verifies it, it sends the pairwise key protected by the key that the neighbor shares with the BS and a nonce to its neighbor as a challenge and waits for the incremented nonce protected by their pairwise key. If the node does not receive the response, it reports suspicious node to the BS. Cluster formation is done by BS. It sends routing paths to CHs, protected by encryption and MAC. CHs are never neighbors of each other. The rest of the protocol is similar to LEACH, the difference is that encryption and MAC are used when sending or forwarding the data and a new node can join the network in runtime in a similar way to the node discovery phase.

The overall security looks better than in most of the LEACH-based secure routing protocols. Relay attack may be possible when attacker replays the neighbor discovery message, but the impact

should not be critical. The biggest setback of this protocol is the public key cryptography that makes it inapplicable to networks with low-end nodes.

3.2.9 **TEESR** [26]

TEESR is a routing protocol intended for heterogeneous sensor net- works. A network is divided into clusters. Cluster consists of SF (Sensing and Forwarding) sensors and CH sensors. CHs have more energy, high data rate and longer transmission range. In pre-deployment phase, each node is assigned a pairwise key shared with the BS.

TEESR protocol is not based on LEACH but consists of similar phases. Neighbor discovery phase involves broadcasting node's ID and a nonce. MAC protects integrity but the key that is used is not mentioned. I assume that a pre-shared global key is used for that. After nodes find all their neighbors, they report the neighbor table to BS. BS creates a neighbor matrix with multiple paths to each node. It also calculates pairwise keys for each pair of neighboring nodes and sends it to them. The confidentiality of these messages was not mentioned and it seems like they are sent in plaintext.

The protocol is described poorly. MAC is, in most cases, calculated from original message concatenated with a nonce but the nonce is not included in the plaintext so the receiving party should not know it. To solve this, the nonce needs to be included in the message or a counter may be used. In case of counter, synchronization problems can occur. The protocol does not mention redistributing these values. It also does not mention redistributing keys used in the neighbor discovery phase. This protocol, as described in the paper, should not work. However, it is possible to make it work with few modifications, like including nonce in messages. Security would be still questionable, though.

The security of this protocol does not seem reasonable, as the keys seem to be sent in plaintext. The protocol is not included in the table with possible attacks, as I cannot evaluate it based on the paper only.

3.2.10 **TTSR** [27]

TTSR is a secure routing protocol for heterogeneous sensor networks. Unlike the rest of the protocols listed in this section, it is designed as a secure routing protocol right from the beginning.

The network consists of high-end nodes (H-nodes) and low-end nodes (L-nodes) that are randomly, uniformly distributed. H-nodes make up 2% of the network and serve as CHs. They are static, location-aware and tamper-resistant. L-nodes possess neither of those features.

For intra-cluster routing, key management scheme for HSNs (Heterogeneous sensor networks) is used to distribute pairwise keys be- tween all neighboring pairs of L-sensors. Authors mention the one proposed in [28] as an example. Each pair of neighboring L-sensors performs a two-way handshake. That ensures that connection works both ways and they both share the same key. It uses a nonce, encryption and MAC with their pairwise key. The CH creates a tree cluster with itself as a root. This is described in [29]. Each L-sensor has also a backup parent in cluster tree and backup CH in case of node failure. Data packets are encrypted and MAC. Protects integrity. After sending, sensor listens whether its parent further propagated the packet. If it was not and retransmission fails, the node will switch to its backup parent. Parent forwards it further the same way. Parent can be either L-sensor or CH. CH is a final destination within intra-cluster routing. After successful delivery to a CH, data is aggregated if required and forwarded to the BS. To achieve this, CH chooses other CHs that are closer to the BS to forward the data. The choice is made based on a position of clusters. If the cluster lays between the CH and the BS, CH of this cluster is included in the path. If any of the intermediate CHs fails, new route is created in a similar way.

This protocol does not seem to suffer to any security vulnerabilities in case of outsider attacker. Insider attacks should only affect single branch in the network. This protocol provides a graceful degradation and should be still secure enough even if the attacker captures multiple nodes. Of course, when the majority of the network is compromised, it cannot stay secure anymore. The only obvious disadvantage of this protocol is higher cost of H-nodes.

3.2.11 Conclusion

Majority of hierarchical secure routing protocols are modifications of the LEACH protocol. Most of the papers do not mention possible attacks in case of the physical tampering. They claim these protocols only either protect from outsider attacks or do not consider this possibility at all. None of these maintain security if the sensors are not tamper-resistant. Some of them achieve partial security (e.g. S-LEACH, SS-LEACH . . .) after compromising few nodes. The impact can depend on chosen parameters. However, many of them are vulnerable even in scenarios where all the

nodes are physically secure. From a security point of view, the best option is clearly the TTSR protocol. Unlike LEACH-based protocols, it does not suffer from obvious attacks. 2% of all nodes need to be tamper-resistant but that ensures that compromise of a node does not affect the rest of the network.

Table 3.1 summarizes attacks that are possible on reviewed hierarchical routing protocols for WSN. These attacks are mostly determined by myself while reviewing protocols and might be inaccurate. They also do not take physical tampering into account. This table makes MS- LEACH protocol look like one of two best options while its security is completely eliminated by extracting the secret from whichever node and therefore should not be considered a final conclusion. There is a high probability that these protocols contain even more vulnerabilities.

Table 3.1: Possible outsider attacks on reviewed hierarchical secure WSN routing protocols

	SelectiveForwarding	BlackHole	Exhauction	HelloFlood	SinkHole	IdentityReplaction	Sybile	RelayWormhole	Blackmail
SLEACH	NO	NO	NO	NO	NO	NO	NO	NO	NO
SecLEACH	NO	NO	NO	NO	YES	NO	NO	YES	NO
LEACH	NO	NO	YES	NO	NO	YES	YES	NO	YES
LEACH	NO	NO	NO	NO	NO	NO	NO	NO	NO
SSLEACH	NO	NO	NO	NO	NO	NO	NO	NO	YES
ESRP	YSE	YSE	NO	NO	NO	YES	YES	NO	YES
SCMRP	NO	NO	NO	NO	NO	NO	NO	YES	NO
TTSR	NO	NO	NO	NO	NO	NO	NO	NO	NO

3.3 GEOGRAPHICAL PROTOCOLS

In geographical routing algorithms, a node does not need to know network topology. Instead, it needs to be able to determine its own location, for example using GPS. The routing is done based on sending and receiving nodes' location. In hierarchical routing protocols, the final destination of the packet was always the sink. In case of geo- graphical protocols, thanks to routing based on location rather than ID, ordinary sensor node may also become a packet destination.

Many geographical routing protocols use greedy algorithms. The downside of this approach are situations when all the neighboring nodes are farther from the destination but the sender does not have a direct communication link to the destination.

Geographical routing protocols tend to be resilient against attacks that utilize hello messages (e.g. HELLO flood, relay attack) thanks to nodes not creating routing tables at the beginning of the protocol run. However, they may be susceptible to Sybil attack, in which case attacker's node claims multiple locations and thus attracts a lot of traffic.

3.3.1 **SIGF** [29]

Secure Implicit Geographic Forwarding (SIGF) is a family of three configurable secure routing protocols based on IGF protocol.

IGF is a stateless routing protocol that is susceptible to number of attacks (e.g. Sybil attack, CTS rushing attack [30]). In this protocol, when sender sends ORTS (open request to send) message with destina- tion coordinations, each node within 60° angle calculates its response time based on their distance, energy and perpendicular distance to a line from the sender to the destination. The more suitable node, the shorter response time. When the response time expires, the node responds with CTS (clear to send) message. The first one to respond will forward the data. The rest of the nodes do not respond after they hear the response from another node. This allows new nodes to enter the network and avoids sending data to a dead, sleeping or missing node. However, it also enables selective forwarding attack by sending immediate CTS to all messages by an attacker node.

SIGF family consists of three protocols: SIGF-0, SIGF-1 and SIGF-2, each inheriting features from the previous one and further improving the security at cost of higher complexity end resource consumption. They are designed to be compatible so the network can switch from lower to higher

security at runtime. SIGF-0 and SIGF-1 are not meant to protect from every attack. They are designed to be used to conserve energy unless an attack is discovered. When the attack occurs, the network should switch to higher security level (SIGF-0 to SIGF-1 or SIGF-1 to SIGF-2).

SIGF-0 and SIGF-1 protocols do not handle node-to-BS authentication. For example, one can create a bogus message and the nodes will happily forward it to its destination. This can be implemented transparently to SIGF protocols, for example by employing pairwise keys with the BS.

- **SIGF-0**

The most energy-efficient protocol of SIGF family. It is completely stateless and provides only probabilistic defenses against an attack. The difference between this protocol and IGF is in the selection of the next-hop candidate. While IGF chooses the first node to reply with CTS, SIGF-0 collects all the responses and then selects one based on configurable options. This fixes the CTS rushing attack vulnerability that IGF suffers to.

- **SIGF-1**

SIGF-1 aims to further defend against selective forwarding, black hole attack and Sybil attack by keeping information about neighbors. This information contain the number of messages sent to each neighbor, number of messages forwarded by the neighbor (obtained by overhear- ing after transmission), last location of the neighbor and delay between sending a message to the neighbor and forwarding the message by the neighbor. Other values are also derived from this information, like success ratio, location consistency, fairness and performance. All these values are used to compute node's reputation. Only nodes with repu- tation exceeding set threshold may be chosen for message relaying.

- **SIGF-2**

SIGF-2 adds cryptographic security to SIGF-1 to provide message authenticity, integrity, confidentiality and freshness. It requires key establishment protocol. Authors mention LEAP [31] as one of the possibilities but more options are available. It uses MAC for message authentication and integrity, message sequence number for freshness and encryption for confidentiality.

3.3.2 SEAR [32]

SEAR protocol focuses on hiding message originator. It offers paramet- rized energy balance control and security level. This provides a way to trade off energy for source location privacy. The only destination is the sink, which can effectively determine data source.

A pairwise key with the sink can be used for confidentiality. PIKE protocol is used for key management and distribution. This protocol only considers passive attackers.

I did not do the full analysis of this protocol as it was performed by Tang et al. in [33]. Results of this analysis prove that this protocol provides excellent source-location privacy.

SEAR shares two authors with newer CASER [34] protocol. These protocols are almost identical with respect to security measures.

3.3.3 Conclusion

Geographical protocols may be immune to attacks that are based on forged routing information due to nature of their routing path selection. However, they tend to be vulnerable to Sybil attacks with attacker presenting multiple locations as they cannot easily verify them.

Two protocols were presented, each focusing on the different area. SIGF protocol family improves IGF routing by eliminating its vulnerabilities, while SEAR presents a new design of securing data origin location. Both of them try to increase efficiency when possible and only use more demanding security features when needed.

The overall security of SIGF family seems to be better than in hierarchical protocols, with exception of TTSR, but it comes with the price of positioning system requirement.

3.4 CONCLUSION

Multiple secure routing protocols were described in this chapter, most of which were hierarchical. This uneven distribution is caused by the fact that many existing protocols are modifications of LEACH protocol. LEACH is attractive as base protocol for further securing thanks to its energy efficiency. It is also immune to few attacks unless a sensor was physically compromised which narrows the number of attacks to protect from. However, with respect to security, none of the

LEACH modifications was close to best routing protocols that are designed to be secure in the first place and improve other qualities only if it does not affect security.

As stated by Karlof and Wagner in [11], confidentiality and fresh- ness are not responsibilities of the secure routing protocol. Despite that, most of the secure routing protocols incorporate these features, sometimes giving them high priority. Although it is a nice feature, these protocols are often vulnerable to attacks and could rather im- prove different security aspects, like authentication. Confidentiality could be added on the higher network layer.

Some protocols strictly focus on defense against single kind of attacks. For example, HSRBH [35] only protects against black hole attacks but does not consider other attacks. Some aim to achieve a sole security goal, like preventing an attacker from determining the data source, e.g. CASER. Even though these protocols manage to achieve these goals, their application is restricted to scenarios where the attacker is unable to launch different kinds of attacks due to reasons unrelated to routing protocols.

Wood et al. claim that no perfect solution exists for secure routing protocols. Whether or not this is true, there is not any known yet. However, there are three outstanding protocols within those described in this chapter, each belonging to a different category. Unlike the rest of them, two of these even consider insider attacks and protect from them with reasonable probability.

Out of all data-centric protocols, SeRINS achieves the highest security. It is one of two abovementioned protocols that handle insider attacks. Among hierarchical protocols, TTSR is the most promising protocol. Like SeRINS, it considers insider attacks but comes with the price of higher sensor cost, as 2% of the nodes need to be tamper resistant. Geographic protocols contradict theory mentioned earlier, that secure protocols should not build on insecure ones but should be designed as secure right from the beginning. The SIGF family, namely SIGF-2 seems to be the best option within this category.

All the evaluation and recommendations in this thesis are done strictly from the security point of view. Energy efficiency, packet over- head and other aspects are not considered, as I do not feel confident enough in this area to make any conclusions. Nevertheless, SIGF and mostly TTSR seem to offer higher energy efficiency than SeRINS, which makes it more interesting for real-life scenarios with battery-powered sensors.

4 EXPERIMENT RESULTS

4.1 QOS METRICS

Quality of service (QoS) is network service requirements that must be met to ensure quality network performance by sending packet flow from source to destination [9]. The WiMAX network will likely include a set of user-specific measurable service features that include end-to-end delay, packet delivery ratio, and statistics. In this paper, the QoS metrics are utilized such as delay, packet delivery fraction, and normalized routing load as follows:-

- END-TO-END DELAY (E2E)

E2E is another fundamental parameter, especially in critical applications. It is defined as the time that packets spend transmitting information from the service node to the destination. E2E can be calculated by using Eq. (4.1).

$$End - To - End\ delay = End\ Time_{np} - Start\ Time_{np} \tag{4.1}$$

As $End\ Time_{np}$ is the start time of sending node n, $Start\ Time_{np}$ is packets p sent via node n that were received successfully at the destination node. E2E can be called the probability of successfully crossing a packet between two points in the network [10].

- Normalized routing load

The normalized routing load is defined as the fraction of all routing control packets sent by all nodes over the number of data packets received at the destination.

$$Normalized\ routing\ load\ = \frac{Number\ of\ routing\ packets}{Number\ of\ send\ packets} \tag{4.2}$$

- PACKET DELIVERY FRACTION

The packet delivery fraction is the fraction of data packets that were created through TCP or UDP sources sent to the target.

$$Packet\ delivery\ fraction = \frac{Number\ of\ received\ packets}{Number\ of\ sent\ packets} \times 100\% \quad (4.3)$$

4.2 METHODS AND MATERIALS

4.2.1 Simulation parameters

This study aims to compare and analyze the performance of different QoS metrics by GRP and LEMANDER routing protocols. The simulation parameters were performed using NS-2 simulator as shown in Table 4.1.

Table 4.1: Simulation parameters

Components	Types
Simulation time	900 (sec)
Simulation area	1500 × 1500 (m)
Channel type	Channel/Wireless channel
Channel frequency	2.4 GHz
Radio propagation delay	Propagation/Two ray ground
Network interface type	Phy/WirelessPhy
MAC type	802.16
Interface queue type	Queue/DropTail/Priqueue
Link layer type	LL
Antenna model	Antenna/Omniaantenna
Max packet	50
Routing protocol	GRP and LANMAR
Traffic type	CBR and TCP

Connection rate	4 (packets/sec)
Connection number	5
Bandwidth	2 (Mbit)
Packet size	512 (Byte)
Maximum nodes number	50 (nodes)
Maximum pause time	50 (sec)
Maximum speed	10 (m/sec)

4.2.2 Simulation scenarios

Figure 4.1 shows a scenario for implementing the GRP and LANMAR protocols using the NS-2 simulator. The MAC protocol and physical medium used is 802.16. The simulation is carried out of network density by 50 nodes with the area considered is 1500 × 1500 m. NS-2 simulator was generated for the implementation of different path creating protocols with the metrics such as end-to-end delay, normalized routing load, and packet delivery fraction.

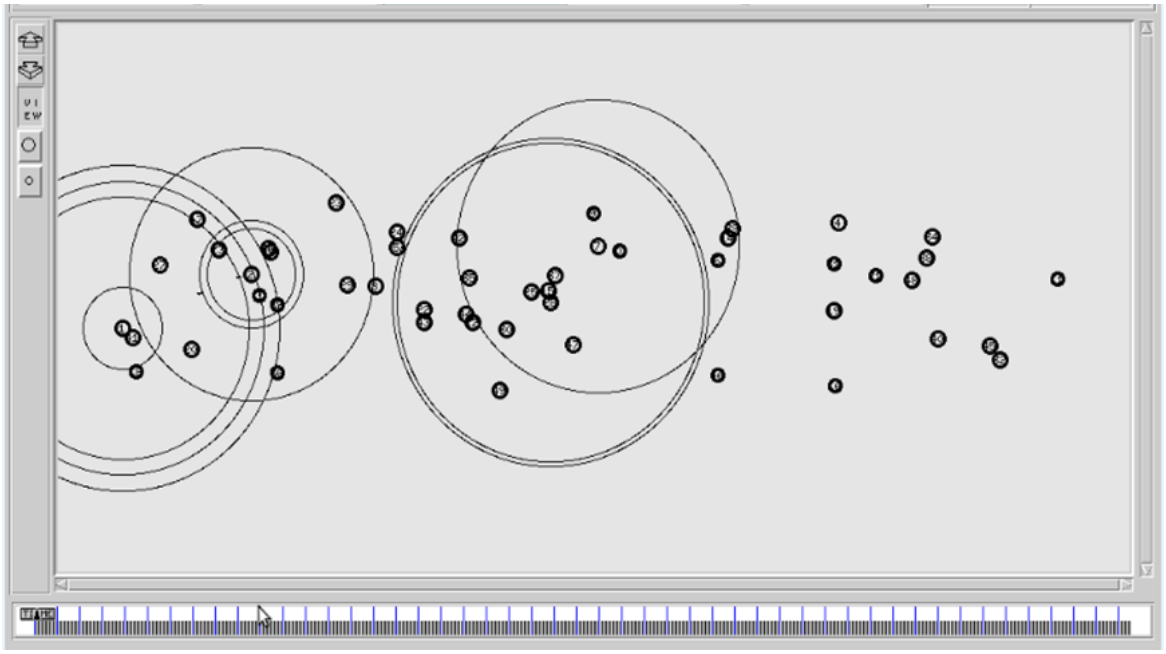

Figure 4.1: Snapshot of the simulation scenario.

Also, the NS-2 simulator was executed with two different scenarios to establish our parameter goals. The normalized routing load, the packet delivery fraction, end to end delay are measured for GRP and LANMAR routing protocols and made a comparison between them, see Table 4.2.

Table 4.2: Simulation parameters

Number of scenarios	Pause time (sec)	Maximum nodes speed movement (sec)	Nodes number
First scenario	0, 10, 20, 30, 40, and 50	10	50
Second scenario	0	10	10, 20, 30, 40, and 50

4.2.3 Results and Dissection

In this paper, the simulation results are shown below in the form of graphs. The performance of GRP and LANMAR routing protocols based on different QoS were measured and analyzed using an NS-2 simulator. In the first scenario by TCP protocol Figure 4.2(a) shows the End-To-End delay versus pause time nodes. The End-To-End delay increases with increasing pause time nodes, as E2E delay of GRP, LANMAR, GRP-drop, and LANMAR-drop protocols were achieved about 0.28 s, 0.35 s, 0.043 s, and 0.075 s in 50 nodes, respectively. When the node's movement stops sometimes, the mileage among the source and target can become far. This indicates the additional time required to forward packets from the sender to the destination. While normalized routing load (NRL) and stop time were decreased by the time, see Figure 4.2(b). So, when the node pause time increased the routing packets reducing. NRL of GRP, LANMAR, GRP-drop, and LANMAR-drop protocols have achieved about 0.25, 0.09, 2.3, and 0.98 in 50 nodes. As when the nodes stopping needs extra time, the number of drop packets reduce and resulting in the routing packets reduces. Figure 4.2(c) shows packets delivery fraction against the pause time of nodes. In this case, the pause time increments for each node, and also the packet number was increasing at the target due to a decrement in the number of drops packets.

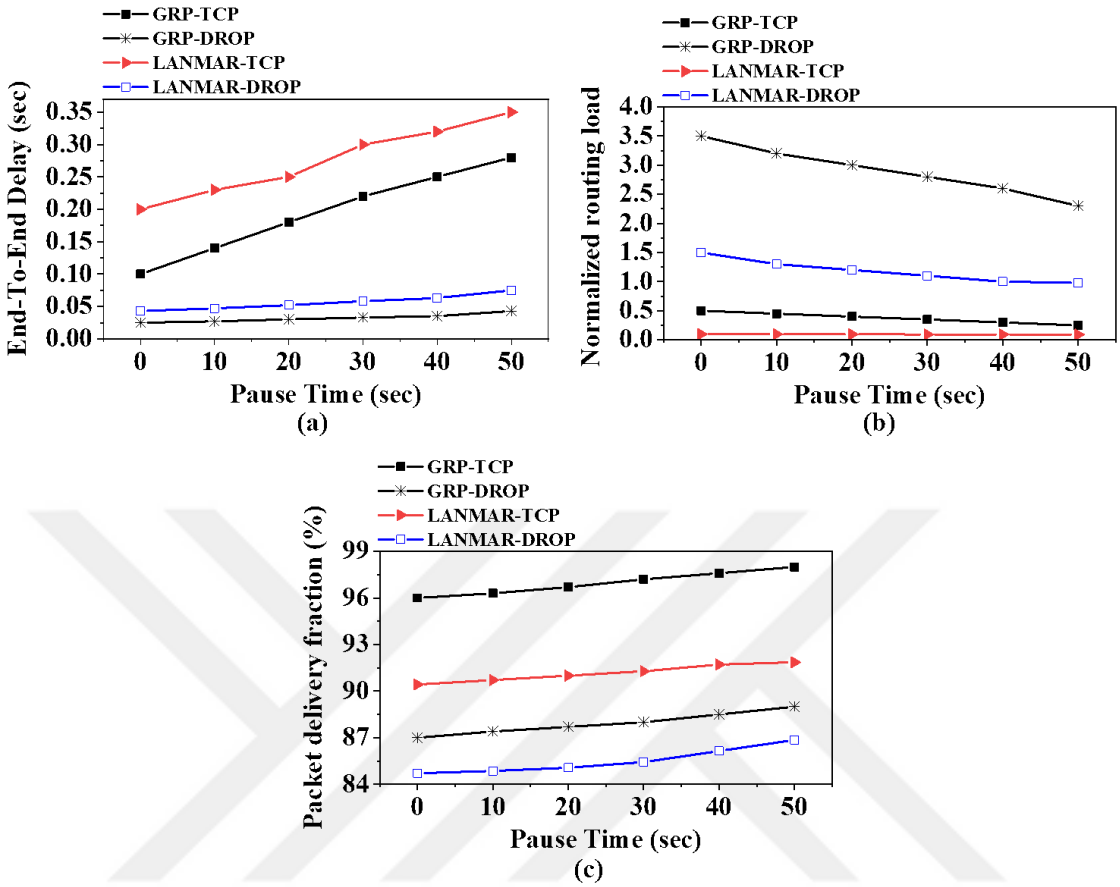

Figure 4.2: First scenario over TCP protocol (a) E2E delay (b) normalized routing load, and packet delivery fraction.

In the second scenario, the two routing protocols were analyzed based on the number of nodes. When the number of nodes increases, the delay of packets and the total number of received packets increase, see Figure 4.3(a). The E2E of GRP protocol has realized about 0.06 s, 0.1 s, and 0.2 s in 10, 30, 50 nodes. While the normalized routing load increases sharply with improved nodes number due to the request of additional routing packets, which is shown in Figure 4.3(b). The packet delivery fraction increased due to the enhanced many received packets at the destination, as GRP and LANMAR protocols have achieved about 95.4 % and 92 % in 50 nodes, see Figure 4.3(c).

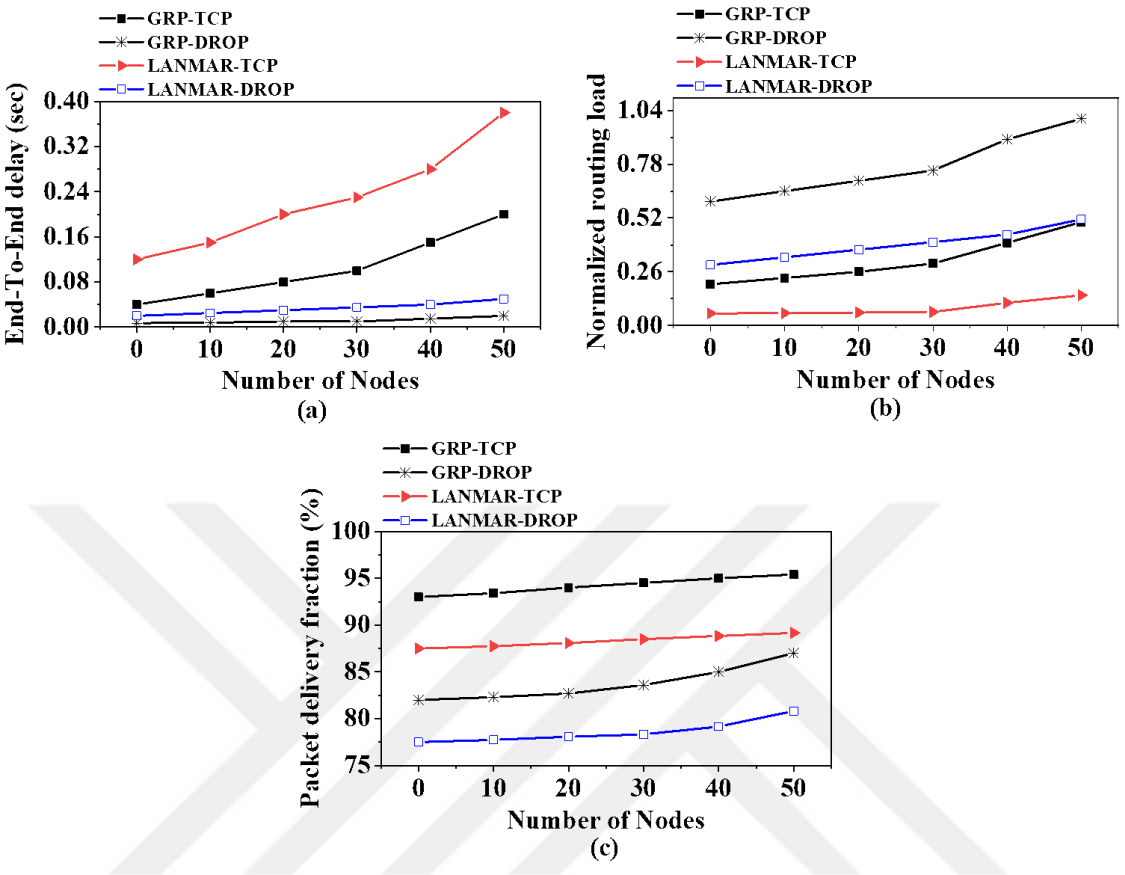

Figure 4.3: The second scenario by TCP protocol (a) E2E delay, (b) normalized routing load, and (c) packet delivery fraction.

5 CONCLUSIONS

In this work, we have compared the performance of new routing protocols using GRP and LANMAR under usual and dropping packet conditions in WiMAX technology. E2E delay of GRP shows less compared to LANMAR. So, it is concluded that E2E delay increases as an increasing number of nodes and pause time due to congestion and new locations that occur for the nodes in a network. Also, the GRP protocol has achieved normalized routing load better performance because additional routing packets are demanded in each transmission. LANMAR has realized less performance in packet delivery because the number of a received packet was lower than another routing protocol. In conclusion, GRP has a scale better with network area and increasing sender number. Also, the GRP protocol improved the flood of routing traffic and retained a reasonable delay over facing incrementing traffic.

FUTURE WORK

- Modeling system using OFDM technique for standard 802.l6e for different speeds. Carry out the modulation using the means. Make the obtained results with theoretical assumptions, e.g. from the point of view of transmission error for different combinations of transmission speeds and mobile station speeds.
- The Mobile WiMAX performance can analyze in different cases utilizing the protocols to get less error.

REFERENCES

[1] S. A. Ahson and M. Ilyas, *WiMAX: Standards and security*. CRC press, 2018.

[2] N. Mubarakah, M. Y. Al-Hakim, and E. Warman, "Energy consumption model on WiMAX subscriber station," in *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 309, no. 1, p. 12002.

[3] J. H. T. Simarata and S. Suherman, "Downlink ratio impact on downstream traffic performances on WiMAX," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 725, no. 1, p. 12057.

[4] B. Madhusrhee, "Performance analysis of aodv, dsdv and aomdv using wimax in NS-2," *Comput. Methods Soc. Sci.*, vol. 4, no. 1, pp. 22–28, 2016.

[5] S. Pathak and B. Kumar, "Performance evaluation of routing protocols for sending healthcare data over WiMAX network," in *2014 International Conference on Signal Processing and Integrated Networks (SPIN)*, 2014, pp. 269–274.

[6] S. J. Soheli, F. A. Nila, and M. A. R. Khan, "Comparative Performance Analysis of DSDV, DSR and OLSR Routing Protocols to Determine the Best Suited Routing Approach through Simulation in Mobile Wimax Network," *Int. J. Comput. Appl.*, vol. 975, p. 8887.

[7] M. Jain and A. Priya, "Impact analysis of transmission range on aodv, dymo and zrp routing protocol on qos issues in wimax," *Int. J. Online Sci.*, vol. 3, no. 10, 2017.

[8] A. S. Al-Hiti, R. Latip, R. K. Sahbudin, and R. A. R. Mahmood, "Comparative Analysis of Routing Protocols over WiMAX," *Adv. Sci. Lett.*, vol. 24, no. 2, pp. 1303–1306, 2018.

[9] S. H. Alsamhi, O. Ma, M. S. Ansari, and S. K. Gupta, “Collaboration of drone and internet of public safety things in smart cities: An overview of qos and network performance optimization,” *Drones*, vol. 3, no. 1, p. 13, 2019.

[10] Z. Ahmed, S. Hamma, and Z. Nasir, “An optimal bandwidth allocation algorithm for improving QoS in WiMAX,” *Multimed. Tools Appl.*, vol. 78, no. 18, pp. 25937–25976, 2019.

[11] M.-L. Messai, “Classification of attacks in wireless sensor networks,” *arXiv Prepr. arXiv1406.4516*, 2014.

[12] P. Pecho, J. Nagy, P. Hanáček, and M. Drahanský, “Secure collection tree protocol for tamper-resistant wireless sensors,” in *International Conference on Security Technology*, 2009, pp. 217–224.

[13] M. Belkadi, R. Aoudjit, M. Daoui, and M. Lalam, “Energy-efficient secure directed diffusion protocol for wireless sensor networks,” *Int. J. Inf. Technol. Comput. Sci.*, vol. 6, no. 1, pp. 50–56, 2014.

[14] S.-B. Lee and Y.-H. Choi, “ARMS: An authenticated routing message in sensor networks,” in *International Workshop on Secure Mobile Ad-hoc Networks and Sensors*, 2005, pp. 158–173.

[15] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, “SPINS: Security protocols for sensor networks. NY: ACM.” Kluwer Wireless Networks Journal (WINET), 2002.

[16] K. Zhang, C. Wang, and C. Wang, “A secure routing protocol for cluster-based wireless sensor networks using group key management,” in *2008 4th international conference on*

wireless communications, networking and mobile computing, 2008, pp. 1–5.

[17] W. Xiao-yun, Y. Li-zhen, and C. Ke-fei, "Sleach: Secure low-energy adaptive clustering hierarchy protocol for wireless sensor networks," *Wuhan Univ. J. Nat. Sci.*, vol. 10, no. 1, pp. 127–131, 2005.

[18] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *Rsa Cryptobytes*, vol. 5, no. 2, pp. 2–13, 2002.

[19] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, "SecLEACH-A random key distribution solution for securing clustered sensor networks," in *Fifth IEEE International Symposium on Network Computing and Applications (NCA'06)*, 2006, pp. 145–154.

[20] P. Lorenz and P. Dini, *Networking--ICN 2005: 4th International Conference on Networking, Reunion Island, France, April 17-21, 2005, Proceedings, Part I*, vol. 3420. Springer, 2005.

[21] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 41–47.

[22] M. El_Saadawy and E. Shaaban, "Enhancing S-LEACH security for wireless sensor networks," in *2012 IEEE International Conference on Electro/Information Technology*, 2012, pp. 1–6.

[23] D. Wu, G. Hu, and G. Ni, "Research and improve on secure routing protocols in wireless sensor networks," in *2008 4th IEEE International Conference on Circuits and Systems for*

Communications, 2008, pp. 853–856.

[24] M. Alshowkan, K. Elleithy, and H. AlHassan, "LS-LEACH: a new secure and energy efficient routing protocol for wireless sensor networks," in *2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications*, 2013, pp. 215–220.

[25] P. Ramani, R. Prasad, S. D. S. Shahul, and S. Swaminathan, "SSN COLLEGE OF ENGINEERING, KALAVAKKAM-603110 DEPARTMENT of ELECTRONICS and COMMUNICATION ENGINEERING Students Publications June 2013-May 2014 International Journal publications: Under Graduate," *Int. J.*, vol. 2014, 2013.

[26] S. Ganesh, "Efficient and Secure Routing Protocol for WSN-A Thesis," *arXiv Prepr. arXiv1708.04500*, 2017.

[27] S. Kumar and S. Jena, "SCMRP: Secure cluster based multipath routing protocol for wireless sensor networks," in *2010 Sixth International conference on Wireless Communication and Sensor Networks*, 2010, pp. 1–6.

[28] N. M. Durrani, N. Kafi, J. Shamsi, W. Haider, and A. M. Abbsi, "Secure multi-hop routing protocols in Wireless Sensor Networks: Requirements, challenges and solutions," in *Eighth International Conference on Digital Information Management (ICDIM 2013)*, 2013, pp. 41–48.

[29] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24–34, 2007.

[30] B. Karp and H.-T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks,"

in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 243–254.

[31] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, "SIGF: a family of configurable, secure routing protocols for wireless sensor networks," in *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, 2006, pp. 35–48.

[32] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the 2nd ACM workshop on Wireless security*, 2003, pp. 30–40.

[33] A. Larsson, *Security and Self-stabilization in Sensor Network Services*. Chalmers University of Technology, 2012.

[34] D. Tang, T. Jiang, and J. Ren, "Secure and energy aware routing (sear) in wireless sensor networks," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 2010, pp. 1–5.

[35] J. Yin and S. K. Madria, "A hierarchical secure routing protocol against black hole attacks in sensor networks," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, 2006, vol. 1, pp. 8-pp.