University of Nairobi

School of Computing and Informatics

ANALYSIS OF THE EFFECT OF WIRELESS CAMPUS NETWORKS ON INTERNET USAGE IN KENYAN UNIVERSITIES

By:

ERIC SIFUNA SIUNDUH

P56/60064/2011

Supervised by:

PROF. ELIJAH OMWENGA

September, 2013

A research project submitted in partial fulfillment of the requirements for the award of Masters of Science Degree in Information Systems

DEDICATION

I wish to express my profound gratitude to the respondents of the 14 universities for their valuable contribution to the success of this research. Special thanks to ICT directors/managers of the 14 universities for playing the roles as both respondents and research assistants in data collection at their respective universities. My sincere gratitude to my project supervisor, Prof Elijah Omwenga for his constant guidance during the research. To my wife Carolyne, I appreciate your patience and support.

DECLARATION

I certify that this research project entitled "Analysis of the Effect of Wireless Campus Networks on Internet Usage in Kenyan Universities" is my own work. The work has not been presented elsewhere for assessment. Where material has been used from other sources it has been properly acknowledged.

SIGNED_____ **DATE**_____

Eric Sifuna Siunduh

Registration No. P56/60064/2011

I certify that this project has been submitted for examination with my approval as the University of Nairobi supervisor.

SIGNED_____ **DATE**_____

Prof. Elijah I. Omwenga

School of Computing and Informatics

University of Nairobi

ABSTRACT

Campus wireless network deployment at Kenyan Universities has become common aiming at increasing internet coverage on campuses. The utilization of internet and IT enabled services is increasingly on campuses with the pace of automation of processes. Use of IT enabled services and the need to impress ICT in teaching, learning and research globally has pushed Universities in adopting technology to disseminate this core mandate.

This study investigated how growth in deployment of wireless campus network and security level implemented affects internet usage in Kenyan Universities.

Data was collected from 14 Universities out of a total of 68 representing 21% of all Universities. Stratified random sampling and purposeful sampling were adopted to come up with the sample size. The respondents were ICT Managers, network administrators, students, finance officers and researchers.

The major findings of this study indicate annual increase of internet usage that ranges from 41% to 142% with wireless campus network deployments. For universities where wireless networks are not deployed, growth in internet usage ranges from 0-20%. Universities with more restrictive the security level implemented attracts high number of users seeking support from IT team to access wireless networks and therefore limits internet usage on campus.

Based on the research findings, the study recommends the following;

1. Universities management should consider ICT as a strategic platform for transforming teaching, learning and improving efficiency and therefore increase IT budgets for deployment of wireless campus network infrastructure to increase coverage on campuses to at least KES10M and above for startup universities.

2. University ICT team should consider to register wireless devices in order to have visibility of user devices to track cyber security cases since 55% of the universities do not register wireless devices.
3. ICT user training should be carried out to finance officers and all other IS users departments.
4. The frequency regulatory body -Communication Commission of Kenya (CCK) to develop a roadmap on identification and allocation of frequency for the deployment of new wireless technologies such as Long Term Evolution (LTE) technology to rapidly expand growth of campus wireless networks or hotspots

Although wireless technology is broadly deployed on campuses, there are challenges with ICT budget allocation for roll out of these networks and IT enabled services by University management. There are also challenges between use of ICT services on wireless network and security of the information systems. Internet usage within the University community depends on the extend of coverage of wireless networks on campuses and availability of relevant IT enabled services as well as security level implemented on wireless networks. A balance needs to be reached between ease of access and security level to be implemented. The study extended knowledge by establishing practical % growth in internet usage with respect to the various dependent variables.

TABLE OF CONTENTS

List of Tables

List of figures

Abbreviations, acronyms and definition of Terms

WLAN	Wireless Local Area Network
LAN	Local Area Network
USA	United States of America
WI-FI	Wireless Fidelity
IEEE	Institute of Electrical and Electronics Engineering
AP	Access Point
LTE	Long Term Evolution
SEUCO	South Eastern University College
UoN	University of Nairobi
DKUT	Dedan Kimathi University of Technology
MUCST	Meru University College of Science and Technology
UoE	University of Eldoret
MMUST	Masinde Muliro University of Science and Technology

Definition of Terms

1. A wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.
2. A hotspot is an area covered by Internet access over a wireless local area network through the use of a router connected to a link to an Internet service provider. Hotspots typically use Wi-Fi technology.
3. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is one of the least secure forms of security.
4. IT Enabled services (ITES), also called web enabled services or remote services or Tele-working, covers the entire scope of operations which exploit information technology for improving efficiency of an organization or campus.
5. Open System Authentication (OSA) is a process by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy (WEP) protocol.

1.0 INTRODUCTION

1.1 Background

Wireless local-area networks (WLANs) are increasingly common on university campuses. A contemporary survey by Kenya Education Network for 52 University campuses in Kenya found that about half already have a limited deployment, nearly all plan to install a wireless network, and 7% have a comprehensive deployment.

It is estimated that about 80% of the 250,000 plus Kenyan University students already have access to almost free and unlimited (24/7) on-campus broadband Internet. The majority of students also have access to off-campus Internet using student owned computers and laptops with 3G modems, 3G-enabled mobile phones or Smart-phones or through private Wi-Fi hotspots e.g. Wazi WiFi, an Access Kenya wireless network service. University students use internet to support their social life through social networks such as face book and twitter. They also use internet for learning and research through e-learning platforms and e-libraries, to access for free e-journals and e-books available on internet. This is demonstrated by the number of hits on the e-learning and e-library platforms.

A student at the University of Nairobi explained that to access internet one had to go to the laboratory but since wireless internet was introduced in 2010, access is available at most places on the campus. Students have learnt how to use internet for researching and outsourcing, Makuma (2011).

There has been increased deployment rate of campus wireless networks in Universities. Some of the efforts to foster the initiative are as follows;

1. Universities have placed ICT as an essential part of their strategies. This has necessitated allocation of ICT budget.
2. Google has rolled out initiatives to support development of wireless campus infrastructure.
3. Google initiatives include donation of switches through KENET, support for wireless infrastructure development in various Universities e.g. Inoorero University, St Pauls University, Kabarak University e.t.c. and setup of Google

cache at KIXP. Currently, universities are generating about 400Mb/s of traffic to Google cache at KIXP, saving this capacity on international links.

4. The 'Wezesha' laptop initiative driven by Ministry of Information and Communication and Kenya ICT Board enabled university students acquire laptops at subsidized rates.

1.2 Previous Research

This research relates to the research previously carried out by David Kotz at the Dartmouth College, Hanover, NH 03755, USA and Kobby Essien of University of Pennsylvania, 120 Hayden Hall, 3320 Smith Walk, Philadelphia, PA 19104, USA. The research title was ''Analysis of a Campus-Wide Wireless Network''. Their research in abstract aims at Understanding usage patterns in wireless local-area networks (WLANs) is critical for those who develop, deploy, and manage WLAN technology, as well as those who develop systems and application software for wireless networks. The study presented results from the largest and most comprehensive trace of network activity in a large, production wireless LAN. The research traced the activity of nearly two thousand users drawn from a general campus population, using a campus-wide network of 476 access points spread over 161 buildings at Dartmouth College. Their study expanded on those done by Tang and Baker (2004) , with a significantly larger and broader population. They found that residential traffic dominated all other traffic, particularly in residences populated by newer students; students are increasingly choosing a wireless laptop as their primary computer. Although web protocols were the single largest component of traffic volume, network backup and file sharing contributed an unexpectedly large amount to the traffic. Although there was some roaming within a network session, we were surprised by the number of situations in which cards roamed excessively, unable to settle on one access point. Cross-subnet roams were an especial problem, because they broke IP connections, indicating the need for solutions that avoid or accommodate such roams, Kotz and Essien (2005)

In the African Tertiary Institution Survey (ATICS) Report by Gakio (2006), out of the 54 campus networks sampled, 94% indicated that they have campus networks. The largest proportion (46%) of the respondents reported they used copper (10Base and 100 BaseT) for their campus backbones, 33% use fibre, while 21% reported they use wireless.

In 1994 the Information Networking Institute of Carnegie Mellon University submitted a proposal to the National Science Foundation to create a"High Speed Wireless Infrastructure". The purpose was to support wireless research but also to attract additional research and create, in essence, a campus-wide user community as a mobile computing laboratory. The CMU campus was ideal for such research, as it was concentrated and even non-technical departments are heavy users of networked computing. The campus wired network consisted of three major components: a high speed campus-wide network, network clients, and network services. The key network services are the File System, electronic mail, bulletin boards, distributed printing, access to library information, access to the supercomputing center, and the Internet.

The Wireless network concept build a high speed wireless access system using wireless local area network technology, utilizing spread spectrum in the ISM (industrial, scientific, and medical) band. This access system is integrated with wireline network. The whole network was eventually an operational utility for the use of anyone on campus with an appropriate computer and wireless device.

1.3 Problem Statement

Although technology such as IEEE 802.11b/g/n is broadly deployed and usage is increasing dramatically, little is known about how these networks are used particularly at the Universities. Furthermore little is known about the relationship between security levels configured on wireless campus network to the growth in internet usage. A clear understanding of this relationship is critical information for those who develop, deploy, and manage WLAN technology, and those who develop

systems and application software for wireless networks. This study intended to present results on the internet usage within the University community with the introduction and growth of campus wireless networks as well as the relationship between implementations of various security configurations of wireless campus networks and the internet usage within the University community.

1.4 Objectives

The overall objective of the study is to analyze internet usage with respect to growth of wireless campus networks. To achieve the overall objective, the following specific objectives were pursued:

1. To examine the relationship between growth of wireless campus network deployment and relate to growth in internet usage on campuses
2. To compare trends in internet usage between campuses that has implemented wireless networks and those that have not.
3. To examine relationship between implementation of various security levels on wireless campus networks and the internet usage

1.5 Research Questions

1. What is the relationship of growth in wireless campus network to internet traffic pattern at the campuses?
2. What are the trends in internet usage between campuses that have implemented wireless networks and those that have not.
3. How does implementation of the various security levels on campus wireless network affect internet and IT enabled service usage on campuses?

1.6 Assumptions and limitations of the research

The study assumes that the following ICT conditions exist at the University campuses under investigation;

1. All have internet connection on campus and fixed network
2. Majority have developed campus wireless networks in the last three years. A few others have not
3. Some campuses with campus networks have Information systems already in place. Others have not.

The limitations of the study were:

1. The limited time available to collect and analyze data collected. Analysis was done as the questionnaires were returned; therefore having results immediately all the questionnaires were received.
2. The errors occurring during data collection arising from those not giving honest answers. To overcome this, I worked with the specific correspondents I had built trust with professionally.
3. Limited finances to facilitate the carrying out of the research. To address this, online questionnaires were used.

1.7 Research Outcomes and Significance to Key Audiences

The research established the relationship that exists between growth in wireless campus network and various internet traffic patterns at the University campuses. The study also established the relation between security level on campus wireless network and Internet usage as well as use of internet enabled services. These served to determine the following;

1. Level of security to be implemented by IT administrators on campus wireless networks that enables maximum access to internet and IT enabled services (such as e-learning platforms and libraries, to access to free e-journals and e-books available on internet by the University community
2. Determine the level of security of the campus network that meets the desired level of confidentiality and privacy of the user online information such as personal information and research/e-learning materials
3. Give assurance to management on the value proposition of wireless network roll-out and security implementation in relation with the image of the University.
4. It informs and gives opportunity to the regulator - Communication Commission of Kenya (CCK) in developing a roadmap on identification and allocation of frequency for the deployment of new wireless technologies such as Long Term Evolution (LTE) technology to rapidly expand growth of campus wireless networks or hotspots

2.0 LITERATURE REVIEW

2.1 Introduction

Public access wireless local area networks (LANs) were first proposed by Henrik Sjödin at the NetWorld + Interop conference in the Moscone Center in San Francisco in August 1993. Sjödin did not use the term hotspot but referred to publicly accessible wireless LANs. Sjödin went on to found the companies PLANCOM in 1994 (for Public LAN Communications, which became MobileStar and then the Hotspot unit of T-Mobile USA) and Wayport in 1996. The term hotspot **was** first advanced by Nokia five years after Sjödin first proposed the concept.

This research relates to the research previously carried out by David **Kotz at the Dartmouth** College, Hanover, NH 03755, USA and Kobby Essien of University of Pennsylvania, 120 Hayden Hall, 3320 Smith Walk, Philadelphia, PA 19104, USA. The research title was ''Analysis of a Campus-Wide Wireless Network''. Their research in abstract aims at Understanding usage patterns in wireless local-area networks (WLANs) is critical for those who develop, deploy, and manage WLAN technology, as well as those who develop systems and application software for wireless networks. The study presented results from the largest and most comprehensive trace of network activity in a large, production wireless LAN. The research traced the activity of nearly two thousand users drawn from a general campus population, using a campus-wide network of 476 access points spread over 161 buildings at Dartmouth College.

Their study expanded on those done by Tang and Baker, with a significantly larger and broader population. They found that residential traffic dominated all other traffic, particularly in residences populated by newer students; students are increasingly choosing a wireless laptop as their primary computer. Although web protocols were the single largest component of traffic volume, network backup and file sharing contributed an unexpectedly large amount to the traffic. Although there was some roaming within a network session, we were surprised by the number of situations in which cards roamed excessively, unable to settle on one access point.

Cross-subnet roams were an especial problem, because they broke IP connections, indicating the need for solutions that avoid or accommodate such roams. Kotz D., Essien K. (2005)

In the African Tertiary Institution Survey (ATICS) Report 2006, out of the 54 campus networks sampled, 94% indicated that they have campus networks. The largest proportion (46%) of the respondents reported they used copper (10Base and 100 BaseT) for their campus backbones, 33% use fibre, while 21% reported they use wireless. Gakio, K. (2006)

In 1994 the Information Networking Institute of Carnegie Mellon University submitted a proposal to the National Science Foundation to create a "High Speed Wireless Infrastructure". The purpose was to support wireless research but also to attract additional research and create, in essence, a campus-wide user community as a mobile computing laboratory. The CMU campus was ideal for such research, as it was concentrated and even non-technical departments are heavy users of networked computing. The campus wired network consisted of three major components: a high speed campus-wide network, network clients, and network services. The key network services are the File System, electronic mail, bulletin boards, distributed printing, access to library information, access to the supercomputing center, and the Internet.

The Wireless network concept build a high speed wireless access system using wireless local area network technology, utilizing spread spectrum in the ISM (industrial, scientific, and medical) band. This access system is integrated with wireline network. The whole network was eventually an operational utility for the use of anyone on campus with an appropriate computer and wireless device, Bennington, et al (2006)

During the dot-com period in 2000, dozens of companies had the notion that Wi-Fi could become the payphone for broadband. The original notion was that users would pay for broadband access at hotspots.

According to Aluoch (2006), connectivity in Africa is poor, unreliable, scarce and very expensive, where available, it is almost never dedicated and users have to contend with frequent service outages at very slow speed. She also revealed the result of the 2006 African Tertiary institutions connectivity survey (ATICS) which indicates that Universities in Africa, on an average pay about US $40.50 per kilobits per second (kbps) per month while some institutions pay as much as US $36 kbps for bandwidth.

2.2 Deployment and Operation Of Campus Wireless Networks

Wi-Fi hotspots have quite been deployed in campus networks for wireless access. Most commercial wireless devices (mobile phones, television, radio, etc.) use licensed radio frequencies. WiFi uses unlicensed spectrum and therefore license fees are not usually required to operate WiFi equipment.

When comparing wireless equipment for use on a campus network, the variables considered are interoperability (i.e. if supports open protocol e.g. 802.11 b/g/n), range (depends on the transmission power of the radio and antenna gain), radio sensitivity(measures the quality of the hardware and the link budget), throughput (the highest possible bit rate as the speed of the equipment); accessories e.g power injectors and availability of spares

Current wireless hotspots deployed on campuses operate in two ways:

1. Using an open public network is the easiest way to create a free hotspot. All that is needed is a Wi-Fi router. Private users of wireless routers can turn off their authentication requirements, thus opening their connection, intentionally or not, for sharing by anyone in range. The disadvantage is that access to the router cannot be controlled.

2. Closed public networks use a hotspot Management System to control the hotspot. This software runs on the router itself or an external computer. The network administrator is able to limit each user's available bandwidth - each

user is therefore restricted to a certain speed to ensure that everyone gets a good quality service.

A campus wireless network user (student or researcher) can only be associated with one Access Point (AP) at a time, managed roaming would mean to either have the AP talk to other APs (e.g. Wireless Distributed System) or have a managing system behind the APs talk to all APs. Streaming of audio and video as learning technologies is becoming increasingly popular, and use large amounts of bandwidth e.g skype, video conferencing, e.t.c.

2.2.1 Class of Traffic Protocols under Investigation

Network-Based Application Recognition (NBAR) tool analyzes and identifies application traffic based on protocols on the wireless network in real time to enable identify class of traffic flowing on the network. The traffic types being analyzed are classified per protocol as follows;

1. **HyperText Transfer Protocol (HTTP)**

   HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed. The sites in consideration in this case includes normal websites and social networks such as facebook, twitter, google sites e.t.c

2. **Hypertext Transfer Protocol Secure (HTTPS)**

   Hyper Text Transfer Protocol Secure (HTTPS) is a secure version of the Hyper Text Transfer Protocol (http). HTTPS allows secure ecommerce transactions,

such as online banking. When a user connects to a website via HTTPS, the website encrypts the session with a digital certificate.

Technically, it is not a protocol in itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. In its popular deployment on the internet, HTTPS provides authentication of the web site and associated web server that one is communicating with, which protects against Man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. In practice, this provides a reasonable guarantee that one is communicating with precisely the web site that one intended to communicate with (as opposed to an impostor), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

3. Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, which let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

4. File Transfer Protocol (FTP)

File Transfer Protocol (FTP), is a protocol through which internet users can upload files from their computers to a website or download files from a website to their PCs. FTP is the easiest way to transfer files between computers via the internet, and utilizes TCP, transmission control protocol, and IP, internet protocol, systems to perform uploading and downloading tasks.

5. Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

6. Kazaar 2

To search for a file on Kazaa, users type the name of the file they want into a box and hit search. Then they select the file they want to download from a list of results. They can select from two file types:

Blue files are made up of content that is controlled by Kazaa users. People who make their content available on Kazaa can license it so that other users can't copy and distribute it without giving them credit. Blue files are free to download.

Gold files contain content from movie studios, music labels and other providers who oversee the use of their material. Gold files are distributed via another P2P network called Altnet and are pay-per-download. Kazaa is free to its users. Kazaa 2 apparently enables one get assigned a download priority

7. Domain Name System (DNS)

Domain Name System (DNS) is a database system that translates a computer's fully qualified domain name into an IP address. Networked computers use IP

addresses to locate and connect to each other, but IP addresses can be difficult for people to remember. For example, on the web, it's much easier to remember the domain name www.amazon.com than it is to remember its corresponding IP address (207.171.166.48). DNS allows you to connect to another networked computer or remote service by using its user-friendly domain name rather than its numerical IP address. Conversely, Reverse DNS (rDNS) translates an IP address into a domain name. Each organization that maintains a computer network have at least one server handling DNS queries. That server, called a name server, holds a list of all the IP addresses within its network, plus a cache of IP addresses for recently accessed computers outside the network. Each computer on each network needs to know the location of only one name server.

8. Skype

Skype is a proprietary voice-over-Internet Protocol (VoIP) service and software application. The service allows users to communicate with peers by voice using a microphone, video by using a webcam, and instant messaging over the Internet. Phone calls may be placed to recipients on the traditional telephone networks. Calls to other users within the Skype service are free of charge, while calls to landline telephones and mobile phones are charged via a debit-based user account system. Skype has also become popular for its additional features, including file transfer, and videoconferencing.

The figure 1 below are graphs depicting some expected shift in traffic per protocol before and after implementation of the wireless campus networks for seven campuses.

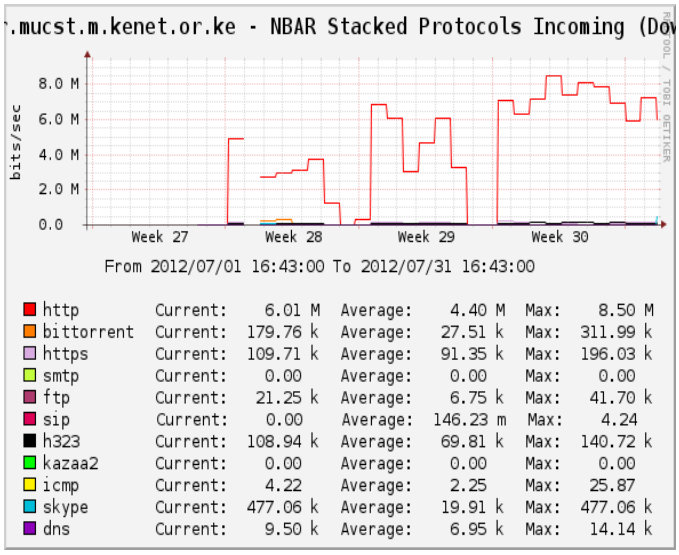


Figure 1-a: MUCST- July 2012 (Source: KENET)

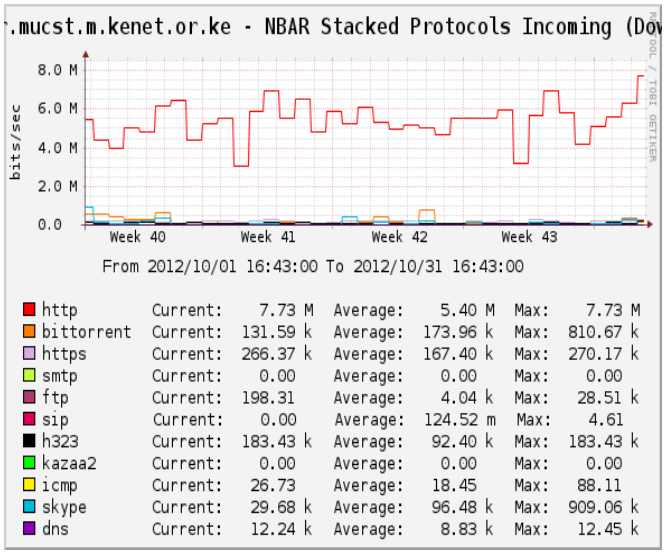


Figure 1-b: MUCST -October 2012 (Source: KENET)

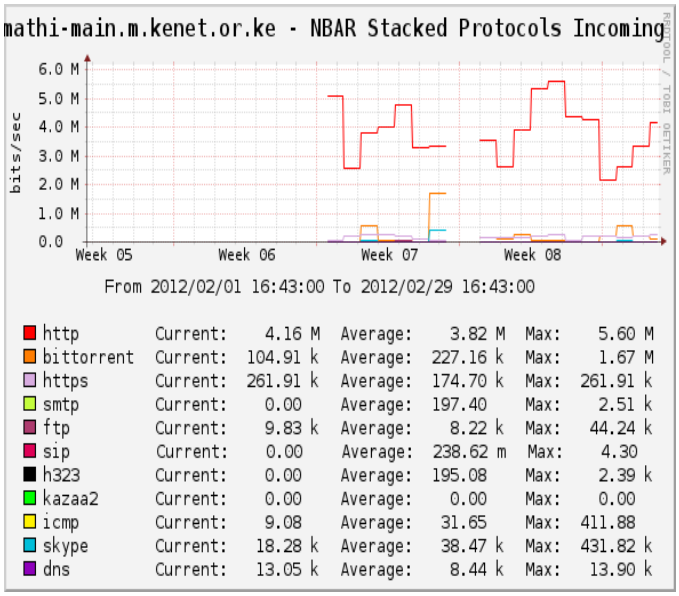


Figure 1-c: KUCT -Feb 2012 (Source: KENET)

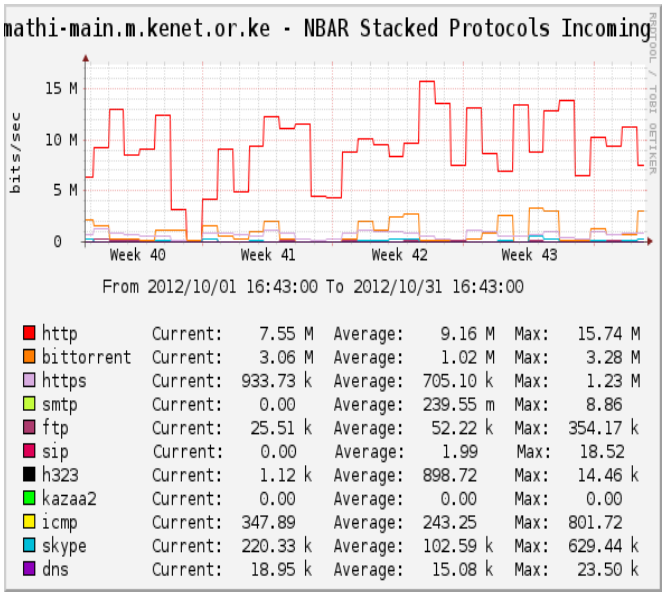


Figure 1-d: KUCT-Oct 2012 (Source: KENET)

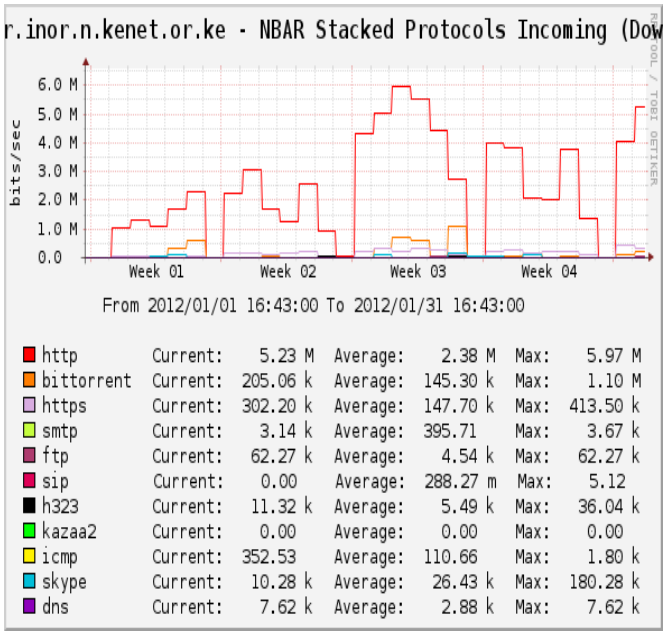


Figure 1-e : Inoorero -Jan 2012 (Source: KENET)

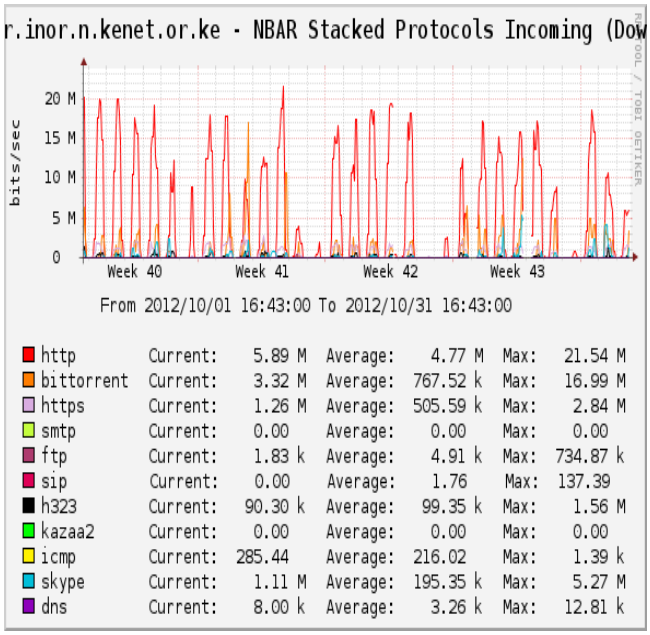


Figure 1-f: Inoorero - Oct 2012 (Source: KENET)

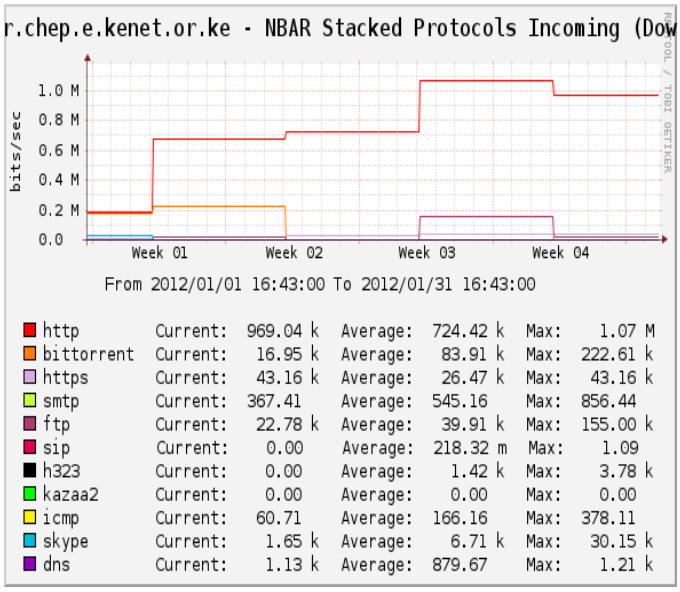


Figure 1-g: Chepkoilel Jan 2012 (Source: KENET)

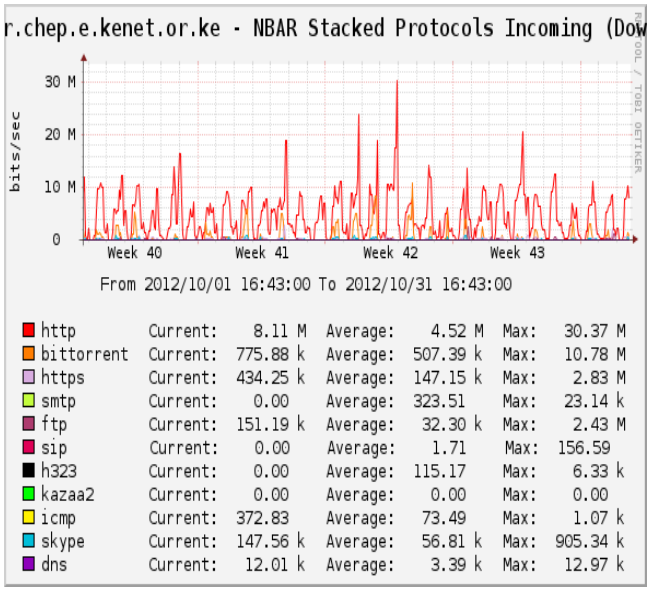


Figure 1-h: Chepkoilel Oct 2012 (Source: KENET)

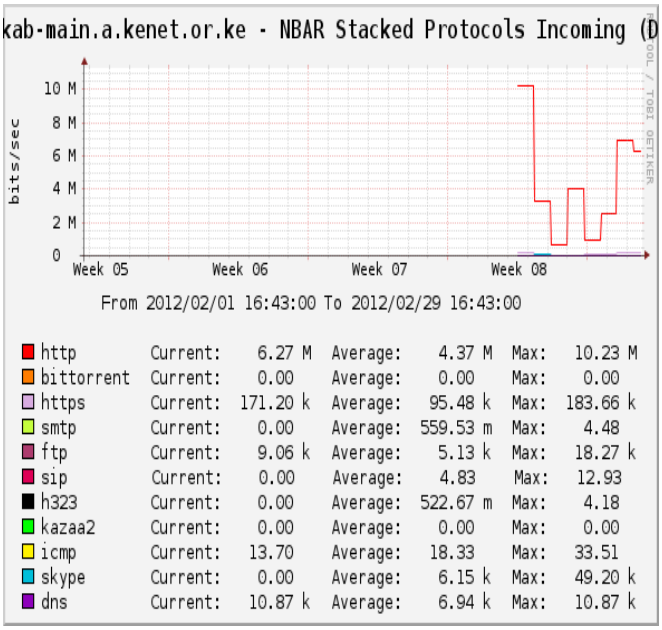


Figure 1-i: Kabarak-Oct 2012 (Source: KENET)

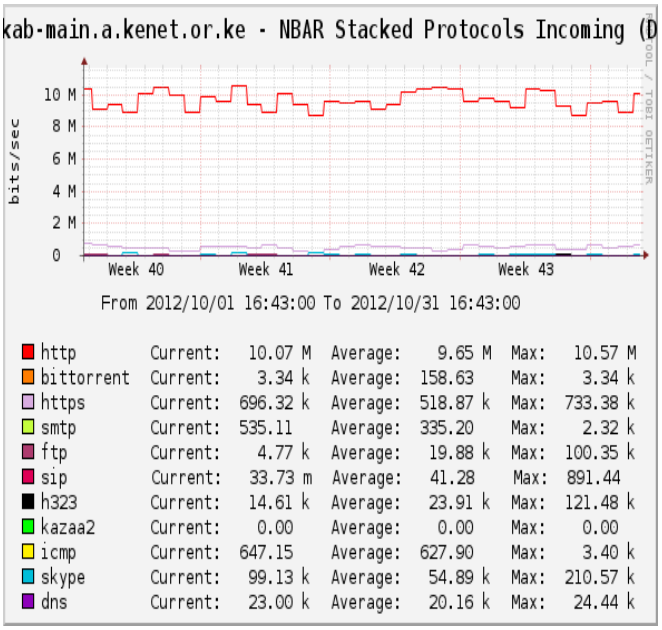


Figure 1-j: Kabarak-Feb 2012(Source: KENET)

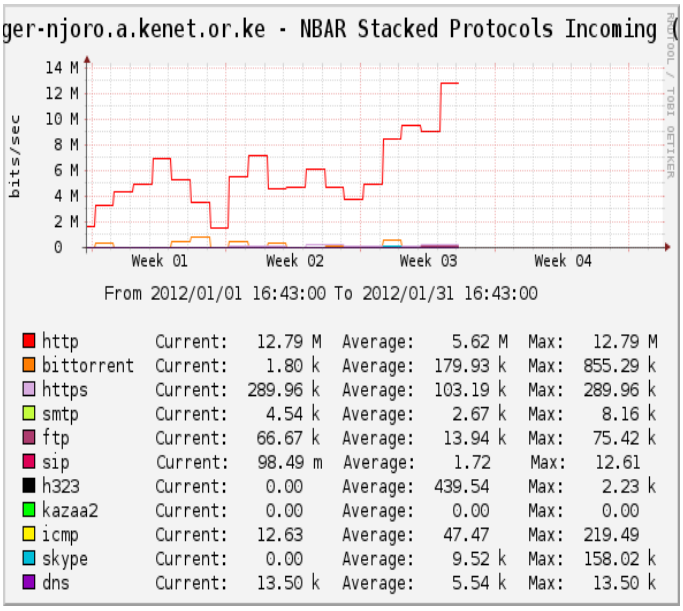


Figure 1-k: Egerton -Jan 2012 (Source: KENET)

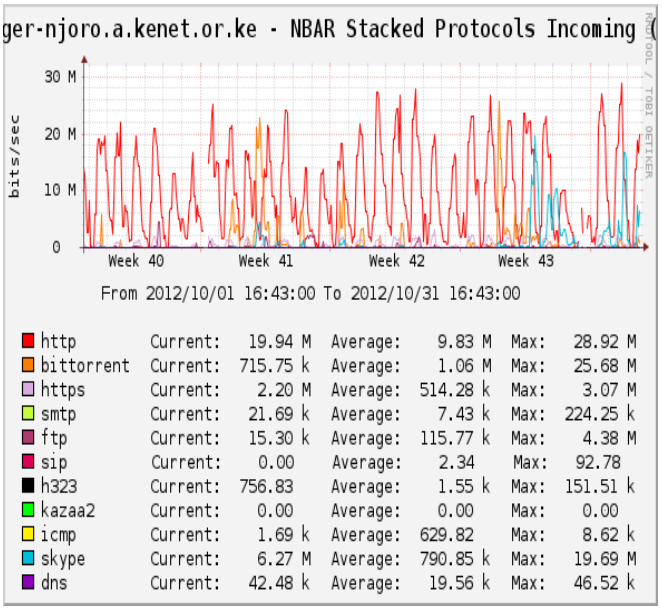


Figure 1-m: Egerton -Oct 2012 (Source: KENET)

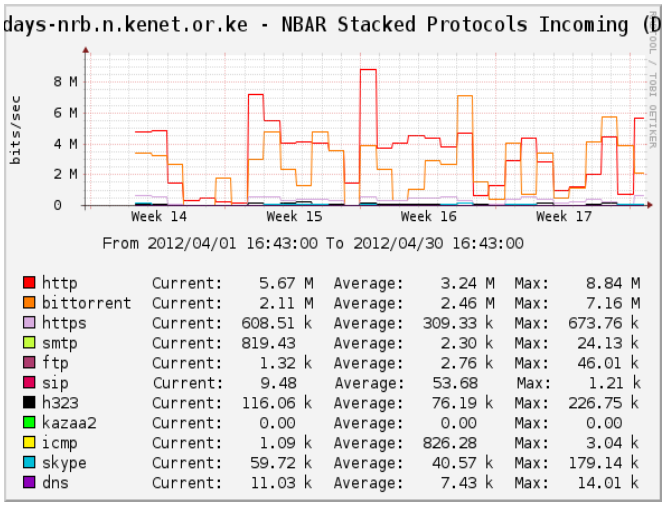


Figure 1-n : Daystar-Feb 2012 (Source: KENET)

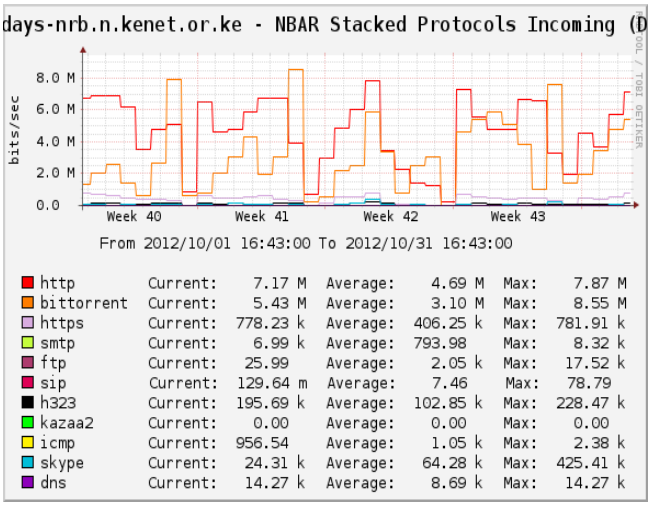


Figure 1-o Daystar-Oct 2012 (Source: KENET)

Figure 1: Graphs depicting usage before and after deployment

2.2.2 Security Configurations on Campus Wireless Networks

Various campuses have implemented different kinds of security configurations on campus wireless networks to meet their security requirements on these networks. The different forms of wireless security that can be implemented on wireless campus networks are discussed below;

1. **Open Wireless Campus Networks**

A Wi-Fi network is said to be open if the WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) security protocols aren't used. An open network gives the user's unrestricted access to the Internet, library catalogs, and web pages with course information. The only limitation to access of these networks is geographical distance from the access points. According to Hole K J (2011), open wireless networks increase the usability because students and faculty do not need to remember passwords and carry authentication devices; give short-term guests easy Internet access without the need for new user accounts and provide the public with effortless access to online catalogs maintained by university libraries.

2. **Restricted area Wireless Campus networks**

This refers to wireless networks which are restricted access to particular services. Access to information systems of the University requires user login credentials. Very sensitive personal information should not be available on open wireless network at all. Services providing sensitive information use strong password for authentication of users. Web browser is an example of this type of security and is ubiquitous on laptop computers, PDA and other devices. To gain access to the wireless network users merely launch a browser, and select the access type from a page that is presented to them automatically. Wireless gateway devices are used for authentication and filtering. The advantage to this method is that it ensures that users can get adequate network access quickly and easily. Because it uses familiar mechanisms it generates a minimal user support requirement.

3. **Highly Restricted Wireless Networks**

In this case, all users go through the IT department for configurations and enabling their wireless devices to access the campus network. A university information systems contains personal information such as medical information, social security numbers, annual salaries, student grades, disciplinary actions e.t.c

In this case, users have to get assistance of IT department for configuration of their wireless devices to get credentials for access to the wireless network. If users authenticate to a wireless university network, then the IT department can track users' activities on campus. Data from many network sessions can be combined to build user profiles.

A university may therefore worry that security breaches on the network leads to negative publicity. Mandatory authentication of all users is therefore introduced to make successful attacks less likely, deflect criticism away from the IT department to the users and bad news are kept secret from the press.

2.3 Conceptual Framework

Conceptual frameworks (theoretical frameworks) are a type of intermediate theory that attempt to connect to all aspects of inquiry (e.g., problem definition, purpose, literature review, methodology, data collection and analysis). Conceptual frameworks can act like maps that give coherence to empirical inquiry. Because conceptual frameworks are potentially so close to empirical inquiry, they take different forms depending upon the research question or problem. The viable conceptual framework for this study is as shown in figure 1 below.

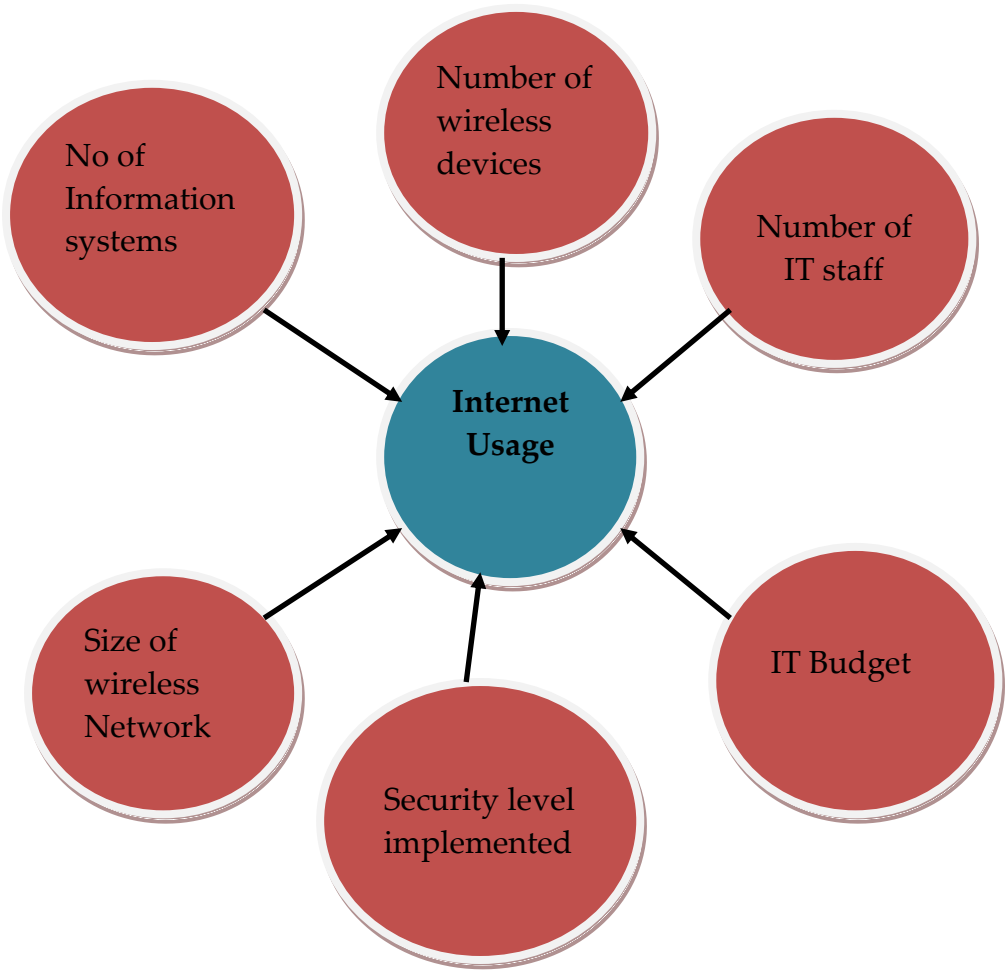


Figure 2: Conceptual Framework

From the conceptual framework, it is noted that all the factors noted interrelate with a common aim of achieving high number of online users and generate high traffic volume.

The independent variables in this framework are as follows;

1. Number of information systems
2. Size of wireless network
3. Number of wireless devices
4. Security Level implemented
5. Number of IT staff
6. IT Budget

The dependent variable in this framework is Internet usage

The relevance of the variables of the conceptual framework may are explained as follows;

Number of information systems

Each campus aspires to automate the processes. Systems that enhance efficiency of processes include finance management systems, student registration system, examination management system, library management systems, decision support systems e.t.c. Deployment of these systems are at different stage per campus. The more the information systems deployed catalyzes the internet usage on campus. This is therefore an independent variable.

Size of Wireless Network

The size of wireless network is determined by the number of access points available on the network and the number of simultaneous users each access point can handle. This is an independent variable which determines the usage.

Number of Wireless Devices

The number of wireless devices available to access the network determines internet usage. Such devices could be laptops, ipads, PCs with wireless cards, smartphones e.t.c.

Security Level implemented

The security level implemented may determine the number of users that access the wireless network. Highly secure networks may require rigorous security features which may be tedious for some users. Open networks may also scare users from having their personal/confidential information transferred via wireless network.

IT Budget and Staff

IT budget determines the size of the wireless network, number of information systems to be deployed and the number of IT staff and their competencies. This in overall determines the adoption of use of online services and therefore increases internet usage.

3.0 RESEARCH METHODOLOGY

3.1 Research Design

The research design involved a through literature review and data analysis that clearly define number and class of Access Points deployed and the maximum capacity that the campus network can achieve and the security levels implemented on the campus networks.

Statistics was collected on the number of devices accessing the network and the traffic statistics before and after the deployment of campus wireless networks.

The study employed correlation analysis, descriptive statistics from the ICT data collected and answering the research questions. The nature of the relationship informed the theories under investigation in this study.

3.2 Data and Information Sources

The respondents for the research were a sample of the following groups;

1. ICT Directors/Managers
2. Systems/Network Administrator's
3. Students
4. Staffs in support units i.e. finance, examinations and registry.
5. Lecturers/ Researchers

The correspondents groups and the roles played by each group is summarized in the table 2 below;

Table 1 : Respondents groups and their roles in the study

Correspondent Group	Role/ Information to be provide
1. ICT Directors/Managers	This group provided information on; • ICT Budget • When the wireless campus network was commissioned • Number of simultaneous users • Bandwidth available on campus • Number of information systems implemented • security level implemented on wireless network and reason for the choice
2. Systems/ Network Administrators	They provided information on; • Usage graphs on wireless campus networks • No of devices accessing wireless networks • Advantages and bottlenecks of security configurations implemented • Usage of information systems implemented • Uptime (reliability) of the wireless networks • Uptime (reliability) of information system deployed
3. Students	• If they have used wireless networks on campus • Availability of wireless devices and ease to acquire • Security steps they go through to access • Information systems they commonly use • Effectiveness of information systems serve their needs
4. Staffs in support units i.e. finance, examinations and registry.	• If they have used wireless networks in offices • Security steps they go through to access • Information systems they use in their work • Reliability of the information system they use

	• Effectiveness of information systems serve their needs
5. Lecturers/ Researchers	• If they have used wireless networks in offices and classrooms • Security steps they go through to access wireless network • Experience on speed to meet researchers needs for high speed data transfer • Reliability of the network • Effectiveness of information systems serve their needs

3.3 Sample Selection and Sampling Technique

The sampling techniques used in this study are a combination of stratified random sampling and purposeful sampling. Stratified Random Sampling and purposeful sampling was employed. Stratified method of sampling involved the division of campuses into groups of public and private Universities, larger Universities with student population of over 10,000 and the other group with those that are less. The status of whether public or private as well as population of students classify campus shared attributes or characteristics. The sample size targeted is at least 15% of the Universities to be covered. The respondent in each category is at least one person.

Table 2: Universities/campuses classified as public or private

University	**Strata**
1. University of Nairobi, main campus	Public
2. Jomo Kenyatta University of Agriculture and Technology, main campus	Public
3. Kenyatta University, main campus	Public
4. Meru University College of Science and Technology	Public
5. Dedan Kimathi University of Technology	Public
6. South Eastern University College	Public
7. Chepkoilel University College	Public

8. Masinde Muliro University of Science and Technology	Public
9. Egerton University, Njoro campus	Public
10. Kabianga University College	Public
11. Daystar University, Athi River campus	Private
12. Strathmore University	Private
13. St Paul's University, Limuru campus	Private
14. Kabarak University, main campus	Private
15. Inoorero University	Private

Purposive sampling represents a group of different non-probability sampling techniques. Also known as judgmental, selective or subjective sampling, purposive sampling relies on the judgement of the researcher when it comes to selecting the campuses that are to be studied. Purposeful sample mainly targets main campuses of the University, and having implemented wireless networks in the last three years preferably with an ERP in place. Using this criterion, the sample selection identified the following campuses;

1. University of Nairobi, main campus
2. Jomo Kenyatta University of Agriculture and Technology, main campus
3. Kenyatta University, main campus
4. Dedan Kimathi University of Technology
5. Strathmore University
6. Kabarak University
7. Daystar University
8. Masinde Muliro University of Science and Technology
9. Egerton University, Njoro campus

The next choice for purposeful random sampling targets campuses with fixed campus networks but no wireless networks at all. Using this criterion, the sample selection identified the following campuses;

1. Chepkoilel University College
2. Laikipia University College
3. St Paul's University
4. South Eastern University College
5. Kabianga University College

3.4 Data Collection Tools and Procedures

The data collection tools were through mail questionnaires, oral interview, telephone interview and internet usage graphs. Questionnaires were used to collect data. The questionnaire had both closed and open ended questions which respondents answered.

3.5 Data Analysis Procedure

To arrive at a conclusion the data collected from questionnaires and interviews was analyzed using measures of central tendency namely; arithmetic mean and mode. Analysis involved computation of increase in wireless access point capacity against growth patterns of different kind of traffic per protocol with a view to finding relations between these variables. A comparison was made between the three security levels implemented on wireless networks against collected data on traffic pattern, and subjecting the same to statistical tests to determine significance in responding to the research question.

3.6 Limitations of the Methodology and how they can be overcome

The major limitation of this methodology was delay in getting feedback from the correspondents. This was overcome by prior engagement and arrangement for data collection.

4.0 PRESENTATION OF RESEARCH FINDINGS

4.1 Introduction

The study aimed to investigate the effects of wireless campus networks on internet usage on campuses in Kenya.

The study aimed to analyze and present results on internet usage with respect to growth of wireless campus networks. The study also presented trends in internet usage between campuses that has implemented wireless networks and those that have not as well as examine relationship between security levels on wireless campus networks and the internet usage.

This study aimed at extending the findings of a similar research titled ''Analysis of a Campus-Wide Wireless Network'' previously carried out by Kotz and Essien (2005)

4.2 Research Methodology

The sampling techniques used in this study were a combination of stratified random sampling and purposeful sampling. Stratified method of sampling involved the division of campuses into groups of public and private Universities Ten public Universities and six private Universities were selected under the sample. The status of whether public or private as well as population of students classify campus shared attributes or characteristics. Sample size targeted was at least 15% of the Universities to be covered. The respondent in each category is at least one person.

The independent variables in this framework were as follows;

1. Number of information systems
2. Size of wireless network
3. Number of wireless devices
4. Security Level implemented
5. IT team
6. IT Budget

Table 3 : Classification of Universities (CUE 2013)

Category of University	**No**
Chartered Public Universities	16
Public University Colleges	15
Public University Campuses	3
Chartered Private Universities	14
Chartered Private University Colleges	6
Universities with Letter of Interim Authority	12
Registered Private Universities	2
Total	**68**

4.3 Analysis and Results

The research targeted to collect data from 16 Universities out of a total of 68. However, data was collected from 14 campuses which represents 21% of the population. Consumption graphs were generated at KENET. Data was collected from ICT Managers, network administrators, students, finance officers and researchers in each campus. The main mode of data collection was via an online questionnaire. Telephone interviews were also deployed to a limited extend.

4.3.1 Findings on relationship between growth in wireless campus network to internet usage

The tables below shows data collected on 12 campuses. The data collected shows number of students per campus, commissioning month for the WLAN, number of access points and average outbound traffic before and after commissioning. The questionnaire used for data collection is attached in Appendix 1.

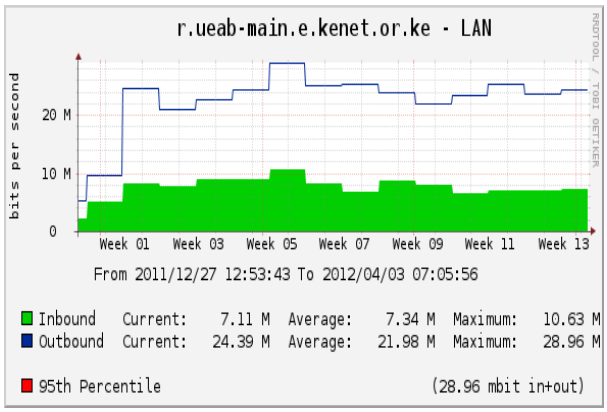
Table 4: Traffic growth with respect to commissioning of WLAN

No	Campus Name	No of Students	MM/YY CWN Implemented	No of APs	Avg outbound capacity before WLAN (Mb/s)	Avg outbound capacity after WLAN (Mb/s)	Difference
1	UEA, Baraton	1,600	Mar-12	15	21.98	31.02	9.04
2	SEUCO	3,500	Not Implemented	0	1.72	1.72	0
3	MUCST	3,500	Aug-12	5	3.13	4.98	1.85
4	DKUT	4,700	Jul-12	12	5.49	13.26	7.77
5	Daystar	4,000	Sep-12	7	9.22	12.96	3.74
6	SPU	1,800	Nov-12	3	1.14	3.71	2.57
7	UoE (Chep)	10,000	Not Implemented	0	N/A	N/A	0
8	MMUST	10,000	Oct-12	5	10.97	17.56	6.59
9	Kabarak	2,500	Not Implemented	N/A	N/A	N/A	N/A
10	UoN	60,000	Feb-10	60	45.18	82.11	36.93
11	KU	40,000	Nov-11	15	27.59	43.73	16.14
12	Egerton Njoro	8,000	Nov-12	7	7.35	10.75	3.4
13	JKUAT	30,000	Jun- 12	12	32.04	51.95	19.91
14	Strathmore		No data				
15	Inoorero		No data				
16	Kabianga		No data				

Table 5: Campuses where WLAN implemented and traffic shift

Campus Name	No of APs	Average outbound capacity before WLAN (Mb/s)	Average outbound capacity after WLAN (Mb/s)	% Increase
UEA, Baraton	15	21.98	31.02	41%
SEUCO	0	1.72	1.72	0%
MUCST	5	3.13	4.98	59%
DKUCT	12	5.49	13.26	142%
Daystar	7	9.22	12.96	41%
MMUST	5	10.97	17.56	60%
KU	15	27.59	43.73	58%
UoN	60	45.18	82.11	82%
JKUAT	12	32.04	51.95	62%
Inoorero	25	2.47	5.22	111%

From table 5 and table 6 above, the average outbound traffic increased immediately after commissioning of the wireless network. The graphs below show the shift in traffic before and after commissioning of WLAN. The increase ranges from 41% to 142%. The increase is not necessarily linear.



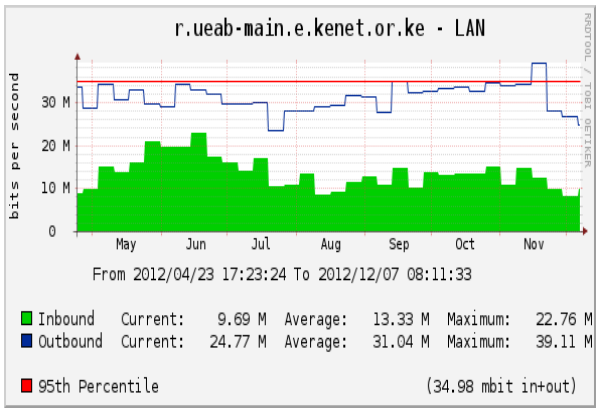
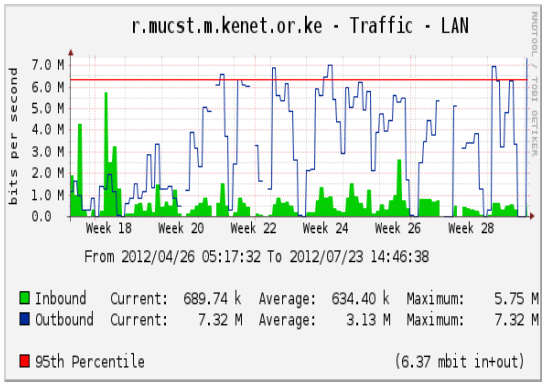


Figure 3-a: UEA Baraton before WLAN (Source: KENET) Figure 3-b: UEA Baraton after WLAN (Source: KENET)



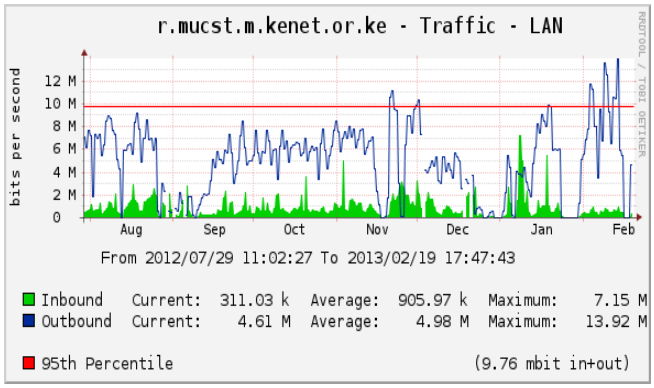
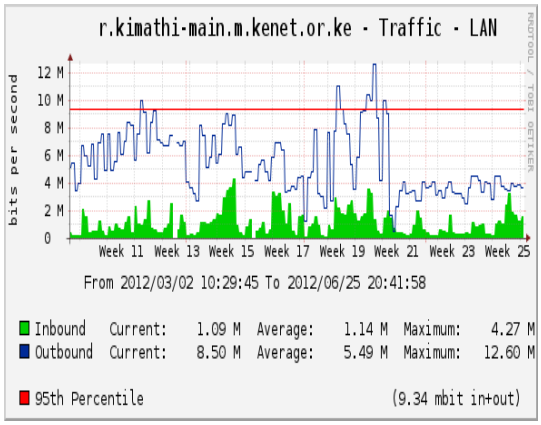


Figure 3-c: MUCST before WLAN (Source: KENET) Figure 3-d: MUCST after WLAN (Source: KENET)



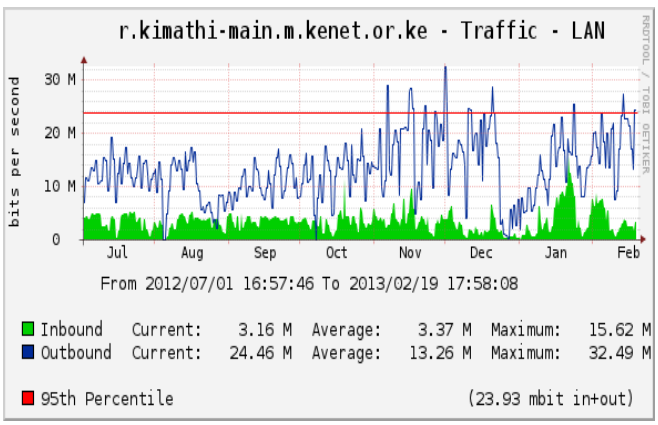


Figure 3-e: DKUT before WLAN (Source: KENET) Figure 3-f: DKUT after WLAN (Source: KENET)

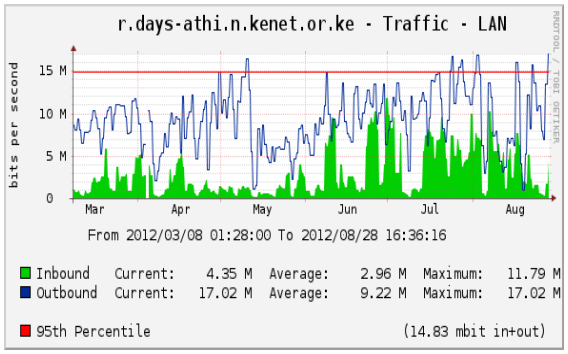


Figure 3-g: Daystar before WLAN (Source: KENET)

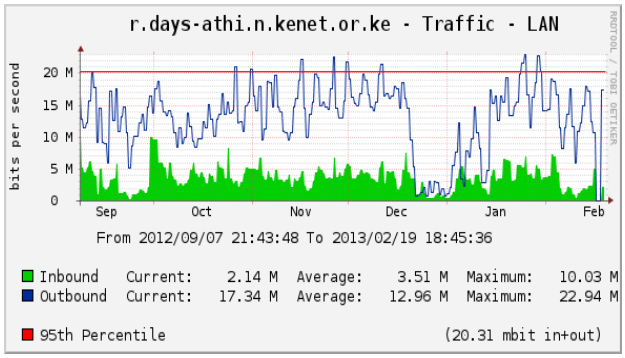


Figure 3-h: Daystar after WLAN (Source: KENET)

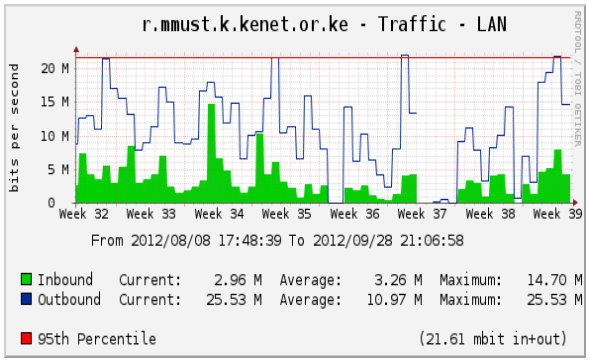


Figure 3-i: MMUST before WLAN (Source: KENET)

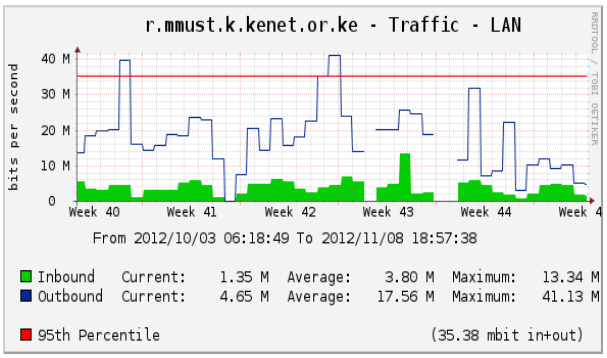


Figure 3-j: MMUST after WLAN (Source: KENET)

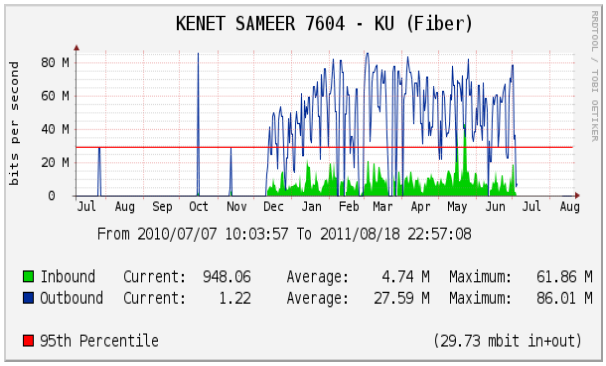


Figure 3-k: KU before WLAN (Source: KENET)

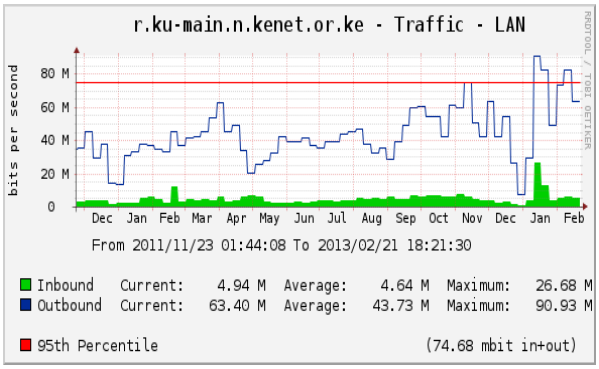


Figure 3-l: KU after WLAN (Source: KENET)

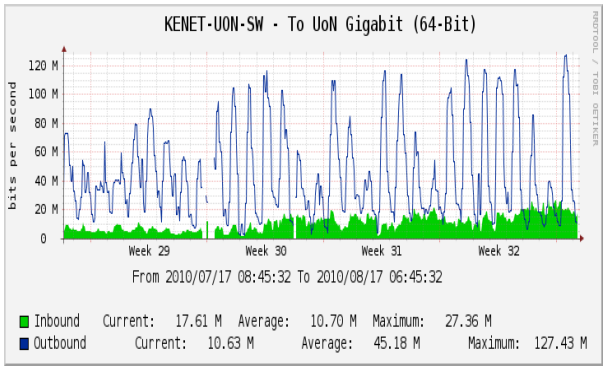


Figure 3-m: UoN before WLAN (Source: KENET)

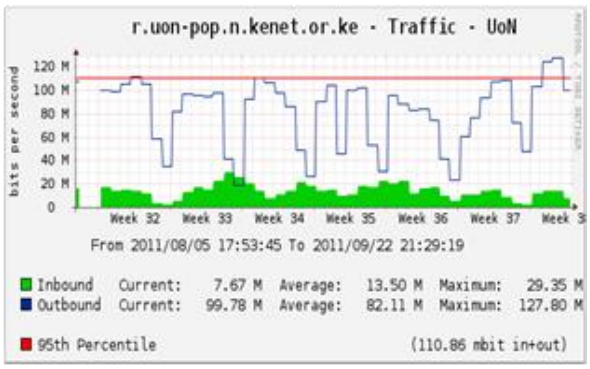


Figure 3-n: UoN after WLAN (Source: KENET)

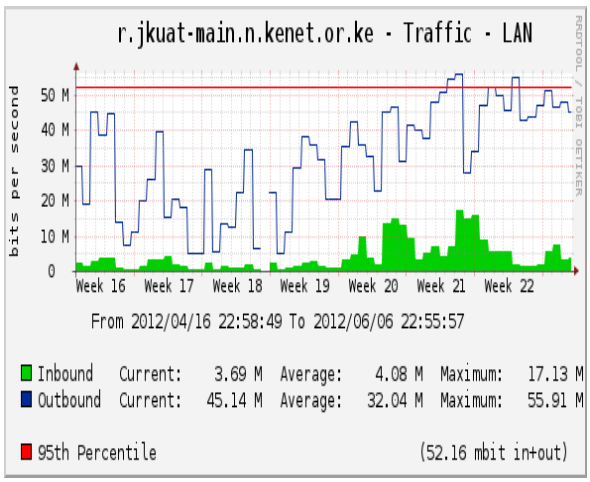


Figure 3-o: JKUAT before WLAN (Source: KENET)

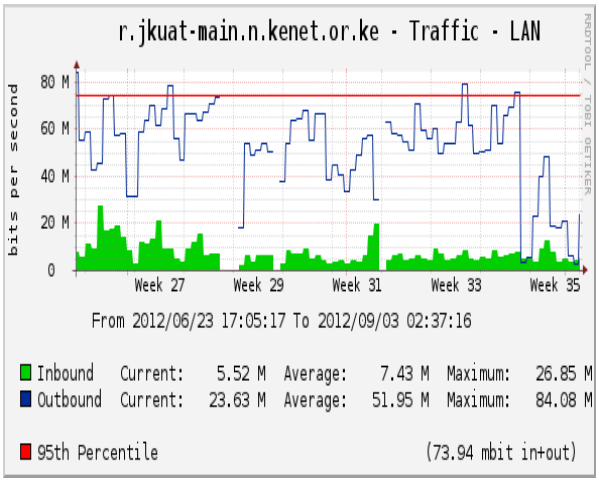


Figure 3-p: JKUAT after WLAN (Source: KENET)

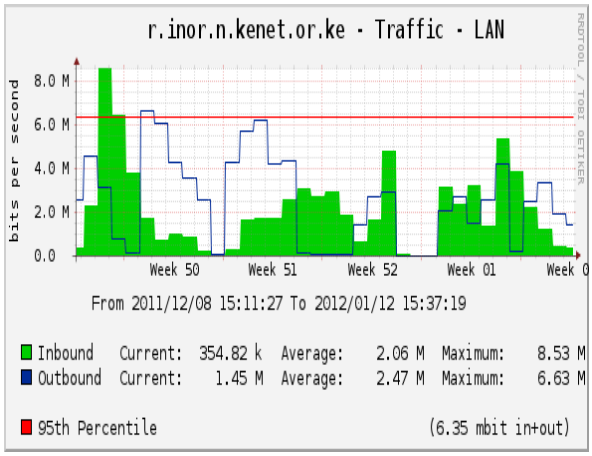


Figure 3-q: Inoorero before WLAN (Source: KENET)

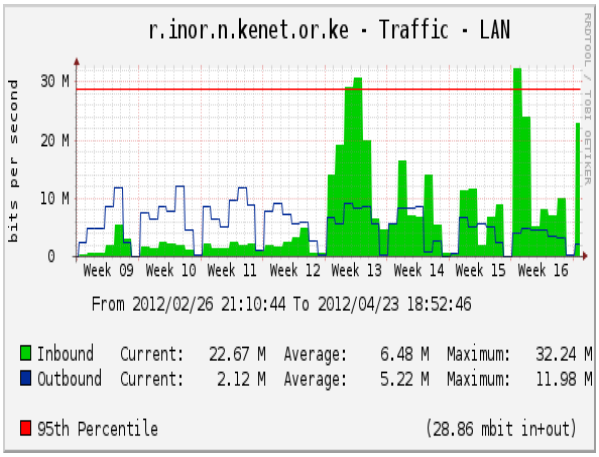
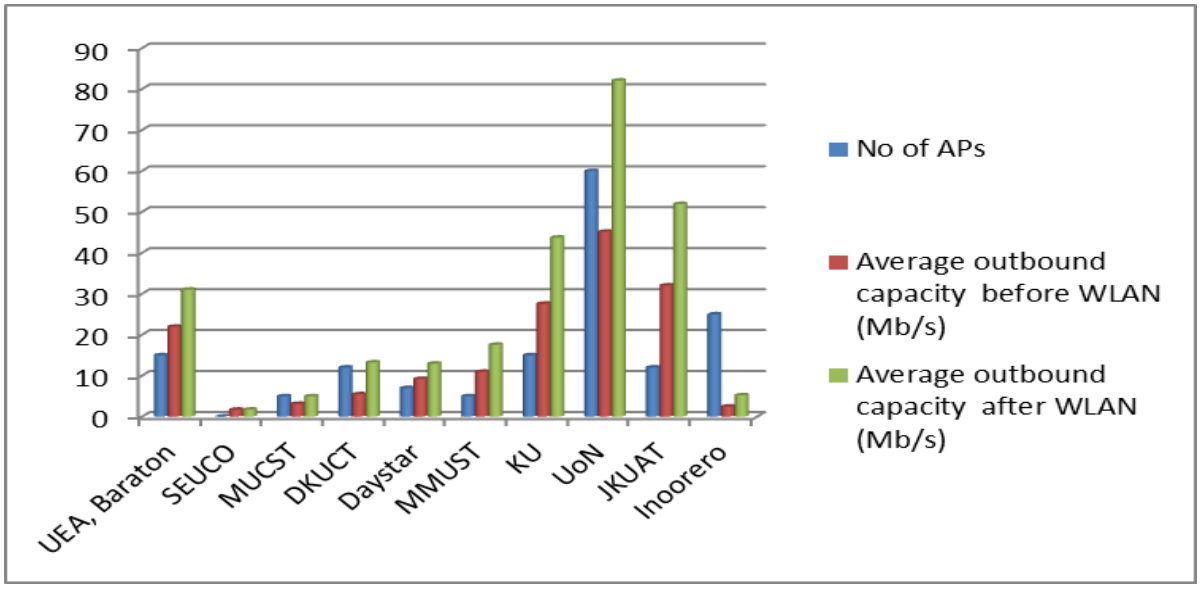


Figure 3-r: Inoorero after WLAN (Source: KENET)

Figure 3: Campus Internet usage graphs before and after WLAN Implementation

Chart 1: No of APs vis a vis average outbound traffic before and after WLAN

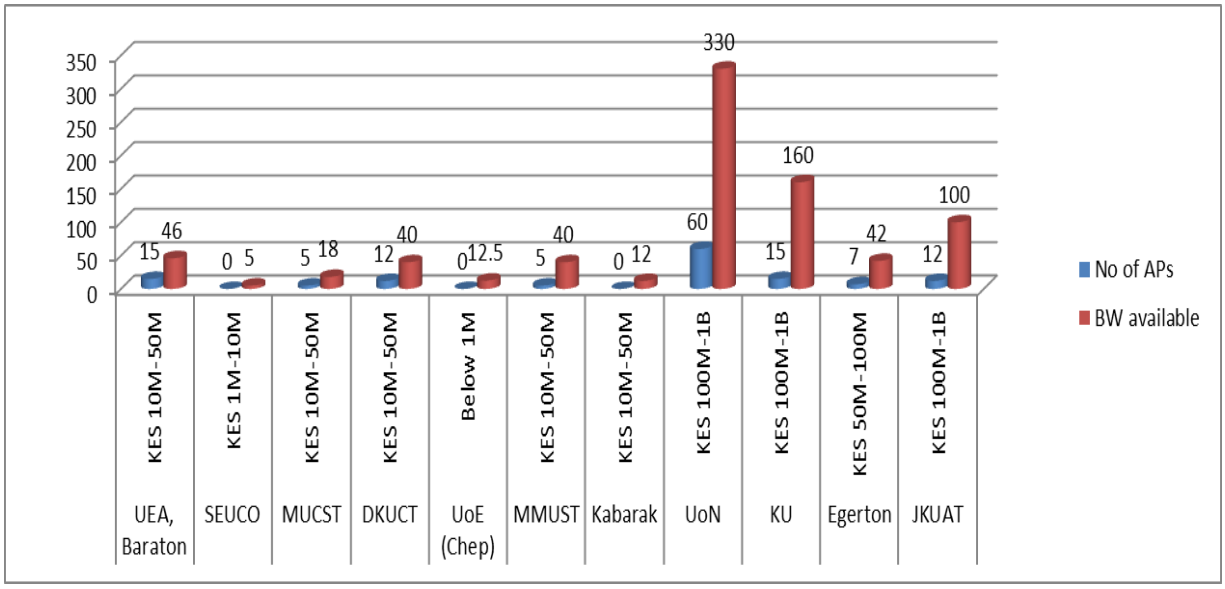


The bar chart above shows the behavior of traffic growth before and after commissioning. Notice that the higher the number of access points deployed, the higher the growth.

Table 6: Effect of ICT Budget

No	Campus Name	Annual ICT Budget	No of APs	BW Available
1	UEA, Baraton	Over 10M	15	46
2	SEUCO	KES 1M-10M	0	5
3	MUCST	KES 10M-50M	5	18
4	DKUCT	KES 10M-50M	12	40
5	UoE (Chep)	Below 1M	0	12.5
6	MMUST	KES 10M-50M	5	40
7	Kabarak	KES 10M-50M	0	12
8	UoN	KES 100M-1B	60	330
9	KU	KES 100M-1B	15	160
10	Egerton	KES 50M-100M	7	42

Chart 2: Relationship between budget, number of access points and bandwidth available

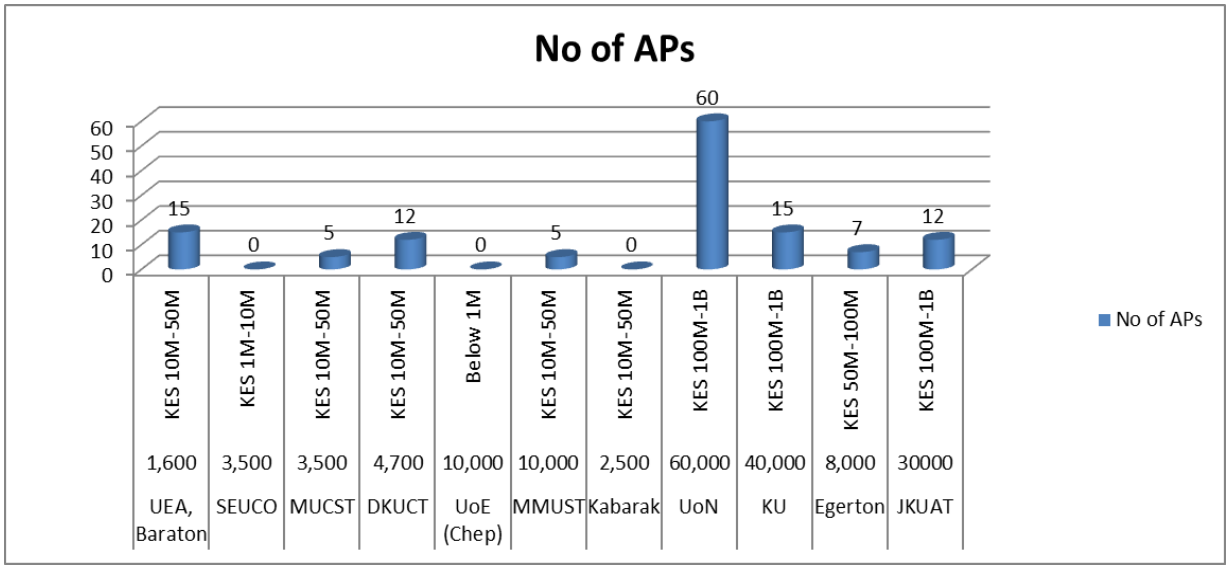


From Table 7 and chart 2, Universities with higher number of access points have higher bandwidth in the ratio of 1:3-8; and indicates that the higher the number of access points, the higher the bandwidth.

Table 7: Relationship between number of students and number of Access Points

No	Campus Name	No of Students	Annual ICT Budget	No of APs
1	UEA, Baraton	1,600	KES 10M-50M	15
2	SEUCO	3,500	KES 1M-10M	0
3	MUCST	3,500	KES 10M-50M	5
4	DKUCT	4,700	KES 10M-50M	12
5	UoE (Chep)	10,000	Below 1M	0
6	MMUST	10,000	KES 10M-50M	5
7	Kabarak	2,500	KES 10M-50M	0
8	UoN	60,000	KES 100M-1B	60
9	KU	40,000	KES 100M-1B	15
10	Egerton	8,000	KES 50M-100M	7
11	JKUAT	30,000	KES 100M-1B	12

Chart 3: Relationship between number of APs and ICT budget



From Table 8 and chart 3, Universities with ICT budgets below KES 1Million have not implemented wireless campus networks. Examples are University of Eldoret and SEUCO. The Universities with ICT budgets above KES 10Million have implemented wireless campus networks. The Universities with ICT budgets between KES 1Million to KES 10Million have either started implementing a few access points and are planning to start implementation.

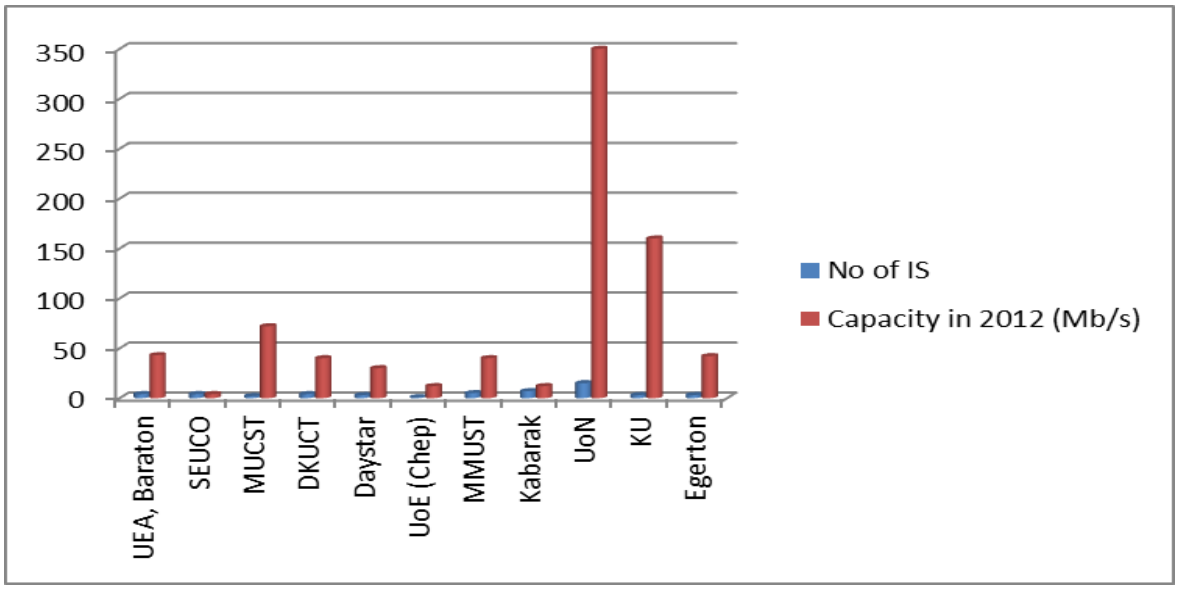
The number of information systems determines the capacity uptake by the University. Table 9 and chart 4 illustrates this relationship. The number of IS

implemented is has no relationship with the number of students on campus. Most commonly implemented information systems are Student Management Information System (SMIS), Human Resource Information System (HRMIS) and Financial Management System (FMS)

Table 8: Relationship between number of information systems and bandwidth

No	Campus Name	No of IS	Capacity in 2012 (Mb/s)	No of Students
1	UEA, Baraton	4	43	1,600
2	SEUCO	4	4	3,500
3	MUCST	2	72	3,500
4	DKUCT	4	40	4,700
5	Daystar	3	30	5,000
6	UoE (Chep)	1	12	10,000
7	MMUST	5	40	1,000
8	Kabarak	7	12	2,500
9	UoN	15	350	60,000
10	KU	3	160	40,000
11	Egerton	3	42	8,000

Chart 4: Relationship between number of IS and bandwidth



4.3.2 Analysis and Results on trends in internet usage between campuses that have implemented wireless networks and those that have not

The data collected indicate that capacities have been growing faster over the last three years for the Universities where wireless networks have been implemented. Capacities have remained constant for the Universities where wireless networks have not been implemented.

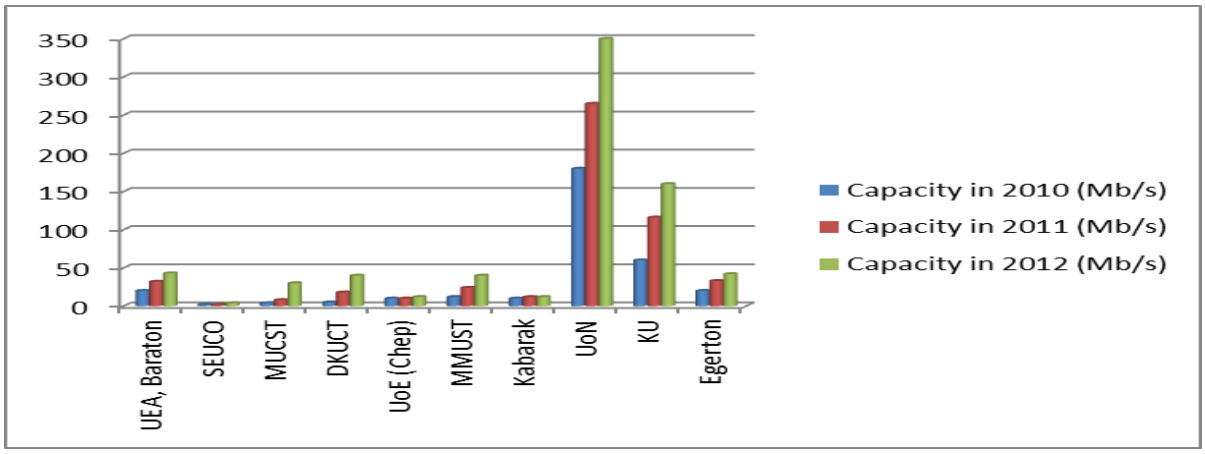
Table 9: Capacity growth from 2010 to 2012

No	**Campus Name**	**No of Students**	**MM/YY CWN Implemented**	**Capacity in 2010 (Mb/s)**	**No of IS**	**Capacity in 2011 (Mb/s)**	**Capacity in 2012 (Mb/s)**
1	UEA, Baraton	1,600	Jun-11	20		32	43
2	SEUCO	3,500	Aug-10	2		2	4
3	MUCST	3,500	Aug-12	4		8	30
4	DKUCT	4,700	Apr-11	5		18	40
5	Daystar		Sep-12				
6	UoE (Chep)	10,000	N/A	10		10	12
7	MMUST	1,000	Oct-12	12		24	40
8	Kabarak	2,500		10		12	12
9	UoN	60,000	Feb-10	180		265	350
10	KU	40,000	Nov-11	60		116	160
11	Egerton	8,000	Nov-12	20		33	42

Table 10: Capacity growth and number of students per campus

Campus Name	Capacity in 2010 (Mb/s)	Capacity in 2011 (Mb/s)	% Growth 2011	Capacity in 2012 (Mb/s)	% Growth 2012	No of Students
UEA, Baraton	20	32	60%	43	115%	1,600
SEUCO	2	2	0%	4	100%	3,500
MUCST	4	8	100%	30	650%	3,500
DKUCT	5	18	260%	40	700%	4,700
UoE (Chep)	10	10	0%	12	20%	10,000
MMUST	12	24	100%	40	233%	10,000
Kabarak	10	12	20%	12	20%	2,500
UoN	180	265	47%	350	94%	60,000
KU	60	116	93%	160	167%	40,000
Egerton	20	33	65%	42	110%	8,000

Chart 5: Capacity growth



From Table 10 and chart 5, the Universities where wireless networks have been implemented tend to grow their capacities at higher percentages annually than those that have no wireless campus networks. SEUCO, University of Eldoret and Kabarak University experienced the lowest increase of 0%, 0% and 20% respectively in between 2010 and 2011.A similar scenario is witnessed for the two year period between 2010 to 2012 where both University of Eldoret and Kabarak University both experienced a marginal increase of only 20%. Increase has no direct relationship to the number of students; for instance, over two year period (2010-2012) University of Nairobi with a student population of 60,000 only increased by 94% while Dedan

Kimathi University of Technology with a student population of 4,700 has grown its capacity by 700%.

4.3.3 Analysis and Results on how implementation of various security levels on campus wireless network affect internet and IT enabled service usage

The tables below analyses the relationship between the security levels implemented and the effect on usage.

Table 11: Security levels implemented and user support

No	Campus Name	Security Level Implemented	Register Devices	No of Devices	Peak BW (Mb/s)	Users supported	Likelihood for Security Level
1	UEA, Baraton	Restricted	No	N/A	30	Low	Medium
2	SEUCO	Restricted	Yes	300	0.539	High	High
3	MUCST	Restricted	No	N/A	18	Low	Medium
4	DKUCT	Restricted	Yes	150	40	Low	Medium
5	Daystar	Restricted	Yes	700	3	Low	Medium
6	UoE (Chep)	Restricted	No	N/A		High	High
7	MMUST	Open	Yes	450	28	Low	High
8	Kabarak	Restricted	No	N/A	15	High	High
9	UoN	Restricted	Yes	450	28	High	High
10	KU	Open	No	N/A		Low	Low
11	Egerton	Restricted	No	N/A		High	High

Security level implemented

Table 12: Summary of Security levels implemented

	Open	Restricted	Highly restricted
No	2	9	0
%	18%	82%	0%

From table 12, 82% of the universities have implemented restricted security levels while 18% have implemented open security levels.

User support

Table 13: User support and relationship to security level implemented

Rating	Users Supported	Support relate to security
High	5	6
Medium	0	4
Low	6	1

From table 13, high number of users seeking support from IT team to access wireless networks relates it to security level implemented

Registration of wireless devices

Table 14: Registration of wireless devices

Register devices	No of Respondents	% no of respondents
Yes	5	45%
No	6	55%

Analysis in Table 14 shows that 55% of the universities do not register wireless devices while 45% register devices. Those who don't register devices have no visibility of the user devices accessing campus wireless networks

Usage data for wireless campus networks

Table 15: Usage data for wireless campus networks by students

	Statement	Student Response							
		SD	D	DS	N	AS	A	SA	No of respondents
1	I use wireless network on campus						4	7	11
2	Wireless end user devices are easy to acquire		3		1	2	3	2	11
3	Security steps I go through to access are easy		1			4	3	3	11
4	Wireless network is always available			1	3	1	5	1	11

Analysis in table 15 shows that 7 out of 11 student respondents representing 64% agree and the rest agree that they use wireless network on campus. Over 50% agree

that wireless end user devices are easy to acquire and security steps to access wireless network are easy.

Table 16 : Usage data for wireless campus networks by finance officer

	Statement	Finance Officer							
		SD	D	DS	N	AS	A	SA	No of respondents
1	I use wireless network on campus	2	1		2		3		8
2	Wireless end user devices are easy to acquire	2		1	1		3	1	8
3	Security steps I go through to access are easy	2	1		4		1		8
4	Wireless network is always available	2		1	1	1	2	1	8

Analysis in table 16 shows that only 3 out of 8 finance officer respondents representing 38% agree that they use wireless network on campus. 50% agree that wireless end user devices are easy to acquire and that wireless network is always available. 87% of the finance officers disagree that security steps to access wireless network are easy.

Table 17: Usage data for wireless campus networks by researcher

	Statement	Researcher							No of respondents
		SD	D	DS	N	AS	A	SA	
1	I use wireless network on campus					1	5	1	7
2	Wireless end user devices are easy to acquire	1			1	2	3		7
3	Security steps I go through to access are easy			1	2	2	1	1	7
4	Wireless network is always available		1	1	1		2	2	7

Analysis in table 17 shows that only 7 out of 7 researcher respondents representing 100% agree that they use wireless network on campus. 71% agree that wireless end user devices are easy to acquire. 57% agree that Security steps I go through to access are easy and wireless network is always available

4.4 Discussions of the Results in relation to research problem and framework

From the analysis, the average outbound traffic increased immediately after commissioning of the wireless network. The increase ranges from 41% to 142%. The increase is not necessarily linear. Notice that the higher the number of access points deployed, the higher the growth. Universities with higher number of access points have higher bandwidth in the ratio of 1:3-8; and indicate that the higher the number of access points, the higher the bandwidth.

Universities with ICT budgets below KES 1Million have not implemented wireless campus networks. Examples are University of Eldoret and SEUCO. The Universities with ICT budgets above KES 10Million have implemented wireless campus networks. The Universities with ICT budgets between KES 1Million to KES 10Million have either started implementing a few access points and are planning to start implementation. The number of information systems determines the capacity uptake by the University. Table 9 and chart 4 illustrates this relationship. The number of IS implemented is has no relationship with the number of students on campus. Most commonly implemented information systems are Student Management Information System (SMIS), Human Resource Information System (HRMIS) and Financial Management System (FMS)

From Table 10 and chart 5, the Universities where wireless networks have been implemented tend to grow their capacities at higher percentages annually than those that have no wireless campus networks. SEUCO, University of Eldoret and Kabarak University experienced the lowest increase of 0%, 0% and 20% respectively in between 2010 and 2011.A similar scenario is witnessed for the two year period between 2010 to 2012 where both University of Eldoret and Kabarak University both experienced a marginal increase of only 20%. Increase has no direct relationship to the number of students; for instance, over two year period (2010-2012) University of Nairobi with a student population of 60,000 only increased by 94% while Dedan Kimathi University of Technology with a student population of 4,700 has grown its capacity by 700%. From table 12, 82% of the universities have implemented restricted

security levels while 18% have implemented open security levels. From table 13, high number of users seeking support from IT team to access wireless networks relates it to security level implemented. Analysis in Table 14 shows that 55% of the universities do not register wireless devices while 45% register devices. Those who don't register devices have no visibility of the user devices accessing campus wireless networks. Analysis in table 15 shows that 7 out of 11 student respondents representing 64% agree and the rest agree that they use wireless network on campus.

Over 50% agree that wireless end user devices are easy to acquire and security steps to access wireless network are easy. Only 3 out of 8 finance officer respondents representing 38% agree that they use wireless network on campus. 50% agree that wireless end user devices are easy to acquire and that wireless network is always available. 87% of the finance officers disagree that security steps to access wireless network are easy. Table 17 shows that only 7 out of 7 researcher respondents representing 100% agree that they use wireless network on campus. 71% agree that wireless end user devices are easy to acquire. 57% agree that Security steps they go through to access are easy and wireless network is always available

4.4.1 Relationship of results to the problem

With reference to the research problem, the research results address the knowledge gap on the relationship that exists between growth in wireless network deployment and internet usage. The analysis indicates annual increase of internet usage that ranges from 41% to 142% with wireless deployments. For cases where wireless networks are not deployed, growth in internet usage ranges from 0-20%. The research also addresses the relationship between security levels configured on wireless campus network to the growth in internet usage. The results indicate that the more restrictive the security level implemented attracts high number of users seeking support from IT team to access wireless networks and therefore limits internet usage on campus.

4.4.2 Relationship of results to the research framework

The conceptual frame work of this study revolves around six independent variables and one dependent variable. The independent variables are number of information systems deployed, size of wireless network, number of wireless devices, security Level implemented, number of IT staff and IT Budget. The only dependent variable is internet usage. The variables were used to develop the research questionnaire. Data collected in the questionnaire was analyzed and the results aimed at answering the research three questions.

4.4.3 Relationship of results to the methodology

The sampling techniques used in this study are a combination of stratified random sampling and purposeful sampling. Stratified sampling and purposeful sampling employed. The research targeted to collect data from 16 Universities out of a total of 68 which was 24% of all campuses. Data was collected from 14 Universities which represents 21% of the population. Consumption graphs were collected both at the institutions and at KENET. Data collected from ICT Managers, network administrators, students, finance officers and researchers in each campus. Research assistants employed were ICT directors to collect data in campuses. The main mode of data collection was via questionnaire. Telephone interviews were also used for data collection to limited extend. The study employed correlation analysis, descriptive statistics from the ICT data to be collected and the answering the research questions

5.0 CONCLUSIONS & RECOMMENDATIONS

5.1 Assessment of the value of this study

The results of the study have established the relationship that exists between growth in wireless campus network and various internet traffic patterns at the University campuses. The study has established the effect of various variables that affect deployment and use of wireless campus networks which in turn relate to internet usage. These variables are drawn from the conceptual framework of the study. These variables include number of information systems deployed, size of wireless network, number of wireless devices, security Level implemented, number of IT staff and IT Budget.

The study has also established the relation between security level on campus wireless network and Internet usage on campuses. The relationships are captured in section 4.4 of this study.

From the outcomes of this study, the value of this study therefore is as follows;

1. Informs the management on the level of ICT Budget that meets internet connectivity of the institution and ICT personnel required.
2. This study lays the foundation for Universities to determine the level of security to be implemented on campus networks that without compromising internet usage. The Level of security to be implemented by IT administrators on campus wireless networks that enables maximum access to internet and IT enabled services (such as e-learning platforms and libraries, to access to free e-journals and e-books available on internet by the University community. The study also guides in determining the level of security of the campus network that meets the desired level of confidentiality and privacy of the user online information such as personal information and research/e-learning materials
3. The study serves to inform University ICT team to register wireless devices in order to have visibility of user devices to track cyber security cases. 55% of the universities do not register wireless devices

4. The study also informs and give opportunity to the regulator - Communication Commission of Kenya (CCK) to develop a roadmap on identification and allocation of frequency for the deployment of new wireless technologies such as Long Term Evolution (LTE) technology to rapidly expand growth of campus wireless networks or hotspots

5.2 Conclusions consistent with and limited to the evidence presented

Although wireless technology is broadly deployed on campuses, there are challenges with ICT budget allocation for roll out of these networks and IT enabled services by University management. There are also challenges between use of ICT services on wireless network and security of the information systems. Internet usage within the University community depends on the extend of coverage of wireless networks on campuses and availability of relevant IT enabled services as well as security level implemented on wireless networks. A balance needs to be reached between ease of access and security level to be implemented. The study therefore extended knowledge by establishing practical % growth in internet usage with respect to the various dependent variables.

5.3 Recommendations for research and practice

1. Universities management should consider ICT as a strategic platform for transforming teaching, learning and improving efficiency and therefore increase the budgets for ICT for deployment of wireless campus network infrastructure to increase internet coverage on campuses. The minimum annual budget should be at least KES10M and above for startup universities.
2. Finance officers need further training in accessing the financial systems on wireless networks. This is based on the result that 87% of them disagree that access to wireless network is easy. This training should be extended to all other IS users.

3. The frequency regulatory body -Communication Commission of Kenya (CCK) to develop a roadmap on identification and allocation of frequency for the deployment of new wireless technologies such as Long Term Evolution (LTE) technology to rapidly expand growth of campus wireless networks or hotspots

This study has extended knowledge from a study conducted in 2006 by David Kotz at the Dartmouth College and Kobby Essien of University of Pennsylvania where their study focused on analyzing Campus-Wide Wireless Network with the aim of understanding usage patterns in wireless local-area networks. Further research needs to be conducted on the effect of automation of processes in Kenyan Universities on internet usage.

5.4 Limitations of the Research

The limitations of this research are as follows;

1. There is need to cover fixed campus networks which has an impact on the reliability of the wireless campus networks
2. Adoption of use of wireless networks has a social relationship with change management which was not covered under this study
3. The response time of the respondents was experienced unexpected lead times in some cases.

6.0 REFERENCES AND URLS

6.1 List of References

1. Makuma L T(2011), *A report on UN IGF Public lecture for the University Students on Broadband Internet and the New World Wide Web opportunities for student-led innovations and entrepreneurship*
2. Gakio K (2006), *Africa tertiary institutions connectivity survey (ATICS) 2006 Report*
3. Kotz and Essien (2005), *Analysis of a Campus Wide Wireless Network*
4. Bennington and Bartel (2006), *Building a high speed campus wide wireless Data Network*
5. Network Working Group (2006), *Recommendation for Wireless Network Security at the University of Michigan*
6. Flickenger et al (2006), *Wireless networking in the developing world, a practical guide to planning and building low cost telecommunication infrastructure, second edition*
7. Echezona and Ugwuanyi (2010), *African Universities Libraries and Internet Connectivity: Challenges and way forward*
8. Flickenger et al (2006), *How to Accelerate your Internet*
9. Flickenger and O'Reilly (2006), *Building Wireless Community Networks*
10. Hole K.J. , Dyrnes E. and Thorsheim P. (2005), *"Securing Wi-Fi Networks," Computer, vol. 38, no. 7*
11. Hole K.J, Netland L.H , et al (2008), *Open Wireless Networks on University Campuses*

6.2 List of URLs

1. Fred et al (2004), *Interactive Wireless Network Design Analysis and Utilities* [online] available at http://www.qsl.n9zia/wireless/page09.html
2. http://graphs.kenet.or.ke
3. CCK fact sheet , 2008 [online] available at http://www.cck.go.ke/consumers/internet_services/downloads/about_internet_servicefull.pdf
4. https://graphs.kenet.or.ke/graph_view.php?action=tree&tree_id=71
5. http://kenet.or.ke/index.php?option=com_content&view=article&id=339%3Ainoorero-university-wednesday-launched-its-wireless-local-area-network&catid=86%3Afeature-stories&Itemid=309&lang=en
6. Kenya - Internet and Broadband Market Report- Overview, Statistics and Forecasts, 2012 [online] available at http://www.budde.com.au/Research/Kenya-Internet-and-Broadband-Market-Overview-Statistics-and-Forecasts.html
7. National Centre for Technology in Education (2008) available at http://www.ncte.ie/documents/advicesheets/20WirelessNetworksNov08.pdf
8. http://www.uta.edu/oit/cs/connections/wireless/
9. White paper on Technical Planning Guide for Fixed Broadband Wireless Internet Access available online on http://www.lomasci.com/data/bwa.pdf

APPENDICES

Appendix 1-Research Questionnaire

Background:

This questionnaire is part of a research that seeks to analyse the ''Effect of Wireless Campus Networks on Internet Usage in Kenyan Universities''. What is campus wireless Networks? Wireless campus network links two or more devices using some wireless distribution method and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. The campus wireless network infrastructure is owned and managed by the university campus.

SECTION A: RESPONDENT INFORMATION

1. Campus Name _____
2. Name of respondent _____
3. Position Of Respondent

- ☐ ICT Manager
- ☐ Network Administrator
- ☐ Student
- ☐ Researcher/Lecturer
- ☐ Finance Officer
- ☐ Other

SECTION B: CAMPUS NETWORK DATA (To be filled by ICT Manager)

1. Has wireless network been implemented on campus
   - ☐ Yes
   - ☐ No
2. If yes when was it commissioned MM/YY _____
3. Number of Access Points _____
4. Max Number of simultaneous users _____
5. Estimated number of students on campus _____

6. What is the capacity of available bandwidth _____
7. Number of information systems implemented_____ list of information systems available _____
8. Security level implemented on wireless network

- ☐ Open
- ☐ Restricted
- ☐ Highly restricted

9. Reason for the choice_____
10. What is the annual ICT Budget

- ☐ Below KES 1M
- ☐ KES 1M-10M
- ☐ KES 10M-50M
- ☐ KES 50M-100M
- ☐ KES 100M-1B
- ☐ Over KES 1B

11. What was the average usage of bandwidth in the following years

2010_____
2011_____
2012_____

SECTION C: CAMPUS NETWORK DATA (To be filled by Network Administrator)

1. Do you register devices that access the wireless network
   - ☐ Yes
   - ☐ No
2. If yes what is the number of devices accessing_____
3. Do you monitor usage (graphing) of the wireless network
   - ☐ Yes
   - ☐ No
4. If yes what is the maximum bandwidth usage during peak hour_____
   Please provide graphs for one month before and after commissioning of wireless network
5. Number of users requesting for support to access wireless network

- ☐ All
- ☐ High
- ☐ Low
- ☐ None

6. What is the likelihood that support depends on the security level implemented on wireless network

- ☐ High
- ☐ Medium
- ☐ Low

7. Do you monitor usage of the information systems implemented

- ☐ Yes
- ☐ No

8. If yes, how do you rate access to information system via wireless access

Finance Management System

- ☐ High
- ☐ Medium
- ☐ Low
- ☐ None

Student Information Management Systems

- ☐ High
- ☐ Medium
- ☐ Low
- ☐ None

9. Do you monitor availability of the wireless network and information systems

- ☐ Yes
- ☐ No

10. If yes, what is the rating of availability of the following

Wireless campus network

- ☐ 100%
- ☐ Over 95%
- ☐ Below 95%

Information systems

- ☐ 100%
- ☐ Over 95%
- ☐ Below 95%

SECTION D: USAGE DATA (To be filled by Student)

Please indicate your level of agreement with the following statements by ticking the appropriate box

Key: Strongly Disagree (SD); Disagree (D); Disagree Somewhat (DS); Neutral (N); Agree somewhat (AS); Agree (A); Strongly Agree (SA)

No	Statement	SD	D	DS	N	AS	A	SA
SQ1	I use wireless network on campus							
SQ2	Wireless end user devices are easy to acquire							
SQ3	Security steps I go through to access are easy							
SQ4	The wireless network is always available							
SQ5	Student information system is always available							
SQ6	Wireless network effectively serves my needs							
SQ7	I use wireless network to access student information system							
SQ8	I use wireless network for educational purposes							
SQ9	I use wireless network to access social websites							
SQ10	Using wireless network is more effective than using fixed network							

List three sites you always visit on wireless network_____

List at least three devices you always use to access wireless network on campus

1. _____
2. _____
3. _____

SECTION E: USAGE DATA (To be filled by Finance Officer)

Please indicate your level of agreement with the following statements by ticking the appropriate box

Key: Strongly Disagree (SD); Disagree (D); Disagree Somewhat (DS); Neutral (N); Agree somewhat (AS); Agree (A); Strongly Agree (SA)

No	Statement	SD	D	DS	N	AS	A	SA
FQ1	I use wireless network on campus							
FQ2	Wireless end user devices are easy to acquire							
FQ3	Security steps I go through to access are easy							
FQ4	The wireless network is always available							
FQ5	Financial management system is always available							
FQ6	Financial management systems improves efficiency of my work							
FQ7	Wireless network serves me effectively							
FQ8	Using wireless network is more effective than using fixed network							

List three sites you always visit on wireless network_____

List at least three devices you always use to access wireless network on campus

1. _____
2. _____
3. _____

SECTION F: USAGE DATA (To be filled by Researcher/Researcher)

Please indicate your level of agreement with the following statements by ticking the appropriate box

Key: Strongly Disagree (SD); Disagree (D); Disagree Somewhat (DS); Neutral (N); Agree somewhat (AS); Agree (A); Strongly Agree (SA)

No	Statement	SD	D	DS	N	AS	A	SA
RQ1	I use wireless network on campus							
RQ2	Wireless end user devices are easy to acquire							
RQ3	Security steps I go through to access are easy							
RQ4	The wireless network is always available							
RQ5	The speeds on wireless network is adequate to meet researchers needs for high speed data transfer							
FQ6	Using wireless network is more effective than using fixed network							

List three sites you always visit on wireless network_____

List at least three devices you always use to access wireless network on campus

1. _____
2. _____
3. _____

CONTACT:

ERIC SIFUNA SIUNDUH

UNIVERSITY OF NAIROBI

C/O SCHOOL OF COMPUTING AND INFORMATICS

P.O BOX 30197-00100

NAIROBI

Cell phone Number: 0735-763796

Email: sifunaes@yahoo.com or sifunaes@gmail.com

Your participation in this study is highly appreciated. Thank you.