Performance Analysis and Application Development of Hybrid WiMAX–WiFi IP Video Surveillance Systems

Smart Charles Lubobya

Supervisors	: Associate Prof. Mqhele. E. Dlodlo
	: Prof. Gerhard de Jager
Co-Supervisor	: Dr Ackim Zulu

This thesis is submitted in fulfilment of the academic requirements

For the degree of

Doctor of Philosophy in Engineering

In the Faculty of Engineering and the Built Environment

University of Cape Town

2016

As the candidate's supervisor, I have approved this thesis for submission

Name: Associate Prof. M. E. Dlodlo

Signed: Signed by candidate

Date: 2016-06-15

As the candidate's supervisor, I have approved this thesis for submission

Name: Emeritus Prof. Gerhard de Jager

Signed: Signed by candidate

Date: 2016/06/17.

Declaration

I declare that this thesis is my own work. Where collaboration with other people has taken place, or material generated by other researchers is included, the parties and/or materials are explicitly stated with references where appropriate.

This work is being submitted for the Doctor of Philosophy in Electrical Engineering at the University of Cape Town. It has not been submitted to any other university for any other degree or examination.

Signed by candidate

Smart Charles Lubobya **15th June, 2016**

Name **Date**

Dedication

To my wife Lydia; my three sons Timothy, Titus and Ted including my daughter Tapelo, I say thank you for your support and inspiration.

Above all, may glory be to our God, the giver of life.

Abstract

Traditional Closed Circuit Television (CCTV) analogue cameras installed in buildings and other areas of security interest necessitates the use of cable lines. However, analogue systems are limited by distance; and storing analogue data requires huge space or bandwidth. Wired systems are also prone to vandalism, they cannot be installed in a hostile terrain and in heritage sites, where cabling would distort original design. Currently, there is a paradigm shift towards wireless solutions (WiMAX, Wi-Fi, 3G, 4G) to complement and in some cases replace the wired system.

A wireless solution of the Fourth-Generation Surveillance System (4GSS) has been proposed in this thesis. It is a hybrid WiMAX-WiFi video surveillance system. The performance analysis of the hybrid WiMAX-WiFi is compared with the conventional WiMAX surveillance models. The video surveillance models and the algorithm that exploit the advantages of both WiMAX and Wi-Fi for scenarios of fixed and mobile wireless cameras have been proposed, simulated and compared with the mathematical/analytical models. The hybrid WiMAX-WiFi video surveillance model has been extended to include a Wireless Mesh configuration on the Wi-Fi part, to improve the scalability and reliability.

A performance analysis for hybrid WiMAX-WiFi system with an appropriate Mobility model has been considered for the case of mobile cameras. A security software application for mobile smartphones that sends surveillance images to either local or remote servers has been developed. The developed software has been tested, evaluated and deployed in low bandwidth Wi-Fi wireless network environments.

WiMAX is a wireless metropolitan access network technology that provides broadband services to the connected customers. Major modules and units of WiMAX include the Customer Provided Equipment (CPE), the Access Service Network (ASN) which consist one or more Base Stations (BS) and the Connectivity Service Network (CSN). Various interfaces exist between each unit and module. WiMAX is based on the IEEE 802.16 family of standards. Wi-Fi, on the other hand, is a wireless access network operating in the local area network; and it is based on the IEEE 802.11 standards.

The existing Wi-Fi systems have the advantages of wider deployment of Wi-Fi IP cameras, as well as cost effectiveness. However, they suffer from the challenges of packet loss, unguaranteed Quality of Service (QoS), reduced throughput and coverage radius. Equally, WiMAX Video surveillance systems do not make efficient use of the channel bandwidth; they are non-scalable; and they have limited WiMAX IP camera deployment. Notwithstanding this, WiMAX networks offer guaranteed QoS; they support higher bit rates, and have wider coverage radii.

A hybrid WiMAX-WiFi video surveillance system consists of wireless Wi-Fi IP cameras linked to a WiMAX network through the CPE, BS, local or remote server and the Internet. Local monitoring is done via the Ethernet connection from the CPE. For remote monitoring, the video signal is then routed to the Internet via an array of WiMAX equipment, and then routed to a central control room where the security experts monitor and interpret the video contents.

The results in this investigation show that the hybrid WiMAX-WiFi surveillance with mesh extension performs better than the one without a mesh extension regarding throughput and dropped bits per second. The improved performance of the meshed system comes at the cost of reduced end-to-end delay and jitter performance. A hybrid WiMAX-WiFi surveillance system with mobility has poor throughput when the nodes move at a speed beyond 1.4m/s; the dropped bits per second rise and fall as throughput degrades even more. Furthermore, the end-to-end delay and the jitter increase with the increase in speed.

An algorithm for low bandwidth application software has been proposed and implemented; and a 100% successful transmission of surveillance images/videos in a low-bandwidth network environment has been achieved. Video compressions with scalable encoders of the H.264/SVC type or the high efficient H.265/HEVC are the best choices for mobile surveillance systems.

Acknowledgements

My sincere appreciation goes to my supervisors Associate Prof. M.E Dlodlo, Emeritus Prof. Gerhard de Jager and Dr A. Zulu for their guidance, support and encouragement during the course of my study at the University of Cape Town. My gratitude also goes to Dr Simon Winberg, for his warm help in my research work.

I am thankful to my family for their prayers and encouragement.

I also appreciate the critique and advice from the members of the Communication Research Group (CRG) in the Department of Electrical Engineering at the University of Cape Town and for reviewing my work.

Table of Contents

List of Figures

List of Tables

List of Acronyms

AC : Alternating Current
ADC : Analog to Digital Converter
AP : Access Point
ASN : Access Service Network
BS : Base Station
BWA : Broadband Wireless Access
CBR : Constant Bit Rate
CCD : Charge-Coupled Device
CCTV : Closed Circuit Television
CDMA : Code Division Multiple Access
CIF : Common Intermediate Format
CMOS : Complementary Metal-Oxide Semiconductor
CPE : Customer Premises Equipment
CPU : Central Processing Unit
CSN : Connectivity Service Network
DC : Direct Current
DHCP : Dynamic Host Control Protocol
DNS : Domain Name System
DSSS : Direct Sequence Spread Spectrum
FOV : Field of View
GSM : Global System for Mobile communication
HEVC : High Efficiency Video Coding
IDE : Integrated Development Environment
IP : Internet Protocol
ISP : Internet Service Provider
ITU-T : International Telecommunication Union-Telecommunication sector
JCT-VC : Joint Collaborative Team on Video Coding
LAN : Local Area Network
LTE : Long-Term Evolution
MS : Mobile Station
MSDU : MAC Service Data Unit

NAP : Network Access Provider

NDVR : Network Digital Video Recorder

NSP : Network Service Provider

NSTC : National Television Standard Committee

OFDM : Orthogonal Frequency Division Multiplexing

OOP : Object-Oriented Programming

PAL : Phase Alternating Lines

PDA : Personal Data Assistant

PC : Personal Computers

QCIF : Quarter Common Intermediate Format

QoS : Quality of Service

RTP : Real-Time Protocol

SVC : Scalable Video Coding

SS : Subscriber Station

TCP : Transmission Control Protocol

TDD : Time Division Duplexing

TV : Television

UDP : User Datagram Protocol

UMTS : Universal Mobile Telecommunications System

USB : Universal Serial Bus

VBR : Variable Bit Rate

VCR : Video Cassette Recording

VHS : Video Home System

WMR : Wireless Mesh Router

Publications

The listed journal and conference papers below have resulted from this thesis; and they have been published and/or accepted for publications:

1. **Journal**

   S. C. Lubobya, M. E. Dlodlo, G. de Jager , A. Zulu, "Throughput Characteristics of WiMAX Video Surveillance Systems." In *Elsevier's Procedia Computer Science Journal*, pp. *571-580,* March. 2015. ISSN: 1877-0509

2. **Book Series**

   S. C. Lubobya, M. E. Dlodlo, G. de Jager , A. Zulu, **"**Link Utilization in Hybrid WiMAX-WiFi Video Surveillance Systems." in *Springer's Advances in Intelligent Systems and Computing*, unpublished.

3. **Conference papers**

   a) S. C. Lubobya, M. E. Dlodlo, G. de Jager, A. Zulu, "Mobile Surveillance Application for Hybrid WiMAX-Wi-Fi Systems", *IEEE Global Wireless Summit*, November 27-30, AARHUS University, Denmark, 2016 .

   b) S. C. Lubobya, M. E. Dlodlo, G. de Jager , A. Zulu, "Mesh IP Video Surveillance Systems Model Design and Performance Evaluation", *IEEE 5th International Conference on Wireless Communications, Vehicular Technology, Information Theory, Aerospace & Electronics Systems*, Hyderabad, India, 2015.

   c) S. C. Lubobya, M. E. Dlodlo, G. de Jager, A. Zulu, "Performance Comparisons of Wireless Mesh IP Video Surveillance Models," *9th IEEE European Modelling Symposium on Mathematical Modelling and Computer Simulation*, pp.415-420, 2015, Madrid, Spain. ISBN: 978-1-5090-0206-1.

   d) S. C. Lubobya, M. E. Dlodlo, G. de Jager, 'Performance Evaluation of the Wireless Tree Wi-Fi Video Surveillance System'. In *IEEE UKSim-AMSS 16th International Conference on Computer Modelling and Simulation,* 26-28 March, *pp. 510-515,* Cambridge, United kingdom, 2014, ISBN:978-1-4799-4923-6

Chapter One

1 Introduction

This thesis discusses the performance analysis of hybrid WiMAX-WiFi video surveillance systems, Fourth-Generation Surveillance System (4GSS), and implements an algorithm for a security (surveillance) software application for mobile smartphones. Surveillance systems are critical for monitoring and detecting crime and disasters in public places such as bus and train stations, airports, car parking lots, shopping malls and the like. This necessity becomes even more critical in developing countries where bandwidth is scarce; yet there is a high demand for surveillance.

Video surveillance models and algorithms that exploit the advantages of both WiMAX and Wi-Fi for scenarios of fixed and mobile wireless cameras have been proposed, simulated and compared with mathematical/analytical models. A hybrid WiMAX-WiFi video surveillance model has been extended to include a Wireless Mesh configuration on the Wi-Fi part, to improve scalability and reliability. The performance analysis of the hybrid WiMAX-WiFi system with an appropriate mobility model has been considered for the case of mobile cameras. A security software algorithm and application for mobile smartphones that sends surveillance images to either local or remote servers has been developed. The developed software has been tested, evaluated and deployed in low bandwidth Wi-Fi wireless network environments.

Traditional Closed Circuit Television (CCTV) analogue cameras installed in buildings and other areas of security interest require the use of cable lines. Cable lines deliver video surveillance data captured by Charge-Coupled Device (CCD) or Complementary Metal-Oxide Semiconductor (CMOS) cameras to the Video Monitoring and Control Centre for users [1]. However, analogue systems are limited by distance; and storing analogue data requires substantial amounts of space or bandwidth. In contrast, Internet Protocol (IP) cameras or network cameras employed in many IP-based networks avoid the above limitations.

An IP Video Surveillance system is a network security system that affords users an opportunity to capture, monitor and record video/image and audio over an Internet

Protocol. The network could be a Local Area Network (LAN) covering a local building, or the Internet covering a global area. A LAN for an IP video surveillance system includes the use of network cameras (also called IP cameras) connected to the switch or router and the monitoring and recording computer.

The IP-based video surveillance system also allows the use of network cameras, which connects to the Internet via a chosen Internet Service Provider (ISP) and access technology. Some of these access technologies are the wired broadband and fibre technologies, or wireless access technologies, such as Worldwide Interoperability for Microwave Access (WiMAX), Long-Term Evolution (LTE), Universal Mobile Telecommunications System (UMTS), Code Division Multiple Access two thousand (CDMA 2000) and Wireless Fidelity (Wi-Fi).

Wired video surveillance systems have numerous advantages, compared to wireless IP video surveillance systems. They are not affected by weather or signal interferences and they have high reliability. However, wired systems have limitations as well. These constraints range from the need for more installation time and cost, to installation practicality difficulties: either due to bad terrain environments, say rocky areas, or to old buildings, where it is impractical to lay cables. A detailed description of most wired network cameras is given in Appendix A; but this work focuses on wireless cameras and their use in hybrid WiMAX-WiFi surveillance systems.

Thus, in areas where wired systems have limitations, like vandalism risks; the wireless solution becomes a natural and reasonable option. Wireless IP video surveillance systems can be used to complement wired systems as well.

1.1 The WiMAX-WiFi IP Video Surveillance System

A WiMAX-WiFi IP video surveillance system consists of a fixed or mobile wireless IP camera, a wireless receiver, switches, routers and viewing PC, or servers [2]. The encoder in the IP camera will capture, digitise and compress the video image, before sending it to the receiver in packet format over a wireless link [2] such as Wi-Fi and WiMAX. For the purpose of viewing, the video is then decoded, using a local personal computer, or remotely via the Internet.

Wi-Fi network cameras also contain some electronics circuitry that enables them to connect to the Internet via the appropriate Internet service provider (ISP). To view the camera, one enters the Internet address (ID number) and the proper password. Password security ensures that only the authorised users can access and see the camera image. Figure 1.1 shows the block diagram of a wireless or WiMAX-WiFi IP video surveillance system

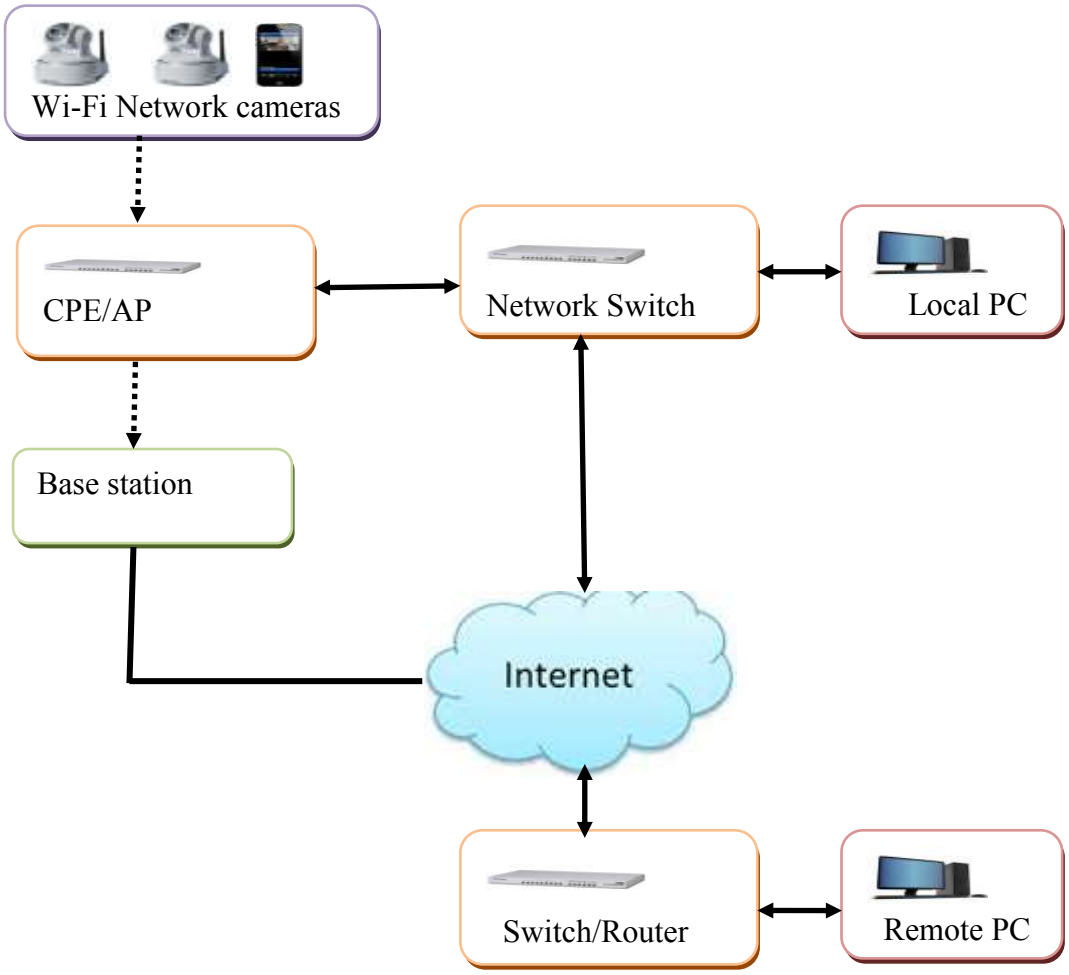

Figure 1.1: WiMAX-WiFi IP Video Surveillance System

Duplex communication is adopted; and this allows the user to control the camera parameters and directs its operation (pan, tilt, zoom, etc.) remotely [3]. Some wireless cameras have both wired Ethernet and wireless interfaces. Wireless IP cameras, like wired IP cameras; employ Ethernet cable interface connectivity to the computer or similar devices. The wireless receiver could be an Access Point (AP), a Wireless Mesh Router (WMR), or Customer Premises Equipment (CPE).

These wireless receivers provide the access to the network cameras. Each wireless receiver consists of a wireless receiver unit or interface and transmitter units. An optional wired/ Ethernet interface for connecting to the broadband network and other devices also exist for some of these access wireless receivers. In video surveillance systems, these devices receive video signals from the wireless network cameras and relay them to the backbone network and local viewing PC or servers.

A wireless receiver can be connected to the wired broadband network using Category 5 or 6 Ethernet cable, or wirelessly by using the WiMAX-WiFi network link. The choice of the backbone network depends on many factors: cost, Quality of services (QoS) offered, supported services, the level of information security desired, among others. In this research, a fixed wireless network has been considered. A fixed wireless network is can be designed and configured into three broad categories: point to point, point to multipoint, or mesh networks (see Appendix B for detailed notes).

1.2 Evolution of Video Surveillance Systems

Video surveillance systems have been evolving over the years, from the First Generation Surveillance Systems (1GSS) to the current Fourth Generation Surveillance Systems (4GSS). Modern technological advances and trends have triggered the need for efficient, sophisticated and scalable video surveillance systems. For example, current video surveillance systems must address the latest trends and requirements such as high quality image signal processing, high bandwidth requirements, handheld communication devices (PDA, mobile phones) and a low-cost storage solution. In moving towards the modern networked IP video surveillance systems, two key technological drivers have been developed. These are the Ethernet LAN and the Internet Protocol technologies [4].

Ethernet LAN technologies make use of shielded twisted-pair and unshielded twisted-pair network cables. With such cables, the network can operate at 10 and 100 megabits per second (Mbps), as well as at 1 and 10 gigabits per second (10Gbps). Most of these Ethernet velocities are compatible with other high-speed technologies, like optic fibre.

The significance of IP technology to networks and video surveillance systems is due to their worldwide acceptance [4]. They can be used as methods of addressing and

connecting specific devices, including Personal Computers (PCs), mobile phones and IP security cameras. Thus, particular camera surveillance data can be viewed and monitored from anywhere on the network - by anyone with network access and proper security authorization.

IP technology in partnership with the Transmission Control Protocol (TCP) may be implemented. The technology also ensures easy device identification, accessibility and error detection [4].

1.2.1 First Generation Video Surveillance Systems

First Generation Video Surveillance Systems (IGSS) began with the use of traditional analogue CCTV video surveillance systems [5]. The system consists of one or more analogue cameras, a time-lapse Video Cassette Recorder (VCRs) and viewing monitors. To allow for multiple cameras to be recorded by using a single VCR and monitor, a multiplexing device typically connects to the cameras and the VCR [6]. Figure 1.2, shows the traditional first generation CCTV video surveillance system.

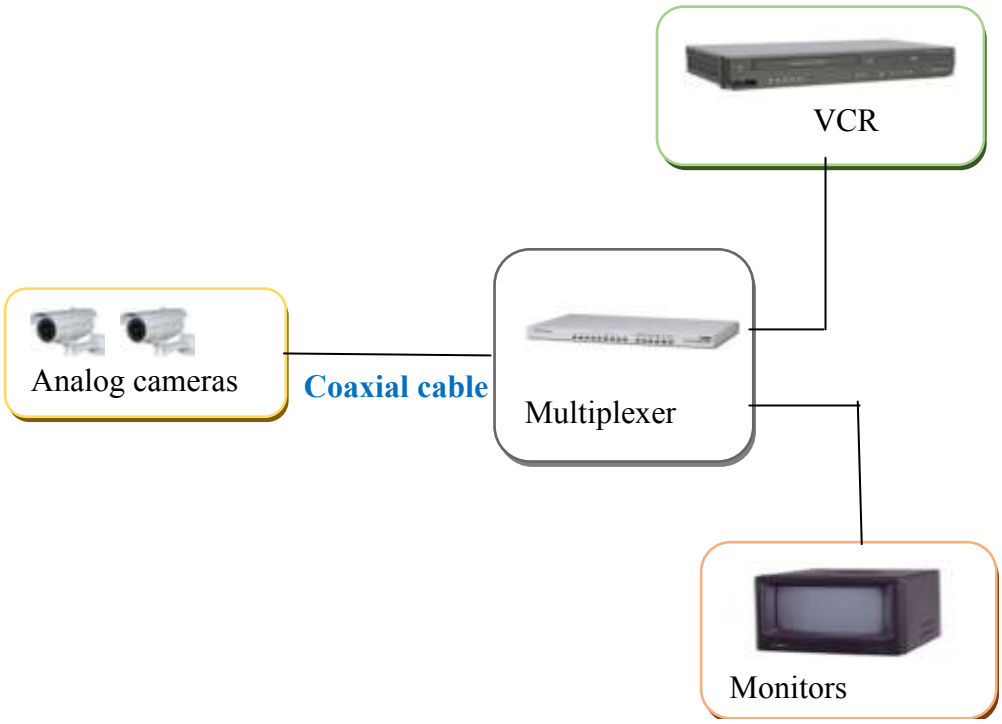

Figure 1.2: Traditional analogue CCTV video surveillance systems

A coaxial cable run from each of the cameras to the multiplexer device is connected to achieve the set-up. This system uses Video Home Service (VHS) tapes for recording

surveillance images/ videos. Each VHS tape can record for two hours with a provision to be re-used [4]. Notwithstanding their simplicity in operation and functionality, CCTV systems are not scalable, the video quality is low; and they have maintenance problems. To increase the storage capacity, as well as to increase the number of cameras to be connected, the CCTV system was improved and upgraded to a hybrid analogue-digital IP video surveillance system shown in Figure 1.3 below:

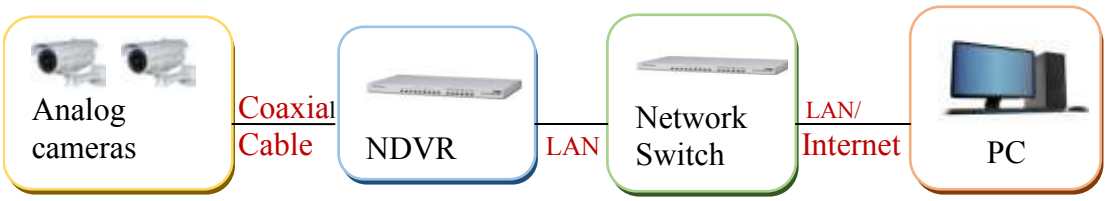

Figure 1.3: Hybrid analogue-digital IP video surveillance system

A hybrid analogue-digital IP video surveillance has two parts: the analogue and the digital part. The analogue part comprises the analogue cameras connected to the Network Digital Video Recorder (NDVR) via a 75-ohm coaxial cable. The digital part consists of the NDVR, which converts analogue image/video to a digital signal, and compresses it before routing it to the LAN and the Internet. A remote PC can be connected to perform the viewing, monitoring and server roles [4]. Appendix C-2 shows an illustration of the hybrid analogue-digital video surveillance system.

1.2.2 Second Generation Surveillance Systems

Second-Generation Surveillance Systems (2GSS) are fully digital in design [5] [7]. They consist of a network or IP cameras connected either to the switch using the Ethernet cable, or wirelessly to the Access Point (AP), or to the WMR or Customer Promises Equipment (CPE). The wired type modern full digital IP video surveillance system is illustrated in Figure 1.4.

Figure 1.4: Full digital IP video surveillance system

A network camera or IP camera is a video camera with computer functionality inside it. It digitises and processes captured analogue images or videos; it encodes them internally, and then transmits the video information digitally over a wired or wireless connection to a computer or similar device [8] [4].

2GSS provide consistent monitoring quality, and they use computer vision methods to put on view the information obtained from the sensors; and the systems transmit significant output signals[5] [7]. In addition, remote camera control features such as pan, tilt, and zoom were added. Second Generation Surveillance Systems became popular - largely because of the additional computer vision algorithms for detection, tracking and monitoring functions. Hence, more intelligent surveillance systems were created[5].

1.2.3 Third Generation Video Surveillance Systems

Third-Generation Surveillance Systems (3GSS) eliminate the single point of control and monitoring, and replaces it with networked cameras and sensors[5]. Cameras and sensors have advanced processors. These advanced camera processors transmit knowledge, in addition to pixels to the central room. In this way, only information required for the detection and description of any abnormal scene, is displayed to the operator [5] [7]. Therefore, enormous communication bandwidth is saved; as only detected objects' information is sent to the central room.

3GSS thrives on the progress made in low-cost but high-performance computing networks. Information processing is spread across various stages of the system. But this generation of surveillance was limited in computation power and lacked processing techniques for robust image transmission. Furthermore, precise and real-time result including a concentration on object recognition, tracking and scene analysis; coupled with state-of-the art communication protocols was needed [5] [7]. Those above combined with many more challenges, led to the birth of the Fourth-Generation Surveillance System.

1.2.4 Fourth Generation Video Surveillance Systems

Fourth Generation Surveillance Systems (4GSS), also called Distributed surveillance systems, are of two types: PC based and embedded platforms based[5]. Figure 1.1 discussed in section 1.1 is one classical example of 4GSS. A paradigm shift from PC-

based systems, to more adaptable embedded systems has characterised the 4GSS. This change led to the need for field environment surveillance, as with forests, game parks and the like[5]. However, most current systems are still PC-based[5]. PC-based systems cannot be used for surveillance in forest environments, because they are large in size, consumes more power and they are not very stable[5].

This weakness is, currently, mitigated by the advances in IC manufacturing whereby low power visual nodes are developed. Table 1.1 shows the summary of the significant changes in each video surveillance generation.

Table 1.1: **The Four Generations of Video Surveillance Systems** [5]

1GSS	**2GSS**	**3GSS**	**4GSS**
No information processing. Only visualisation	Digital information processed at central level.	Distributed digital processing at various network levels	Embedded processing on lightweight nodes
Scene analysis done by human operators	System displays acquired images, sends output signal to concentrate on crime situations.	only information for detection and description of crime situation is displayed	Knowledge transmitted and feedback from control station
disadvantages: unstable detection, high bandwidth, difficult retrieval	demerits: single point of failure	Drawback: lower stability, high power, large volume.	Challenges due to embedded nature: limited resources

1.3 IP Video Surveillance Requirements

Another important consideration when planning for video capture is the IP video surveillance requirements. Three major requirements should be considered: network bandwidth and storage space; the QoS; and the network requirements. The following subsections describe the network bandwidth, the QoS requirements and nature of network design.

1.3.1 Network Bandwidth and Storage Requirement

The video capture is important in determining among other things, the network bandwidth and the storage space requirements. This need is satisfied, when the number of network cameras, frame size and frame rate are known. It gives the maximum possible network bandwidth or capacity required in the system in bits per second.

Network bandwidth is the maximum capacity (in bits per second) of the network to transmit a given traffic type on a network. The network bandwidth determines the right traffic type and the size needed on a chosen network architecture [9]. The video, voice and data have different network bandwidth requirements, beyond which it would not be possible to transmit on the network. In IP video surveillance, a correct choice of the number of IP cameras, frame size and frames per second determine the network bandwidth.

Thus, for a frame count, F_c and frame duration t, the frame rate (fps) is given by:

$$fps = \frac{F_c}{t} \tag{1.1}$$

Motion pictures are normally captured at 24 fps. At that rate, the human eye would view these images as fluid motion. Televisions use 30 fps (NTSC) or 25 fps (PAL) as do analogue video cameras [10]. In the lab, it is possible to stream video up to 30-60fps. However, this would be impossible for IP surveillance applications owing to the wider bandwidth and storage requirements. In practice, frame rate values range from 1fps to 20fps, with 10fps as a comfortable medium. However, 25fps to 60fps are also used in certain applications, such as, casinos, banks, etc. The following are some industry guidelines [10]:

- 30 fps for casinos
- 12 to 15 fps for cash register, teller stations
- 5 fps for office hallways
- 1 to 3 fps for parking lots, overview scenes and traffic cameras
- less than 1 fps for sports Stadia on non-event days [10]

Each IP camera will process a video signal and transmit packet frames, at the data rate (A_n) in bits per second given by:

$$A_n = [\frac{MSDU\_byte}{frames} \times \frac{8bits}{byte} \times \frac{1frames}{t}] \; bps \tag{1.2}$$

in which, t is the outgoing inter arrival time or frame duration. t is also related to the video frame rate, as shown in equation (1.1). The MAC Service Data Unit (MSDU) bytes size in equation (1.2) is nearly equal to the frame size in bytes. For digital colour video, frame size has both *vertical* and *horizontal* pixel components consisting of 8bits each for Red, Green and Blue colours. Thus frame size in bytes is given as:

$$FS = [\frac{(vertical \times horizontal)pixel \times 24bits}{8}] \; bytes \tag{1.3}$$

However, modern codecs, like one governed by the H.264, MPEG-4 part 2 and H.265 standard, converts colour from the RGB colour scheme to $Y : C_r : C_b$ colour scheme [11]: These colour schemes use 8 bits for the combined luminance (Y), Red and blue chrominance ($C_r : C_b$) to represent each of these colour schemes. Appendix C, shows the calculations of 8 bits for the $Y : C_r : C_b$ colour scheme: Thus equation 1.3 can be written as:

$$FS = [\frac{(vertical \times horizontal)pixel \times 8bits}{8}] \; bytes \tag{1.4}$$

The generated data rate traffic per camera will be:

$$A_n = [FS \times fps \times 8] \;\; bps \tag{1.5}$$

where the constant 8 is for converting byte into bits. Increasing camera resolution demands a corresponding increase in bandwidth needs. In designing cameras, various resolutions are achievable depending on the type of video: digital or analogue. Consider two video resolutions cameras: (352x288) and (1902x720). If the two cameras have the same frame rate, as well as the same compression ratio, a 352x288 video resolution would require less bandwidth than the 1902x720 video resolutions given by equations (1.3) to (1.5).

Network bandwidth and storage space requirements depend on some factors. Common factors, among others, include the frame rate and size, the required period of video archive, the number of network cameras. Bandwidth and storage space requirements increase with the increase in the number of cameras. The network bandwidth in bits per second can then be computed from:

$$B = [FS \times fps \div n_p \times 8] \quad bps \tag{1.6}$$

Where *FS* is the frame size in bytes, *fps* is the frames per second and n_p is the **planned number** of connected cameras. Frame size is a function of camera resolution and video compression standard adopted. It is measured in bytes, although a bigger unit, the kilobyte, is also used. In equation 1.6, the overall bandwidth may be divided by 1024 when the frame size is given in kilobyte and unit of measure would then be in Mbps. Frame size mostly depends on camera resolution and the type of video compression standards adopted. Camera resolution is a measure of pixels.

Related to the network bandwidth, is the measured load. The measured load (L) is the actual bit rate of the connected cameras. Its value may be equal to, or less than the bandwidth. It can be calculated from equation (1.7); in which case, n_a is the **actual number** of connected cameras.

$$L = [FS \times fps \times n_a \times 8] \, bps \tag{1.7}$$

When the duration of storage of surveillance video is known, the storage space (S_N) needed on the disk, can also be calculated.

$$S_N = GB \times t_s \tag{1.8}$$

Where: *GB* is Gigabytes per day, which translates into Megabytes per hour multiplied by hours of operation per day; and t_s is the required period of storage. Raw and uncompressed videos with high frame rates increase the bandwidth requirements.

There should be a careful selection of frame rate. The frame rate must satisfy business needs; but it must not exceed the required size; since it influences both bandwidth and storage requirements [12].

1.3.2 Quality of Service Requirements

Quality of Service is essential for higher quality network performance requirements in video surveillance. QoS guarantees that surveillance video/images in the network are given a specified priority. As an example, video surveillance traffic could have a higher priority than the data traffic in a network. Effectively, this means that higher priority traffic is processed before the lower priority traffic. Thus, the critical traffic is given precedence; since it guarantees unswerving signal transmission.

In video surveillance systems, QoS also guarantees stabilized jitter, reduced frame loss, or packet loss and minimized end-to-end delay. Furthermore, without QoS, video and other traffic types would be processed and transmitted equally by the network. Transmissions too would depend on the network's best-effort [9]. Hence, the correctness of the system architecture is measured and determined by QoS performance; and it must satisfy the jitter, end-to-end and packets loss requirements for video transmission over the Internet.

1.3.3 Network Design Requirement

Cabasso [8] further adds that the network topology design should be, seriously, considered in IP Video surveillances. Any proposed system should optimise the network architecture for efficient bandwidth utilisation. Some network architectures are less capable and consume more bandwidth. In the proposed IP video surveillance models stated in Chapter Three and Chapter Four, well-designed network architectures have been devised; and the appropriate topologies recommended.

1.4 Wireless IP Video Surveillance Challenges

Although there are several merits and opportunities in wireless IP video surveillance systems, challenges still exist. These include, but are not limited to, security issues, encoder designs, power supply, environmental constraints and bandwidth requirements. A discussion on some of these difficulties is given below, and this thesis attempts to resolve the problem of bandwidth requirements [see section 1.5(c)].

1.4.1 Security Threats

IP cameras (and there could be hundreds of them in a single system), like any other IP device, are vulnerable to Security threats. Secure IP cameras are critical for a practical

and usable IP video surveillance system. The overall wire or wireless network is also subject to viruses and man-in-the middle attacks. Hackers can attack the network from anywhere in the world [8]. Both video streams and control signal data type can be targeted for attack or manipulation. An unsecured surveillance system or network may be a dangerous tool for terrorist attacks in the monitored and protected environments[13].

Depending on the system degree of compromise, hackers' attacks to an IP video surveillance system fall into two categories: Firstly, the hacker attack the video data flow, steals confidential information or tampers with it, and deceives the recipients. Thus, data confidentiality and integrity are lost. Hackers will decipher the encryption keys used to maintain the confidentiality of the video data. Any modified video or control data reduces the video stream integrity; and receivers would receive the wrong video clips. Secondly, the hackers steal private information and utilize it to control or destroy the data.

Additionally, the attacker may reuse the initially recorded videos in the networks and deceive operators and recipients as real-time. The second attack is riskier than the first; as it may lead to a complete loss or damage of surveillance videos [13]Various methods and schemes have been devised, to mitigate these security threats.

One method is designing systems that include a virtual or physical dedicated camera network [14]. This method is a good starting point; but it may not comprise the complete solution. Other methods include more sophisticated encryption algorithms: both in the wired and the wireless interface, as suggested by the authors in [15].

1.4.2 Wide Camera Bandwidth Requirements

One major challenge and shortcoming of IP cameras is their wide bandwidth requirement [16]. Camera bandwidth depends on the video frame rate, resolutions, and type of video codec, among others (see discussion of bandwidth parameters in section (1.3.1). The frame rate is a speed measure of successive pictures in realizing a video. Alternatively, it is a measure of the frames processed per second. A high frame rate leads to a faster and smoother video and *vice versa*. Two types of frame rates exist: progressive and interlaced. The former is where one full frame is followed by

the other full frame; while the latter is where one half video images are displaced by every alternation of the frame.

1.4.3 Nature of the Compression Codec or Standard Adopted

The nature of the video compression format inside the digital signal process determines the payload of the video. With wireless IP video cameras, the compression is achieved inside the camera, before it is sent to the server [10]. The payload size determines the bandwidth requirements and the possible number of cameras to be used in a wireless surveillance system. Depending on the compression format and the standard adopted, the payload or frame size in equation (1.3) can reduce in size by a factor or ratio.

The level of reduction in size depends on the type of codec and the compression ratio or divisor. Table 1.2 shows some common video surveillance codecs and compression ratios [17].

Table 1.2: Video Codec Compression ratio

Codec	**Compression ratio (C_r)**
M-JPEG	1:20
MPEG-4Part 2	1:50
H.264	1:100
H.264/SVC Base profile	Nearly double the H.264/AVC base profile
H.265/HEVC	Double the H.264/AVC high profile

For example, most H.264/SVC codecs can reduce the frame size, and eventually the transmitting rate by 50 to 80 per cent. Thus, equation (1.5) can now be written as:

$$A_n = [FS \times C_r \times fps \times 8]\, bps \tag{1.9}$$

in which C_r is the compression ratio and the constant 8 is for converting byte into bits. The compression of raw videos/images is a major factor in optimizing network bandwidth in IP video surveillance. A video codec enables the compression or the decompression of digital video; and it must adhere to specific video compression quality requirements.

Video compression can be implemented by using several video compression standards. Most digital security cameras use MJPEG, Motion Picture Expert Group (MPEG)-4 part 2, or the new MPEG-4 version 10, standard formats. Others adopts the International Telecommunication Union-Telecom (ITU-T) compression standard formats, such as: H.263, H.264, which is equivalent to the MPEG-4 version 10, and a more recent H.265/HEVC introduced in 2013.

In 1998 MPEG-4, also known as standard ISO/IEC14496, was Published. Thus MPEG-4 Part 2 (ISO/IEC 14496-2) was the first proposed standard for video compression. MPEG-4 Part 2 is based on a Discrete Cosine Transform (DCT) and motion estimation of quarter-pixel precision. However, MPEG-part 2 had slim applications in video surveillance due to little quality-to-data rate [18].

MJPEG video compression is a lossy digital video version of the JPEG compression family. MJPEG is a higher quality video codec because it uses all the required frames per second. As a consequence, the file size for MJPEG compression are larger and bandwidth requirement is higher compared to the H.264/AVC [19].

The H.264/AVC compression standard was initially published in 2003 but jointly developed by the ITU-T and MPEG. It has since been revised and updated into many profiles and applications [11]. It is an improvement of earlier standards MPEG 2 and MPEG 4 visual and promises better compression efficiency, flexibility; transmission and storage of video. Unlike previous standards, the discrete cosine transform is replaced by the more efficient integer transform on block size of 4×4 or 8×8 pixels [11]. additionally, motion estimation is performed on varying block sizes: 4×4, 4×8, 8×4, 8×8, 8×16, 16×8 and 16×16 [11]. The H.264 format has wider use in the security industry or video streaming and recording than others [10] because of its improved video compression efficiency and hence occupies less bandwidth and storage space compared to its predecessor standards.

The H.265/HEVC standard was developed to answer the growing need for higher compression of videos or moving pictures. Therefore, in 2010, the ISO/IEC Moving Picture Experts Group (MPEG) and the ITU-T Video Coding Experts Group (VCEG) met and established a Joint Collaborative Team on Video Coding (JCT-VC) [20],

giving birth to the H.265/HEVC standard. H.265/HEVC encoder compresses videos with a higher quality and lower bit rates than the other encoders.

This specification covers a broad range of applications for video content. They include, among others, digital storage media, Internet streaming, video conferencing, television broadcasting, remote video surveillance, medical imaging, mobile streaming and communications [20]. In video surveillance, the compression must take care of the bandwidth and the storage requirements.

1.4.4 Environmental Constraints

Scene lighting has an effect on the performance of any color video security systems. Regardless of application, Indoor or outdoor, the amount of obtainable light and its color energy spectrum must be measured, evaluated, and compared with the sensitivity of the cameras to be used [3]. Natural, as well as artificial lighting should be adopted depending on the nature of the surveillance scene and the time: –day or night. Good lighting also impacts the fps setting needed. Better lighting would necessitate less frames per second needed and vice versa. Weather constraints can adversely affect the performance of cameras.

A cloud cover weather condition causes a loss in light intensity and it reduces the reflections required for video capture. Extreme sunny weather cause dazzle [18]; while fog, rain, mist and snow too can affect the quality of captured video images. Though algorithms have been developed to mitigate the effects of weather, there are still some challenges posed by the weather.

1.4.5 Power Supply

The majority of IP Camera components operate from the 12-VDC supplied by wall-mounted AC-DC power supplies [3]. The AC source varies from country to country. In the USA, the power supply varies from 90-130V, with a nominal value of 117V at 60Hz frequency; while in the UK and in most Commonwealth countries, the power source varies from 200-250V, with a nominal voltage of 220 at 50Hz frequency [3]. The biggest challenge with the power supply in most developing countries is that power is available only for limited time periods due to power outages, load-shedding and in some cases, under voltage supply. For video surveillance applications,

alternative power supplies should be provided in the form of batteries, solar and diesel-powered generators.

1.5 Problem Statement

Traditional wired CCTV systems require the extensive use of cables and other accompanying accessories, to cover a wide area, a cost not easily attainable and sustainable for most developing countries in Africa and elsewhere. Furthermore, wired systems are prone to vandalism; they cannot be installed in rocky areas and old buildings, whose nature makes it unsuitable for cable installations. In the light of the above, the problem statement is as follows:

a) Existing WiMAX-based video surveillance systems can cover a wide area, guarantees Quality of Service (QoS); but WiMAX cameras tend to be costly. In addition, these systems are not scalable; as only one camera connects to one uplink channel. Therefore, these systems do not make efficient use of the uplink channel.
b) Wi-Fi-based video surveillance systems have the advantage of wide Wi-Fi camera deployment; but they are limited by coverage area. Cameras in Wi-Fi networks perform poorly when transmitting signals while in motion.
c) Surveillance in blind spots [areas not covered by a wired surveillance system] and low-bandwidth Wi-Fi environments remain a challenge; because of the wireless nature of the transmission channel.

We propose a hybrid WIMAX-WiFi solution with Wi-Fi wireless mesh extension, to exploit the advantages of the two wireless network technologies, for video surveillance applications.

1.6 Motivation for the Research

With the ever-increasing incidents of crime in public and private places, such as bus and train stations, shopping malls, parking lots and airports, etc.; research in video surveillance systems continues to attract interest. Furthermore, wireless surveillance systems have received narrow acceptance regarding deployment in most organisations and industries due to the bandwidth limitations, the reduced throughput and packet loss. The world has not fully utilised mobile devices, such as smartphones, as tools for surveillance.

The research is also expected to contribute to the technological growth of the unified communication of wireless networks and wider acceptance by all the stakeholders.

1.7 Research Objectives

The main objective of this research is to:

> Develop a reliable model for a Hybrid WiMAX-WiFi Video surveillance system with improved performance

The specific objectives are to:

1) Propose the mathematical performance models and video transmission algorithm, and to investigate the performance of WiMAX and hybrid WiMAX-WiFi video surveillance systems, including one with mesh extension, for varying numbers of wireless IP cameras and determine the optimum number of cameras per CPE.
2) Propose the mobility algorithm and investigate the effect of mobility on performance for hybrid WiMAX-WiFi video surveillance system consisting of mobile cameras, moving at normal human walking speed.
3) Propose a software application algorithm for cell phones, and to develop the low bandwidth application software for hybrid WiMAX-WiFi, or cellular networks that can be installed on smart mobile devices. The application must be able to route the captured images/video and transmit this to the server for monitoring and identification.

1.8 The Research Hypotheses

The hypotheses are stated as follows:

(a) Mesh hybrid WiMAX-WiFi system performs better than the non-meshed equivalent system.

(b) Up to normal human walking speed, a mobile camera transmits surveillance images/videos and achieves nearly the same throughput as when it is stationary.

1.9 The Research Questions

In this research, we address some of the questions regarding the proposed hybrid WiMAX-WiFi video surveillance system models. The fundamental questions at the core of this research are:

1) How does an unmeshed WiMAX-WiFi network perform in comparison with meshed WiMAX-WiFi under varying numbers of nodes or cameras? Does the hybrid system give a better link and Signal-to- Noise ratio when compared with the baseline WiMAX surveillance system?
2) What factors determine throughput in mobile WiMAX-WiFi surveillance systems? What is the effect of mobility on the performance of a hybrid WiMAX-WiFi surveillance system?
3) Can we develop low bandwidth application software that can be used to provide mobile surveillance, when using a smart device like a Smartphone? If so, to what extent can the developed software be used to transmit images/videos on a WiMAX-WiFi surveillance or cellular network?

1.10 Contributions of this Thesis

In this research, we have made the following contributions:

a) Developed a detailed model and video transmission algorithm of a hybrid WiMAX-WiFi video surveillance and carried out a performance comparison of the WiMAX and hybrid WiMAX-WiFi video surveillance systems. Additionally, the research has investigated the optimum number of cameras to be connected on hybrid WiMAX-WiFi surveillance - given the measured throughput values, and taking into consideration the network bandwidth requirements.

b) Proposed and implemented a traffic-flow (throughput) algorithm; investigated the effect of mobility on the performance of a hybrid WiMAX-WiFi surveillance system. The optimum human walking speed range, while transmitting surveillance images/videos, for improved performance across all age groups has been ascertained.

c) Developed and implemented a software algorithm for low bandwidth mobile wireless surveillance application software for the hybrid WiMAX-WiFi video

surveillance system; that can be installed in mobile cameras or mobile devices such as smartphones. The developed application can route the captured and compressed surveillance images/ video to the server on a WiMAX-WiFi or a cellular network.

1.11 Scope of the Thesis

This thesis is limited to wireless IP video surveillance systems for hybrid WiMAX-WiFi networks. We also focus the application of the developed video application on the hybrid WiMAX-WiFi network- even though its implementation can extend to 3G and 4G cellular networks. Mobile devices with camera functionality operating in a low bandwidth wireless environment are specifically targeted. This research has a particular focus on mitigating crime in most developing countries-especially in areas that are prone to vandalism and those in which it would not be possible to lay cables due to the hostile terrain.

1.12 Chapter Outline

The remainder of the thesis is organised as follows:

Chapter Two: Provides detailed literature reviews on WiMAX and WiMAX-WiFi networks, the underlying network architecture for WiMAX and hybrid WiMAX-WiFi video surveillance systems. Standards for WiMAX and Wi-Fi network and the benefits of WiMAX-WiFi integration, including QoS provisions for WiMAX, have been discussed. The chapter also discusses the motivation towards use of WiMAX-WiFi networks in IP video surveillance and performance metrics, like jitter, end-to-end delay, Signal-to-Noise Ratio and throughput.

Chapter Three: Describes the proposed meshed and unmeshed WiMAX-WiFi video surveillance models. Various elements and devices of such systems have been explained. A detailed description of the proposed and implemented hybrid WiMAX-WiFi video surveillance traffic flow (throughput) models and an algorithm for valid video transmission for these models have been made. Other performance metrics, such as link utilisation and packet loss have

also been described. The performances of the proposed hybrid WiMAX-WiFi models are compared with that of the baseline WiMAX video surveillance models through simulations in OPNET. All the cameras are transmitting to the remote server.

Chapter Four: Describes the proposed and implemented hybrid WiMAX-WiFi video surveillance network model with mobile camera devices. The chapter derives the mathematical model for throughput and proposes a new performance algorithm for mobile cameras connected to a hybrid WiMAX-WiFi network. An analysis of the results on the effect of mobility in a mobile WiMAX-WiFi surveillance system, with mobile devices employing the H.265/HEVC encoder has been given for proof of concept. The mobile system results are evaluated for various mobility velocities and the optimum speed for improved performance suggested, through simulation in OPNET. The performance metrics comprise: throughput, dropped bits, link utilisation, end-to-end delay and jitter.

Chapter Five: Describes some of the conventional software development process models and gives related work on surveillance application software. The chapter then proposes a model for mobile surveillance application development. A new algorithm for surveillance software that is suitable for a low bandwidth Wi-Fi environment is proposed. The implementation processes of the proposed new algorithm from the modelling of the software, construction using Android Studio and final deployment has been described and evaluated in detail. This chapter also gives the test results for the deployed application software.

Chapter Six: Gives the summary of the research, its conclusion, and some recommendations, based on the simulations and the experimental results obtained. Finally, some potential future work is also proposed.

Chapter Two

2 Fixed and Mobile WiMAX Networks

This chapter describes WiMAX and hybrid WiMAX-WiFi networks, the underlying network architecture for WiMAX and hybrid WiMAX-WiFi video surveillance systems which are discussed in Chapters Three and Four. Section 2.1 explains the various units and sub-units that comprise a WiMAX networks. These units include the Subscriber Station (SS), the Access Service Network (ASN), the Connectivity Service Network (CSN), Mobile Stations (MS) and Wireless Mesh Routers (WMR). Various interfaces between these units are also explained. Section 2.2 and section 2.3 discuss the WiMAX MAC layer protocols and Quality of Service classes, respectively.

In section 2.4 the common Institute of Electrical and Electronics Engineers' (IEEE) standards for WiMAX networks are explained. The use/application of WiMAX network in IP video surveillance is discussed in section 2.5; while section 2.6 explains the hybrid WiMAX-WiFi network. A description of Wi-Fi and Wi-Fi standard follows in section 2.7 with section 2.8 discussing the motivation towards WiMAX/WiFi video surveillance. Some of the performance metrics in video surveillance are discussed in section 2.9. Finally, section 2.10 give the overall WiMAX and WiMAX-WiFi video surveillance implementation focus; and the chapter summary follows in section 2.11.

2.1 Fixed and Mobile WiMAX Network Architecture

In general, there are two types of WiMAX networks: the Fixed and the Mobile WiMAX networks. 'Fixed' is used here in the context of fixed end nodes and 'mobile' in the context of mobile end nodes. The fixed WiMAX is divided into two parts: one in which all the fixed nodes connect directly to the Base Station (BS), and the other in which the fixed nodes connect to the BS via the Customer Premises Equipment (CPE). The mobile WiMAX is also divided into two parts: one in which the mobile nodes connect directly to the BS and the other in which the mobile nodes connect to the BS via the CPE.

Recently, there have been improvements to the advanced WiMAX, which uses a Time Division Duplexing (TDD) technique and is compatible with LTE [21]. The

discussion on LTE is beyond the scope of this work. The CPE is an interface device for WiMAX and Wi-Fi wireless technology; that is, it has two radio links-one for WiMAX, and the other for Wi-Fi.

WiMAX is designed to support a theoretical throughput of 75Mbps for fixed wireless Metropolitan Access Networks (MAN). However, in practice, it can only support up to 10 Mbps for a distance of around 10 km, line-of-sight [22].

WiMAX also supports mobility for WiMAX MS at vehicular velocities [23]. For mobile wireless communication, the throughput falls drastically, to less than 1 Mbps, when the mobile nodes speed is 100 km/hr [24]. Such a fall in throughput at that speed is attributed to multipath fading due to many objects that surround the receiver and/ or transmitter. These objects reflect and diffract the original signal thereby causing overlap of multiple copies of transmitted signal, each differing in attenuation, delay and phase shift, at the receiver. Signal overlap also creates interferences, attenuation or amplification of the received signal power [21]. In addition, WiMAX offers high scalability and rapid deployment [22].

Figure 2.1 below shows the detailed network architecture for WiMAX and hybrid WiMAX-Wi-Fi networks.

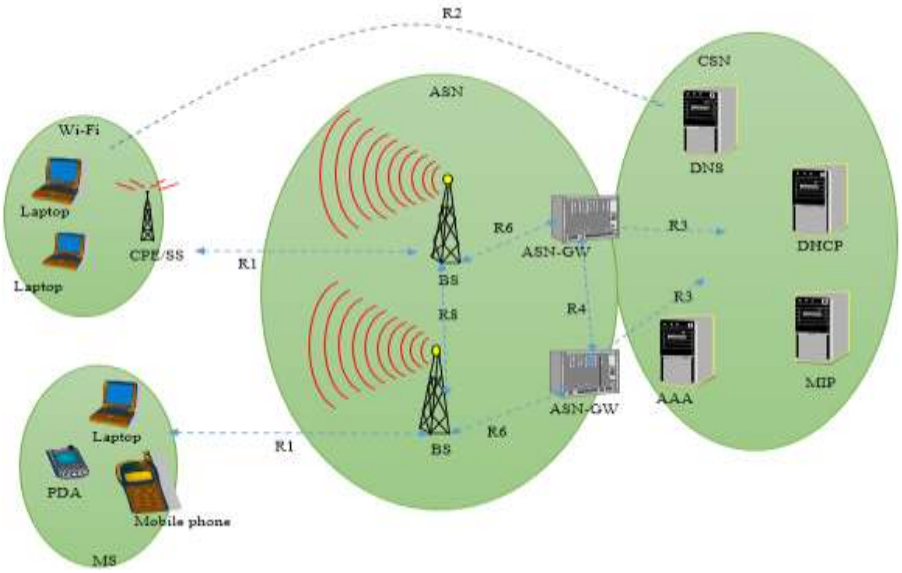

Figure 2.1: WiMAX and hybrid WiMAX-WiFi Network Architecture

The architecture for fixed and mobile WiMAX is similar, except that mobile WiMAX operates under IEEE 802.16e standard; while fixed WiMAX uses IEEE 802.16d standard on the WiMAX link. From the fixed and the mobile WiMAX architecture, the hybrid WiMAX-WiFi architecture can also be realised.

The fixed WiMAX architecture can be an all WiMAX network, in which the end devices communicate with the BS. It can also be one, in which the fixed end-devices communicate with the BS via the CPE, and form the hybrid WiMAX-WiFi network. The end-nodes may be fixed cameras, desktop computers, etc. The devices should have WiMAX interface cards or a radio link for communication with the BS.

The mobile WiMAX architecture can be an all WiMAX network in which end devices communicate with the BS; or one, in which the mobile nodes connect with the WiMAX link via the CPE. Examples of such devices include the MS or phones, laptops and cameras on mobile devices. MSs are mobile user equipments and may be located in the premises or outside the premises of the user. They communicate directly to the BS.

2.1.1 Access Service Network

The ASN consists of a single or several BSs, and the gateway routers to the connectivity service network. It provides service access to the MS. The BS could be stand-alone towers, or their antennas mounted on rooftops of multi-storey buildings, or other elevated structures such as water towers, grain silos, etc [25]. Alternatively, the BS may be mounted on a vehicle in those places, where it is not practical to erect fixed structures [26].

The role of the BS is to manage radio resources for the WiMAX network, provide the air interface to the SS and MS and to provide connectivity between the network service provider equipment and the subscriber stations. Additional, it provides micro-mobility management functions, such as traffic classification, radio resource management, session management, handoff triggering and QoS policy enforcement.

Within the ASN, all traffic is aggregated at the ASN gateway (ASN-GW). The ASN-GW may also provide other functions such as admission control, radio resource management, management of user profiles and encryption keys.

The ASN forms the Network Access Provider (NAP) sub-system. The NAP subsystem provides connectivity between the end-user and the network service provide. This sub-system house the: Foreign Access and Home Access service system units, as well as the BS and the ASN-Gateway.

2.1.2 The Connectivity Service Network

The CSN provides the Internet connections to the WiMAX radio equipment [27]. It has various modules and sub-units; such as the Authentication, Accounting and Authorization (AAA) Modules, Dynamic Host Control Protocol (DHCP), DNS and the Home Agent (HA). The CSN provides authentication, accounting and authorization through the AAA server. The CSN's DNS/DHCP server provides IP address allocation for end-user devices; while its Home Agent (HA) provides Mobile-IP functionality [28].

Other functions include [28] : (1) subscriber billing and inter-operator payment; (2) supporting communication between Network Access Providers; (3) Inter-ASN mobility administration between Access Service Network s (4) controlling of policies for Internet access [23].

The CSN is contained within the Network Service Provider (NSP) subsystem. The NSP subsystem provides a link between the Internet and the network access provider sub-systems. It consists of home and visitor connectivity service network modules. The NAP and NSP subsystems provide a link between the end user and the Internet. In between these sub-systems and units are the interfaces R1 to R8 [28].

2.1.3 Interfaces R1 to R8

The R1 interfaces with the MS or CPE and the ASN. The R2 is the logical interface between the MS or CPE and the CSN. It is associated with Service Authentication, Authorization, IP Host Configuration management, and mobility management [29]. The R3 interfaces the ASN and the CSN. It supports Authentication, Accounting and Authorization, and enforcement of policies including mobility management. It also covers the bearer- plane methods, such as tunnelling – to transfer the IP data between modules [29].

The R4 interface consists of the control and the bearer plane protocols from/to various modules inside the ASN that co-ordinate mobility among MSs between ASNs. The R5 interfaces the CSNs and the home or visited Network Service Provider. The R6 interface comprises the control and the bearer-plane protocols which the ASN-GW and the BSs use for intra-communication.

The R8 consists of the control-plane and, sometimes, the bearer-plane data flows within the ASN that ensures speedy and flawless handover [29].

2.2 WiMAX MAC Scheduler Service Types

The WiMAX MAC QoS scheduler accommodates five QoS classes: the Unsolicited Grant Service; the Real-Time Polling Service; the Non-real-time Polling Service; the Best Effort; and the Extended Real-Time Polling Service. Table 2.1 summarises the five QoS classes.

Table 2.1: **MAC Scheduler Service Types** [30]**.**

Scheduler Service	**Application**	**Specification**
Unsolicited Grant Service (UGS)	-VoIP without silence suppression -T1/E1 emulation -Continuous bit rate applications (No polling – fixed bandwidth)	Max. sustained rate Max. latency tolerance Jitter tolerance
real time Polling Service (rtPS)	Streaming audio and/or video Variable bit rate applications (MS is polled regularly)	Max. sustained rate Min. reserved rate Max latency tolerance Traffic priority
extended rtPS (ErtPS)	VoIP with silence suppression (No polling dynamic bandwidth)	Max. sustained rate Min. reserved rate Max. latency tolerance Jitter tolerance Traffic priority
non rtPS (nrtPS)	FTP (MS is polled periodically)	Max. sustained rate Min. reserved rate Traffic priority
Best Effort (BE)	Web browsing Data transfer (MS must request all bandwidth)	Max. sustained rate Traffic priority

Unsolicited Grant Service (UGS): The UGS class is intended to support real-time service flows, which create fixed-size data packets periodically [30]. Examples of such services include T1/E1 and Voice over IP with no subdued silence. The BS gives the specified size of unsolicited data grants without any request from the SS at periodic intervals. Consequently, the overhead and latency of the SS requests are eliminated; since the SS does not make any bandwidth requests.

Real-Time Polling Service (rtPS): For real-time polling service and variable data packets, such as MPEG, H.265/HEVC, H.264/AVC videos including T1/E1 type data service, the rtPS is ideal [30]. The rtPS supports real-time uplink service flows. The SS must request and specify the size of the desired grant, even though it still supports the variable grant size. The weakness of this class is that the overheads and the latency increase due to the SS‘s requests.

Non-real-time Polling Service (nrtPS): The nrtPS QoS class supports latency-tolerant data types consisting of variably sized data packets. Such data must specify the minimum data rate [30]. A handy example of service type is the File Transfer Protocol (FTP) service. This service is best for unicast polls, which are regularly transmitted to ensure and assure service flow even during network congestion times. Thus, in every interval of 1s or even less, the BS grants unicast polls to nrtPS connections [30]. The SS in the non-real time polling service, like the real-time polling service, requests bandwidth, except that nrtPS may utilise random access transmission opportunities for sending the bandwidth requests.

Best Effort (BE): The BE QoS services class is best for applications that do not have any specific delay requirements. The BE supports data streams and provides a scheduling service, for which no minimum resources allocations are granted [30]. Every service is considered based on the available space. Thus, the BE services do not guarantee QoS. Examples include an email, or the short length FTP. The SS in BE service must also request bandwidth from the BS.

Extended Real-Time Polling Service (ErtPS): The ErtPS is intended to sustain real-time service flows that, periodically, generate variable-sized data packets. An example of this service type is the Voice over IP services with silence suppression [30]. The

ErtPS combines some characteristics of UGS and rtPS. The BS gives the variable size of unsolicited data grants without any request from the SS at periodic intervals [30].

2.3 WiMAX MAC Layer Protocols

The WiMAX IEEE 802.16 standard specifies Point-to-Multipoint (P2MP) and optional mesh, as sharing modes for the wireless medium. In both modes, communications are subdivided into 0.5ms, 1ms or 2ms frames. The IEEE 802.16 MAC allows for bandwidth bid, and it is therefore connection-oriented.

In the P2MP mode, the BS acts as a star point; and it coordinates all the uplink and downlink communication by the SS and the BS. During uplink, the SS requests bandwidth by the contention and the polling (contention free) modes. In the contention mode, during the predefined contention window, the SS requests bandwidth from the BS. When multiple SS requires this bandwidth at the same time, a back-off mechanism handles all the contention and the bandwidth is allocated, according to a set quality of service schedule. In contention-free mode, the BS allocates bandwidth request for each active SS.

In the mesh approach, the BS and SS nodes are organised in an *ad hoc* manner. The SS communicate directly with each other and the BS. The mesh nodes that connect directly to the backhaul network are called mesh BSs. The communication arrangement among nodes, can be shared equally [15].

2.4 WiMAX/IEEE 802.16 Standard

The WiMAX standards have, in the last 15 years evolved regarding application, operating frequencies and multiplexing technology:

In 2001, the primary WiMAX standard IEEE 802.16 was established to provide wireless access to broadband coverage [11]. The WiMAX networks could operate in the licensed frequency band of 10 to 66GHz [11]. For efficient operation, a clear line-of-sight propagation was needed between the BS and the end-user. Typically, the data rate of 12Mbps or less is/ was attainable, although up to 70 to 134Mbps data rate could be achieved. In a P2MP topology, a maximum of 50km coverage radius can also be achieved. Later standards superseded this standard.

The IEEE 802.16a standard was established in 2003. It is a standard applicable to both line-of-sight and non-line-of-sight environments. It operates in the 2 to 11GHz licensed and non-licensed frequency bands. Like its predecessor, the radius coverage of about 50km from the BS and a data rate of less than 70Mbps are achievable. Topologically, it can be configured for both P2MP and mesh topologies. It was followed by IEEE 802.16b standard, which operates in the 5 to 6GHz frequency band. This standard was superseded by the IEEE 802.16d.

The IEEE 802.16c was established in 2002, a year earlier than the establishment of IEEE 802.16a and IEEE 802.16b standards. The 10 to 66GHz frequency band is its frequency band. It has also been superseded and replaced by the IEEE 802.16d standard. The IEEE 802.16d standard was established in 2004, as an amendment to IEEE 802.16a/b/c. It has a data rate of 70Mbps with P2MP and has mesh topology configurations.

In 2005, the IEEE 802.16e standard was formulated as an enhancement to the IEEE 802.16d standard. It is also called the mobile wireless MAN or the mobile WiMAX; it is applicable in non-line of sight environments. It has a data rate of 15Mbps and better support for QoS. Other important features of this standard include: Orthogonal Frequency Division Multiple Access (OFDMA) modulation schemes [13]; and it operates between 2 to 6GHz licensed frequency band [1] [13]; with typical frequencies of 2.3, 2.5 and 3.5GHz bands. It supports devices, such as the mobile phones, Personal Data Assistant (PDA), Note Book and Laptops for accessing Internet. It also supports the Multiple-Input Multiple-Output (MIMO) antennas at the transmitter, and at the receiver, for improving the spectral efficiency.

The other WiMAX standard is IEEE 802.16m. It has a maximum data rate of 100Mbps for mobile stations and 1Gbps for fixed stations. The IEEE 802.16m standard covers a distance of up to 100km [14].

2.5 Application of WiMAX Networks in Video Surveillance

WiMAX networks discussed in section 2.1 have been deployed for various applications and services. WiMAX networks have also been used for video surveillances applications. One such applications scenario is where WiMAX cameras are mounted at various points such as highway for monitoring vehicle traffic offences

[31]. Others include but not limited to monitoring of forest fires and control of cutting of trees; and monitoring of animals in game parks. In the medical field WiMAX network have been used for sending surveillance images in emergency and disaster hit areas; whereby medical personnel at a disaster location would capture medical images and send to the nearest health centre for further advice and diagnosis [31]. The medical personnel at the health centre would then send prescribed course of action and treatment back to the disaster location via WiMAX network based video surveillance system. Other applications include flood monitoring, telemetric and telemetry [31]

Figure 2.2 shows a typical WiMAX network used for video surveillance. The WiMAX camera could be fixed on some pole, building, tree and the like or mounted on a vehicle or helicopter or drone. Other applications include flood monitoring, telemetric and telemetry [31]

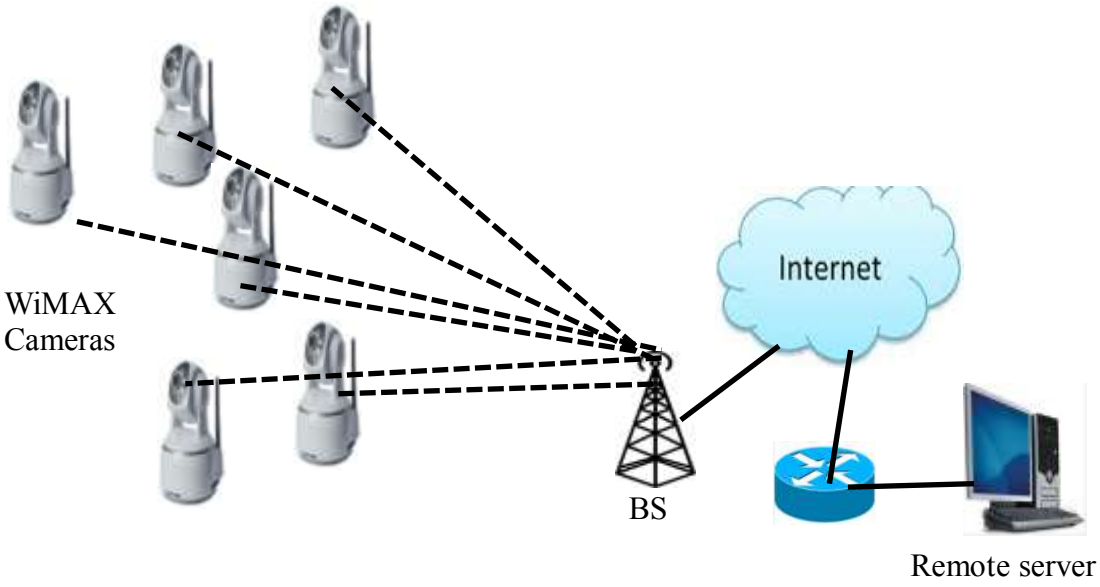

Figure 2.2: WiMAX Network used for Video Surveillance

Other applications of WiMAX technology include provision of high speed data, voice and video communications services as backhaul network. Wi-Fi hotspot and cellular networks can benefit from WiMAX technology QoS in which case WiMAX technology would be used to formulate backhaul network.

2.6 Hybrid WiMAX-WiFi Network

The hybrid WiMAX-WiFi network architecture consists of two basic units: the ASN and the CSN as discussed in section 2.1. However, the additional SS, also called the

CPE, makes this network unique. The SS unit resembles the MS in many respects. The heterogeneity between the Wi-Fi and WiMAX technologies occurs in the SS unit.

The SS, also called the CPE is the equipment installed at the customers' premises. It can be configured in the same way as the MS to connect to the base station. A mobile station is designed to move up to vehicular velocities. The MS, unlike the SS, is generally battery powered [26]. The SS has additional Wi-Fi interfaces, and in some cases, Ethernet interfaces, for connecting to the end-nodes.

One or more end-nodes can be connected to the CPE by using a Category 5 or 6 Ethernet cable, or wirelessly using the unlicensed frequency bands of the IEEE 802.11 family of standards. The typical node-to-CPE distance is 50-300m, depending on the Wi-Fi standard adopted. The CPE is similar to the access point of Wi-Fi networks. The Wi-Fi part of the hybrid WiMAX-Wi-Fi can further be meshed to increase scalability by using WMRs.

2.7 Wi-Fi/IEEE 802.11 Standard

Bernarji et al. [32] state that there are three well known IEEE 802.11 standards: IEEE 802.11a, IEEE 802.11b and IEEE 802.11g. These standards operates in the unlicensed Industrial, Scientific and Medical (ISM) frequency bands.

The IEEE 802.11a operates in the 5GHz frequency band. It uses l OFDM; and it has a data rate of 54Mbps with less signal interference, a coverage range of 50m; also it has the same MAC layer as IEEE 802.11b. When it comes to deployment, its principal drawback in comparison with IEEE 802.11b/g is its compatibility; since it works on a different frequency band [32].

IEEE 802.11b is the most widely deployed wireless standard family. It operates in the 2.4GHz frequency unlicensed band, and has a coverage distance of 100m, with a data rate of 11Mbps [32]. It uses a Direct Sequence Spread Spectrum (DSSS), a more reliable modulation technique than Frequency Hopping Spread Spectrum (FHSS).

Like the IEEE 802.11b, the IEEE 802.11g operates in the 2.4GHz unlicensed frequency band; and it has a coverage distance of 100m. However, it has a data rate of 54Mbps; and it uses Orthogonal Frequency Division Multiplexing (OFDM) [32]. Therefore, IEEE 802.11g has a backwards compatibility with IEEE 802.11b.

Other IEEE 802.11 standards include IEEE 802.11e/f/i/n. This work discusses the WiMAX-WiFi surveillance models; and it is restricted to the IEEE 802.11a/b/g as described above.

2.8 Motivation towards WiMAX and Wi-Fi Video Surveillance

There are several motivating factors towards the use of WiMAX-WiFi in video surveillance systems today. WiMAX technology offers the following strengths:

- **Support for both Line of Sight (LoS) and Non Line of Signt (NLoS)** -WiMAX is suitable for ubiquitous service offering in both rural and urban areas because of its ability to support both LoS and NLoS connections[30].
- **High speed and wide bandwidth**-WiMAX provides high speed and wide bandwidth. This facilitates delivery of real time applications such as video faster than other technologies and best satisfies the needs of individual and enterprises customers. Cellular coverage makes its deployment extremely fast and relatively inexpensive [30].
- **Support for existing services and applications**- Several real-time services and applications are already provided on WiMAX networks. Thus applications which already exist on wired networks are classified under service classes and listed in Table 2.1 of section 2.2 [30].
- **Qos guarantees** – WiMAX video surveillance systems benefit from the QoS guarantee provisioning provided by WiMAX networks. For example, the real-time packet service (rtPS) guarantees the minimum reserved and maximum sustained rate, maximum latency tolerance and prioritise video traffic; which are some of the key requirements for video surveillance [32]. Other technologies such as WCDMA or 3G have limited support for QoS and higher priority traffic may completely starve lower priority traffic during periods of high usage [30].
- **All IP Solution -** Another important advantage of WiMAX is that it is an all IP solution and therefore benefits from all the advantages of packet switching. In contrast, 3G is not an all IP solution, though IP is overlaid and mapped on the underlying circuit-switched core layer. The mapping point in the core layer can be far away from the delivery point, creating queuing and scheduling inefficiencies [30].

- **OFDMA and adaptive modulation** - Like LTE, WiMAX uses the efficient OFDMA and adaptive modulation at physical layer, the two advantages that are missing in 3G systems [30].

However, WiMAX technology/networks have limited WiMAX IP camera deployment and configuration options to the access layer, among others.

Wi-Fi technology has advantages that enable it to be used for video surveillance:

- ✓ **Wider deployment** - Wi-Fi is among the most deployed wireless technologies in the world owing to its simplicity and flexibility [30]. Wi-Fi devices, including Wi-Fi IP cameras, are cost effective.

- ✓ **Ubiguitious Communication** -This technology provides people with a ubiquitous communication. Users now require receiving high-speed video, audio, voice and web services even when they are moving in offices or travelling around campus.

However, Wi-Fi suffers from the challenges of packet loss, unguaranteed quality of service, reduced throughput and coverage radius. Another disadvantage that Wi-Fi , including WCDMA and LTE, is that the MAC uses acknowledgements which results in delays and overhead. High Speed Downlink Packet Access *(*HSDPA), a 3G, technology includes Hybrid Automatic Repeat reQuest (Hybrid ARQ or HARQ) to allow it to dynamically adjust to network conditions, but lacks the flexibility possessed by WiMAX. In addition, the channel size is fixed, unlike in WiMAX where the channel size is changeable [30].

The hybrid WiMAX-WiFi systems exploit the advantages of both wireless network technologies.

2.9 Performance Metrics

2.9.1 Theoretical Maximum Throughput at the CPE

A Wi-Fi video surveillance system throughput is the fraction of the time that a channel uses successfully to transmit MAC Service Data Units (MSDU) payload bits [33]. Alternatively, it is the number of successful payload bits transmitted per unit time or per second [33] [34]. In video surveillance, cameras send the payload bits in the network. In hybrid WiMAX-WiFi network throughput is the sum of the data rates

delivered to the AP or the CPE from IP Cameras [35]. For a star topology, we can derive this theoretical maximum throughput ($S_{flow_{CPE}}$ in bps) mathematically as [36]:

$$S_{TM} = \frac{E}{t} \quad bps \tag{2.4}$$

Where: E is the MSDU payload in bits and t is the delay in the MSDU payload.
For Wi-Fi, the MSDU payload in bits can be written as:

$$E = (8x) \quad bits \tag{2.5}$$

The variable x is the byte length equal to *FS* as derived from equation (1.8) while the constant, 8, arises because there are eight bits in one byte. The delay in the MSDU payload is computed on the basis of the type of Wi-Fi transmission MAC scheme; either Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) or Request To Send/ Clear To Send (RTS/CTS). The choice between CSMA/CA and RTS/CTS depends on what link constraints should be considered. The CSMA/CA has an asymmetrical MAC layer; and therefore, it has asymmetrical link constraints; while the RTS/CTS has regular ones [37].

In general, delay (*t*) in seconds in the MSDU payload is given as:

$$t = \left(t_{DIFS} + t_{SOFS} + t_{Bo} + t_{RTS} + t_{CTS} + t_{Ack} + t_{Data}\right) \times 10^{-6} \quad s \tag{2.6}$$

The delay constitutes the Back off (Bo), the Acknowledgement (Ack), Request To Send (RTS), Clear To Send (CTS), Data, Distributed Inter Frame Spacing (DIFS) and Short Inter Frame Spacing (SIFS). For a CSMA/CA, the RTS and CTS delay components are excluded. The individual delay component values have been calculated in the work of [36]. The total delay per MSDU is simplified to a function of the MSDU size in bytes, x as:

$$t = \left(ax + b\right) \times 10^{-6} \quad s \tag{2.7}$$

The theoretical maximum throughput (in *bps*) for equation (2.4) can be calculated from [36]:

$$S_{TM} = \frac{8x}{ax + b} \times 10^{6} \qquad bps \tag{2.8}$$

Where, the variable x is the byte length as in equation (2.5); the constants a and b depend on the type of CSMA/CA or RTS/CTS scheme used. The constant a is the sum of the delay component that affect the data rate while b is the sum of all the delay

components that that do not depend on the MSDU **and are** not affected by the data rate**.** A table summarizing the constants a and b for the two MAC schemes was put forth in the work of [36]; and it is given in Table 2.2 and Table 2.3.

Table 2.2: **Summary of the Constants a and b for the RTS/CTS MAC Schemes**

RTS/CTS	**Data Rate (Mbps)**	a	b
FHSS	1	8.25	1763.5
	2	4.125	1623.25
DSSS	1	8	1814
	2	4	1678
HR-DSSS	5.5	1.45455	1591.45
	11	0.72727	1566.73
OFDM	6	1.33333	337.5
	12	0.6667	273
	24	0.33333	244.75
	56	0.14815	225.94

Table 2.3: Summary of the Constants a and b for the CSMA/CA MAC Schemes

CSMA/CA	**Data Rate (Mbps)**	a	b
FHSS	1	8.25	1179.5
	2	4.125	1039.25
DSSS	1	8	1138
	2	4	1002
HR-DSSS	5.5	1.45455	915.45
	11	0.72727	890.73
OFDM	6	1.33333	223.5
	12	0.6667	187
	24	0.33333	170.75
	56	0.14815	159.94

2.9.2 Signal-to-Noise Ratio

The Signal-to-Noise Ratio (SNR) is the ratio of the measured signal power, E_b to the noise power, N_o within a given communication channel.

$$SNR = \frac{E_b}{N_o}$$

This ratio can be expressed in decibels.

$$SNR = 10Log\frac{E_b}{N_o} \tag{2.8}$$

The noise component may include background and interference noise. The background noise considers galactic, urban, or thermal noise. The interference noise is the noise attributed to signals in the transmission channels that the receiver cannot

decode [9]. They include electromagnetic adjacent channel, inter-symbol and co-channel interferences among others. Interference sources on a video sequence includes thermal noise in the camera, acquisition noise, noise added by the transmitting antenna. The WiMAX receiver separates the valid received signal power from the aggregated background and interference noise [9].

2.9.3 Average End-to-end Delay

Average end-to-end delay or latency, is the transmission time of packets from a sender all the way to the receiver. In IP video systems, there is usually some latency between the actual event being captured, and when the image appears on a monitor [9] at the receiver.

The causes of such delays could be source processing, propagation, transmission and network delays [38]. Other delay causes are: queuing, switching, decoding and buffering delays. In traffic engineering, delay is a function of the number of source nodes on the network. The higher the number of source nodes, the greater would be the number of packets on a given channel and route.

End- to-end delay is essentially the ratio of the difference between the times taken for the packet to move from the source to the destination to the total number of packets received. It can be calculated from equation (2.9) [39].

$$Delay_{average} = \frac{\sum_P ATime_p - STime_p}{n_p} \quad \text{s} \tag{2.9}$$

Where $ATime_p$ is the time when the packet p arrives at the destination and $STime_p$ is the time when the packet p leaves the source and n_p is the total number of packets [38]. Thus, n_p depends on the number of nodes N. Each CPE or MR has one or more source nodes associated with it. High end-to-end delay values signify network congestions and therefore indicate lower efficiency of the communication protocols [39].

2.9.4 Average Jitter

Jitter is the variation in the time between packet arrivals. Alternatively, jitter is the absolute value of the delay difference between selected packets [40]. It is a measure of system consistency and the stability of the network. Jitter is caused when packets

arrive at different times due to different queuing times or due to the different routes taken by the communications[30]. Jitter results in the intermittent video image display. The video application endeavours to buffer the video to minimise jitter by gathering and combining several inbound packets. When the buffer threshold of the stored packets is reached, the application processes the packets, and the video image is displayed smoothly. If we consider two consecutive packets having time stamps t_1 and t_2 leaving the source nodes to the destination at time stamps t_3 and t_4, then the jitter would be given by [41]:

$$Jitter = (t_4 - t_3) - (t_2 - t_1)\ s \tag{2.10}$$

If the source node time-stamp intervals are higher than the destination node time-stamp interval, then the jitter is said to be negative jitter [41] *i.e.*,

$$NegativeJitter = (t_2 - t_1) - (t_4 - t_3) \tag{2.11}$$

This value must be, on average, less than 60ms in one-way packet transmission; and ideally, it should be less than10ms [40].

2.10 Overall IP Video Surveillance Implementation

We set up the three hybrid WiMAX-WiFi transmission network: Unmeshed WiMAX-WiFi, meshed WiMAX-WiFi, and the mobile WiMAX-WiFi, as proposed in the models of Chapters Three and Four. The three models were compared to the existing WiMAX model for fixed and mobile cameras. In implementing the models in OPNET simulator, we used the wireless workstation to represent Wi-Fi IP cameras; since OPNET does not have a particular node for wireless IP cameras. Figure 2.3 shows the overall structure of the implemented systems.

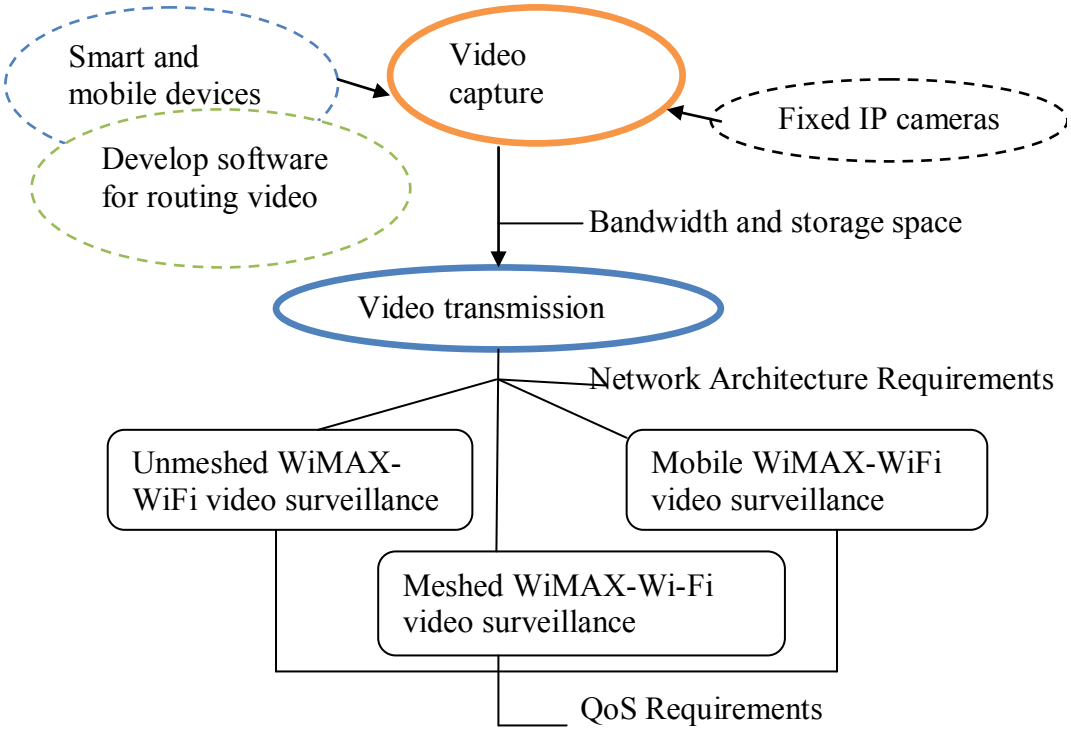

Figure 2.3: WiMAX-WiFi IP Video Surveillance Implementation

2.11 Chapter Summary

This chapter has presented the detailed description of the WiMAX and hybrid WiMAX-WiFi networks, including the appropriate WiMAX and Wi-Fi IEEE standards. This literature review framework is important in understanding the video surveillance models developed in Chapters Three, Four and Five. Specific WiMAX and hybrid WiMAX-WiFi network sub-units and elements, like the CPE, ASN, CSN, BS and interfaces have been described.

The literature review has shown that it is possible to exploit the advantages of WiMAX and Wi-Fi technologies, to achieve a hybrid system that has higher throughput, guaranteed quality of service yet be easily deployed to cover both long and short distances. Various QoS classes have been discussed to understand how WiMAX prioritises different data types, video inclusive. Typical performance metrics such as the delay, the jitter and the throughput have been discussed. Finally, a description of IP video surveillance requirements and overall WiMAX and WiMAX-WiFi video surveillance implementation focus, as described in the next three chapters, has been made.

Chapter Three

3 Hybrid WiMAX-WiFi Video Surveillance Systems

This chapter builds on Chapter Two; and it compares the performance of existing WiMAX surveillance models with the two hybrid WiMAX-WiFi surveillance models, the meshed and the unmeshed. The comparison is relevant in determining the application of the hybrid WiMAX-WiFi system and for knowing the optimum number of cameras that can connect to one CPE. Further, the comparison is critical in ascertaining the link utilisation percentage of the WiMAX uplink channel for WiMAX and hybrid WiMAX-WiFi systems. The chapter disputes or confirms the first hypothesis; and it addresses the first objective, as stated in Chapter One.

In the next section, the related work on WiMAX video surveillance systems has been discussed ending with our proposed work. Section 3.2 and 3.3 describes in detail the meshed and the unmeshed WiMAX-WiFi video surveillance network models. In section 3.4 and section 3.5, a derivation of the traffic flow (throughput) models and the video transmission algorithm have been given for the WiMAX and hybrid WiMAX-WiFi surveillance systems. Other performance metrics such as link utilisation jitter, end-to-end delay and packet loss have also been described, and proof of concepts through simulation using OPNET demonstrated. Section 3.6 and Section 3.7 outline the simulation methodology and the assumptions made and constraints respectively. Section 3.8 gives and discusses the results obtained from simulations. The chapter summary is provided in section 3.9.

3.1 Related Work on WiMAX Video Surveillance

Kafhali et al. [42] presented a performance analysis for the bandwidth allocation in IEEE 802.16 Broadband Wireless Access (BWA), in which the throughput was measured against traffic intensity (packets/frame). They noted that an increase in traffic intensity had a corresponding increase in throughput - until saturation point. Yousaf et al. [43] conducted, among others, TCP and UDP throughput tests for the downlink and uplink channels of WiMAX network. The throughput tests were carried out under varying modulation types and at varying distances. The throughput results

on the stressed WiMAX link were satisfactory, even at the lowest transmission power (13dBm) and for a distance of up to 9.4km.

Dagar and Sharma [44], in their work on IP TV over the WiMAX network, demonstrated that the distance or coverage range of a WiMAX BS affects the throughput. In their work, they connected subscriber station (SS) at 10km, 20km, 30km and 50km from the base station. The throughput measurements were carried out for the downlink channel. The SS at 10km outperformed the rest; and the distance or coverage range was the reason.This means that the closer the SS or MS is to the base station, the higher the throughput would be.

Oyman et al. [45] provided a synopsis of the technology choices for achieving multicast and unicast video transmission over WiMAX and LTE networks. They quantified and compared the video service capacities of these systems in practical environments, and discussed new methods that could be used for enhancing the video capacity and the quality of user experience [45].

In the work of Li et al. [46], a model was proposed to investigate delay and throughput variations, to optimise the system design through correct parameter configurations. Several simulations were conducted to demonstrate the accuracy of the model. However, this work was limited to the wireless mesh WiMAX network.

In this chapter and work, we develop a detailed analysis model and video transmission algorithm of a hybrid WiMAX-WiFi video surveillance and carried out a performance comparison of the WiMAX and hybrid WiMAX-WiFi video surveillance systems. Additionally, the research investigated the optimum number of cameras per CPE on hybrid WiMAX-WiFi surveillance, given the measured throughput values, and taking into consideration the network bandwidth requirements.

3.2 Hybrid WiMAX-WiFi Video Surveillance Model

Figure 3.1 shows the architecture and a detailed diagram of the hybrid WiMAX-WiFi video surveillance. The hybrid WiMAX–WiFi video surveillance system incorporates fixed Wi-Fi IP cameras connected to the WiMAX network via some outdoor and fixed CPE or SS.

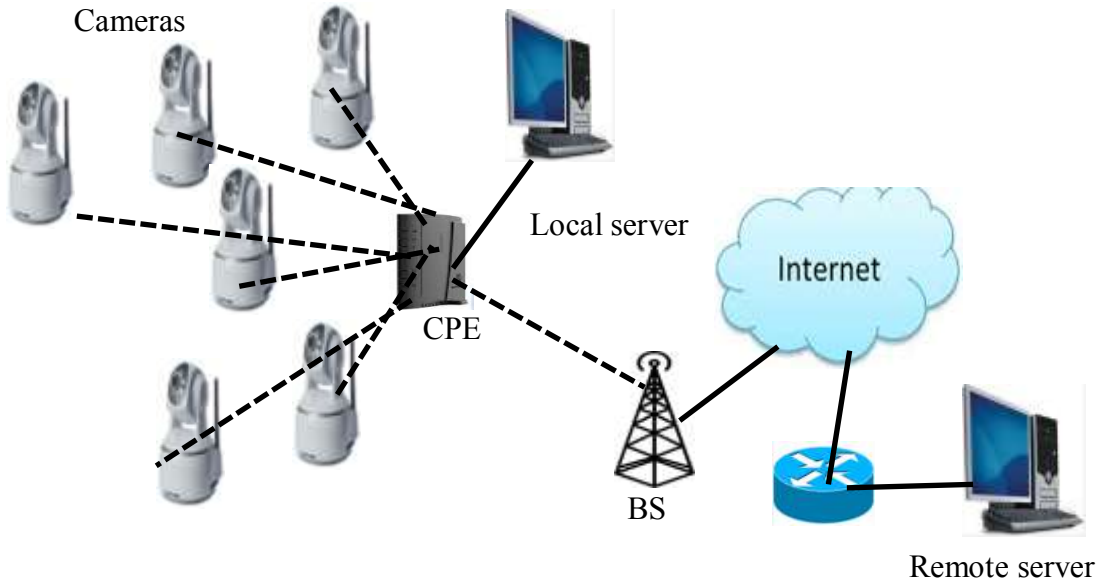

Figure 3.1: Unmeshed WiMAX-WiFi Video Surveillance Systems

3.3 Meshed WiMAX-WiFi Video Surveillance model

The meshed WiMAX-WiFi IP Video Surveillance model is shown in Figure 3.2. The model is similar to the unmeshed WiMAX-WiFi model of Figure 3.1; but it consists of fixed Wi-Fi IP cameras connected to the WiMAX network via the WMRs.

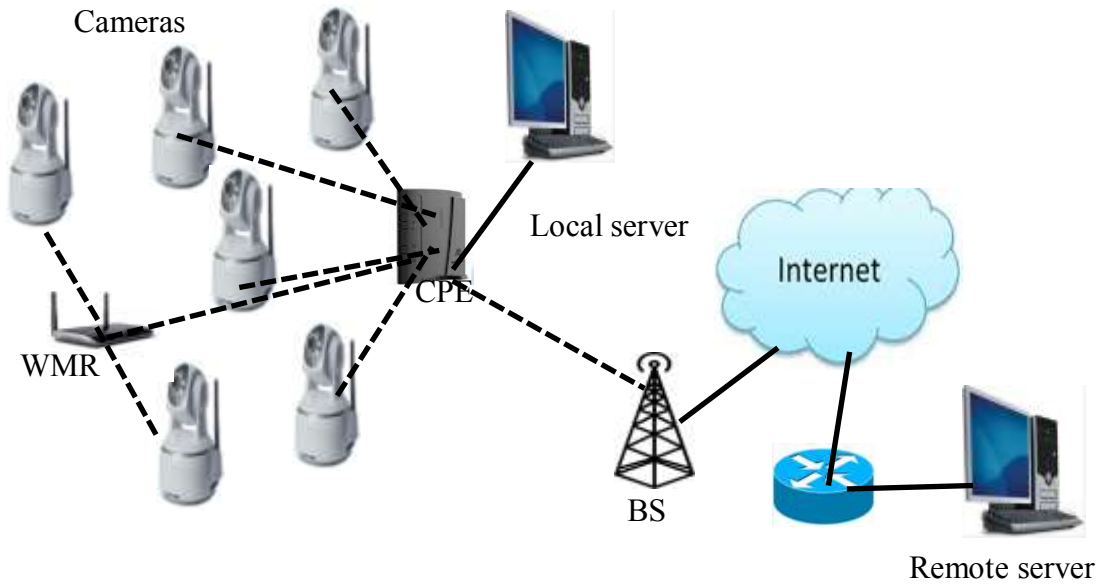

Figure 3.2: Meshed WiMAX-WiFi Video Surveillance Model

The IP cameras are not meshed clients; that is, they do not send surveillance video from one IP camera to the other. This feature is purposely advanced here, to minimise

hop count; since video surveillance information routed to the local or remote server only hops from Wi-Fi IP cameras to the WMRs and the CPEs. The hop count defines the number of times a signal traverses between the IP cameras and the CPEs or Mesh Gateways (MGs) [47].

3.3.1 Wireless Mesh Routers

Wireless mesh routers are relay devices, whose function is to convey the information received from access points and end-devices to the mesh gateways. They can also function as access points in mesh networks, when it is desirable to reduce the hop count. Wireless mesh routers consists of a minimum of two wireless interfaces: The first being the gateway or Access Point (AP) or CPE which is also called the AP module and the second to the sensors or cameras with an optional sensor proxy (SP).

The AP module interfaces with the sensors while the sensor proxy carries the compression and decompression functions similar to the wireless bridge discussed in [48]. Within the maximum coverage range for the CPE, there would not be any need for a WMR.

3.3.2 The Customer Premises Equipment

Customer Premises Equipment has at least two wireless interfaces: AP modules, a CPE module, and sometimes the sensor proxy similar to the one for the wireless mesh router. The AP module receives the video surveillance images/video from the sensors and the wireless mesh routers via its Wi-Fi interface and relays it to the CPE Module. The CPE module sends out the received signal or data from the AP module to the WiMAX BS. Thus, the CPE module is essentially the WiMAX wireless interface. The typical IP camera to CPE distance is 50-300m, depending on the Wi-Fi standard adopted.

CPEs are similar to access points of Wi-Fi networks. One or more IP cameras can connect to a CPE, using a Category 5 or 6 Ethernet cable through a switch, or wirelessly using the Wi-Fi interface governed by the unlicensed frequency bands of the IEEE 802.11 family of standards.

3.3.3 Remote and Local Server

Real-time videos/images from several cameras are transmitted to the local monitoring viewer PC and the video storage server. The surveillance videos can also be monitored via the Internet, using a remote monitoring viewer personal computer (PC) and a video storage server. At either local or remote monitoring points, security experts detect and interpret the video contents. The remote and local servers are installed with appropriate software for detection, tracking and analysis of videos.

3.3.4 Fixed Cameras

Modern wireless IP cameras are designed with both wired and wireless interfaces. Wireless Network cameras operate in any of IEEE 802.11, IEEE 802.16, IEEE 802.15 family of standards, specified ITU-R defined unlicensed and licensed frequency band, and a specified multi-access scheme and modulation technique combination. This work considers wireless cameras in the Wi-Fi, IEEE 802.11 family suite. Further, the flexibility in design and operation enables an area of 50-300m to be secured.

Wireless IP cameras come in various shapes and designs. Some are designed to be fixed on a wall, ceiling or pole; while others are mobile. Video sensors could be made for either day use, or incorporated with Infra-Red Light Emitting Diodes (IR-LED) for both day and night use [49]. Wireless network cameras capture video images; digitise and compress them before routing them to the designed wireless network. Figure 3.3 shows a wired-wireless network camera and its associated features.

Figure 3.3: Features of A Wireless Network Camera-802.11b/g [50]

The basic internal elements common to most wireless IP camera includes the lens, sensors, the analogue-to-digital converter, a digital signal processor, a memory unit and the Internet interface unit. Other elements (not shown on the diagram), include the wireless radio interfaces; Ethernet wired interfaces, power ports and optional memory cards. For the detailed structure of wireless fixed cameras (see Appendix D).

3.4 Modelling Traffic Flows in hybrid WiMAX-WiFi Surveillance Systems

3.4.1 Generated Traffic Flows at the Cameras

In Chapter One, we showed the generated rate of captured video/images, and how it depends on frames size, frame rate and the compression ratio of the video codec. This generated rate was illustrated in equations (1.2) through (1.4). We can use the knowledge gained from graph theory [51], and derive the generated traffic flows or the generated rate. Figure 3.4 illustrates the traffic flows generated by the wireless IP cameras and their transmission to the CPE in a hybrid WiMAX-WiFi network. If we let the supply devices, which in this case are wireless IP cameras, be denoted as node i and the traffic flow aggregating device, the CPE, as the nodes k.

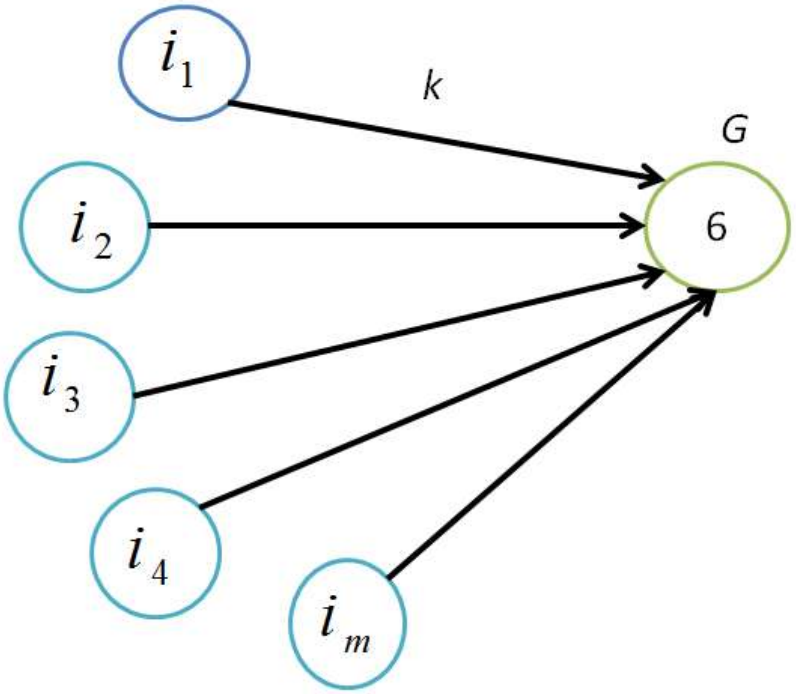

Figure 3.4: Flow Diagram Illustrating Camera-CPE Connectivity

Then the processing and transmitting rate or supply flow per cameras, A_{ik} available at node i would be:

$$A_{ik} = \frac{FS \times F_c \times 1 \times 8}{t} bps \quad (3.1)$$

The constants 1 and 8 denote one (1) camera and eight (8) bits per byte respectively. Now, substituting equation (1.1) into (3.1) we have:

$$A_{ik} = [FS \times fps \times 1 \times 8] \ bps \quad (3.2)$$

3.4.2 Flow Throughput for unmeshed WiMAX-WiFi System

Throughput is the rate of flow of information. It should not be confused with IEEE 802.11family of standard data rate, which is the rate at which the data bits in individual 802.11 data frames are sent. Flow throughput can be measured between two points in a network. It can be between the source nodes and the AP, or the WMR, or the CPE; and it can also be between the WMRs and MGs. Flow throughput is defined as the sum of all the traffic sent by source nodes (IP cameras) to the WMRs or AP or CPE.

When measured between the WMR and CPE, throughput is the sum of all the traffic sent by the WMR to the CPEs within the observable period [52]. It is a measure of the bandwidth consumed by each router or access point in the network. The Minimum throughput values should range between 10kbps and 5Mbps [40], for video transmission.

The hybrid WiMAX-WiFi video surveillance model of Figure 3.1 can be modelled to analytically derive the flow the throughput for any number of IP cameras, by using the graph theory. Figure 3.5 shows a traffic flow diagram of a hybrid WiMAX-WiFi network.

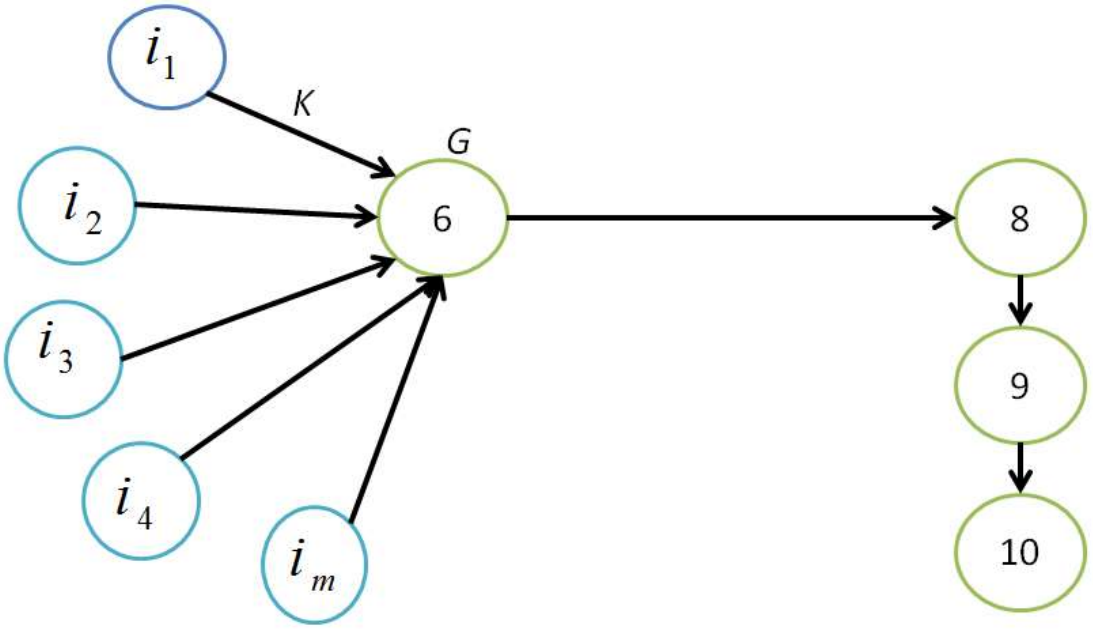

Figure 3.5: Flow Graph of a Hybrid WiMAX-WiFi System

The traffic model consists of: The supply devices, which, in this case, are wireless IP cameras denoted as node i_m. Node 6 represents the customer premises devices; while node 8 is the base station. Nodes 9 and 10 represents the Internet and the remote server/viewing PC, respectively.

Let G be a set of directed links to the CPE, and k be the set of possible routes to CPE. Then, we can describe the links and the routes with tables or matrices, as:

$$A_{ik} = \begin{cases} 1 & \text{If the link G lies on route } k \\ 0 & \text{Otherwise} \end{cases} \tag{3.3}$$

This defines the matrices A_1 called the link route incident matrices, which are such that

$$A_1 = A_{ik}{}_{i\in I, k\in G} \tag{3.4}$$

Now, each column of matrix A_1 corresponds to one of the routes k; while each row in A_1 corresponds to the link i. The columns of route k consist of 1s and 0s. The ones signify those links which are on route k; and the zeros indicate those ones which are not. For the rows, the ones for link G indicate the routes, which pass through that link. Then:

$$x_i = x_{k_{k\in G}} \tag{3.5}$$

The flow throughput is then the summation of the individual traffic flows from each camera.

$$S_{flow_{CPE}} = \sum_{i \in I} A_{ik} x_k \; bps \tag{3.6}$$

The number $(x_k, k \in G)$ forms a vector. The above equations can then be represented concisely in matrix form. To represent the flow throughput at the CPE, equation (3.6) simplifies to:

$$S_{flow_{CPE}} = (A_1 x_1) \;\; bps \tag{3.7}$$

3.4.3 Flow Throughput for Meshed WiMAX-WiFi System

We defined flow throughput as the sum of all the traffic sent by source nodes (IP cameras) to the WMRs and/or AP or CPE. Figure 3.6 shows a traffic flow diagram of a hybrid WiMAX-WiFi network with WMR.

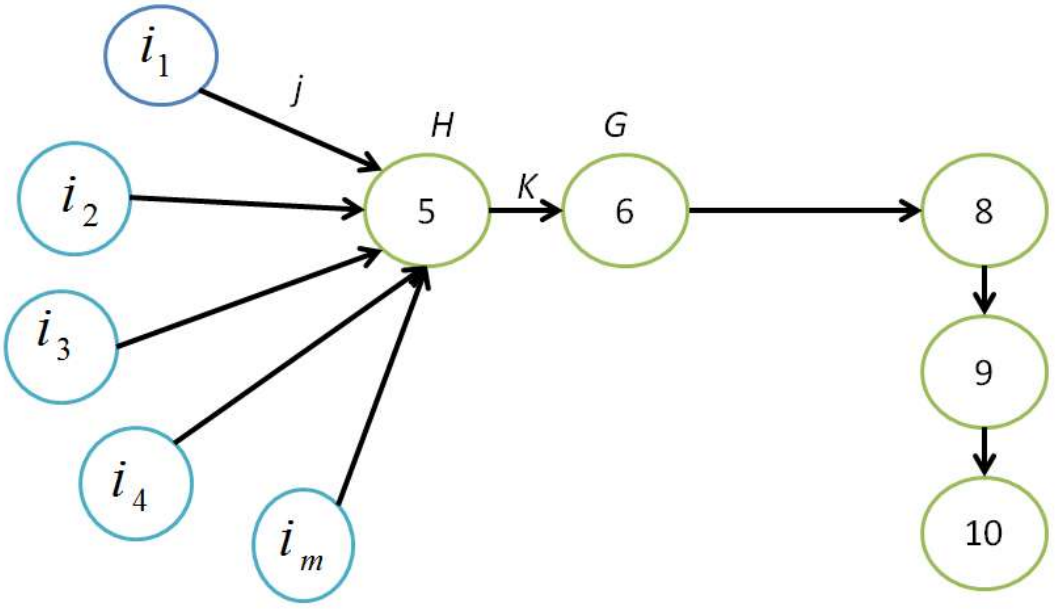

Figure 3.6: Flow Graph of the meshed WiMAX-WiFi System

The traffic model consists of: the supply devices which in this case are the wireless IP cameras denoted as node i, the WMR, node 5. While node 6 represents the customer premises device; and node 8 is the base station. Nodes 9 and 10 represent the internet and remote server/viewing PC.

We can model the mesh network traffic flows to determine the performance of these networks regarding flow throughput. Let H be the set of directed links to the WMR, G be a set of directed links to the CPE; and k be the set of possible routes to CPE. Then we can describe the links and routes with tables or matrices as:

$$A_{ij} = \begin{cases} 1 & \text{If the link H lies on route } j \\ 0 & \text{Otherwise} \end{cases} \tag{3.8}$$

$$A_{jg} = \begin{cases} 1 & \text{If the link } G \text{ lies on route } k \\ 0 & \text{Otherwise} \end{cases} \tag{3.9}$$

This defines the matrices A_1 and A_2 called the link route incident matrices, which are such that:

$$A_1 = A_{ij}{}_{i \in I, j \in H} \tag{3.10}$$

$$A_2 = A_{jk}{}_{j \in J, k \in G} \tag{3.11}$$

Now, each column of matrix A_1 corresponds to one of the route j; while each row in A_1 corresponds to the link n. The columns of route j consist of 1s and 0s. The ones signify those links which are on route j; and the zeros indicate those ones which are not. For the rows, the ones for link H indicate the routes, which pass through that link. A similar arrangement is true for route k. Let x_j be the flow in bits per second on route j and x_K be the flow in bits per second on route k. Then,

$$x_j = x_{j_{j \in H}} \tag{3.12}$$

$$x_k = x_{k_{k \in G}} \tag{3.13}$$

We can calculate the mesh and gateway flow throughput as:

$$S_{flow_{MR}} = \sum_{i \in I} A_{ij} x_j \tag{3.14}$$

$$S_{flow_{CPE}} = \sum_{j \in J} A_{jk} x_k \tag{3.15}$$

The numbers ($x_j, j \in H$) and ($x_k, k \in G$) forms a vector. The two equations above can be represented concisely in matrix form. To represent the flow throughput at the mesh routers, equation (3.14) simplifies to:

$$S_{flow_{MR}} = (A_1 x_1) \tag{3.16}$$

While for the flow throughput at the CPE, equation (3.15) reduces to:

$$S_{flow_{CPE}} = (A_2 x_2) \tag{3.17}$$

In the work done by [53] [37], it was demonstrated that flow throughput decreases with the increase in the number of hop counts. To minimise this decrease in throughput, each interface connects to one channel at a time. However, the authors in [54] propose a maximum of three interfaces; since the available channels in Wi-Fi networks are limited. In Practice, the IEEE 802.11 defines at least 11 channels, from which channels 1, 6 and 11 are non-overlapping [54]. Each link in the WMR-CPE connection has an associated unique channel, which can be allocated statically or dynamically.

3.4.4 Packet Loss

Packet loss is essentially the number of video packets not reaching the preferred destination. The most frequent causes of packet loss are network overloads which result in individual data packets being rejected by overloaded routers, and technical faults in individual network components or connection [30]. A packet loss ratio of greater than 1% is unacceptable for video streaming [55]. Mathematically, packet loss may be expressed as a percentage:

$$P_L = \frac{L - S_{flow_{CPE}}}{L_{bps}} \times 100 \tag{3.18}$$

Where: P_L is the packet loss percentage, L is the average load bit per second as defined in equation (1.7); and $S_{flow_{CPE}}$ is the average throughput in bits per second, as derived in this chapter.

3.4.5 Link Utilisation

Link utilisation (LU) is the ratio of the amount of data carried on the link or current data transfer rate to the link's capacity [56] [57]. Mathematically, the link utilisation can be written as:

$$LU = \frac{S_{flow_{cpe}}}{B} \tag{3.19}$$

where $S_{flow_{CPE}}$ is the number of packets or bits transmitted in a unit interval of time.

The link utilisation can also be expressed as a percentage, in which a very high percentage indicates a busy link; and a very low percentage indicates an idle network. Ideally, during congestion, LU = 1 or 100% [57]. A moderate percentage is preferred.

3.5 Performance Algorithm for Valid Video Transmission

The algorithm begins with the capture of video/images from the wireless cameras. The captured video is then compressed based on the appropriate video compression standards, like the H.264/AVC, MPEG-4 part 10 and motion JPEG. The compression process is done inside the camera itself. Before transmission, two important decisions have to be made: Firstly, if the MSDU byte size of the compressed video exceeds 4095 bytes; it becomes too large for the Wi-Fi MAC part of the CPE. That would make some video packets to be dropped. Secondly, if the MSDU byte size is less than or equal to 4095 bytes, then the aggregate of throughput flows should be sent to the CPE.

However, this should be after making the second important decision, which is, if the aggregated traffic flows ($S_{flow_{CPE}}$) exceeds the network bandwidth, as per equation 1.6, then the number of wireless cameras should be reduced.

The aggregated throughput is then compared to the bandwidth and the theoretical maximum, as per equations (1.6) and (2.4) or (2.8) respectively. Finally, the algorithm measures the packet loss, the jitter and the end-to-end delay for the video surveillance models, taking into account the constraints discussed in section 3.7. The performance algorithm summary is illustrated through a flow chart, as shown in Figure 3.7.

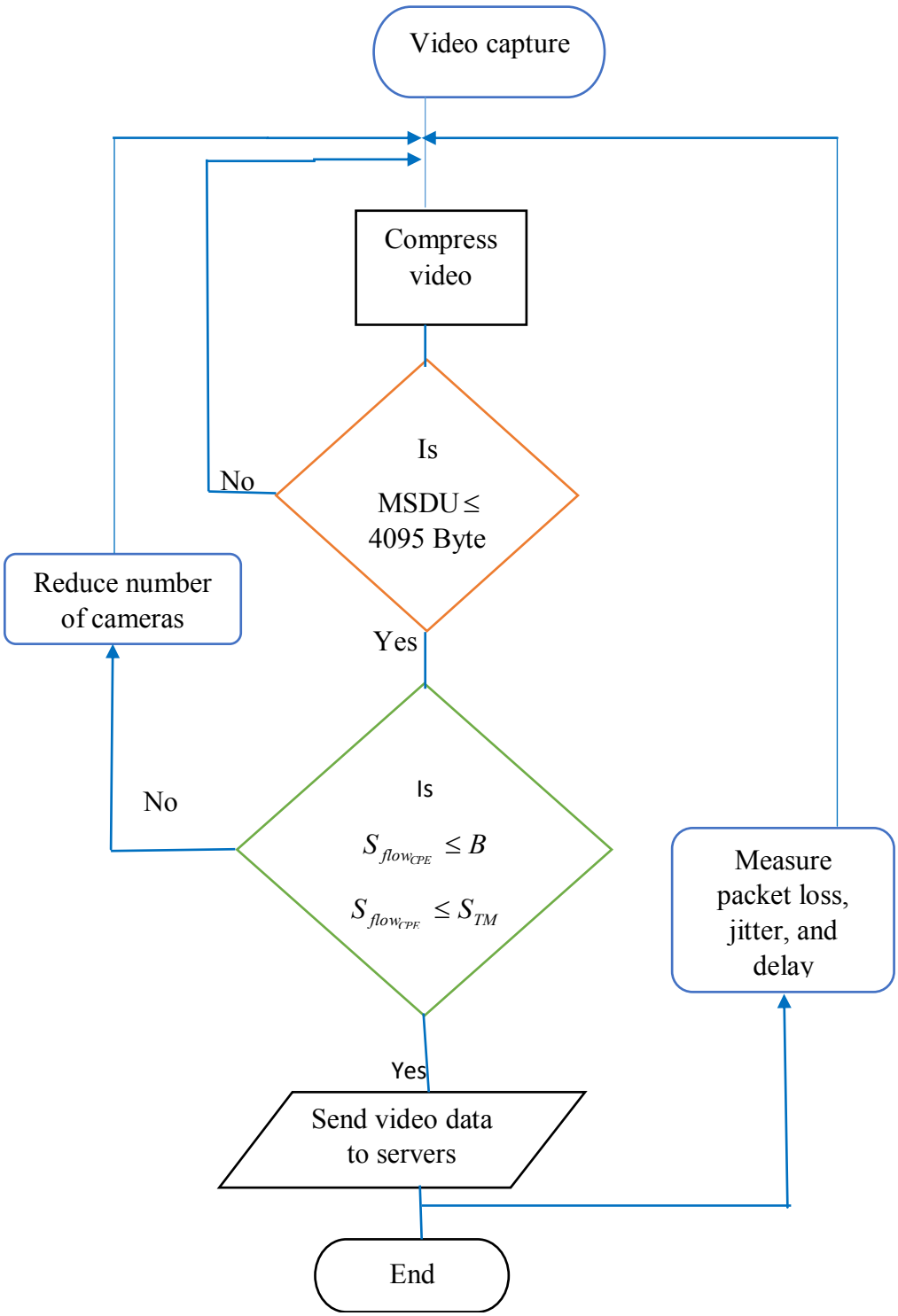

Figure 3.7: An Algorithm for Valid Video Transmission

3.6 Simulation Set-Up

The simulation set-up for the meshed and unmeshed WiMAX–WiFi video surveillance system was arranged, as shown in Figure 3.1 and Figure 3.2 of section

3.2 and section 3.3, respectively. The simulations also validate the performance of video surveillance systems using the performance metrics as derived in section 3.4; in line with first objective. The Wi-Fi cameras, the BS, CPE and WiMAX parameters were configured, as in Appendix E. The fixed wireless cameras that fall within the coverage range of the CPE connect directly to the CPE; while those outside the coverage range connect to the WMR. In each scenario, an average measurement of the throughput, the end-to-end delay, the jitter, dropped bits was recorded, and plotted against the number of nodes or cameras. A constant bit rate, 1420 byte, 352x288 video resolutions at 15fps video was used in the simulations. Since the source videos from the IP cameras are unidirectional, transmitting from the cameras to the network, the incoming stream inter-arrival time was configured to 'none' in the application definitions. Table 3.1 shows the configured applications and their attributes:

Table 3.1: **Configured Application and Video Characteristics**

Video type	CIF, CBR
Number of cameras	4-32
Video resolution	352x288
Frames per second (fps)	15
Average frame size (bytes)	1420
Video codec (Encoder)	H.264/AVC

Table 3.2 shows the detailed frequency/channel allocation and the configurations for the IP cameras, WMRs and CPE gateways.

Table 3.2: Frequency Allocation and Configuration of the Devices

Device Name	**BSSI number**	**Channel**	**Frequency (MHz)**
Cameras	1	1	2412
WMR	1	1	2412
	2	6	2437
CPE	2	6	2437

The frequency differences between the IP cameras and the CPE are deliberately made high to minimise interferences. The number of hops between the cameras has been reduced to two; since increasing the hop counts degrade the performance as

established in section 4.3. The simulation is run for 4, 8, 12 up to 32 cameras and each scenario runs for twenty (20) minutes. The average measured values for throughput, dropped bits, end-to-end delay and jitter are compared with the unmeshed WiMAX-WiFi video surveillance system analysed in Chapter Three.

3.6.1 Simulation Tool

We used OPNET Modeler 14.5 simulation software to measure the QoS performance, including traffic flows. OPNET Modeler [58] [59] is a discrete event simulator. It offers a complete simulation development environment for the modeling of computer and communication networks [60] [61]. The simulator is used for research and development, as well as for commercial purposes. It assists in the design and analysis of the communication networks, protocols and applications. The package allows for the design and analysis of telecommunications networks, protocols and applications, including video streaming of the video packets of varying resolutions and frame sizes. We adopted the IEEE 802.11b and RTS/CTS Mac layer in our simulations; because the RTS/CTS offer symmetrical link constraints.

3.6.2 Video Data Type

The captured and compressed video data type takes two options or streaming modes: the Constant Bit Rate (CBR) or the Variable Bit Rate (VBR). Each of the two options has merits and demerits, depending on the purpose and other considerations. In limited bandwidth environments, and when scene motions are always stable, the CBR mode is a natural choice.

However, CBR modes can lead to the loss of valuable data, especially when the bit rate of the images increases thereby creating blurry images. Where there are variations in the scene motions and adequate bandwidth capacity, the VBR mode should be considered.

The VBR has merits; since it minimises the risk of losing valuable data packets; and therefore, avoids the possibility of blurry images [12].

3.7 Constraints and Assumptions

The following constraints have been considered to define a valid video transmission: Firstly, it is necessary to satisfy the throughput requirements by ensuring that no video packets are dropped. Secondly, one should impose a delay guarantee; as an upper bound on the total time taken for video transmission from the IP camera to the mesh routers. Finally, one should impose a jitter guarantee on the total time taken for video transmission from IP cameras to the video server. We assume that the wireless link is the bottleneck in analysing delay, and this underpins these considerations. An end-to-end delay of between 150-200ms [40] and a maximum jitter of 60ms [55] are recommended for video for video delivery over IP. All IP cameras are sending UDP packets to the nearest mesh router or CPEs using a single radio.

Video transmission in a surveillance system is typically unidirectional, traversing from the IP cameras to the video servers and viewing computers. Further assumptions are made as follows: (i) the IP cameras and the mesh routers are not interfering with other communications; (ii) the IP cameras are restricted to the unlicensed frequency band in the IEEE 802.11 family of standards, in which Wi-Fi is operated; (iii) IP cameras are clustered, according to the nearest mesh router. Each group has its channel linking to a nearby mesh router or CPE.

3.8 Results and Discussion

In this section, we present the performance comparison of the WiMAX, unmeshed and meshed WiMAX-WiFi video surveillance systems as per first objective. The comparison is essential in ascertaining the eligibility of hybrid WiMAX-WiFi systems (Meshed and unmeshed) for video surveillance application in the context of throughput, packet loss and latency. This section also proposes, from the results, the optimum number of cameras that can be connected to one CPE for the specified payload and frame rate. The best method for implementing each system is equally suggested. Therefore, three surveillance systems are compared and analysed regarding throughput, packet loss, end-to-end delay, and jitter.

3.8.1 Throughput

This subsection shows the measured average throughput results, as a function of the number of cameras transmitting to a remote server. Figure 3.8 shows the measured throughput analysis of the proposed meshed and unmeshed WiMAX-WiFi and the WiMAX video surveillance system. The performance of the three systems is compared with the maximum load per given number of cameras. This load may be equal to or less than the network bandwidth and is given as shown in equation (2.2) in chapter two.

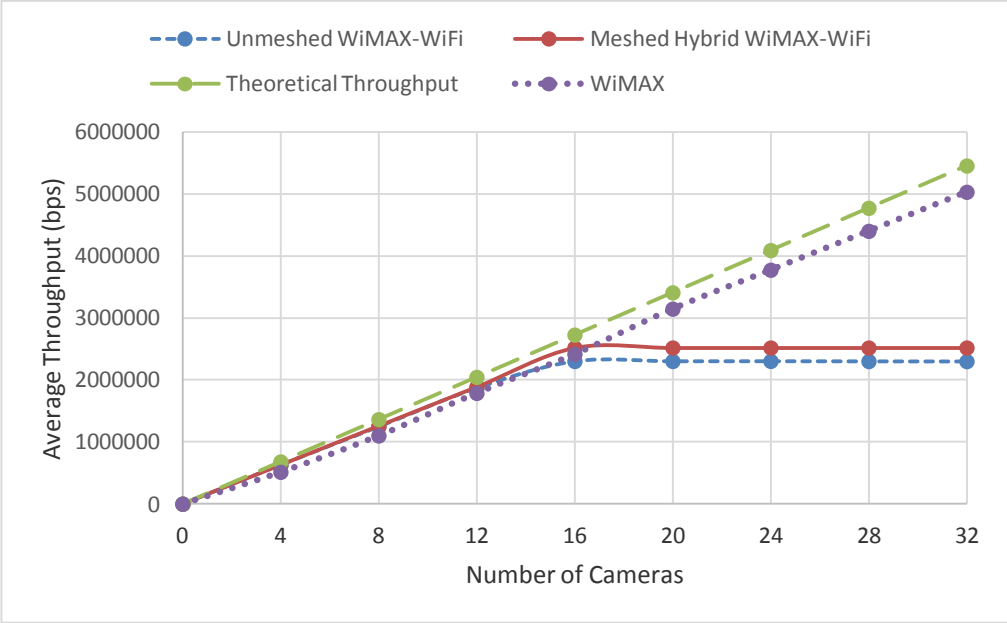

Figure 3.8: Measured WiMAX Throughput as Number of Cameras Increase

The average throughput increases with the increase in the number of cameras for all the three systems. However, beyond sixteen cameras the throughput for the two hybrid WiMAX-WiFi systems saturates with any increase in the number of cameras having null increase in throughput. These results are in contrast to the WiMAX, whose throughput continues to increase with any increase in the number of cameras, the limit being the capacity of the WiMAX network.

A further look at the two hybrid systems shows that for the first twelve cameras, the hybrid WiMAX-WiFi throughputs are marginally higher than those for the WiMAX system; and that the meshed WiMAX-WiFi has better throughput than the unmeshed

WiMAX-WiFi system. The implication of the hybrid WiMAX-WiFi systems results is that the CPE can accommodate up to sixteen cameras in a single and simultaneous uplink transmission for the 1420 byte, 15fps Video.

Conversely, if more cameras are loaded on a CPE, a low payload and/or low frame rate cameras should be used.

3.8.2 Packet Loss

In this section, a comparison and analysis of the packet loss of the WiMAX uplink for the WiMAX and the hybrid WiMAX-WiFi are made. This analysis follows the throughput performance analysis conducted, as shown above. The packet loss is a measure of how many packets per second the WiMAX link loses. The measurement was done with a varying number of cameras. Figure 3.9 shows the results for the three video surveillance systems.

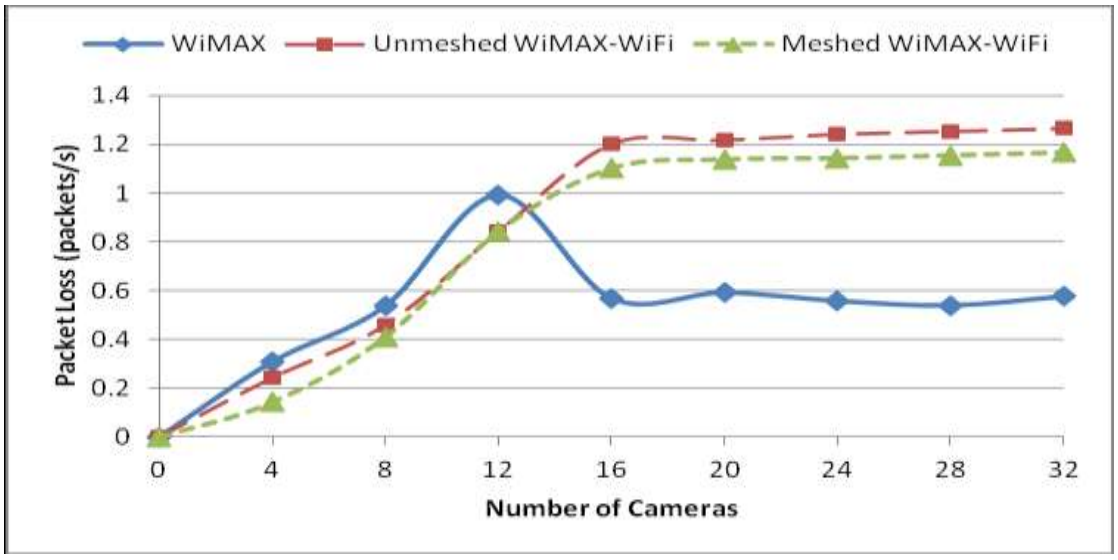

Figure 3.9: WiMAX Uplink Packet Loss Measurements

From the results, the hybrid WiMAX-WiFi performed relatively better for the first 12 cameras than did the WiMAX system, recording an average packets loss of between 0 and 0.56s. However, beyond 12 cameras the hybrid WiMAX-WiFi system packet loss increases to 1.2; while the WiMAX system maintains a relatively low packet loss of 0.55s to 0.6s. This, low packet loss result, explains why the throughput was better for the hybrid WiMAX-WiFi for the first 12 cameras, but poor between 12 and 32 cameras. Conversely, the throughput continued to increase between 16 and 32

cameras for the WiMAX system because of the marginally low packet loss for the same number of cameras.

The inclusion of the WMR reduces packet losses, due to the reduced bit loss between the camera and CPE. The WMR mitigates loss of video/images from cameras located in the distances beyond the coverage range of the CPE.

Where high resolution (and therefore high MSDU byte size) video surveillance IP cameras are used, fewer IP cameras could be used to minimise the packet loss, while transmitting, within, the theoretical maximum throughput value of the given IEEE 802.11/IEEE 802.16 standards.

3.8.3 Link Utilisation

We established that Link utilisation has a value of between 0% and 100%, where 100% means that the link's capacity is fully consumed. A high link utilisation percentage is indicative of a busy network (efficient link utilisation); while low link utilisation indicates that the connection is idle (poor link utilisation). Figure 3.10 shows the measured results of link utilisation for a WiMAX link during the transmission of surveillance signals to the remote server.

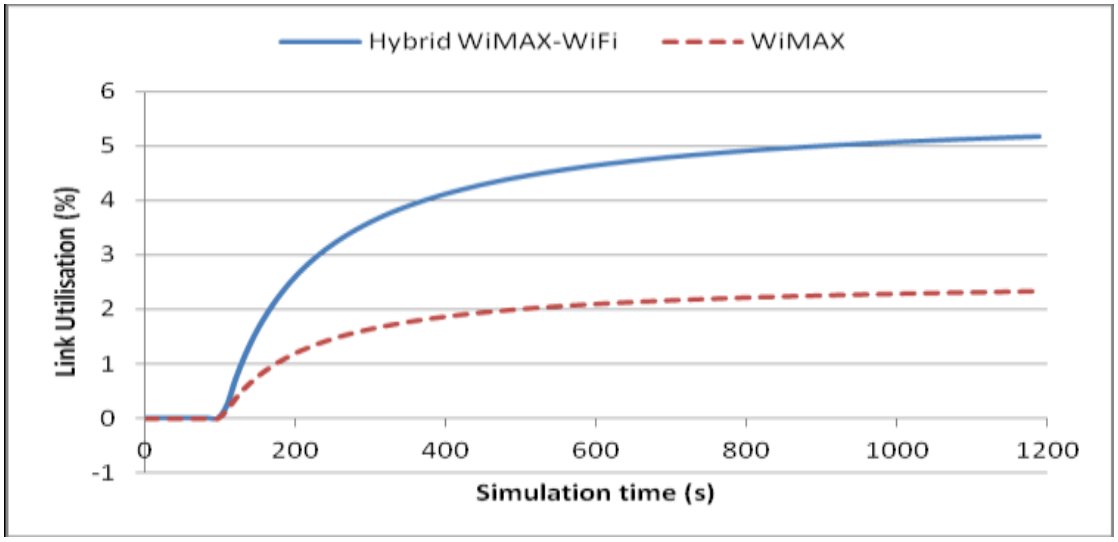

Figure 3.10: Link Utilisation Measurements of the WiMAX Uplink

The dedailed parameter and channel condition values for the WiMAX and Wi-Fi systems are shown in Table 3.1 and Appendix D. However, we chose sixteen (16)

cameras for each system considering that during the first 16 cameras both systems records nearly the same values of throughput. In the WiMAX scenario 16 WiMAX cameras all transmit to the BS using 16 channels, one for each camera. In the hybrid WiMAX-WiFi 16 Wi-Fi i cameras transmit to the BS via the CPE using one uplink channel. The measured link utilisation percentage on the WiMAX uplink channel for the WiMAX and hybrid WiMAX-WiFi systems show the following results: The 16 WiMAX camera utilizes the 16 WiMAX uplink resources with the measured maximum utlisation percentage of 2.33%. The sixteen Wi-Fi cameras connecting through the CPE utilizes the one WiMAX uplink channel and achieves a link utilisation percentage of 5.34%. These results necessarily mean that the hybrid WiMAX-WiFi system has better usage of the WiMAX uplink channel than does the WiMAX system for nearly the same throughput.

3.8.4 Signal-to-Noise Ratio

The Signal-to-Noise Ratio (SNR), which is the measure of signal strength in the midst of noise; external and internal noise, is a critical performance metric. In this section, we show the measured results of SNR on the WiMAX link for a case, when all the cameras are transmitting directly to the BS; and for the other, when all the cameras are transmitting to the BS via the CPE. In Figure 3.11, the measurements of SNR for the WiMAX and the hybrid WiMAX-WiFi systems are shown.

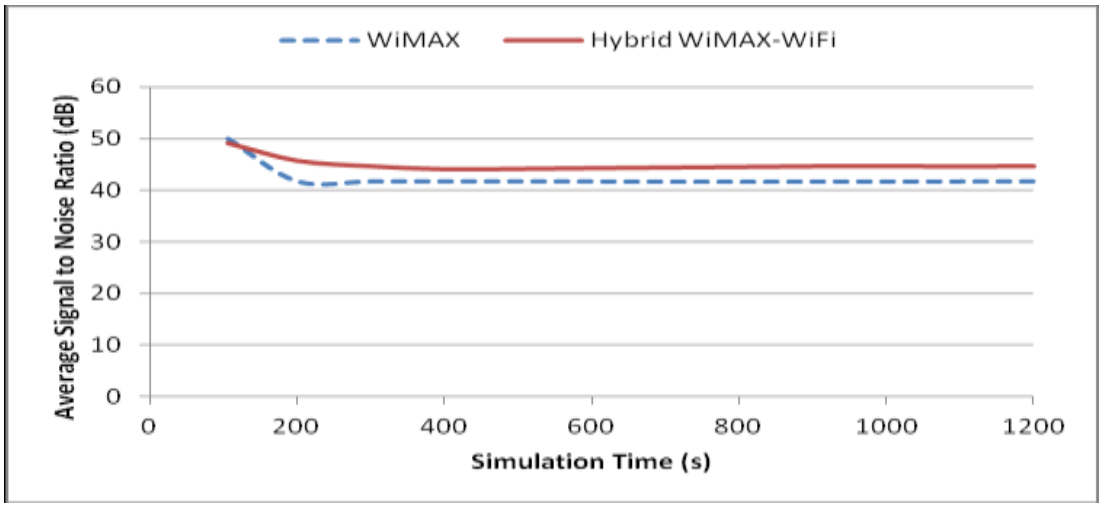

Figure 3.11: Measurement of Average Signal-to-Noise Ratio

Again sixteen cameras have been considered for this comparison for the same reason given in section 3.8.3 above. The results indicate that the hybrid systems have a better

SNR for the same number of cameras, and when measured over the same period. The reduced interference in the hybrid WiMAX-WiFi system, accounts for its better performance; since it uses only one channel; while the WiMAX system has several channels, each for one camera creating adjacent channel interference and increasing noise.

3.8.5 End-to-end Delay

The average end-to-end delay measures the delay in the arrival of video packets between the source (cameras) and the destination (video server) nodes. As stated, this measurement is important as it helps in understanding congestion levels in a system. From the results of Figure 3.7, one can suggest and conclude that the number of cameras that each CPE should have for normal operation is sixteen (16); this being an achieved value before saturation or congestion occurs. However, the system's performance should also take into account end-to-end delay and jitter performance, among other performance metrics.

Figure 3.12 shows the average end-to-end delay measurement for the WiMAX, the meshed, and the unmeshed WiMAX-WiFi systems; as the number of cameras increases from 0 to 32 when transmitting surveillance videos/images to the remote server.

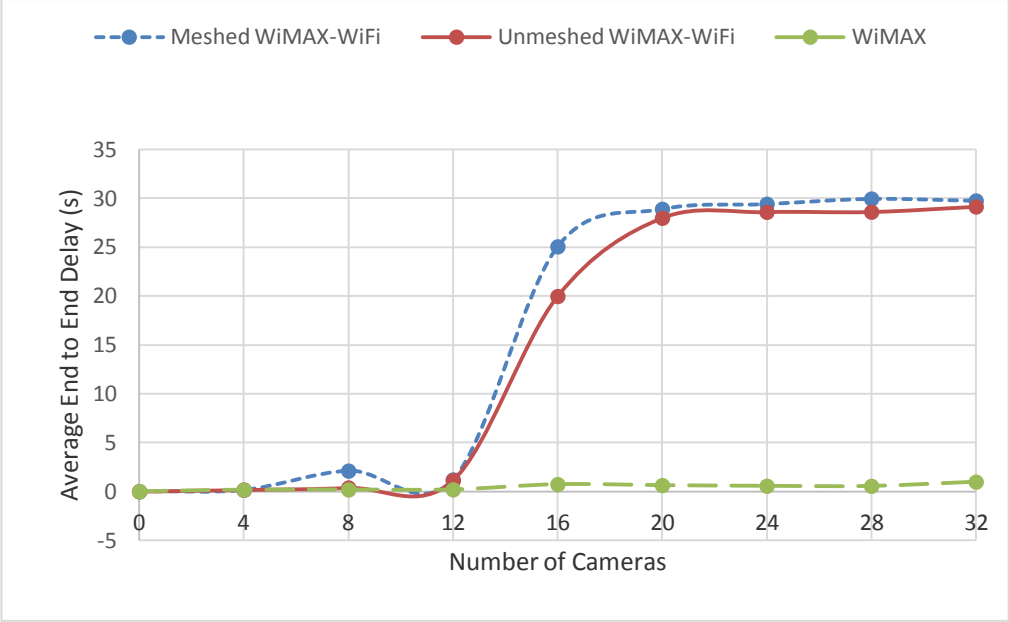

Figure 3.12: End-to-end Delay Measurements

As seen from the diagram, the three surveillance systems perform well for the first 12 cameras with a measured average end-to-end delay of 0.017s and the WiMAX system maintain this value, regardless of the number of cameras used. However, the mesh and unmeshed WiMAX-WiFi systems' performance deteriorates after 12 cameras; measuring an average end-to-end delay of between 0.017 to 29s. With such high end-to-end delay values, the two systems cannot be loaded beyond 12 nodes per CPE, at a payload of 1420 bytes and 15fps; since this exceeds the maximum recommended values of between 150-200ms, according to the authors in [55] [40].

Many reasons cause this poor performance of the two hybrid systems after 12 cameras: collisions, congestions, and buffer overflow occurrences and the consequent loss of data packets [55] [62]. Furthermore, every node put on the wireless link acts as a bottleneck that delays the traffic flow. Therefore, the inclusion of WMR is a bottleneck that gives rise to queuing delays and traffic latency.

In general, the results show that transmission to a remote server comes with a high end-to-end delay in the hybrid systems.

3.8.6 Jitter

Jitter, which is the variations in the arrival of video packets at the destination nodes, is measured in seconds. Jitter measurement helps in knowing the length of intermittent video image display in seconds. As stated, all jitter values below 60ms are considered to be normal in video transmission. Figure 3.13 shows the jitter measurements as the number of cameras increases. The WiMAX system has jitter measurements averaging 0.023s for every increase in the number of cameras up to 32. This value falls within the acceptable range for video transmission. The mesh and the unmesh WiMAX-WiFi systems record an equally accetable range of jitter values - averaging 0.032s for the first 12 and 14 cameras, respectively. Beyond 12 and 14 cameras, the jitter performance degrades to between 0.032s and 100s at 32 cameras. Again, the poor jitter can be attributed to imperfect channel conditions coupled with node bottlenecks in the WiMAX devices along the transmission path, among others.

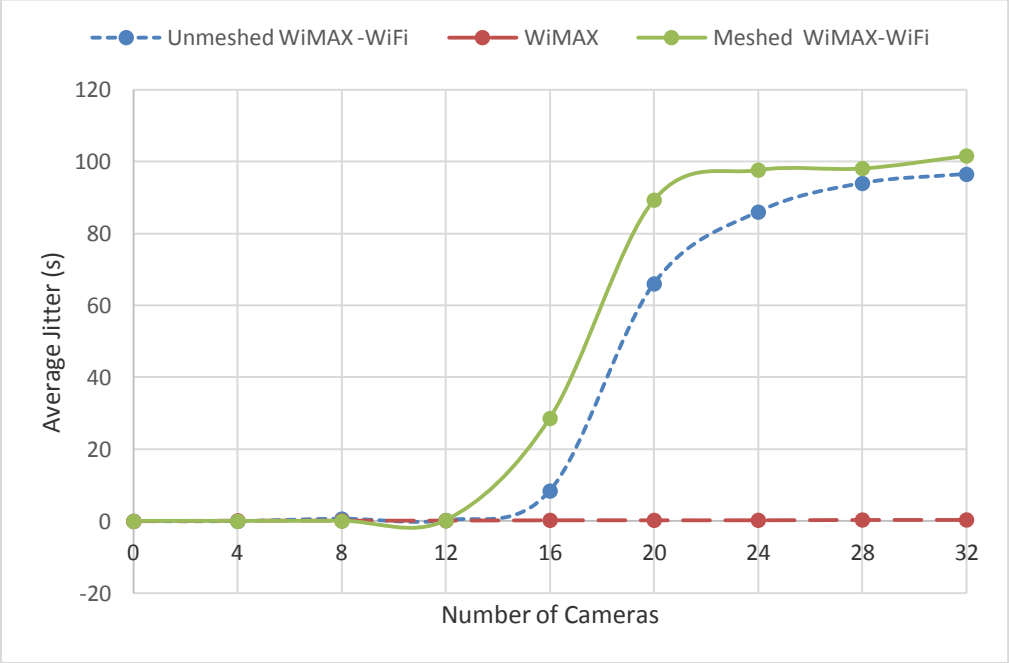

Figure 3.13: Jitter Measurements as the Number of Cameras increases.

As established and demonstrated in the algorithm, for a valid video transmission the video jitter must not exceed 60ms, according to [55]. Effectively, this means that for proper operation of the CPE at 1420 byte size and 15fps, up to 12 and 14 cameras or nodes should be used. Any further increase in the number of IP cameras produces a corresponding increase in jitter values.

3.9 Chapter Summary

This chapter has described and analysed the WiMAX, meshed and unmeshed WiMAX-WiFi video surveillance models. Related work on a baseline WiMAX video surveillance systems have been reviewed and a case for a hybrid WiMAX-WiFi video surveillance system established. Mathematical Analytical models for the throughput, the jitter, the end-to-end delay, the packet loss and other related performance metrics have been derived; and the proof of concepts through simulation has been demonstrated.

An algorithm for throughput or traffic flows for defining valid video transmission has been proposed and tested in simulation. The results show that for the first 12-16 cameras, the two hybrid WiMAX-WiFi systems have better throughput, link utilisation, SNR and packet loss values than the baseline WiMAX system. The jitter

and end-to-end delay values for the hybrid WiMAX-WiFi are nearly equal to the WiMAX system. Furthermore, the meshed WiMAX-WiFi system performs better than the non-meshed system regarding throughput and dropped bits but the non-meshed system performs well on end-to-end delay and jitter, under similar conditions. Therefore, both meshed and unmeshed WiMAX-WiFi systems are eligible for video surveillance application.

At a video payload of 1420 bytes and a frame rate of 15fps, a customer provided equipment can allow up to 16 cameras, without exceeding the acceptable packet loss of 1%. However, when end-to-end delay and jitter recommended limits are considered, that is 150ms-200ms and 60ms, respectively, a maximum of 12 cameras should be allowed per CPE.

The chapter has confirmed our first hypothesis and satisfied the requirements of the first objective. From the link utilisation results, we may conclude that the hybrid WiMAX-WiFi makes better use of the uplink WiMAX channels than does the WiMAX system.

Chapter Four

4 Mobility in Hybrid WiMAX-WiFi Video Surveillance Systems

In the previous chapter fixed wireless cameras were adopted in the analysis and measurements. That approach is useful; but it has limitations; since it cannot cover all blind spots. Mobile cameras can cover these blind spots in line with objective number two. Therefore, this chapter analyses the effect of mobility on mobile WiMAX and hybrid WiMAX-WiFi surveillance systems. This analysis is critical for determining the usability of such systems - especially at pedestrian and running velocities which are essential when implementing the developed software of Chapter Five. Furthermore, this analysis helps in ascertaining the optimum mobility rate at which throughput is highest. In the next section, we shall discuss related work on mobile WiMAX surveillance, and state our suggested contribution.

Section 4.2 proposes and describes the mobile WiMAX-WiFi video surveillance network model and explains the mobile camera role in video surveillance. In section 4.3 and section 4.4, we derive the mathematical model for throughput and propose a new performance algorithm for mobile cameras connected to a baseline mobile WiMAX and hybrid WiMAX-WiFi network. Section 4.5 and section 4.6 describe the three conventional mobility models and recommends one for surveillance application; additionally, they also outline the simulation methodology using OPNET. An analysis of the results on the effect of mobility in mobile WiMAX and mobile WiMAX-WiFi surveillance system using the H.265/HEVC video codec is given in section 4.7.

The results for the two systems are evaluated for varying mobility velocities and the optimum speed for improved performance is suggested. The performance metrics are throughput, dropped bits per second, link utilisation, end-to-end delay and jitter. These metrics carry the same definitions and descriptions, as outlined in Chapter Two and Three; and they are also considered here in the context of objective two of this thesis.

4.1 Related Work on the Mobile WiMAX/WiFi Surveillance System

The term "Mobile" here implies the mobile nature of end-devices or cameras. Ahmad and Habibi [24] proposed a public transport vehicle mounted scheme, for estimating the utility of diverse cameras. With this scheme, a decision on which camera (s) to switch off, would be effected based on the utility estimate made as a way of improving the overall utility of the video surveillance system. Panayides et al. [63] proposed an H.264/AVC-based framework for transmitting atherosclerotic plaque ultrasound video over mobile WiMAX networks using a 4CIF video format. Their results showed that equivalent clinical quality can be obtained at considerably reduced bit rate demands, and that QPSK1/2 is largely the robust modulation scheme when transmitting video in locations with low SNR.

Mahasukhon et al. [64] studied the performance of wireless broadband technologies like WiMAX in a railroad environment. Their focus was to investigate the impact of mobility on the wireless system throughput for moving trains at high velocities. They observed that: using best-effort scheduling; 11 kilometres distance, 70km/h speed; a throughput of 2.9Mbps was achievable using the QPSK 1/2 modulation scheme. Hence, a possibility for deployment in railroad environments [64] was created. Juan et al. [65] investigated the performance of scalable video streaming services in mobile WiMAX systems in which they used both CIF and QCIF in the simulations.

They showed that the execution of several links was critical in realising the scalable video streaming that has feedback information for accessing transmission bandwidth [65]. Charitos and Kalivas [66] deployed a hybrid vehicular wireless network consisting of IEEE 802.11b/g/e and IEEE802.16e, within a tunnel setting for surveillance purposes. They then analysed the performance of such a system during handovers following a fire or explosive emergency situation for two trains travelling at 60km/h and 80km/h respectively. Their results showed that the train at 60km/h had higher throughput and SNR and reduced handover latency than the train travelling at 80km/h.

In the work of Ritter et al., [67] the average flow or throughput of a mobile Wi-Fi link was derived by separating the throughput-reduction causes into two parts: the first was as a result of lost packets, and the second was due to extra latency at the link level during transmission retrials. Zhang and Ansari [68] argue that WiMAX

networks provide an effective and efficient platform for video content delivery. They further suggest the use of a mobile WiMAX-WiFi video monitoring system with fixed sensors and mobile SS, for telemedicine. This is essentially an IEEE 802.16e/ IEEE 802.11a/b/g integration. Several works such as those in [69] [70] and many others in which IP cameras are used have been of the MPEG, H.264/AVC type.

In this chapter, we proposed and implemented a traffic flow (throughput) algorithm; investigated the effect of mobility on the performance of hybrid WiMAX-WiFi surveillance system. The optimum human walking speed or pedestrian speed range, while transmitting surveillance images/videos, for improved performance across all age groups has been ascertained. Furthermore, this work integrates IEEE 802.16d with IEEE 802.11a/b/g at the SS or CPE, whereby the SS is fixed; but the cameras or nodes are mobile.

The effect of mobility on throughput, SNR, end-to-end delay and jitter was investigated through analysis and measurements by using the OPNET modeller simulator and the H.265/HEVC encoder. The chosen mobility model and the mobile camera speed range are Random Way-point Models and were 0 to 10m/s, respectively.

4.2 Mobile WiMAX-WiFi Video Surveillance Model

The design model is similar to the Hybrid WiMAX-WiFi system discussed in Chapter Three, except for the mobile wireless IP cameras. It consists of a CPE, the BS and local and remote servers. The customer provided equipment is essentially an access point for WiMAX networks. It is similar to the Access point; in that it has Wi-Fi and Ethernet interfaces, communicating to the end-devices by using the ISM frequency bands. However, CPEs have additional WiMAX interfaces for communication to the BS. WiMAX links have guaranteed QoS; and various classes can be configured, depending on the type of services required. A Mobile WiMAX-WiFi video surveillance model structure is shown in Figure 4.1.

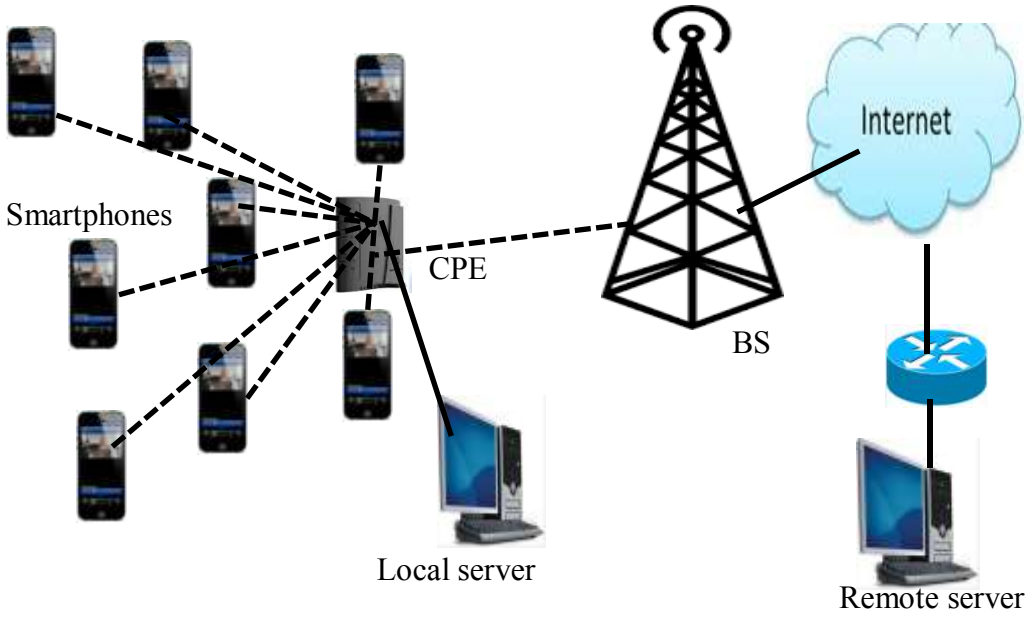

Figure 4.1: Mobile WiMAX-WiFi Video Surveillance System

The smart and mobile cameras or devices can connect to WiMAX network via the CPE. The mobile device uses the Wi-Fi interface, which the mobile user activates for connection to the CPE. The mobile device can also connect to the 3G, 4G and higher generation mobile cellular networks for surveillance purpose at the cost of data units. The captured images can then be routed over hybrid WiMAX-WiFi network and viewed locally via a local server at the CPE, which is equipped with an Ethernet cable. Additionally, the images/videos can also be viewed remotely via the Internet.

4.2.1 Smartphone Wireless IP Cameras

A Smart mobile wireless IP camera is used to acquire the necessary video surveillance images/videos. These cameras are commonly designed as an embedded hardware on most mobile smartphones; and they have sensors and various wireless interfaces. A smartphone is a high-featured and multi-functional cellular phone [71]. Key features include email, external Universal Serial Bus (USB) options, a mini browser, large screen, large memory capacity, Global Positioning System (GPS) capability and basic PC functionality. Smartphones are equipped with two different processors for accessing communication network and performing computations. These processors are the Baseband and Application processors. Figure 4.2 shows a high featured and multi-functional smartphone that is used as a surveillance camera.

Figure 4.2: A multi-functional and high featured Smartphone used as a Camera

The Baseband Processor (BP) is a specialised processor for employing the Global System for Mobile communication (GSM) protocol stack and enabling the Smartphone to access different types of wireless network technologies, such as CDMA, EDGE, WCDMA, WiMAX or LTE, Wi-Fi, ZigBee and Bluetooth 4.0. Its function is to manage radio communications and to control functions, like the signal modulation, radio frequency shifting and encoding [71]. The Application Processor (AP) is a multicore general purpose processor, which is used for providing a user interface and running applications [71]. The processor consists of a processor core (ARM926EJS), multimedia modules, wireless interfaces and device interfaces.

The multimedia module consists of the picture, video and audio sub-modules. The picture sub-module decodes and encodes still images. The video sub-module encodes and decodes the videos; while the audio sub-module encodes and decodes voice signals. The data of various types may be transmitted from one point to the other by using the wireless and device interfaces. The wireless interface includes Wi-Fi, Bluetooth and cellular interfaces; while the device interface includes the Micro USB interface.

4.2.2 Structure of Smartphone Cameras

The structure of the smartphone camera is similar to that of the fixed wireless cameras, as discussed in Chapter Three. However, the smartphone camera allows image as well as video capture. Thus, it consists of the lens, sensors and analogue-to-

digital converters and digital-to-analogue circuitry. Additionally, it has the image and video sub-module enclosed within the application processor. Figure 4.3 shows the structural diagram of a smartphone IP camera system.

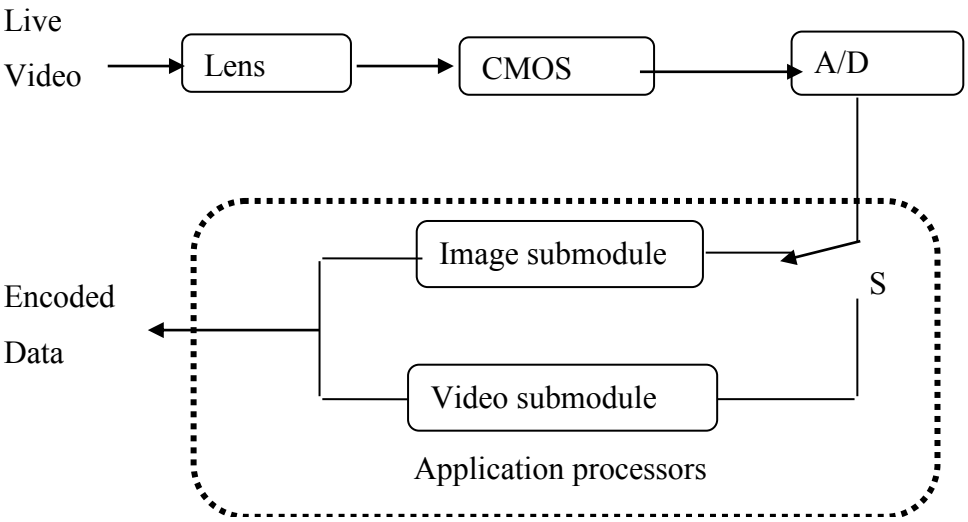

Figure 4.3: Smartphone Structure: Capture and Encoder Units Elements

The encoded image/video data are transmitted to the CPE or cellular network via the baseband processor. The CPE and Cellular networks have Wi-Fi and Ethernet interfaces too [37]. The images thus transmitted, must first be compressed in order to make effective and efficient use of the network bandwidth. This later point becomes significant when it is desirable to use several mobile smartphones for surveillance purposes.

4.3 Analytical Throughput Model

In chapter three, we established that, for fixed cameras in the hybrid WiMAX-WiFi surveillance system, the average throughput is given by:

$$S_{flow_{CPE}} = \sum_{i \in I} A_{ik} x_k \tag{4.1}$$

In a mobile WiMAX-WiFi video surveillance network, mobile cameras move from the stationary position to the new position at a given speed in the CPE coverage. Determining the mobile camera–CPE connectivity can take time. During this process, the throughput of the CPE is expected to diminish significantly; as the access device spends more time measuring the Received Signal Strength Indicator (RSSI) and

determining the best mobile node-connectivity orientation. If the likelihood of having a CPE cell hear a specific synchronisation packet P_S is [67]:

$$P_s = P_c * P_h * (1 - P_l) \tag{4.2}$$

Where: P_c is the likelihood of listening on a specific channel by a mobile node; P_h is the probability that a mobile node is listening; and P_l is the likelihood of the sync packet getting lost because of noise. The chance of at least one mobile node getting a synchronisation packet, P_A, depends on the average number of mobile nodes seen by a CPE and the number of synchronisation packets transmitted by the cameras. If n synchronisation packets are sent and m mobile nodes seen, then the chance of a specific mobile node seeing at least one synchronisation packet, P_o as:

$$P_O = 1 - (1 - P_s)^n \tag{4.3}$$

Consequently, the probability that a node of m mobile nodes hears at least one (of n) synchronisation packet P_A may be written as:

$$P_A = 1 - (1 - P_o)^m \tag{4.4}$$

To acquire at least one radio, the average time T_A, needed is approximately [67],

$$T_A = \sum_{n=1}^{\infty} (T_B + (n-1)T_S) P_A (1 - P_A)^{n-1} \tag{4.5}$$

Where: T_B is the packet sending acquisition time; and T_S is the difference between start and end burst times. T_G is time spent by the mobile node before going out of range.

$$T_G = \frac{d\sqrt{2}}{v} \tag{4.6}$$

Where: v is the velocity in m/s of the mobile node; d the average distance in metres from the CPE to the cameras. The numerical factor $1/\sqrt{2}$ comes from the fact that the camera is travelling in a random direction from the CPE [63].Consequently, the mobile node loses communication with the network P_c % of the time.

$$P_c = \frac{T_A}{(T_G + T_A)} \tag{4.7}$$

If we assume P_o to be small and indiscriminately distributed over the User Datagram Protocol (UDP) transfer, we can derive the average throughput. When the cameras are stationary, the UDP performance is proportional to the maximum throughput less the square root of the dropped packets percentage; for small dropped packets percentage. The dropped packet percentage is proportional to P_c. Accordingly, $S_{flow(v)}$, throughput can be written in terms of velocity and distance as [67]:

$$S_{flow_{(v)}} = S_{flow_{CPE}}\left(1 - \sqrt{\frac{T_A}{\frac{d\sqrt{2}}{v} + T_A}}\right) \tag{4.8}$$

The average throughput of a link is predicted to be less when cameras are moving than when they are static; because the CPE radio modem spends less time determining the best cameras-CPE connectivity link. The average received signal strength indicator seen by a mobile node is also less than that seen by a stationary node. The faster the mobile node is moving, the more time it spends acquiring and the less time it has to provide throughput - thereby resulting in a decrease in the throughput as the mobile unit's speed increases.

4.4 Proposed Throughput Algorithm

We propose an algorithm for the actual throughput when transmission to the local and or remote server for the mobile WiMAX-WiFi video surveillance system using Equations 4.1 to 4.8 below. Once the average time T_A needed to acquire at least one radio and the time spent by the mobile node before going out of range, T_G are known; the throughput, as measured by the CPE, can be determined. Let d be the average range (in metres) for a node travelling at velocity, v in metres per second.

Input: **Process**

1 $B = FS \times fps \times n_p \times 8$ // *Bandwidth based on number of cameras,* n_p.

2 $T_A = \sum_{n=1}^{\infty}(T_B + (n-1)T_S)P_A(1-P_A)^{n-1}$ //*Time to acquire at least one radio*

3 d =*Average range in metres*

4 v =*Velocity in metres*

Output:

1 ***For*** $v = \{0,1,2,3,4,5,....\}$ ***do***

2 $T_G = \frac{d}{\left(v \times \sqrt{2}/2\right)}$ //Time before node goes out of range

3 $P_c = \frac{T_A}{\left(T_G + T_A\right)}$ //percentage of time the node is out of communication

4 *If* $v = 0$;

5 $S_{flow_{(v)}} = S_{flow_{CPE}}$

6 *Else*

7 $$S_{flow_{(v)}} = S_{flow_{CPE}}\left(1 - \sqrt{\frac{T_A}{\frac{d\sqrt{2}}{v} + T_A}}\right)$$

8 $S_{flow_{(V)}} \le S_{TM} \le S_{flow_{CPE}} \le B$ // S_{TM} is the theoretical throughput

9 *End if*

10 $LU = \frac{S_{flow_{(v)}}}{B}$ //measure the link utilisation percentage

11 *End for*

12 *Return inputs*

13 *End.*

If the velocity is equal to zero, the throughput has a maximum value equal to equation (4.1).This maximum value reduces with the square root of packet loss when the velocity is greater than zero.

4.5 Mobility Models

Mobility models are intended to describe the movement style or pattern of the mobile users, and how their location, direction of movement, pause distribution, speed and acceleration change over time. The model attempts to mimic the movements of real mobile nodes that change the speed and direction with time [72]. The Mobility models emulate a real world scenario for the way in which people might move, for example, a conference setting or museum. Three common mobility models are: the Random Direction, the Random Waypoint, and the Mobgen Steady State models.

4.5.1 The Random Waypoint Model

The Random Way-point Model assigns an initial location, destination, and speed for each node. The initial location and destination points are chosen independently and uniformly within the coverage and movement area of the nodes. Independent of both

the initial location and destination, the speed is chosen as a uniform interval [73]. An optional new destination and speed may be selected upon reaching the destination from the uniform distribution. This selection can be done independently of previous destinations and velocities [74]. The Random Way-point Mobility Model causes the clustering of nodes near the centre of the simulation area.

In the Random Way-point Mobility Model, a mobile node is defined stochastically by the following process [75]:

$\{D_i, T_i, V_i\}$, for i = 1, 2. . .

Where: D_i is the random variable related to the coordinates of the i^{th} Way-point, T_i is the pause time at the i^{th} Way-point and is a constant; and V_i is a random variable related to the node speed during its movement toward the i^{th} Way-point. D_0 is the initial node position also selected uniformly and randomly in a spatial domain, R [75].

4.5.2 The Random Direction Mobility Model

In the Random Direction Mobility Model, an initial direction, speed and a finite travel time are assigned to each node. During simulation, the node then travels to the border area in the specified direction. Once the nodes have reached the boundary, they pause for a specified time; they then choose another angular direction (between 0 and 180 degrees) and continue in a pre-specified direction. The Random Direction Mobility Model avoids the clustering of nodes in one area[74].

4.5.3 Mobgen Steady-State Mobility Model

For the Mobgen steady-state mobility model, the first locations are uniformly chosen; that is, all the nodes have a regular pause period at the first locations. About, fifty per cent of the nodes are moving, and fifty per cent are paused until the node velocities and locations converge to their steady-state distributions. The performance metrics values for a given protocol, under the influence of the distributed speed and position, converge to steady-state values [74].

A Random Way-point Model has been chosen; because it is simple, the widely used mobility model in modern research; and it is considered to be the basis for the construction of other mobility models [76]. Furthermore, in the Random Waypoint

model, velocity (v) and pause time (t) are the two key parameters that determine the mobility behaviour of nodes. When the pause time is zero the model mimics the random walking model and this was the key factor in choosing the random way point model.

4.6 Simulation Set-Up

The mobile WiMAX-WiFi video surveillance simulation network consists of the BS, CPE, The Internet, routers and two servers (local and remote), as shown in Figure 4.1. These devices have been configured in a manner similar to the hybrid WiMAX-WiFi system of Chapter Three [see Appendix E], but with few changes. Firstly, the CPE and WiMAX cameras are configured with IEEE 802.16e, instead of the IEEE 802.16d; since IEEE 802.16e is a standard for mobile WiMAX. The network now uses mobile nodes instead of fixed nodes. It expresses the scenario of several mobile devices, like the Smartphone, being used for video surveillance purposes. Simulations have been carried out by OPNET Modeller 14.5 Simulator.

Because of the power limitations of mobile devices, we configured the node applications and profiles with highly compressed and efficient video codec, like the H.264/SVC or the latest H.265/HEVC codec. In this scenario, we adopted the VBR standard, H.265/HEVC video codec, Star Wars 4 video trace compiled by the authors in [70], which has a 352x288 resolution. We selected the H.265/ HVEC standard video formats owing to the compression efficiency of the H.265/HEVC HV encoder.The trace video has a frame rate of 15fps. Table 4.1 shows the detailed trace video characteristics of the configured application for this scenario.

Table 4.1: **Configured Application and Trace Video Characteristics**

Parameter	**Value/feature**
Name of trace files	Star Wars 4
Number of cameras	32
Video resolution	352x288
Frames per second (FPS)	15
Average frame size (bytes)	912.59
Video codec (Encoder)	H.265/HEVC

All the nodes were configured for random mobility using the mobility configuration object pellet. The detail parameters and their values were configured, as shown in Table 4.2, whereby thirty-two mobile nodes or cameras, were all set with a mobility speed of 0 to 10m/s, with no pause time, and adopting the Random Way-point Mobility model.

Table 4.2: Mobility Models Parameters and Values

Parameter	**Value**
Simulation Time	1200s
Number of nodes	32
Environment Size	100m x 100m
Mobility Velocities	0-10m/s
Pause Time	0
Mobility Models	Random Waypoint Model,

Now studies in human locomotion or gaits, indicate that a human being can walk up to 4m/s with 2.2m/s being the transition from walking to running [70] [71] [79]. The normal walking speed differs from one age to the other. In Brazil, for example, women of between 60-69 years have an average normal walking speed in metres per second of 1.07±0.17, while men in the same age range have a normal walking speed of 1.26±0.15[80]. Female adults of 40-49 years have a normal walking speed in metres per second of 1.27±0.20 while the males of a similar age group have a normal speed of 1.35±0.11[80].

Therefore, we set up our mobility parameters to take care of these normal human walking velocities. The idea is to investigate the effect of mobility for people who capture a surveillance scene and want to transmit it on a mobile WiMAX-WiFi network, while walking normally and/or running. The same concept can be applied to non-human moving objects such as cars, train and the like moving at normal human walking velocities.

Two systems have been compared and analysed: the mobile WiMAX system with mobile WiMAX cameras connecting to the BS, and the mobile WiMAX-WiFi system with mobile Wi-Fi cameras. In each scenario throughput, dropped bits, link utilisation, end-to-end delay and jitter measurements were carried at varying mobility velocities:

0, 1, 2, 3, 4….10m/s. For the mobile WiMAX-WiFi system, we also considered a case of transmitting to a local server, in addition to transmission to the remote server.

4.7 Results and Discussion

This section carries a performance analysis on the effect of mobility for mobile WiMAX and mobile WiMAX-WiFi surveillance systems. The analysis is critical for determining the usability of such systems - especially at pedestrian and running velocities which are essential when implementing the developed software of Chapter Five. Furthermore, this analysis helps in ascertaining the optimum mobility rate at which throughput is highest. The performance metrics are throughput, packet loss, link utilisation and latency (End-to-end delay and jitter)

4.7.1 The Effect of Mobility on Throughput

Figure 4.4 shows the average video throughput variation, as the velocity of the mobile camera increases, for the mobile WiMAX and the mobile WiMAX-WiFi surveillance systems. The calculated theoretical throughput values using equation 4.8, are compared to the measured results. Throughput helps in determining the amount of traffic (video/images) bits that flows through the access device; CPE or WMR.

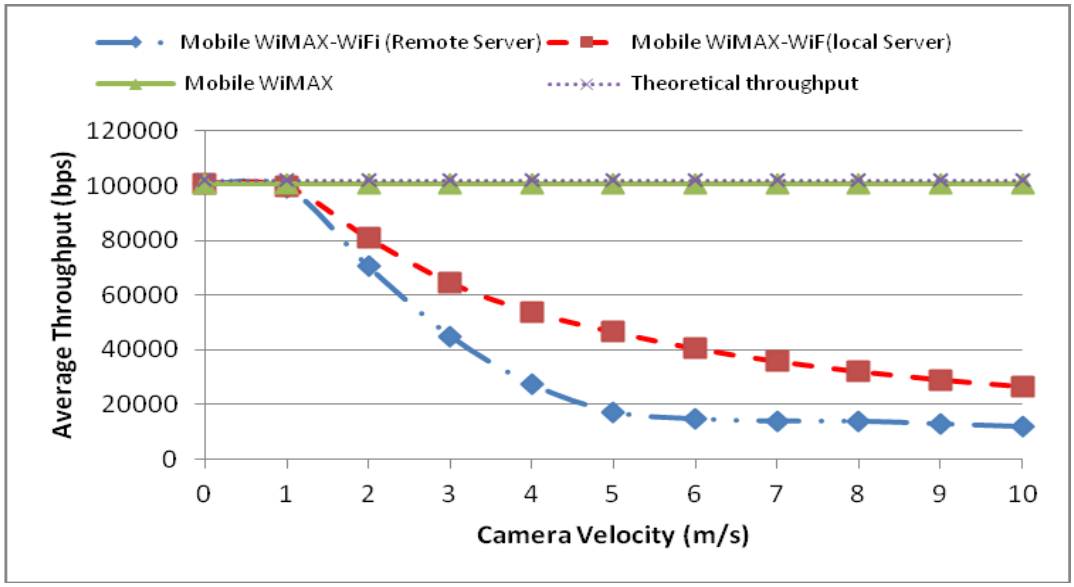

Figure 4.4: Effect of Mobility on Throughput as Speed Varies.

The mobile WiMAX-WiFi is transmitting to the remote and local server; while the mobile WiMAX is transmitting to the remote server. The measured results are

compared with the constant theoretical throughput of 101kbps. For the mobile WiMAX-WiFi system, throughput reduces as the speed increases, regardless of the destination server. This drop in throughput as the speed increases is attributed to the network and transmission delay - among other reasons. At 0m/s, essentially before movement begins, the throughput is highest measuring a performance value of 101Kbps when transmitting to the local server and 99Kbps when transmitting to the remote server. The results also show a small reduction in throughput when transmitting to the remote server, than with the local server.

This difference in throughput values is attributed to high packet drops due to the long distance between the cameras and the remote server. The distance factor was established in the work of [44].

Furthermore, the results indicate that the optimum walking speed needed for high throughput and surveillance operation is between 0 and 1.4m/s.

However, for the mobile WiMAX, throughput remained constant at 100kbps for the mobility range 0 to 10m/s. This result suggests that for a low mobility speed, the mobile WiMAX system throughput is not significantly affect.

4.7.2 The Effect of Mobility on Dropped Bits

From the results of Figure 4.5, from 0 and 1m/s speed, the mobile WiMAX-WiFi surveillance system performed well when transmitting to both the local and the remote servers - recording null dropped bits per second.

However, between 1m/s and 4m/s speed, there is a gradual and linear increase in bit rate loss averaging 10bps to 3700bps and 10bps to 3000bps for the remote and local server respectively. There is another progressive and linear decline between 4m/s and 10m/s. This fall in dropped bits per second and the consequent reduction in throughput, as depicted in Figure 4.4, is due to the reduced Received Signal Strength Indicators (RSSI) between the wireless cameras and the CPE, because of the increased mobility.

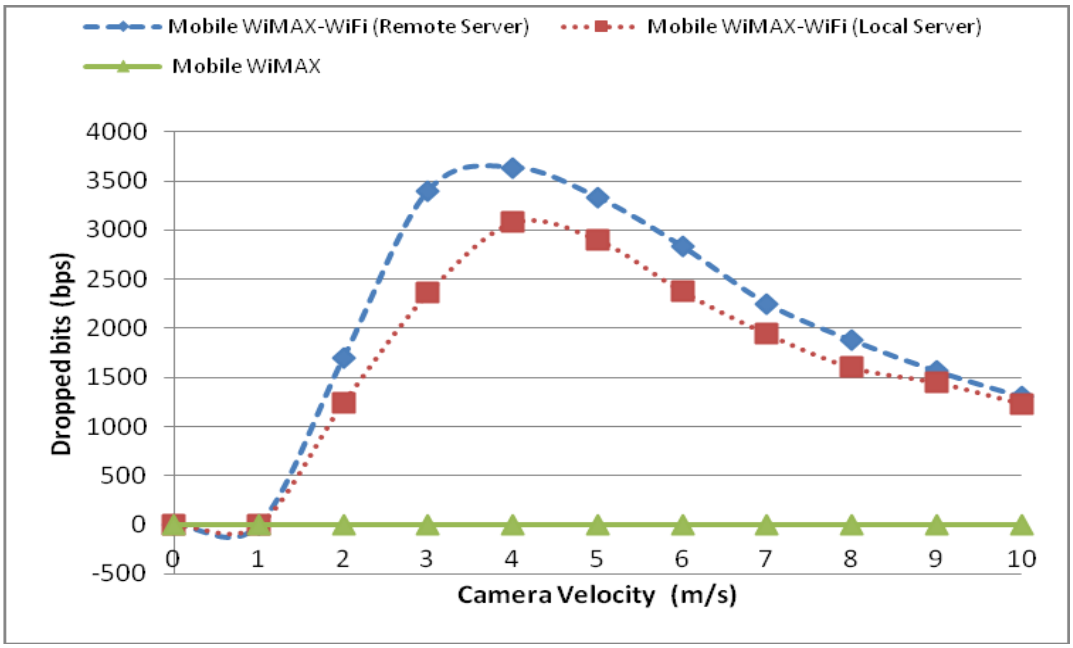

Figure 4.5: Average Dropped Packets as Speed Varies

The available load for the 32 nodes is 101kbps. The 3700bps and 3000bits represent 4% and 3% loss for the remote and local server, respectively, which is above the accepted values, according to equation (2.8). A speed of 1.5m/s gives a percentage drop in packets of 0.990099%. This percentage drop at 1.5m/s mobility indicates surveillance possibilities at an average normal human walking speed of 1.4m/s.

On the other hand, the mobile WiMAX showed good (low dropped bits per second) performance in dropped bits, regardless of the mobility speed, and that explains why throughput was high for the same mobility values, as discussed in Figure 4.4.

Ideally, all sent video bits or packets from the IP cameras should arrive at the local or remote server. Any loss in bits reduces the quality of the transmitted videos. However as stated in section 3.6, the packet or bit loss must not exceed 1%.

4.7.3 The Effect of Mobility on Link Utilization

As stated in Chapter Three, link utilisation is the ratio of throughput to capacity expressed as a percentage. The mobile WiMAX system is compared with the mobile WiMAX-WiFi system. The idea is to ascertain which of the two systems makes efficient use of the uplink WiMAX channel for the same number of cameras. Figure 4.6 shows the link utilisation variations, as the cameras mobility velocity increases.

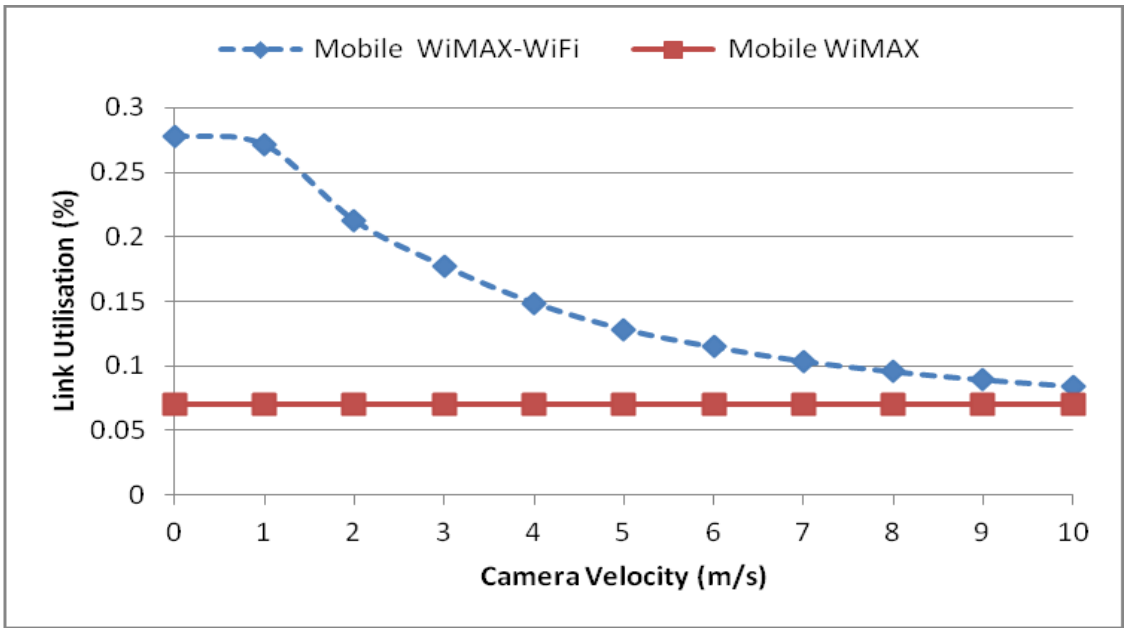

Figure 4.6: Link Utilization Variations with Speed

The results show that the mobile WiMAX-WiFi system has a higher and better link utilisation percentage than the mobile WiMAX. However, the link utilisation for the mobile WiMAX-WiFi system remains high from 0 and 1.4m/s and decreases to between 0.28% and 0.07% from 1.4 m/s to 10 m/s.

For the mobile WiMAX, link utilisation remained low, between 0.06 and 0.065%, regardless of the mobility velocity. This measurement implies that from 0 to 1.4m/s, the mobile WiMAX-WiFi system has a high link utilisation (efficient use of the link); while the mobile WiMAX has reduced link utilisation (uplink channel is idle most of the time).

4.7.4 The Effect of Mobility on End-to-end Delay

Knowing end-to-end delay values helps in knowing congestions levels and therefore indicative of lower efficiency of the communication protocols [39]. In Figure 4.7, we show the average video end-to-end delay variations, as the speed of the mobile node or camera increases for both the mobile WiMAX and the mobile WiMAX-WiFi surveillance systems. For the mobile WiMAX-WiFi systems, the remote server end-to-end delay average 0.09s, compared to 0.03s for the local server. These results represent an end-to-end delay factor of 3, in favour of the local server. This factor is attributed to some reasons, one being the distance from the access node, as

established in [44]. As for the remote server, the video packets pass through many nodes, which are bottlenecks themselves, before arriving at the final destination.

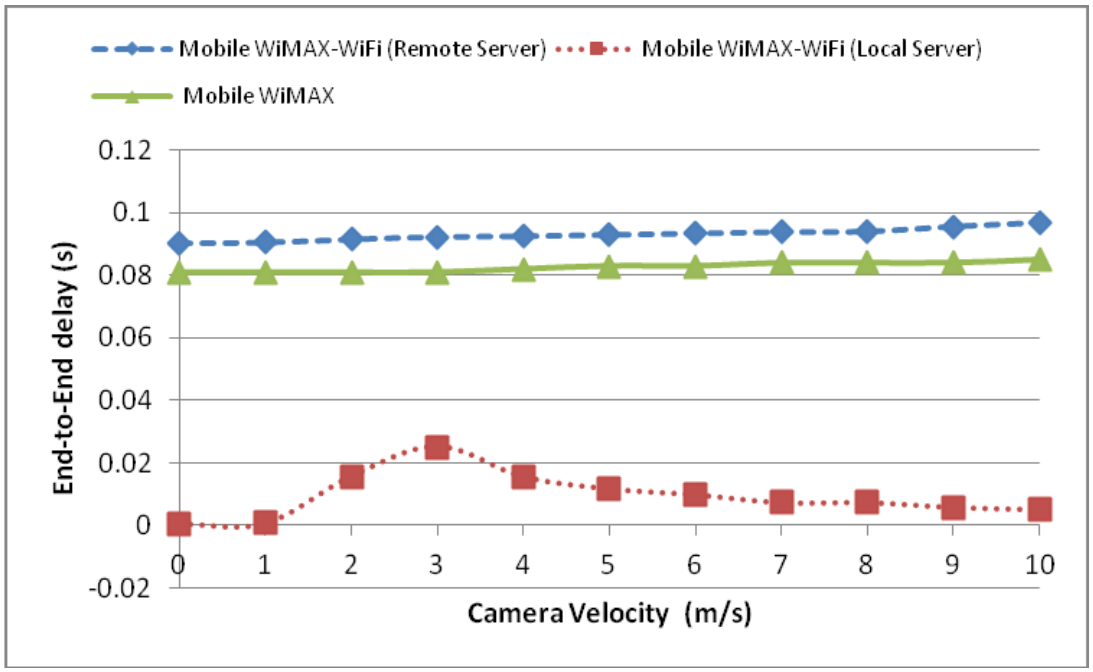

Figure 4.7: Average Packet End-to-end Delay as Speed Varies

As a result, the video signal encounters more processing, network, propagation, transmission and buffering delays when transmitting to the remote server than the local server. Therefore, transmission, propagation and network delays are low when sending to the local server than when sending to the remote server. Notwithstanding this, all the measured end-to-end delay values are all below the acceptable range of 150-200ms for video transmission.

However, for the mobile WiMAX, the end-to-end delay varies between 0.8s to 0.83s as the mobility speed increases from 0 to 10m/s. Thus, when transmitting to the local server, the two systems closely match each other in terms of end to end delay; and they are all within the acceptable range of 150ms to 200ms.

4.7.5 The Effect of Mobility on Jitter

The jitter results are important to ascertain the latency level of the proposed model and to ensure that it does not exceed the maximum allowable value for video transmission. The variations of jitter as the speed increase results for mobile nodes, in

a mobile WiMAX and mobile WiMAX-WiFi surveillance system, transmitting to the local and remote server, are shown in Figure 4.8.

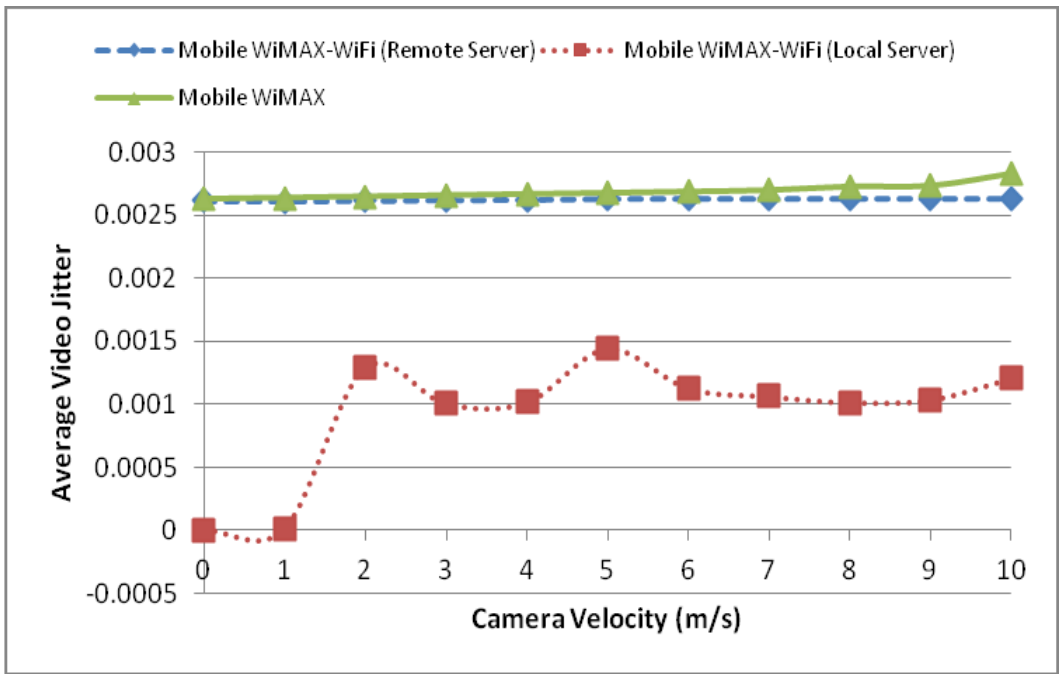

Figure 4.8: Average Jitter Delay as Speed Varies

For the two systems, and mobility speed of 0 to 1m/s, the jitter performance is null, when transmitting to a local server. When the speed increases to between 1m/s and 10m/s, the jitter measurement for transmitting to the local server increases; but it is lower than for sending to the remote server. At 5m/s there is an unusual slight jump in jitter which is considered normal due to the imperfect channel conditions.

All the jitter measured results are below the maximum allowed jitter performance values; they do not exceed 60ms. Mobile WiMAX-WiFi surveillance systems have better jitter performance regardless of destination server than mobile WiMAX systems. This means that a few more nodes can be added - without significantly degrading the transmitted video.

4.8 Chapter Summary

This chapter has described the Mobile WiMAX-WiFi video surveillance network model with mobile camera devices. We derived the mathematical model for throughput and proposed a new performance algorithm for mobile cameras connected to a mobile WiMAX-WiFi network. The algorithm has been tested through

simulation. An analysis of the results on the effect of mobility in a mobile WiMAX-WiFi surveillance system with mobile devices employing the H.265/HEVC encoder has been given for proof of concept. The mobile systems' results have been evaluated for varying mobility velocities; and the optimum speed for improved performance suggested. The performance metrics are throughput, packet loss, link utilisation, end-to-end delay and jitter.

The results have shown that the mobile WiMAX-WiFi system performed well at the mobility speed of between 0 and 1.4m/s; measuring success on throughput, dropped bits per second and link utilisation. Beyond the speed of 1.4m/s, the performance degrades. Mobile WiMAX-WiFi system have better jitter and end-to-end delay measurements, when transmitting surveillance images to the local server is better than when transmitting to the remote server. When it is desirable to transmit to a remote server, the number of cameras and video payload, including frame rate should be reduced. The implications of these results are that the mobile WiMAX-WiFi systems can be used at pedestrian or a normal human walking speed. They cannot be used for cases where one is cycling, or driving at a mobility speed beyond 1.4m/s or 5km/h.

Mobile WiMAX surveillance when used from 0 to 10m/s, are not affected by mobility; and they give high throughput and reduced dropped packets. Measured flow throughput values agree with the derived flow throughput equations, derived in Chapter Three and in this Chapter.

In the next chapter, we build on the findings of Chapter three and Chapter four by proposing a new mobile application algorithm and software application for video surveillance. The developed software application is tested on a live hybrid WiMAX-WiFi network; for the purpose of video/image compression and transmission of surveillance images/videos.

Chapter Five

5 Surveillance Application Software for Mobile Phones

This chapter proposes a mobile surveillance process model and an algorithm and shows how the application software for smartphones operating in the hybrid WiMAX-WiFi environment was developed. This chapter rides on the background of the literature on WiMAX and the hybrid WiMAX-WiFi as discussed in Chapter Two and the proven performance of hybrid WiMAX-WiFi surveillance systems as, demonstrated in Chapter Three and Chapter Four.

The next section describes some of the related work on surveillance application software; and it proposes the surveillance application software for smartphones. The conventional software development process models have also been discussed - leading to our proposed process model for mobile surveillance application development, as will be mentioned in section 5.2.

Using the proposed process model, we developed a new algorithm for surveillance software suitable for low bandwidth WiFi environments as explained in section 5.3. Section 5.4 gives the constraints and assumptions made. The implementation detail and processes involved in modelling, construction and final deployment of the software, are discussed in section 5.5. Section 5.5 also gives the test results for the deployed application software; while the chapter summary follows in section 5.6.

5.1 Related Work on Mobile Surveillance Applications

Shinde et al. [81] proposed a classic approach to security provision for a home-based system robot and environment surveillance whereby any changes in the movement of the robot could be seen via the camera erected on the robot or the ceiling. Similarly, any capture crime scene would be received through SMS alert messages or Internet-based service messaging using the Android mobile phones. The Cisco Video Surveillance Operations Manager Mobile App allows one to view live video from a mobile device, such as an Android-based tablet or phone [82]. The Wire path IP Surveillance app allows one to view surveillance videos from encoders, IP cameras, and Network Video Recorders (NVRs) on an Android Smartphone or tablet [83].

Ononiwu et al. [84] wrote a recent paper on video surveillance with intrusion detection via a mobile device. They set an electronic system designed to observe an area from a distance by using electronic equipment with the enhanced ability automatically to detect the presence of any moving body into the region being seen (watched). The system had an extra capability to provide users with remote access to the visual display on a mobile device via the internet video streaming [84].

In this work, we proposed a software application algorithm for mobile or smartphones; and we developed the low bandwidth application software for hybrid WiMAX-WiFi, Wi-Fi-broadband and cellular networks environments.

5.2 Existing Software Development Models

Application software is a stand-alone programme that solves a particular business or security need. Application software comprises tailored processes for companies or technical information to assist the business. The software development models are carefully chosen processes or methodologies for the development of the project, in order to achieve the project's objectives and goals. Usually, these models specify the various stages in the processes or methodologies, including the order in which they should be carried out.

The testing techniques of the developed software are mostly determined by the type of model selected. Software engineers have developed several models for software development life cycle, each with a specified achievable objective. The existing software development models include the Waterfall model, the V model, the Incremental model, the Rapid Application Development *(*RAD) model, the Iterative model, the Agile model, and the Spiral model. A description of some of these models is given below to best understand our proposed process model, as described in section 5.3.

5.2.1 Waterfall Models

The Waterfall Model, also known as the **linear-sequential life cycle model** was the first introduced software development process model [85]. Each stage in the waterfall model is finished completely before the next stage begins. This model is ideal for small projects, with specific requirements. Reviews are made at every step, to

determine whether the project is still viable, or should be discarded. At the completion of the project, testing is performed. Figure 5.1 shows the various stages of the waterfall models.

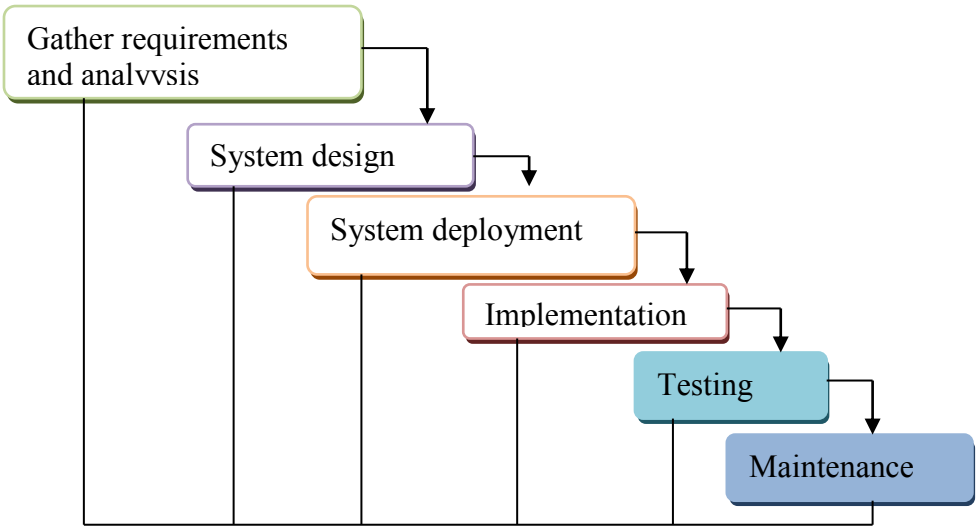

Figure 5.1: The Waterfall Model

While this model has certain advantages, such as simplicity and easy management, due to its lean size; it also has weaknesses. The model is not flexible to changes, when it reaches the testing stage; and it has no overlap phase [86]. As such, this makes it risky and uncertain. The model is also not ideal for complex and object-oriented projects.

5.2.2 The Incremental Model

The incremental model has a well-thought out complete number of requirements that are divided into various builds depending on the size of the project. Each build has its smaller modules for design, testing and implementation, as shown in Figure 5.2. The first three partly built processes produce a working software version. The next built process adds functions to the previous module releases, and the process continues until the complete product is achieved.

This model has several advantages: It can generate quick working software during the software life cycle; it has flexibility of design, testing and implementation; it is easier to test and debug; it allows for customer feedback, as well as low initial delivery costs and risks. However, it requires a precise planning of the whole project and the overall cost may be more at the end of the project.

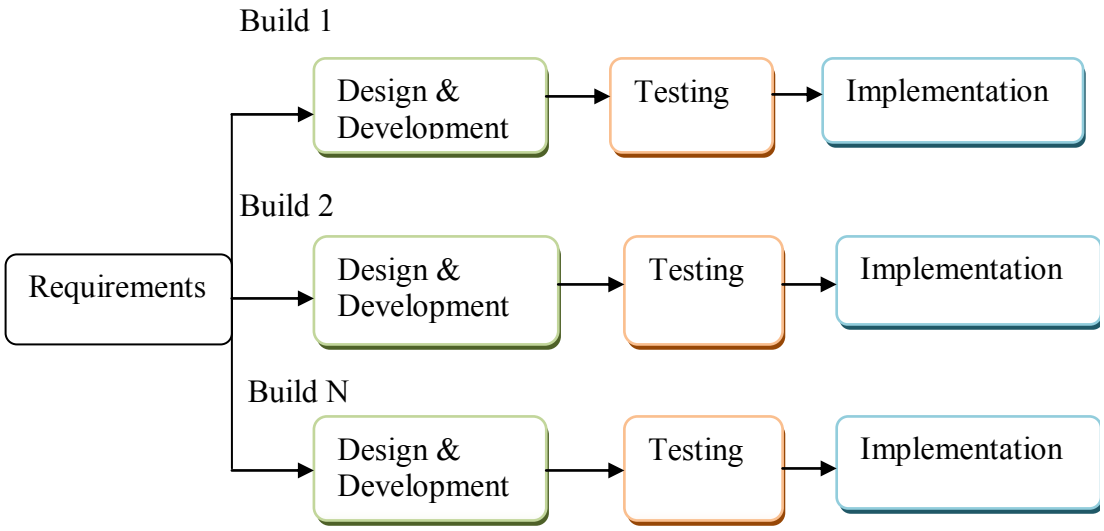

Figure 5.2: The Incremental Software Development Model

5.2.3 The Iterative Model

Daud [87] suggests that an iterative model is considered to have a more efficient and reliable approach for software development. An iterative software development model, as shown in Figure 5.3, starts with a sketch specification of requirements. Part of the software is specified, implemented, and reviewed, and any further requirements are then identified [85].

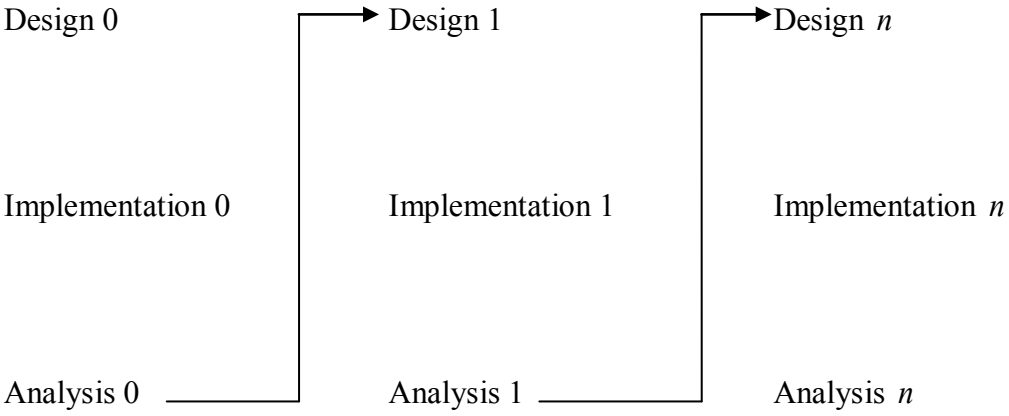

Figure 5.3: The Iterative Software Development Process Model

The process is repeated and for each cycle, a new version of the software is produced. The advantages of this model are that it is easy to track defects at an early stage of the software development; since complete product building, and improvement are done in phases. The model also allows for user feedback, making the end-product to be widely accepted. The major weaknesses of this model are the rigid iterations that have no

overlaps [86]; and it may have a costly system architecture as all its requirements are not gathered in advance.

5.2.4 The Spiral Software Development Process Model

The spiral model places more emphasis on risk analysis[86]; and it is comparable to the incremental model. A software development process in the spiral model passes through four stages in iterations: Planning, Risk Analysis, Engineering and Evaluation [85]. In the planning stage, the project requirements are assembled, and the risks involved are assessed. Both business and system requirement specifications are determined. Each successive spiral builds on the first spiral from the planning stage.

Next, the model identifies the risks and any possible solutions. The Prototype production follows the risk analysis after which suggested alternate solutions are implemented [85]. The engineering stage is the stage at which the software is developed and tested while the evaluation stage allows for evaluation of the software and project; and the spiral continues. Figure 5.4 shows the spiral software development process model:

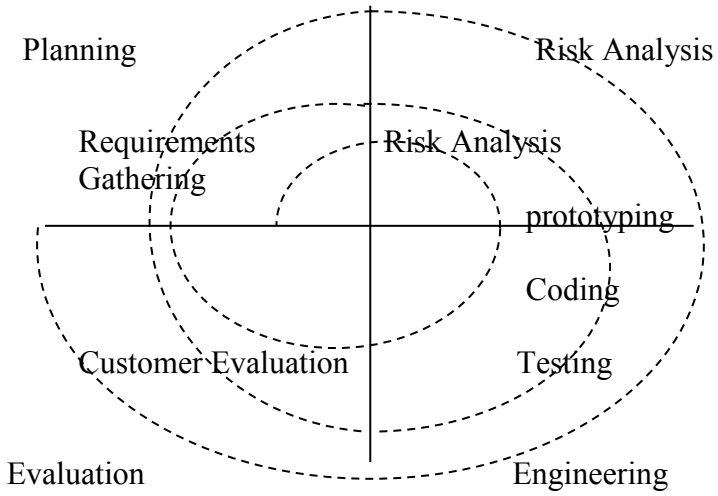

Figure 5.4: Spiral Software Development Process Model

This model has the advantage that it includes additional software functionality, in time, during the design and implementation stages. The design also allows for early software production during the life cycle of the software. However, the model needs the expertise to conduct the risk analysis; and success depends on positive gains in the risk results. It, therefore, does not work well for small projects.

As stated, the above process models help to best understand our proposed process model described in the next section. The merits of each process model have been carefully examined - leading up to the design of our process model.

5.3 The Implemented Software Development Process Model

Figure 5.5 shows a proposed and implemented process model for the mobile wireless surveillance application software.

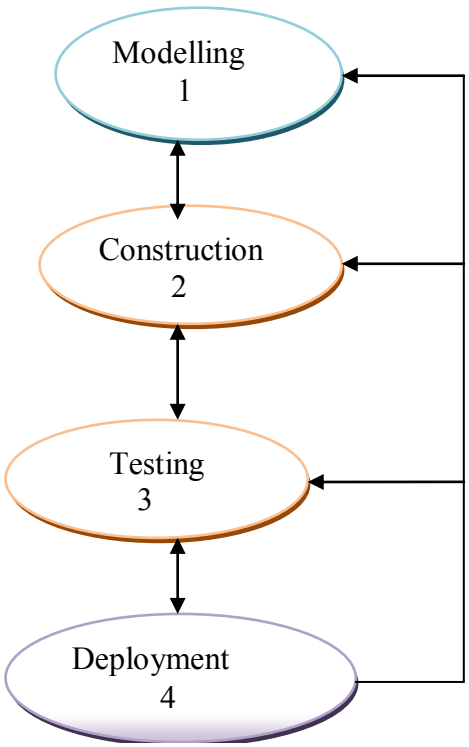

Figure 5.5: The Implemented Software Development Process Model

The process model design is ideal for small to medium size projects and has the advantage of simplicity, short software development time and low implementation cost. Like the iterative and incremental process models, this model also allows for users to obtain feedback, making the end-product to be widely accepted. The process model has four stages: modelling, construction, testing and deployment.

The sub-sections that follow, discuss a detailed description and the implementation of the four stages.

5.3.1 Modelling the Mobile Surveillance Application

The modelling stage involves the creation of models that allow the developer and the user to understand the software requirements better. It allows users and designers to formulate the problem, and to state the software needs or requirements. The mobile surveillance application was modelled, as shown in the algorithm of Figure 5.6

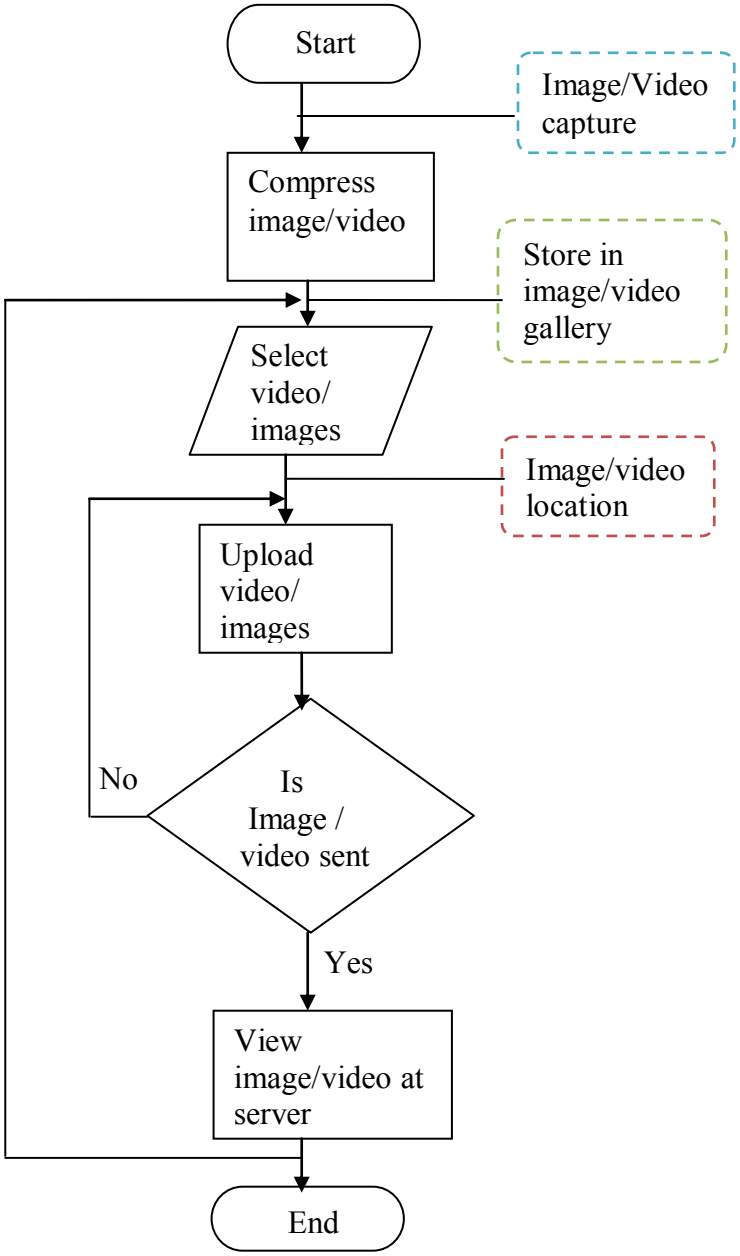

Figure 5.6: Mobile Wireless Surveillance Algorithm

A mobile device captures video/images using the camera that comes with it; and these videos and images are kept in the image gallery. The video/images' quality at this stage is high, lossless or uncompressed. One can choose to upload and send these

pictures in their uncompressed format at the cost of added bandwidth and loss in data units, if a 3G or 4G mobile cellular network link is used.

Due to the limited bandwidth of the wireless link, the video images are compressed and stored in an image gallery - before the uplink transmission to the server for monitoring and viewing.

The developed mobile wireless surveillance software should provide a mechanism for selecting the video and/or image to be sent to the server. Once the image has been sent to the server, it can be viewed after the decompression process. The developed software allows the user to state the location of the captured image for easy identification during monitoring and viewing at the server end. The location name also serves as the image/video name. The location name also guides law-enforcement officers in identifying the crime scene.

5.3.2 Construction of the Application

The construction stage involves code generation, compiling and debugging. Figure 5.7, shows the construction process during software development; and it illustrates the tasks involved in the coding, compiling and debugging cycle.

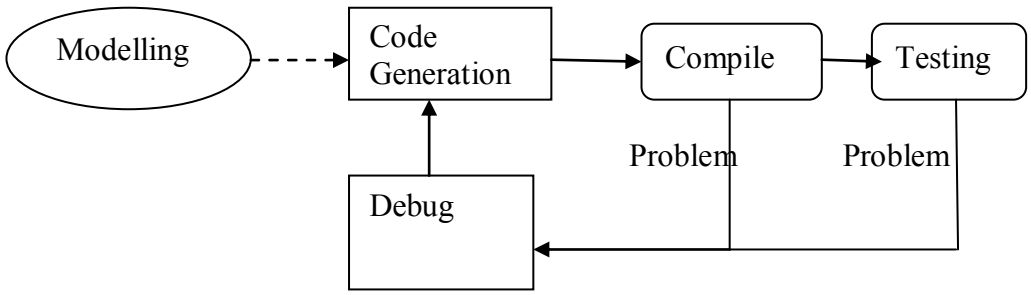

Figure 5.7: Software Construction Process Model [88]

The central task in this process is coding. The codes must take into consideration the problem statement or requirements specifications identified in the modelling process. There are several errors detected during the compiling of codes and testing. To detect these errors, debugging is performed. Debugging is a process of problem analysis and resolution[88]. Once the problem has been identified and corrected, the code is modified to reflect the corrections made; and the code is then re-compiled.

5.3.3 The Testing of the Application

The compiled codes are tested; and when they pass, released to prepare for product deployment. If the codes fail, the debugging and testing process is re-commenced.

5.3.4 Deployment of the Application

The deployment process involves delivery of the product to customers and feedback, based on the evaluation made. Depending on the feedback given, the software is re-modelled, re-constructed and redeployed - as an upgrade to the first version of the software. At times, it may be necessary to maintain the model design, but only change the construction stage.

5.4 Constraints and Assumptions

In designing and developing the mobile security application software, the following constraints have been considered: Firstly, most cell phones have limited memory and cannot store large files of video images. Secondly, the existing mobile or Smartphone encoders are of the H.264/AVC non-scalable types, which put a further strain on camera memory and storage. The non-moving images are encoded mainly by using the JPEG standard.

Furthermore, since the application is intended to be used in low bandwidth wireless network environments, it becomes reasonable to tailor our application for JPEG images; although it is adaptable to most video encoder types. We assume that the local and the remote servers have adequate space to store the transmitted surveillance images and that both real and non-real time surveillance images are transmitted.

5.5 Software Application Development process

The software application development was developed by using a desktop computer equipped with Windows 7 Enterprise, 64-bit operating systems with an Intel (R), Core (TM) i5 CPU processor and 8GB Random Access Memory (RAM). The computer was installed with Java Software Development Kennels (SDK) and Android Studio version 1.5.1 Integrated Development Environments (IDE). An Android Samsung Smartphone (SM-G313H Model) version 4.4.2 was set with developer option activated and it was used for testing the codes and the application software.

5.5.1 Android Studio Integrated Development Environments

The Android Studio is the Integrated Development Environment (IDE) for Android that was announced in May 2013 at the Google developers event; and is intended to serve as an alternative to Eclipse [89], (see Figure 5.8 for the IDE snapshot). Android Studio is Google's newest solution to many Android development woes [89] [90]. Android Studio is based on the Java IDE called IntelliJ [89]. It operates under the Java programming language and the eXtensible Mark-up Language (XML).

The XML is an open standard for sharing data and information between computers and computer programs, as explicitly as possible [91]. The Android Studio IDE is specifically designed for Mobile phones, tablets and similar smart devices. Supported platforms include Windows, Mac OS X and Linux.

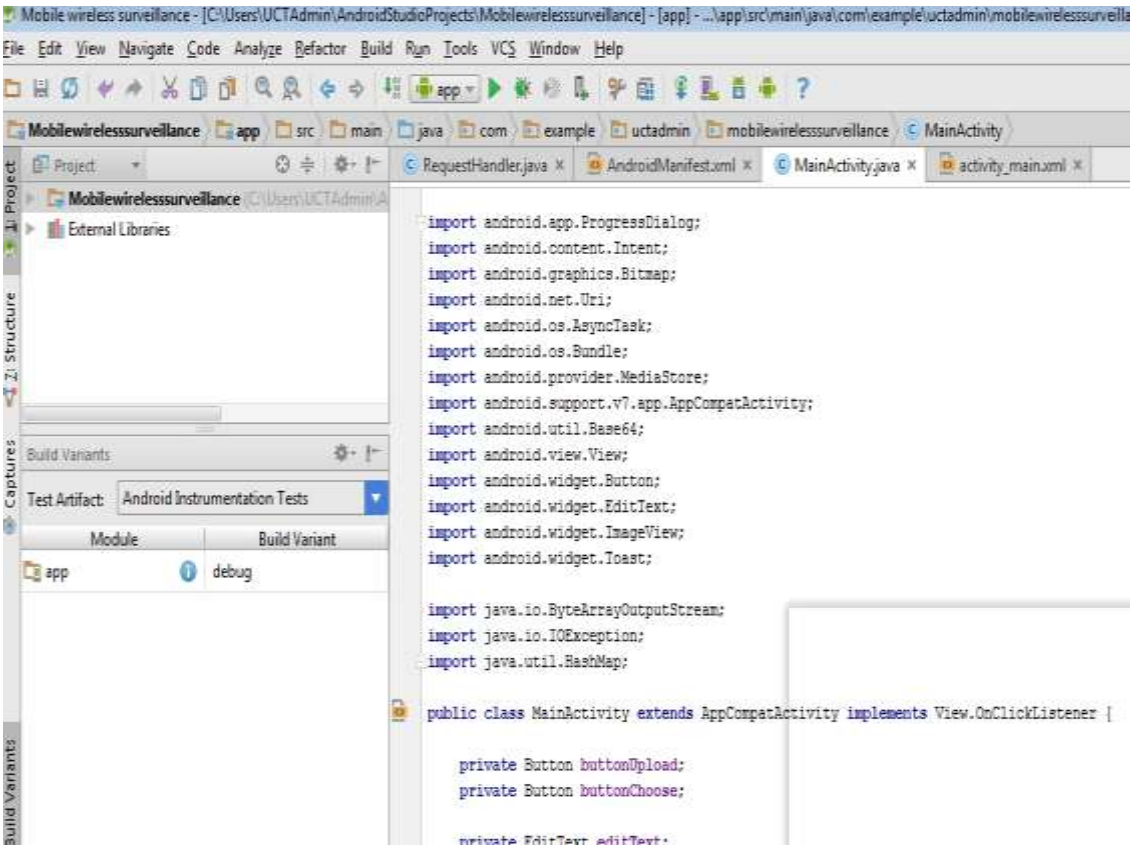

Figure 5.8: Android Studio with the Editor, Project, and Android panels

5.5.2 Code and Software Development of the Applications

The android studio allows code generation, compiling, debugging and testing of Java and XML Codes. The generated mobile surveillance codes consist of two XML files and two Java files. The first XML file is the AndroidManifest.Xml file, which outlines the XML version, the application or label name and the permission specifications (Internet and external storage) among other features. The code snippet is shown below:

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.example.uctadmin.mobilewirelesssurveillance">

    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission
android:name="android.permission.READ_EXTERNAL_STORAGE"/>

    <application
        android:allowBackup="true"
        android:icon="@drawable/icon"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
```

The second XML file is the activity_main.xml, which describes the image selection and upload button. This file also defines the codes for viewing the image before uploading to the chosen server, including the optional text provision for indicating the location or place, where the image was captured. The text also serves as a unique file name for the image in the server. The code snippet is shown below:

```
<Button
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:text="Choose Image"
    android:id="@+id/buttonChooseImage" />

<ImageView
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:layout_weight="1"
    android:id="@+id/imageView" />

<EditText
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:id="@+id/editText"
    android:hint="Location Name" />
```

```
<Button
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:text="Upload Image"
    android:id="@+id/buttonUpload" />
```

The main Java file, named *MainActivity.java*, holds the primary codes of the applications. It describes various classes: private, protected and public for the selection, compression, viewing and uploading of the images. This file also specifies the destination address of the transmitted images. The detailed codes are shown in Appendix F.

The second Java file is the request *handler.java,* and it consists of the request handler class for connection, read time-out and connect-time out, among others. The code snippet is shown below:

```
public class RequestHandler {

    public String sendPostRequest(String requestURL,
                                  HashMap<String, String> postDataParams) {

        URL;

        StringBuilder sb = new StringBuilder();
        try {
            url = new URL(requestURL);

            HttpURLConnection conn = (HttpURLConnection)
url.openConnection();
            conn.setReadTimeout(15000);
            conn.setConnectTimeout(15000);
            conn.setRequestMethod("POST");
            conn.setDoInput(true);
            conn.setDoOutput(true);
```

The developed application has the features, as they are depicted in Figure 5.9. It has the image select button, the image upload button and the text editor for indicating the place of the scene occurrence. This field also gives the image name in the local or remote server. When the choose-image button is pressed, a pop-up page directing the users to the folder where the images or videos are stored; and it is opened. Users select the captured image, and type the location name of where the image was captured; and abbreviations are allowed.

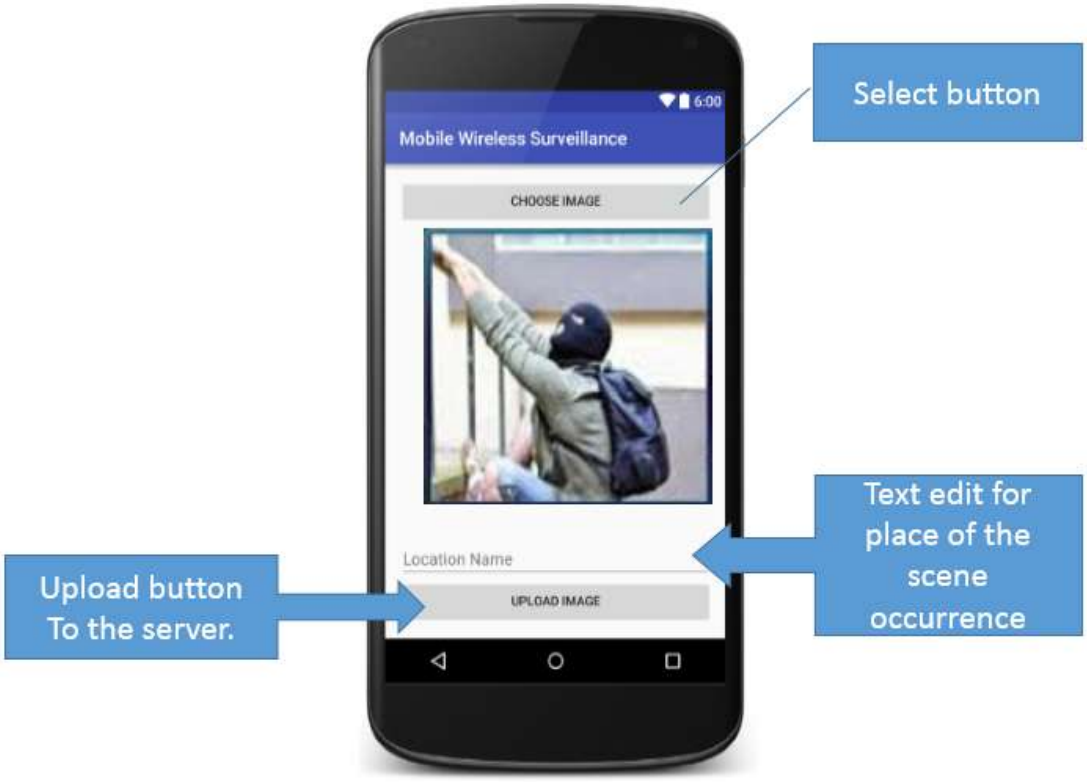

Figure 5.9: Features of Application Software after Development

5.5.3 Testing and Deployment of the Application

To test the codes and the application, we activated the USB debugging mode setting for the Smartphone under the Smartphone developer options. In this case, a real Android Smartphone, Android version 4.4.2, model SM-G313H is connected to the personal computer, which houses the codes to be tested. The Wi-Fi network is either activated for transmission on the WiMAX-WiFi network, or the mobile data option for transmission over the cellular network.

The application is then run and has an option to test on a real or an emulator device. The real device is selected and the application then brings the features of Figure 5.9. The image/video is then selected from the image/video gallery, and sent to a particular IPv4 IP address in the server.

When the image is uploaded, a "successful upload" message pops-up (see Figure 5.11) to indicate that the image/video has been sent. The sent image/video can be sent to either a local or remote server/viewing PC, or to both. In either of the server options, a specific video/image folder was created for the reception and verification of

all surveillance images/videos transmitted by smartphone. The Java codes specify the destination IP address for the server(s); and this address is unknown by smartphone users.

The Images/videos are decompressed, stored and named according to the name given at transmission.

Figure 5.10: **Diagram Showing Successful Operation of the Mobile Surveillance Application in a Wi-Fi Environment**

The deployment process involves delivery of the product to customers and feedback based on the evaluation made. The tested mobile wireless surveillance application software is first converted into an Android Application Package (APK) format. The APK format is the executable file format for smartphone devices. This format allows the surveillance application to be easily installed or uninstalled.

Once the APK format of the application has been created and saved, it is ready for deployment to any smartphone. The APK file is then run on several smartphones and the users send images to the server. The mobile devices are also used as cameras for capturing surveillance video/images. Figure 5.12 and Figure 5.13 show, typically, how the deployment has been done on real networks.

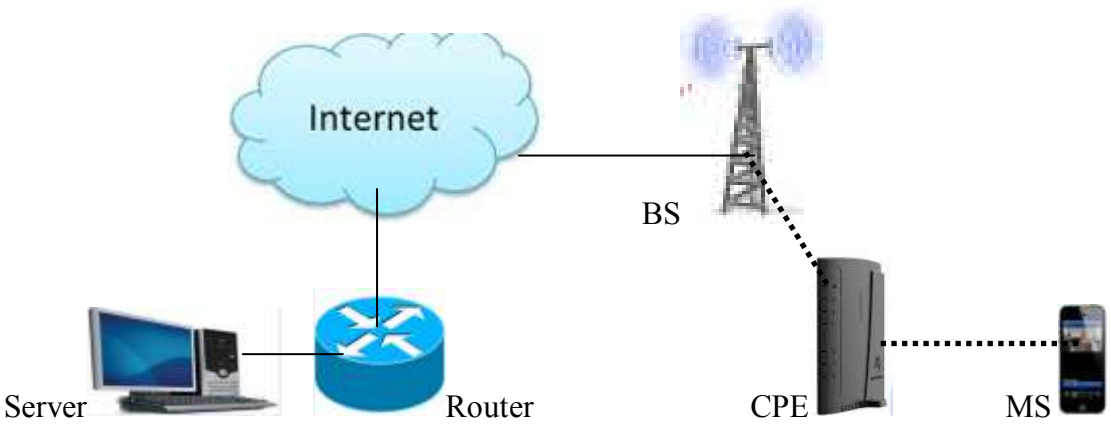

Figure 5.11: Deploying Application in a Hybrid WiMAX-WiFi Network in Zambia

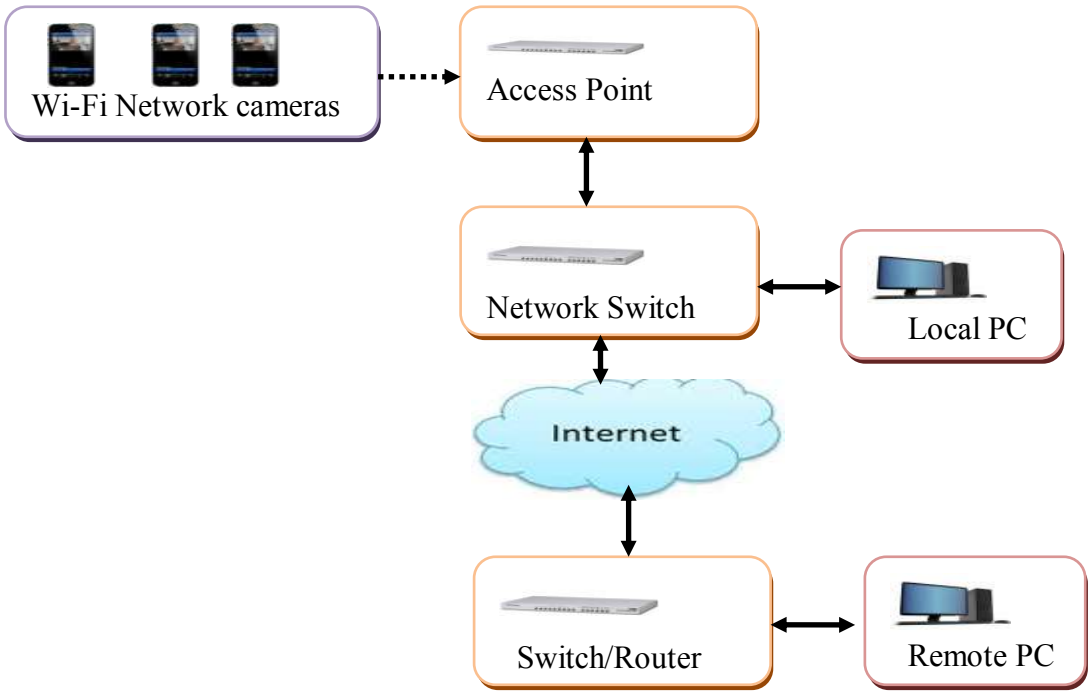

Figure 5.12: Deploying the Application in a Wi-Fi - Broadband Network at UCT, South Africa

5.6 Chapter Summary

This chapter has described the related work on surveillance application software; and it has discussed some of the typical software development process models. Based on the existing process model, a new process model has been proposed. The new process model borrows some strength of the conventional software development models like the waterfall, iterative, spiral, etc. Furthermore, a new algorithm for mobile surveillance application software has been proposed and implemented.

The new algorithm and the developed software application are ideal for use in low-bandwidth mobile WiMAX–WiFi surveillance systems. The new software can compress surveillance images/videos; and using a smartphone, transmits them to the server in any Wi-Fi environment.

The developed software has been tested on real smartphones, the hybrid WiMAX-WiFi network and broadband network with Wi-Fi access. The software has performed as envisaged and the requirements of the third objective of this thesis.

It is possible to capture and transmit surveillance image/video at the pedestrian speed not exceeding 1.4m/s, as simulated in Chapter Four and demonstrated on the actual mobile camera in this chapter.

Chapter Six

6 Conclusion and Future Works

This chapter provides the conclusions of the thesis, arising from the simulation and experimental approaches, results and general work done on hybrid WiMAX-WiFi video surveillance systems. The hybrid WiMAX-WiFi systems have been compared with the conventional WiMAX surveillance systems, in order to mitigate the problem of scalability, scarce WiMAX cameras, camera cost, blind spots and limited Wi-Fi bandwidth. Three set objectives to address these problems have been formulated and implemented through Chapter Three, Four and Five. Chapter Two provided the underlying literature basis for the implementations.

Section 6.1 gives the conclusions on the general literature survey, the significant results/findings and implications. Section 6.2 provides the recommendations for implementing the hybrid WiMAX-WiFi surveillance systems while section 6.3 gives some suggested future directions for further research.

6.1 Conclusions

This thesis has discussed the performance analysis of hybrid WiMAX-WiFi video surveillance systems of the Fourth Generation Surveillance System (4GSS) type. Surveillance systems are critical for monitoring and detecting crime and disasters in public places such as bus and train stations, airports, car parking lots, shopping malls and the like. This necessity becomes even more critical in developing countries where bandwidth is scarce, yet surveillance requirements rank top.

WiMAX is a wireless metropolitan access network technology that provides broadband services to connected customers. Major modules and units of WiMAX include the Customer Provided Equipment the Access Service Network which consist one or more Base Stations and the Connectivity Service Network Various interfaces exist between each unit and module. WiMAX is based on the IEEE 802.16 family of standards. Wi-Fi, on the other hand, is wireless access network operating in the local area network. It is based on the IEEE 802.11 standard. Existing Wi-Fi systems have the advantages of wider deployment of Wi-Fi IP cameras, cost effectiveness, etc. but

they suffer from the challenges of packet loss, unguaranteed Quality of Service (QoS), reduced throughput and coverage radius. Equally, the WiMAX Video surveillance systems do not make efficient use of the channel bandwidth; they are non-scalable, and they have limited WiMAX IP cameras deployment, etc. Notwithstanding this, the WiMAX networks offer guaranteed QoS, support higher bit rates; and they have wider coverage radii. The integration of both WiMAX and Wi-Fi exploits the advantages of the two wireless technologies. The Wi-Fi part of the hybrid WiMAX-WiFi has been meshed, to improve the scalability and the reliability.

Meshed and unmeshed WiMAX-WiFi video surveillance models and algorithms for scenarios of fixed wireless cameras have been proposed, simulated and compared with the conventional fixed WiMAX model.

The results have shown that:

- Throughput increases linearly but below the theoretical maximum, load and bandwidth value.

- The meshed WiMAX-WiFi surveillance system has higher throughput than both the unmeshed WiMAX-WiFi and the conventional fixed WiMAX systems during the first 12 to 16 cameras. This result is consistent with the 15fps and 1420 bytes payload, H.264/AVC video because meshed systems allow for the coverage of nodes beyond the coverage range of a Wi-Fi CPE.

- The unmeshed WiMAX-WiFi system showed lower and better values of end-to-end delay and jitter than the meshed equivalent.

- Additionally, the hybrid WiMAX-WiFi has better link utilisation and Signal-to-Noise Ratio performance, when compared with the existing WiMAX system.

The implications of these results are that, at a video payload of 1420 bytes and frame rate of 15fps, a customer provided equipment can allow up to 16 cameras without exceeding the acceptable packet loss of 1%. However, when end-to-end delay and jitter recommended limits are considered, that is 150ms-200ms and 60ms

respectively, a maximum of 12 cameras should be allowed per CPE. The hybrid WiMAX-WiFi is more scalable than the WiMAX surveillance system.

A Hybrid WiMAX-WiFi video surveillance model and algorithm for scenarios of mobile wireless cameras have also been proposed, simulated and compared with the WiMAX model. A Random-Way Point-Mobility model has been considered for the case of mobile cameras moving between 0 and 10m/s.

The results show:

- When the nodes move at a speed beyond 1.4m/s, there is a general degradation in throughput.
- Mobile systems drop more bits per second than the fixed system, when the mobility speed exceeds the normal human walking speed of 1.4m/s.
- A corresponding rise in end-to-end delay and jitter performance for a mobile WiMAX-WiFi surveillance system.
- Video compression with scalable encoders of the H.264/SVC type or the highly efficient H.265/HEVC codec is the best choices for mobile surveillance systems.

The implication of these results is that the hybrid WiMAX-WiFi systems can, effectively, be used at pedestrian or normal human walking velocities. They cannot be used for cases, where one is cycling, driving at a mobility speed beyond 1.4m/s, or 5km/h.

Finally, the thesis has proposed and implemented a model for software development targeting mobile wireless surveillance. An algorithm for compression and transmission of surveillance images in low bandwidth hybrid WiMAX–WiFi environment has been implemented to achieve application security software for smartphones. A security software application allows the sending of surveillance images to either local or remote servers by using any Smartphone with H.264/AVC and JPEG codec.

- The developed software has been tested on real smartphones and WiMAX-WiFi network; and it has performed as envisaged.

The performance analysis was limited to IEEE 802.11b/g standard on the Wi-Fi link and IEEE 802.16d standard on the WiMAX link. A clear line-of-sight between the transmitting devices was assumed.

6.2 Recommendations

Hybrid WiMAX-WiFi video surveillance systems are recommended, not as a substitute but as a complement to wired systems. They can be used in an environment where it is practically impossible to use wired systems. As stated this may include areas, such as: old traditional buildings, rocky environments as well as areas prone to vandalism. It can also be used in places that have low bandwidth.

We also recommend that the video cameras should have frame rate limitations of between 1 to 15fps for H.264, MJPEG and MPEG-4 non-scalable encoders; and the payload byte size should not exceed 1500bytes at 15fps. High frame rates should be utilised, where scalable encoders are used, such as, in H.264/SVC and H.265/HEV encoders. Furthermore, we note that most wireless IP cameras use the non-scalable MPEG-4 and H.264/AVC codec which have low video compression ratios or divisors; and therefore, they limits the number of cameras that can be connected wirelessly. A paradigm shift towards more scalable and compression efficient encoders of the H.264/SVC and H.265/HEVC should be pursued.

It was observed that the CPE has a limitation in terms of the number of cameras it can handle at a time - especially when remote servers are used. For optimum and efficient operation, the number of cameras should not exceed 12 for a 1420 byte, 15fps transmitting over 10km distance in a hybrid WiMAX-WiFi network.

6.3 Future Work

In future, this work could be extended to look at the effect of throughput, jitter and end- to-end delay for a case, where both the cameras and CPE are mobile. It would be a case of a CPE installed in a bus or train and passengers with cell phones sending surveillance videos/images to a mobile CPE, which would route the surveillance images/videos to a remote server via a nearby fixed BS.

Furthermore, this work assumed a manual capture of image/videos; which under panic and unforeseen crime situations would be difficult to achieve. Future work should

explore the possibility of automatic video/image capture, compression and transmission of surveillance image/video using smartphones.

The developed mobile surveillance application can be installed on any Android smart phone with H.264 and JPEG encoder. In future, a similar application could consider smartphones with H.265/HEVC encoders and non-Android platforms.

REFERENCES

[1] R.-Y. Chang and C.-L. Lee, 'IP Video Surveillance Applications over WiMAX Wireless Broadband Technology', in *IEEE Fifth International Joint Conference on INC, IMS and IDC*, 2009, pp. 2100–2102.

[2] M. Ibekwe, S. Vitek, M. Klima, and P. Dostal, 'Modeling and Evaluation of Image Quality in Wireless Surveillance Networks', in *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2012, pp. 345–352.

[3] H. Kruegle, *CCTV Surveillance: Analog and Digital Video Practices and Technology*, Second. Elsevier Butterworth–Heinemann, 2007.

[4] Anixter Inc, 'IP Video Surveillance Guide', *Anixter Inc*, 2301 Patriot Boulevard, Glenview, IL 60026-8020, pp. 1–36, Sep-2012.

[5] M. Al Najjar, M. Ghantous, and M. Bayoumi, *Video Surveillance for Sensor Platforms: Algorithms and Architectures*, vol. 114. New York: Springer Science+Business Media, 2014.

[6] R. Carlo, R. Visvanathan, and F. Gian Luca, 'Special Issue on Video Communications, Processing, and Understanding for Third Generation Surveillance Systems', *Proc. IEEE*, vol. 89, no. 10, pp. 1415–1422, 2001.

[7] T. D. Räty, 'Survey on contemporary remote surveillance systems for public safety', *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 40, no. 5, pp. 493–515, 2010.

[8] J.Cabasso, 'Analog vs. IP Cameras.' [Online]. Available: http://www.aventuracctv.com/newsletter/DOCS/Aventura_Newsletter_02_Analog_vs_IP_Cameras.pdf. [Accessed: 02-Jun-2014].

[9] Moxa, 'Three Key Design Considerations of IP Video Surveillance Systems Three Key Design Considerations of IP Video Surveillance Systems.' Moxa Inc, pp. (1–4) – (1–11), 2012.

[10] J. W. King, 'Planning and Design', in *Cisco IP Video Surveillance Design Guide*, August 18., 2009, pp. 4–1–4–37.

[11] I. E. G. Richardson, *The H.264 Advanced Video Compression Standard*, 2 nd. West Sussex, PO19 8SQ, United Kingdom For: John Wiley and Sons, Ltd, 2010.

[12] J. E. Leedy, P. D., & Ormrod, 'Planning and design.', in *IP Video Surveillance Fundamentals Overview*, 2014, pp. 1–38.

[13] Z. Liu, E. Hauser, and J. Liu, 'Secure Internetworking Video Surveillance for DHS Protection Mission', in *The Department of Homeland Security Conference-Working Together: Research & Development (R&D) Partnerships in Homeland Security*, 2005, pp. 1–12.

[14] Razberi Technologies, 'Taking a First Step Cyber Security on Video Surveillance Systems.' Razberi Technologies Inc. 13755 Hutton Dr, Suite 500 Farmers Branch, Texas 75234, Texas, pp. 1–5, 2015.

[15] F. Hanane, S. C. Shyam, and R. Prasad, *Voice over IP in Wireless Heterogeneous Networks*. Springer Science+Business Media, 2009.

[16] M. J. Muzammil, 'Design of Multi-threaded Real Time Embedded Video Acquisition System from IP Cameras', in *3rd International Conference on Computer, Control & Communication (IC4)*, 2013, pp. 2–6.

[17] S. Ponlatha and R. S. Sabeenian, 'Comparison of Video Compression Standards', vol. 5, no. 6, 2013.

[18] J.-Y. Dufour, *Intelligent Video Surveillance Systems*, First. UK: ISTE Ltd, 27-37 St George's Road 111 River Street London SW19 4EU, 2013.

[19] A. C. Caputo, *Digital Video Surveillance and Security*, Second. butterworth-Heinemann, 2014.

[20] R. ITU-T, 'Series H: Audiovisual and Multimedia Systems: Infrastructure of audiovisual services – Coding of moving video', no. April 04, pp. 1–298, 2013.

[21] WiMAX Forum, 'WiMAX Advanced : Deployment Scenarios Based on Input from WiMAX Operators and Vendors TSC Approved WiMAX Forum Proprietary', *WiMAX Forum Propr.*, pp. 1–24, 2014.

[22] I. Ahmad and D. Habibi, 'A novel mobile WiMAX solution for higher throughput', in *Proceedings of the 16th International Conference on Networks (ICON)*, 2008, pp. 1–5.

[23] K. Dagar, 'Performance Evaluation of Video on Demand (VoD) over WiMAX', *International Journal of Advanced Research in Computer Engineering and Technology*, vol. 4, no. 5, pp. 2039–2043, 2015.

[24] I. Ahmad and D. Habibi, 'High Utility Video Surveillance System on Public Transport using WiMAX Technology', *IEEE Wireless Communication and Networking Conference*. Sydney, NSW, pp. 1–5, 2010.

[25] S. Omerovic, 'WiMax – Overview.' [Online]. Available: http://www.lait.fe.uni-lj.si/Seminarji/s_omerovic.pdf. [Accessed: 08-Feb-2016].

[26] K. Dagar, 'Performance Evaluation of Video on Demand (VoD) over WiMAX A Comparative Performance Analysis of AODV and DSR Routing Protocols for of Vehicular', *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 4, no. 5, pp. 2039–2043, 2015.

[27] E. Farrukh, E. A. Panaousis, and C. Politis, 'Performance Evaluation of secure video transmission over WiMAX', *Int. J. Comput. Networks Commun.*, vol. 3, no. 6, pp. 131–144, 2011.

[28] J. G. Andrews, A. Ghosh, and R. Muhamed, 'WiMAX Network Architecture', in *Fundamentals of WiMAX Understanding Broadband Wireless Networking*, Upper Saddle River, NJ: Pearson Education, Inc. One Lake Street Upper Saddle River, NJ 07458, 2007, pp. 335–362.

[29] P. Yegani, 'MiMAX Overview', *Cisco Systems*, 2005. [Online]. Available: http://www.ietf.org/proceedings/64/slides/capwap-0.pdf. [Accessed: 08-Feb-2016].

[30] R. Prasad and F. J. Velez, *WiMAX Networks:Techno-Economic Vision and Challenges*. New York: Springer Science+Business Media B.V., 2010.

[31] S. Ahson and M. Ilyas, *WiMAX: Applications*, 1 st. New York CRC: Taylor & Francis Group, 2008.

[32] S. Banerji and R. S. Chowdhury, 'Wi-Fi & WiMAX : A Comparative Study', *Indian Journal of Engineering*, vol. 2, no. 5, pp. 1–5, 2013.

[33] A. N. Isizoh, 'Throughput Analysis of IEEE802 . 11b Wireless Lan With One Access Point Using Opnet Simulator', *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 7, pp. 137–139, 2012.

[34] I. Al Khatib, 'Wireless LAN access points as links with adaptive bandwidth: throughput and feedback control', *10th International Conference on Telecommunications (ICT)2003.*, pp. 754–760.

[35] M. Gobindgarh and E. P. Kaur, 'Comparative Throughput of WiFi & Ethernet LANs using OPNET Modeller', *International Journal of Computer Applications*, vol. 8, no. 6, pp. 8–11, 2010.

[36] J. Jun, P. Peddabachagari, and M. Sichitiu, 'Theoretical Maximum Throughput of IEEE 802 . 11 and its Applications', in *Second IEEE International Symposium on Network Computing and Applications (NCA)*, 2003, pp. 1–7.

[37] J. Jun and M. L. Sichitiu, 'The Norminal Capacity of Wireless Mesh Networks', *IEEE Wireless Communications*, pp. 8–14, Oct-2003.

[38] K. Jaswal, Jyoti, and K. Vats, 'OPNET Based Simulation and Investigation of WiMAX Network using Different QoS', *International Journal of Research in Engineering and Technology*, vol. 03, no. 05, pp. 575–579, 2014.

[39] N. Meghanathan, D. Nagamalai, and N. Chaki, 'Performance Analysis of AODV and DSDV Protocols Using RPGM Model for Application in Co-operative Ad-hoc Mobile Robots', in *Advances in Intelligent Systems and Computing*, vol. 1, Berlin Heidelberg: Springer-Verlag, 2012, pp. 642–649.

[40] J. M. Hamodi and R. C. Thool, 'Investigate the Performance Evaluation of IPTV Over WiMAX Networks', *International Journal of Computer Networks and Communications(IJCNC)*, vol. 5, no. 1, pp. 81–95, 2013.

[41] J. Huang, O. Yang, and F. Lawal, 'Sending Safety Video over WiMAX in Vehicle Communications', *Future Internet*, vol. 5, no. 4, pp. 535–567, 2013.

[42] S. E. L. Kafhali, A. E. L. Bouchti, M. Hanini, and A. Haqiq, 'Performance Analysis for Bandwidth Allocation in IEEE 802.16 Broadband Wireless Network using BMAP Queueing', *International Journal of Wireless andMobile Networks,* vol. 4, no. 1, pp. 139–154, 2012.

[43] F. Z. Yousaf, K. Daniel, and C. Wietfeld, 'Analyzing theThroughput and QoS Performance of WiMAX Link in an Urban Environment', in *WIMAX New Development*, Shanghai, China: Unit 405, Office Block, Hotel Equatorial Shanghai No.65, Yan An Road (West), INTECH, 2009, pp. 308–320.

[44] K. Dagar and P. Sharma, 'Performance of Internet Protocol TV over WiMAX', *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 4, no. 6, pp. 2507–2513, 2015.

[45] O. Oyman, J. Foerster, and I. Corporation, 'Toward enhanced mobile video services over WiMAX and LTE', *IEEE Communications Magazine,* August, pp. 68–76, 2010.

[46] Y. Li, C. Wang, X. You, H.-H. Chen, and W. She, 'Delay and Throughput Performance of IEEE 802.16 WiMAX Mesh Networks', *IET Commun.*, vol. 6, no. 1, p. 107, 2012.

[47] D. Benyamina, A. Ha, and M. Gendreau, 'Wireless Mesh Networks Design —

A Survey', *IEEE Communication Survey Tutorials*, vol. 14, no. 2, pp. 299–310, 2012.

[48] Q. Wang, Y. Lin, and H. Zhan, 'A hybrid wireless system for power line monitoring', in *IEEE PES Innovative Smart Grid Technologies*, 2012, pp. 1–6.

[49] F. Nilsson, *Intelligent Network Video: Understanding Modern Video Surveillance Systems*. Boca Raton: CRC Press Taylor & Francis Group, LLC 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, 2009.

[50] Wanscam, 'Wireless/Wired Network Camera.' [Online]. Available: http://nadezhin.ru/ljfiles/wanscam1.pdf. [Accessed: 11-Feb-2016].

[51] F. Kelly, 'The Mathematics of Traffic in Networks', *Princet. companion to Math.*, vol. 1, no. 1, pp. 862–870., 2008.

[52] A. Ouni, H. Rivano, and F. Valois, 'Capacity of wireless mesh networks : determining elements and insensible characters.', *in IEEE International Workshop on Planning and Optimization of Wireless Communication Networks*, 2010.

[53] T. Ngo, H. Nishiyama, N. Kato, Y. Shimizu, K. Mizuno, and T. Kumagai, 'On the throughput evaluation of wireless mesh network deployed in disaster areas', *International Conference on Computing, Networking and Communications (ICNC)*, pp. 413–417, 2013.

[54] F. Kaabi, S. Ghannay, and F. Filali, 'Channel Allocation and Routing in Wireless Mesh Networks: A survey and qualitative comparison between schemes', *International Journal of Wireless and Mobile Networks*, vol. 2, pp. 132–150, 2010.

[55] Y. Chen, T. Farley, and N. Ye, 'QoS Requirements of Network Applications on the Internet', *Information-Knowledge-Systems Management*, vol. 4, pp. 55–76, 2004.

[56] S. S. Adarshpal and Y. H. Vasil, *The Practical OPNET User Guide for Computer Network Simulation Title*, vol. 53, no. 9. CRC Press,Taylor & Francis Group, 2013.

[57] C. K. Camlibel, A. A. Julius, R. Pasumarthy, and M. A. S. Jacquelien, *Mathematical Control Theory I Nonlinear and Hybrid Control Systems*. New York: Springer US, 2015.

[58] S. S. Adarshpal and Y. H. Vasil, *The Practical OPNET User Guide for Computer Network Simulation*. CRC Press,Taylor & Francis Group, 2013.

[59] Z. Lu and H. Yang, *Unlocking the Power of OPNET Modeler*, 1st ed. Cambridge: Cambridge University Press, 2012.

[60] I. S. Hammoodi, 'A Comprehensive Performance Study of OPNET Modeler For ZigBee Wireless Sensor Networks', in *2009 Third International Conference on Next Generation Mobile Applications , Services and Technologies*, 2009, pp. 357–362.

[61] G. Singh and A. Grover, 'Simulation and analysis : The effect of mobility on IPTV (VOD) over WiMAX using OPNET', *International Journal of Physical Sciences*, vol. 8, no. 26, pp. 1401–1407, 2013.

[62] M. M. A. Ghazala, M. F. Zaghloul, and M. Zahra, 'Performance Evaluation of Multimedia Streams Over Wireless Computer Networks (WLANs)',

International Journal of Advanced Science and Technology, vol. 13, pp. 61–74, 2009.

[63] A. Panayides, Z. C. Antoniou, Y. Mylonas, M. S. Pattichis, A. Pitsillides, and C. S. Pattichis, 'High-Resolution, Low-Delay, and Error-Resilient Medical Ultrasound Video Communication Using H.264/AVC Over Mobile WiMAX Networks', *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 3, pp. 619–628, 2013.

[64] P. Mahasukhon, H. Sharif, M. Hempel, T. Zhou, and T. Ma, 'Distance and throughput measurements in mobile WiMAX test bed', *Military Communications Conference (Milcom),* pp. 154–159, Oct. 2010.

[65] H.-H. Juan, H.-C. Huang, C. Huang, and T. Chiang, 'Scalable Video Streaming over Mobile WiMAX', *IEEE International Symposium on Circuits and Systems*, pp. 3463–3466, 2007.

[66] M. Charitos and G. Kalivas, 'Heterogeneous hybrid vehicular WiMAX-WiFi network for in-tunnel surveillance implementations', *IEEE International Conference on Communications (ICC)*. Budapest, pp. 6386–6390, 2013.

[67] M. Ritter, R. J. Friday, R. Garces, W. San Filippo, and C.-T. Nguyen, 'Mobile connectivity protocols and throughput measurements in the Ricochet Microcellular data network (MCDN) system', in *Proceedings of the 7th annual international conference on Mobile computing and networking (MobiCom)*, 2001, pp. 322–331.

[68] N. Zhang, Yan Ansari, 'Wireless Telemedicine Servics Over IEEE 802 .16 /WIMAX Networks', *IEEE Wireless communications*, February, pp. 30–36, 2010.

[69] M. Yang, J. Y. Tham, D. Wu, and K. H. Goh, 'Cost Effective IP Camera for Video Surveillance', *4th IEEE Conference on Industrial Electronics and Applications,* pp. 2432–2435, 2009.

[70] P. Seeling and M. Reisslein, 'Video Transport Evaluation with H.264 Video Traces', *IEEE Commun. Survey Tutorials*, vol. 14, no. 4, pp. 1142–1165, 2012.

[71] M. Shiraz, M. Whaiduzzaman, and A. Gani, 'A study on anatomy of smartphone', *Journal Computer Communication & Collaboration.*, vol. 2013, no. 1, pp. 24–31, 2013.

[72] R. R. Radhika, *Handbook of Mobile Ad Hoc Networks for Mobility Models*, vol. 1. New York, USA: Springer Science+Business Media, 2011.

[73] M. Amnai, Y. Fakhri, and J. Abouchabaka, 'Throughput-Delay Optimisation with Adaptive Method in Wireless Ad Hoc Network', pp. 0–3, 2010.

[74] M. Amnai, Y. Fakhri, and J. Abouchabak, 'Impact of Mobility on Delay-Throughput Performance in Multi-Service Mobile Ad-Hoc Networks', *Int'l J. Commun. Netw. Syst. Sci.*, vol. 04, no. 06, pp. 395–402, 2011.

[75] P. Santi, *Mobility Models for Next Generation Wireless Networks: Ad Hoc, Vehicular and Mesh Networks*, 1st ed. West Sussex: John Wiley & Sons Ltd The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom For, 2012.

[76] B. Pazand and C. Mcdonald, 'A Critique of Mobility Models for Wireless Network Simulation', in *6th IEEE/ACIS International Conference on*

Computer and Information Science (ICIS), 2007, pp. 141–146.

[77] N. A. Borghese, L. Bianchi, and F. Lacquaniti, 'Kinematic determinants of human locomotion', *Journal of Physiology*, vol. 494, no. 3, pp. 863–879, 1996.

[78] R. Tanawongsuwan and A. Bobick, 'A Study of Human Gaits across Different Speeds', *Georgia Institute of Technology*, pp. 1–13, 2003.

[79] L. L. Long and M. Srinivasan, 'Walking, running, and resting under time, distance, and average speed constraints: optimality of walk-run-rest mixtures.', *Journal of The Royal Society Interface*, vol. 10, p. 20120980, 2013.

[80] R. D. Novaes, A. S. Miranda, and V. Z. Dourado, 'Usual gait speed assessment in middle-aged and elderly Brazilian subjects.', *Revista Brasileira de Fisioterapia*, vol. 15, no. 2, pp. 117–122, 2011.

[81] M. Shinde, R. Shinde, N. Thavare, and A. Baviskar, 'Security Based Home Surveillance System Using Android Application', *International Journal of Research in Engineering and Technology*, vol. 3, no. 4, pp. 814–815, 2014.

[82] Cisco Systems, 'Cisco Video Surveillance Operations Manager Mobile App User Guide', pp. 1–10, 2013.

[83] Wirepath Surveillance, 'WPS-IP Surveillance App Setup Guide.' pp. 1–7, 2015.

[84] G. Ononiwu, G. Okorafor, J. Onojo, and R. Opara, 'Low Cost Video Surveillance System With Intrusion Detection', *Int. J. Emerg. Technol. Res.*, vol. 1, no. 7, pp. 79–98, 2014.

[85] N. M. A. Munassar and A. Govardhan, 'A Comparison Between Five Models Of Software Engineering', *International Journal of Computer Science (IJCS)*, vol. 7, no. 5, pp. 94–101, 2010.

[86] D. Jamwal, 'Analysis of Software Development Models', *International Journal of Computer Science and Technology*, vol. 1, no. 2, pp. 61–64, 2010.

[87] M. I. Daud, 'Secure software development model: A guide for secure software life cycle', *In Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. I, pp.17-19,2010.

[88] F. Tsui and O. Karam, 'Software Process Models', in *Essentials of Software Engineering*, 2010, pp. 98–101.

[89] M. Wolfson and D. Felker, 'Developing with Android Studio', in *Andriod Developer Tools Essential: Android Studio to Zipalign*, 1 st., Califonia: O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. O'Reilly, 2013, pp. 71–88.

[90] C. Haseman and K. Grant, *Beginning Android Programming:Develop and Design*. USA: Peachpit Press, 2014.

[91] E. L. Morgan, *Getting Started with XML: A Manual and Workshop*. Boston, MA, USA.: Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Special, 2004.

[92] G. Popovic, N. Arsic, B. Jaksic, B. Gara, and M. Petrovic, 'Overview , Characteristics and Advantages of IP Camera Video Surveillance Systems Compared to Systems with other Kinds of Camera', *Int. J. Eng. Sci. Innov. Technol.*, vol. 2, no. 5, pp. 356–362, 2013.

[93] P. Remagnino and A. G. ; Jones, *Video-Based Surveillance Systems*, 1st ed. New York: Kluwer Academic Publishers, 2002.

[94] R. M. Abid, T. Benbrahim, and S. Biaz, 'IEEE 802 . 11s Wireless Mesh Networks for Last-Mile Internet Access : An Open-Source Real-World Indoor Testbed Implementation', vol. 2010, no. October, pp. 725–738, 2010.

[95] H. Kruegle, *CCTV Surveillance: Video Practices and Technology*, Second edi. Oxford, UK: Butterworth-Heinemann, 2011.

[96] Axis Communications, 'CCD and CMOS sensor technology.' [Online]. Available: http://www.axis.com/files/whitepaper/wp_ccd_cmos_40722_en_1010_lo.pdf. [Accessed: 02-Jun-2014].

[97] S. M. S. Bari, F. Anwar, and M. H. Masud, 'Performance Study of Hybrid Wireless Mesh Protocol (HWMP) for IEEE 802 . 11s WLAN Mesh Networks', no. July, pp. 3–5, 2012.

[98] C. Pearson, 'High-Speed , Analog-to-Digital Converter Basics', *Texas Instruments Incorporated*, Texas, pp. 1–26, Jan-2011.

[99] N. Gray, 'ABCs of ADCs: Analog-to-Digital Converter Basics', *National Semiconductor Corporation*, pp. 1–35, Jun-2006.

[100] T. M. Nelson, 'Analog-to-Digital Conversion', Diss. Utah State University, Department of Electrical Engineering, 1965.

[101] I. E. G. Richardson, *H.264 and MPEG-4 Video Compression*, 1 st. England: John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2003.

[102] A. May, J. Teh, P. Hobson, and J. Reichel, *Scalable video requirements for surveillance applications*. London: The Institution of Electrical Engineers.Michael Faraday House, Six Hills Way, Stevenage, SG1 2AY, 2004.

Appendix A- Types of Video Surveillance Cameras

A-1 Cube cameras

As the name suggests, these kind of cameras have a cubic shape, as shown in Figure A-1. They can be used both for outdoor and indoor applications. Cube cameras have a fixed focal length, a limitation which should be taken into consideration although it can be adjusted manually. Another limitation is the poor support on Power over Ethernet (PoE) [92]. However, cube cameras have several advantages, such as, the support for wireless technologies and improved frame rates with 70% of them having a frame rate of 15fps [92]. In a weak light environment and for improving efficiency, some cube cameras integrate IR LED diodes. Modern cube cameras have a built-in battery, in addition to the available AC power provision, a removable flash storage and USB cable connectivity for charging the battery. Some are portable as well.

Figure A-1: A Diagram Illustrating the Cube Camera

A-2 Box camera

Box network cameras are flexible and simple; and they are obtainable at relatively low prices. The flexibility feature enables them to be directed towards some specific angles with ease. Figure A-2 shows an example of a box camera

Figure A-2: A Diagram Illustrating the Box Camera

Popovic [92] argues that users prefer box cameras to other network cameras because of their changeable objective; as they can be used to view scenes at both far and near

distances. About 90% of these type of cameras have this feature, contrary to the 33% of a dome cameras.

Box cameras also offer greater frame rate than do dome cameras. Box cameras may provide excellent esthetics. However, they may be complicated to install; and a 12VDC supply can also power them by using a Power over Ethernet (PoE) cable.

A-3 Dome cameras

Figure A-3 shows the physical structure of the Dome cameras. These cameras are mainly installed right next to the wall, or to the ceiling; and that makes them discrete. They can be powered with a minimum of 12VDC with some needing up to 24VDC power supply. They also support many IP based protocols like TCP, UDP, RTP, HTTL, etc. and compression standards like MPEG-4 part 2 and motion JPEG. Dome cameras are usually closed inside, which means they have limited movements; although this depends on the design of dome camera [92].

Figure A-3: A Diagram Illustrating the Dome Camera

Dome cameras come in different sizes: mini, medium and large dome cameras. Mini-dome cameras are aesthetically better than the larger types. In general, dome cameras have the advantage that they are resistant to vandal behaviour; so, there is no need for a separate case, when installed outdoors. They have an integrated IR LED for dim light/night surveillance and shorter installation time. However, they have a short coverage distance of about 20m [92]

A-4 Bullet cameras

Bullet network cameras may be considered as unique types of box cameras. They have the advantage of efficiency in bad light conditions; since most of them have integrated IR reflectors [12]. Added advantages include a wide coverage distance than the dome, usually less than 50m, as well as easy installation, especially in outdoor environments; and like the dome, they do not need a special case [92]. Figure A-4 shows an example of a bullet camera.

Figure A-4: A Diagram illustrating the Bullet Camera

A-5 Covert cameras

Covert cameras could be hidden in ceiling boards, smoke detectors, walls and any other place which can easily be noticed as shown in Figure A-5. These cameras carry out surveillance in a manner, so that the perpetrators of crime should not be aware of their location.

Figure A-5: A Diagram illustrating the covert Camera hidden behind a smoke detector

A-6 Pan –Tilt- Zoom cameras

Pan-tilt-zoom, stationary, yet rotating and zooming, cameras are ideal cameras for indoor and outdoor environments. One PTZ surveillance camera can be used to cover a large area or can be used to monitor one particular point of interest and this is the main advantage of this type of camera [93]. Figure A-6 shows an example of the PTZ camera.

Figure A-6: A Diagram Illustrating the PTZ Camera

Appendix B - Wireless Fixed Access Networks

B-1: Point-to-Point Network

A point-to-point network, sometimes abbreviated PTP or P2P, is the simplest wireless network, where information is transmitted from one point to the other (Figure 9.4). Due to the directional nature of the system, directional antennas are used to provide the highest bandwidth for the link. The system can also be adjusted for minimal interference and the highest level of security. If line-of-sight is available, it would also be possible to use a high-performance optical link between two adjacent buildings located on opposite sides of a highway.

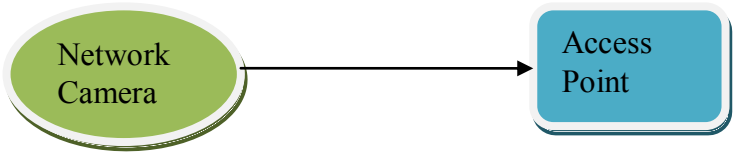

Figure B-1: A network camera being connected to a point-to-point topology

B-2 Point-to-Multipoint Network

A point-to-multipoint network, sometimes abbreviated PTMP or P2MP, is the most common type of wireless network (see Figure B-2). An example of such a network is an FM radio station transmitting radio signals to many radio receivers. Because of the nature of the network, the central point uses an Omni-directional antenna. The surrounding points use a directional antenna, unless they are mobile. A car is one such example, in which case an Omni-directional antenna would be preferred. A point-to-multipoint network can be of broadcast and simplex nature, as in the FM radio case;

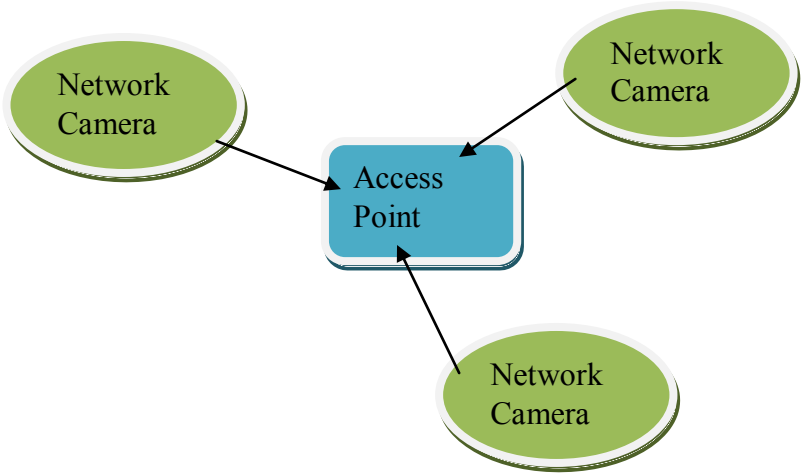

Figure B-2: Network Cameras connected to a point-to-multipoint topology

or it could provide a full duplex, with the data being sent in both directions, as in a regular wireless LAN (local area network) application.

B-3 Mesh Network

A wireless mesh network (WMN) is characterised by several connection nodes that provide individual and redundant connection paths between one another. To accommodate this, select routing protocols that guarantee data exchange via the most appropriate connection path used. When selecting a path, factors such as bandwidth, transfer errors, and latency are taken into account. The number of nodes between two data points is defined as the number of "hops." The more hops, the longer the latency. Keeping latency and the number of hops down is critical in applications, such as live video and particularly in cases where PTZ cameras are used.

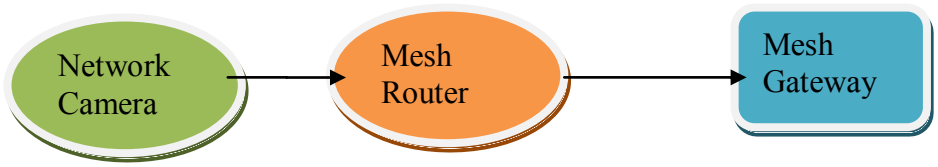

Fig.B-3: Network Camera Connected in a Mesh topology

Wireless Mesh Networks are emerging as a technology of the time due to many factors or features such as self-healing, easy-to-deploy, scalability and reliability [94]. Setting a WMN requires less wiring and configuration overheads. Self- healing comes about because of the redundancy of the wireless links. With this redundancy, alternative links are used in the event of a fault in one link; and continuity of service is guaranteed [94].

When used to provide the last-mile wireless access, WMN tremendously reduces the cost and the configuration overheads; when it is compared with current solutions, e.g., Wi-Fi (IEEE 802.11) LANs [94]. Wi-Fi LANs suffer from the cost and the overheads of setting the wired backbone that connects the different APs (Access Points) [94]. For example, any AP connected to the adjacent cell requires wiring to the wired backbone network, and that increases the settlement cost. In WMN minimal installation is required, except for the mesh gateways to the wired backbone or the WiMAX network.

Appendix C – Bit Calculation per Codec Colour Scheme[11]

There are two basic colour schemes used in colour video; the RGB and YCbCr colour schemes. Each colour scheme has a different bit requirement as shown in Table C below:

Table C: Bit Calculation per Codec Colour Scheme

Codec Colour Scheme	Colour Definition/Calculation	Bits Per Colour	Total Bits
RGB	Red	8.000	24
	Green	8.000	
	blues	8.000	
$Y:C_b:C_r$	$Y = 0.299R + 0.587G + 0.114B$	8.264	8
	$C_b = 0.564(B - Y)$	-0.149	
	$C_r = 0.713(R - Y)$	-0.188	

Appendix D-Structure of Fixed Cameras

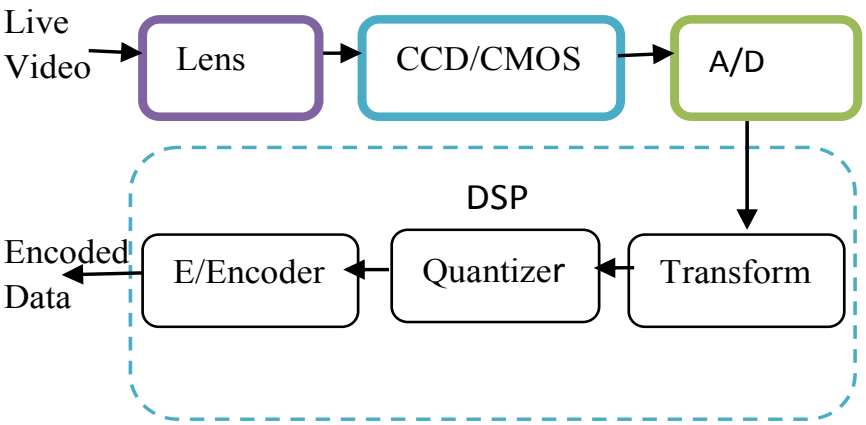

Figure D-1: Fixed Wireless IP Camera Structure: Capture and Encoder Units

D-1 Lens

The camera lens is analogous to the human eye lens. It collects the reflected light from the scene, natural or artificial, and focuses it into an image by using sensors (CCD or CMOS) [95]. There are several types of lenses and the main ones being: **Fixed Focal Length (**FFL) manual iris lenses, Variable Focal Length (VFL) and zoom lenses. Each of these lenses can have the option of an automatic iris. Other types include: the pin hole, which is used for covert application, the split image for multiple scenes and on a single camera [95]. The larger the lens diameter, the more light will be gathered, the brighter the image on the sensor, and the better the final image on the monitor would be [3]. The keys to video capture are the focal length, the distance between the lens and the surveillance scene, the field of view and the size of the sensors. The field of view (FOV) is defined as the width or height of a scene to be monitored by the security cameras. It is the area visible to the human eye or lens.

The FOV depends on several factors: video format, focal length and the distance from target object. The focal length is the distance between the lens and the sensor. The shorter the focal length, the wider is the FOV and vice versa. The *focal length* of any lens, worldwide (as of 1950), is measured in *millimetres* [19].

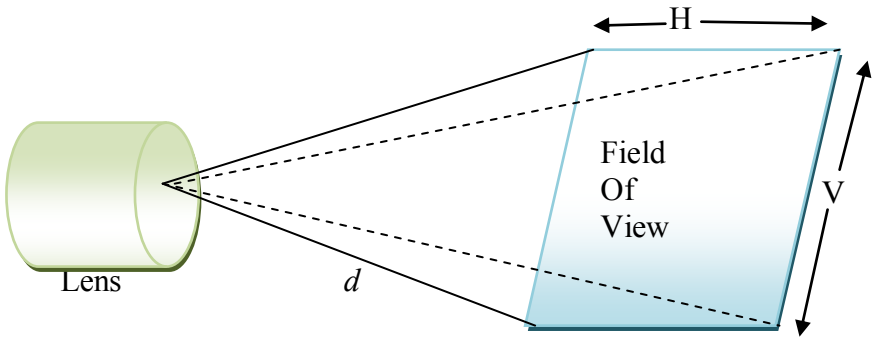

Figure D-2: Camera Lens Illustrating the Field of View at Distance d

The FOV increases as one increase the distance to the object; but this is at the expense of poor quality of the object or surveillance video. Increasing or extending the field of view has the advantage of reducing the number of cameras needed [18]. From the above factors, the FOV can be determined as:

$$FOV = \frac{d \times O_d}{l_f}$$

(C.1)

Where: d is the distance between the camera and object; S is the sensor size in millimetres and l_f is the focal length.

CCD or CMOS sensor sizes come in different formats. Standard sensor sizes measured in inches include ¼, 1/3, 2/3 and 1. Each camera specifies these sizes. However, many CCD cameras use the 1/3; while the megapixel camera uses ½ or 1-inch size. The FOV increases, as you increase the sensor size and vice versa. As an example, for a camera lens of 3mm focal length, sensor size of ¼ (3.2mm) and located 4m from the surveillance scene, the horizontal width FOV would be 4.266m.

D-2 CCD or CMOS Sensors

The CCD or CMOS are image sensors which capture the signal from the lenses. The choice between CCD and CMOS depends on some factors such as application, cost and availability. The CCD contains hundreds of thousands of pixels, each containing a capacitor and a light sensitive element [8] The capacitor stores the charge proportional to the amount of light received and then converts this charge into voltages. These voltages are later transferred to the analogue/digital converter [18]. CCDs have image

quality advantages compared with CMOS, better light sensitivity and less noise [96][8]. However, CCD sensors have disadvantages; they are bulky and they require more electronics circuitry, cost more to produce and have higher power consumption factor than the CMOS equivalent sensors [5].

The CMOS sensors operate in a similar way as the CCDs; except that they do not store charge. Instead, light incidents on the pixel surfaces are converted directly into voltages [97]. Additionally, every pixel in a CMOS sensor consists of an amplifier and an analogue/digital converter. Other software components that perform cropping and multi-view streaming functions are also included. These functions cannot be performed in CCD sensors, which usually have only one converter.

Furthermore, a CMOS sensor is better adapted to megapixel resolutions, because the time taken to read the charges is far less in a CMOS sensor than in a CCD sensor [18]. CMOS sensors are also less expensive than CCDs; because they are easier to manufacture, and are less greedy in terms of power [18]. However, CMOS sensors have been considered to be of poorer quality in terms of the Signal-to-Noise Ratio [18].

D-3 Analogue to digital convertor

Analogue-to-digital converters (ADC) are devices that sample continuous analogue signals and convert them into digital words [98]. In the wireless IP cameras, the analogue to digital (ADC) circuit converts the voltages and currents [99] from the CCD or CMOS into equivalent digital signals. Figure 2.3 illustrates a basic analogue to digital conversion process:

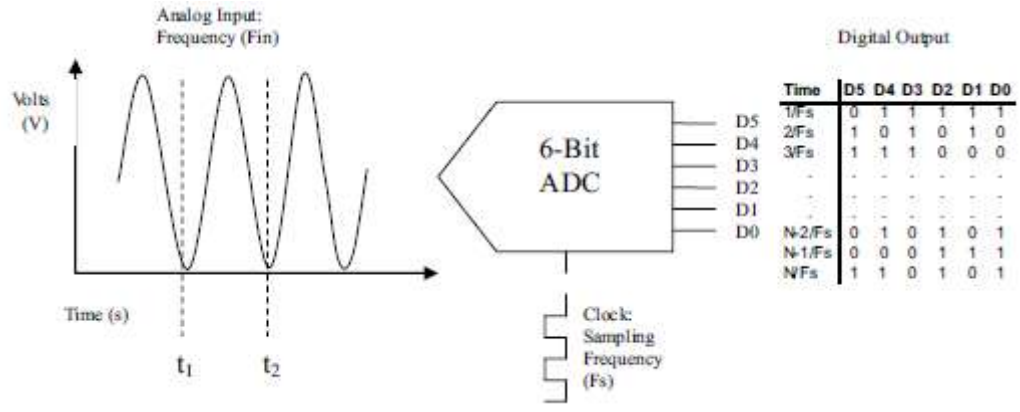

Figure D-3: Basic Analogue-to-Digital Converter [98]

The figure shows how an analogue signal applied to the input of the ADC, at the input frequency (fin), is converted to a digital signal or words at the sampling frequency (Fs). The analogue-to-digital circuit comes in different categories: sigma-delta ADCs, high-resolution ADCs, and high-speed ADCs [98]. They can also be classified as Flash or parallel, Digital Ramp or counter, Successive Approximation, Tracking, Slope or Integrating and Delta-Sigma (ΔΣ) ADCs [100]

D-4 Digital Signal Processor

The DSP is the heart of an IP camera. Among other units, it consists of the transform, the quantizer and the encoder. The DSP does the image processing, the compression, the encoding; and it is from this unit that IP protocols, like IEEE 802.11b/g are added [8]. The digital signal is fed to the transform subunit; and it involves the use of discrete cosine transforms, wavelet transforms or the integer transforms.

The transform converts the video from the spatial domain to the frequency domain [101]. High-frequency signals are then filtered as a way of removing redundancies [101]. IP camera video encoders are required to be scalable, and they use advanced signal transforms such as wavelet and integer transforms [102].

Appendix E: Detailed parameter and device configuration

E-1: Profile Configuration

The profiles to match the application definitions are configured to depict the activity pattern of the specified applications. Therefore, the starting time, the duration and the end of application are specified during the profile configurations. To this end, one can have one profile that defines one or more applications as well as one profile for each application used. In our case, we have one profile that supports video applications. The profile was configured with the simultaneous operational mode; and it had a starting time of 100 seconds whereby each camera generates packets in simultaneously.

E-2: Video Server Applications Configurations

The video servers were all configured to support the video profile services. The server address was put down as remote; or local video servers were taken one at a time. The remote server was connected to the Internet via a serial cable; while the local server was connected by using a 1000Base-X Ethernet cable.

E-3: The Base Station Configuration

The base station was set to support the real time polling service (rtPS) quality of service class and video transmission. The detailed BS parameter set is illustrated in Table 0.1.

Table 0.1: **BS Parameters**

Parameter name	**Parameter value/features**
Antenna gain	15dBi
Maximum transmit power	5W
Receiver power threshold	-110dBm
Service class name	Silver
Physical layer technology	IEEE 802.16d
Physical Profile	Wireless OFDMA 20MHz
Physical profile type	OFDMA

E-4: CPE Parameters Configuration

The CPE WiMAX parameters were set in a similar way as the BS parameters of Table 4.2. The antenna gain for the CPE was set at 14dBi. Additionally, the uplink and downlink parameters were set, as shown in Table 0.2. The Wi-Fi link was set to a transmit power of 0.5W at a data rate of 54 Mbps with Orthogonal Frequency Division Multiplexing (OFDM) access scheme, as specified by IEEE 802.11g with the access point functionality enabled.

Table 0.2: Uplink and Downlink Parameters

Parameter name	**Parameter values/features**
Antenna gain	14dBi
Transmit power	3W
Service class name	Silver
Modulation type	64-QAM ½
Buffer size	64Kb
Average SDU byte size	1500 bytes
Multipath channel model	ITU Pedestrian A

E-5: Wi-Fi IP Cameras Configuration

All the WiFi IP cameras were connected to the CPE; and they were configured for IEEE 802.11g Wi-Fi connectivity. The IP cameras' applications were configured to support the video profile definitions. In addition, some destination preferences were also configured. For remote video surveillance, the destination preference was the remote video server while for local surveillance the local server was used. These destination preferences were taken one at a time. Other Wi-Fi IP camera parameters were set, as shown in Table 0.3:

Table 0.3: **Wi-Fi Device Parameter Set-Up**

Physical layer technology	**Extended IEEE 802.11b/g**
Data rates	11/54Mbps
Transit power	0.005W
Thermal noise power threshold	-95dB
Access point functionality	disabled
Buffer size	1,024,000

Appendix F: Main Activity Java codes

```
import android.app.ProgressDialog;
import android.content.Intent;
import android.graphics.Bitmap;
import android.net.Uri;
import android.os.AsyncTask;
import android.os.Bundle;
import android.provider.MediaStore;
import android.support.v7.app.AppCompatActivity;
import android.util.Base64;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.ImageView;
import android.widget.Toast;

import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.util.HashMap;

public class MainActivity extends AppCompatActivity implements
View.OnClickListener {

    private Button buttonUpload;
    private Button buttonChoose;

    private EditText;
    private ImageView;

    public static final String KEY_IMAGE = "image";
    public static final String KEY_TEXT = "name";
    public static final String UPLOAD_URL =
"http://196.42.89.137/Photopic/upload.php";

    private int PICK_IMAGE_REQUEST = 1;

    private Bitmap bitmap;


    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        buttonUpload = (Button) findViewById(R.id.buttonUpload);
        buttonChoose = (Button) findViewById(R.id.buttonChooseImage);

        editText = (EditText) findViewById(R.id.editText);
        imageView = (ImageView) findViewById(R.id.imageView);

        buttonChoose.setOnClickListener(this);
        buttonUpload.setOnClickListener(this);
    }

    private void showFileChooser() {
        Intent intent = new Intent();
        intent.setType("image/*");
        intent.setAction(Intent.ACTION_GET_CONTENT);
        startActivityForResult(Intent.createChooser(intent, "Select
Picture"), PICK_IMAGE_REQUEST);
    }

    @Override
    protected void onActivityResult(int requestCode, int resultCode, Intent
data) {
        super.onActivityResult(requestCode, resultCode, data);
```

```
        if (requestCode == PICK_IMAGE_REQUEST && resultCode == RESULT_OK &&
data != null && data.getData() != null) {
            Uri filePath = data.getData();
            try {
                bitmap =
MediaStore.Images.Media.getBitmap(getContentResolver(), filePath);
                imageView.setImageBitmap(bitmap);
            } catch (IOException e) {
                e.printStackTrace();
            }
        }
    }

    public String getStringImage(Bitmap bmp){
        ByteArrayOutputStream baos = new ByteArrayOutputStream();
        bmp.compress(Bitmap.CompressFormat.JPEG, 100, baos);
        byte[] imageBytes = baos.toByteArray();
        String encodedImage = Base64.encodeToString(imageBytes,
Base64.DEFAULT);
        return encodedImage;
    }


    public void uploadImage(){
        final String text = editText.getText().toString().trim();
        final String image = getStringImage(bitmap);
        class UploadImage extends AsyncTask<Void,Void,String> {
            ProgressDialog loading;
            @Override
            protected void onPreExecute() {
                super.onPreExecute();
                loading = ProgressDialog.show(MainActivity.this,"Please
wait...","uploading",false,false);
            }

            @Override
            protected void onPostExecute(String s) {
                super.onPostExecute(s);
                loading.dismiss();
                Toast.makeText(MainActivity.this, s,
Toast.LENGTH_LONG).show();
            }

            @Override
            protected String doInBackground(Void... params) {
                RequestHandler rh = new RequestHandler();
                HashMap<String,String> param = new HashMap<String,String>();
                param.put(KEY_TEXT,text);
                param.put(KEY_IMAGE,image);
                String result = rh.sendPostRequest(UPLOAD_URL, param);
                return result;
            }
        }
        UploadImage u = new UploadImage();
        u.execute();
    }


    @Override
    public void onClick(View v) {
        if(v == buttonChoose){
            showFileChooser();
        }
        if(v == buttonUpload){
            uploadImage();
        }
```

```
        }
    }
```