Article

The Effectiveness of Wi-Fi-Network Technology on Campuses and Residences for an Improved Learning Experience and Engagement

Kenneth Nwanua Ohei
https://orcid.org/0000-0002-5923-2012
University of Johannesburg, South Africa
kohei@uj.ac.za
kennethohei@gmail.com

Roelien Brink
https://orcid.org/0000-0002-0261-6701
University of Johannesburg, South Africa
rbrink@uj.ac.za

Abstract

The information and communication technology revolution is broadly recognised for its fundamental role in the effective operation of higher education institutions. There is a need to understand the way in which wireless local area networks at universities are viewed by registered users, the people that develop, implement and maintain these networks, and those planning on adopting these networks. The study's objective is to unravel the usefulness of these networks in a higher education environment to promote effective learning engagements at campuses of the University of Johannesburg in South Africa. Universities provide Wi-Fi network initiatives on campuses to create an effective learning environment, and wireless local area network connections at universities mean that Wi-Fi-enabled devices can be leveraged for educational purposes. The provision of Wi-Fi-enabled computers, mobile devices and electronic gadgets has revolutionised the realm and methods of communication, which is channelled towards improving and enhancing internet coverage on campuses and at student residences. This study explores the effectiveness of Wi-Fi networks and hotspots on campuses and at student residences to improve students' learning engagement. The study used mixed-research methods, including a document analysis to gather information from information and communication systems and a survey to gather responses from the respondents. The findings suggest that Wi-Fi availability at universities is perceived as useful and effective since students benefit from a range of improved learning experiences, easy access to educational content, enhanced performance, and quality and education delivery.

Keywords: access point, affordability, hotspot, Wi-Fi network, WLANs effectiveness

UNISA university of south africa PRESS

Mousaion
https://upjournals.co.za/index.php/LIS
Volume 39 | Number 1 | 2021 | #7842 | 26 pages

https://doi.org/10.25159/2663-659X/7842
ISSN 2663-65X (Online), ISSN 0027-2639 (Print)

Introduction

The affordability, availability and accessibility of Wi-Fi networks have radically strengthened the use of these networks by university educators, staff and students to communicate and conduct their respective business operations (Ding and Dan 2012; Sevtsuk 2009). The availability of Wi-Fi networks on campuses results in greater flexibility for the university community as it offers various features, including the freedom to use the network at any designated location. The study's objective was to unravel the usefulness of wireless local area networks (WLANs) in a higher education environment to promote effective learning engagements at campuses of the University of Johannesburg (UJ) in South Africa.

Wi-Fi networks are available at campuses and students' residential areas to offer the students access in their preferred study space. This has resulted in WLANs being regarded as a superior tactic to connect users. However, some reports argue that the accessibility and availability of WLAN communication can attract criticism in terms of information security (García Pineda et al. 2011; Ji 2017). Nevertheless, an effectively managed and well-executed wireless network configuration in the university environment can lead to increased security, and security concerns can be properly dealt with by the information and communication system (ICS) departments (Crow et al. 1997; Ding and Dan 2012; Jacob and Issac 2008).

Several steps should thus be followed to establish the affordability and use of Wi-Fi at campuses and student residences. The extent to which Wi-Fi networks had an impact on the teaching and learning environment and the way in which they have stimulated students' learning engagement and outcomes should also be considered. Therefore, this study was guided by the research questions: What are the benefits of using Wi-Fi networks based on users' perceptions? What is required for a user to gain access to the university's Wi-Fi network? In what way is connectivity implemented? The following section offers a brief definition of some concepts used in the study to provide clarification and the underpinning foundation upon which the study was based (Bradley 2017a, 2017b).

Definition of Terms

Hotspots: Hotspots can be used through Wi-Fi technology. In this study's context, Wi-Fi hotspots are areas in which internet access is covered through a WLAN that is enabled through a router that is linked to an internet connection with a service provider.

Open, restricted, or highly restricted wireless campus networks: Campus networks are regarded as open when the wired equivalent privacy (WEP) and Wi-Fi protected access (WPA) security standard protocols do not exist. In this way, an open network gives users unrestricted access to the internet and library catalogues, among other things. Restricted Wi-Fi networks on campus offer restricted access to specific services. The privileges to use the university library, computer labs, and information systems require

user login credentials. Finally, Wi-Fi networks on campus are highly restricted, and all users go through the university's ICS department for configurations and to enable their wireless devices to access the campus network. This is for the purpose of tracking and authenticating users' activities on the university network.

WEP/WPA: WEP or WPA2 is referred to as wireless security that is set to prevent unauthorised privileges, access, or malicious harm to computers using wireless networks. WPA2 entails stronger data protection and network access control, although the most frequent type of wireless security used is WEP WPA.

Wi-Fi: This is a commonly used term to denote wireless fidelity. Wi-Fi is a popular wireless network technology that utilises radio waves to provide wireless high-speed internet and network connections. Wi-Fi is essentially a trademarked expression that means Institute of Electrical and Electronics Engineering (IEEE) 802.11.

WLAN: This is a network that connects two or more devices using a wireless sharing method (normally spread spectrum or orthogonal frequency division multiplexing (OFDM) radio), and generally delivers a connection linked to an access point to the broader internet. In this way, users gain accessibility, the mobility to navigate within a local coverage area, and remain connected to the network (Khorov et al. 2018; Kowsar and Biswas 2017; Sevtsuk 2009).

Research Problem

WLANs have become widely accepted and have improved the quality of education provided to students at various universities. Wi-Fi network technology, such as IEEE 802.11b/802.11a/802.11g, 802.11n and 802.11ac are typically used by educational institutions, yet there is limited knowledge about its usefulness, benefits, and the power of the networks that are predominantly deployed at the universities (Sevtsuk 2009). There has also been limited research on the reliability, transparency, bandwidths, hotspots and security configurations that are used to report on the use, affordability and convenience of Wi-Fi in achieving academic goals. Moreover, it has been determined that UJ's Wi-Fi distribution on campus is unstable owing to the lack of appropriate network delivery. This study argues that ICSs at UJ will benefit from a reduction in physical cabling requirements for internet delivery and service.

Literature Review

Effectiveness of Wi-Fi Networks

Wi-Fi networks at universities have a tremendous impact on the pedagogical environment and provide a quality educational standard and effective learning experience for students and staff (Sevtsuk 2009). WLANs at universities are a strategic effort to improve the learning process, to provide an environment that is conducive to learning, easy access to educational content, and quality educational performance, and to ensure good educational content delivery.

The incorporation of technology, namely IEEE 802.11b/802.11a/802.11g, 802.11n and 802.11ac, and many other network technologies offering services to higher educational institutions (HEIs), has become a turning point in supporting educational goals, offering students a suitable platform to fully engage in their academic activities (Fong and Wong 2017; Han 2008; Hassan et al. 2018; Yaqoob et al. 2017). This generation of students, termed the "digital" generation, has maximised the use of technology and has progressively developed an interest in using digital technologies (Lee, Leow, and Kong 2020). Similarly, educators have increasingly embraced the use of Wi-Fi-enabled computers and electronic devices for educational purposes.

Wi-Fi networks allow cabling-related issues to be eliminated (Valkanis et al. 2019). Moreover, this study explored security concerns related to user authorisation, authentication and credentials, and the information and communication technology (ICT) infrastructure and cost implications of bandwidth. Despite these issues, the use of Wi-Fi networks means that HEIs offer an effective learning experience for students, and university staff have an effective working engagement that is fundamental to any thriving institution. In this way, the HEI meets the required needs and demands of the higher education sector, allowing it to have a competitive advantage over other tertiary institution rivals.

Wireless Network Configurations

As mentioned, little is known about the way in which wireless networks are configured, especially in instances where Wi-Fi hotspots are established, allowing users to gain access to such networks. This section offers a brief description of the IEEE standards and protocols, and provides the rationale that justifies the effect, usefulness, benefit and power of these wireless networks that have predominantly been deployed at universities. Therefore, an in-depth conceptualisation of the way in which the IEEE 802.11 is deployed, in line with the architectural procedures and technologies on campuses and student residences, is envisaged.

Several authors (Crow et al. 1997; Dixit and Pandharipande 2007; Khorov et al. 2018; Wang, Li, and Li 2017) report that the IEEE 802.11 standard is considered network access that is responsible for providing connections within wireless locations and in wired networking set-ups. Setting up the IEEE 802.11 protocol and other related technologies means enabling the mobile user. In this case, the mobile user is a location management device that is enabled to allow a flow of connections to travel from a distance (such as libraries, lecture rooms, and the cafeteria) while still being able to grant access to networked data (Wang, Li, and Li 2017).

According to Bradley (2017a), the 802.11 coherent architecture includes several key elements or mechanisms, namely, the station (STA), access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS). Most of the elements of the 802.11 coherent architecture, such as the STAs and wireless APs, are significant in mapping out the direction of the hardware

devices. Notably, the wireless STAs include an adapter card or an embedded chip to enable a wireless connection, allowing the wireless AP to function as a link between the STAs and the present network support to allow network access. Figure 1 shows the 802.11 architectural procedures (Alexandra 2015; Murad and Eltawil 2020).

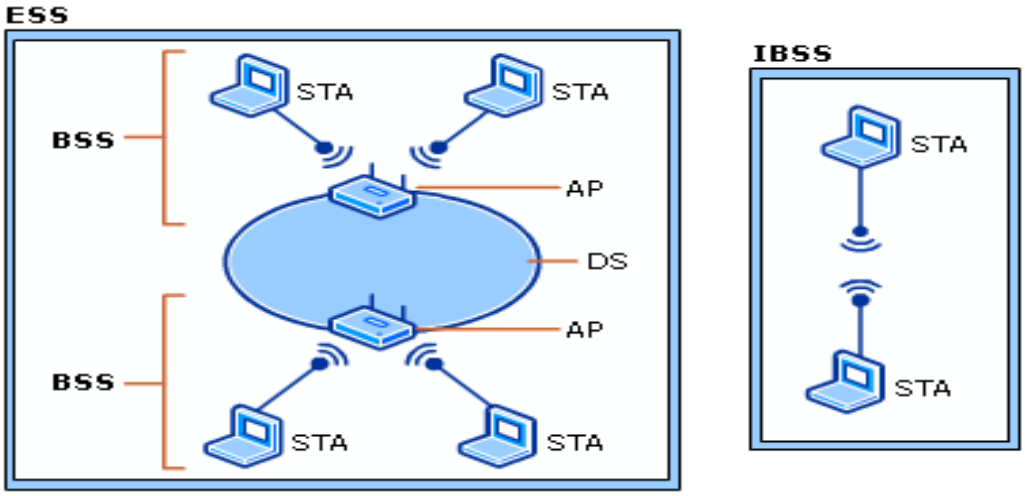

Figure 1: The function modes

Figure 1 demonstrates the way in which the APs of various BSSs are interrelated by the DS. This promotes user mobility since the STAs can change directions from one BSS to another BSS. APs may be connected with or without wires. Hence, the DS is the coherent element deployed to connect BSSs for the purpose of permitting the roaming of STAs between BSSs. The 802.11-related protocols and technologies are briefly discussed in the following section (Akhtar and Ergen 2018; Microsoft 2003).

Protocols

The IEEE 802.11 wireless standard outlines the specification for the physical layer and the media access control (MAC) layer. The IEEE 802.11 standard protocol explains port-based network access control that is deployed to authenticate network access for Ethernet networks. Furthermore, the extensible authentication protocol then serves as a point-to-point protocol (PPP)-based verification platform used for point-to-point local area network (LAN) segments. In conjunction, the WEP is responsible for data integrity and privacy, which involve cryptography, encoding and decoding the data sent between wireless electronic gadgets, smart devices and nodes.

The WPA is purported to serve as an enhanced standard over the WEP standard, providing a more sophisticated approach to data encryption, verification and network authentication (Cisco 2011). In terms of wireless network bandwidth and the communication schemes for wireless transmission, the most commonly deployed are the Frequency Hopping Spread Spectrum (FHSS) which is associated with 802.11, the

Direct Sequence Spread Spectrum (DSSS) which presents 802.11b, and the OFDM transmission schemes which are interlinked with 802.11a and 802.11b/g standards that exist at the physical sub-layer. The bit rate for the original IEEE 802.11b/g standard is 2 Mbps by means of the FHSS transmission scheme and the S-Band Industrial, Scientific, and Medical (ISM) frequency band, which functions in the frequency proximity of 2.4 to 2.5 GHz (Jacob and Issac 2008).

In addition, 802.11b is the standardisation of the physical layer to support higher bit rates. It provides two added speeds (5.5 Mbps and 11 Mbps) using the S-Band ISM. The DSSS transmission scheme is used to provide these higher bit rates. Furthermore, 802.11b utilises the same frequency band as microwave ovens, cordless phones, wireless video cameras, and Bluetooth devices. The IEEE 802.11a functions at a bit rate as high as 54 Mbps and uses the C-Band ISM, which functions in the frequency dimension of 5.725 to 5.875 GHz.

Finally, IEEE 802.11g functions at a bit degree as high as 54 Mbps but uses the S-Band ISM and OFDM 802.11g. Therefore, 802.11g offers a movement path for 802.11b networks to a frequency-compatible standard technology with a higher bit rate.

Wireless networks are typically based on the IEEE 802.11b/g standards, which have universally been deployed at several universities and organisations (García Pineda et al. 2011). Jacob and Issac (2008) claim that wireless affordability in an institution relates to a direct link between cost-effectiveness and solutions to make the most of all educational networks' benefits. This will result in improved accessibility of Wi-Fi-enabled laptops, electronic devices and gadgets, smartphones and others that connect to the Wi-Fi hotspots on campus and in residential environments. In this case, the AP to networks is not restricted to one AP, such as the computer lab or the library, but a range of hotspots. The associated benefits of using WLANs at universities include students' convenience and comfort. Subsequently, the university Wi-Fi networks allow numerous electronic devices and gadgets, laptops and smartphones access at reduced infrastructure cost. It is also compatible with numerous devices owing to the dynamic nature of the network and connectivity. Figure 2 demonstrates the way in which the physical layer and MAC layer that communicates up to the logical link control (LLC) layer is specified (Akhtar and Ergen 2018; Bradley 2017a, 2017b; Microsoft 2003).

The components listed in the 802.11 architectural procedures are categorised into the MAC sub-layer of the data-link layer or the physical layer. In the sections that follow, the definition of wireless technologies, Wi-Fi limitations, bandwidth and WLAN standards are discussed.

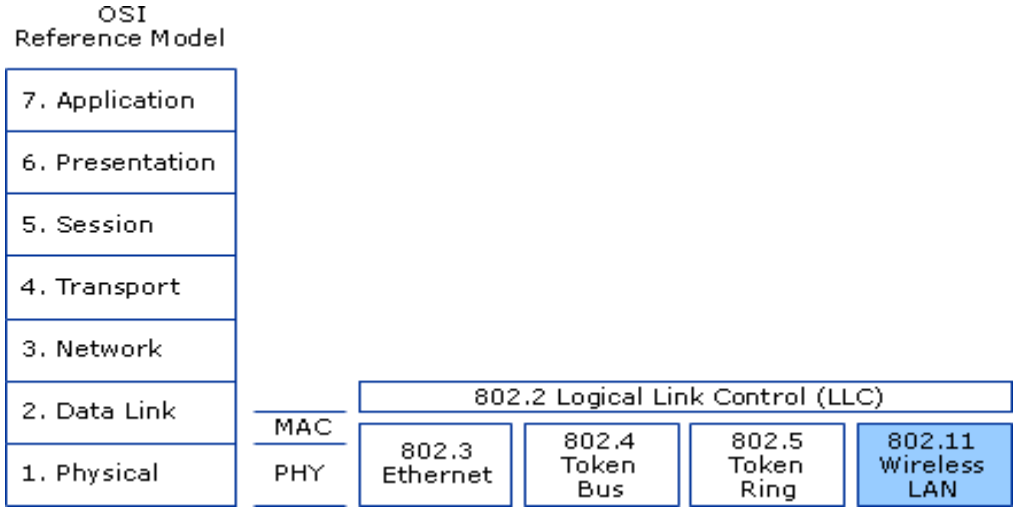

Figure 2: 802.11 and the open systems interconnection (OSI) model

Wireless technologies

WLANs use infrared or radio waves to provide networks for wireless devices and allow users to transmit data to others in the coverage area without the limitation of wire and cable (McCormick 2017). WLANs have different wireless network protocols, such as IEEE802.11, Bluetooth, Homer and HiperLAN. Many wireless devices support WLANs, including mobile phones, gaming consoles, some cameras, tablets, and GPSs. WLANs may also simultaneously support over a hundred devices (Han 2008; Mohd Ali, Sibley, and Glover 2017).

WLANs have unique advantages. Firstly, WLANs are more flexible and mobile than wired components and are not limited by cables. Users may have access to or receive information from any network coverage point in real time. Secondly, WLANs have good scalability; users can add more APs to effectively expand the network and meet the needs of specific applications and installations. Thirdly, WLANs no longer require many wires and cables, thereby reducing the workload of network cabling. Finally, it is easier to set up a WLAN than a wired one, as it is not easily affected by the natural environment or disasters.

Limitations

There are also limitations to WLANs. Firstly, WLANs are based on radio frequency for data transmission. Walls or buildings will block the transmission of radio frequencies, reduce the signal, and then influence the WLANs' performance. Secondly, some devices have the same frequency as the 802.11 series and may cause radio signal interference. Thirdly, WLANs are less secure than wired LANs. When LANs travel through the air, they could be intercepted, and some unauthorised devices may thus tap into users' WLAN. Fourthly, the coverage areas of WLAN are limited; WLANs have a

certain range of coverage; increasing the coverage area requires an increase in wireless hotspots, therefore increasing the cost. Moreover, if wireless devices hack into a user's network, their bandwidth will be stolen (Han 2008; Salous et al. 2016; Siunduh 2013).

Bandwidth

There are three main transmission media for WLANs (Microsoft 2003; Wang, Li, and Li 2017). The first is a microwave, and the range of frequencies is 1 GHz to 40 GHz. A microwave is not a true sense of LAN technology, but it is used to interconnect the LANs of buildings. It is suitable for point-to-point transmission and satellite communications. The second medium is radio, and the range of frequencies is 3 KHz to 300 GHz (McCormick 2017). This transmission medium is currently widely used because the radio wave offers wide coverage and is suitable for all applications. The difference between broadcast radio and microwave is that the radio does not require antennas; the radio former is omnidirectional, and the microwave former is directional. The third transmission medium is infrared, which uses a transmitter and receiver to modulate non-coherent infrared light. The difference between infrared and microwave transmission is that infrared will not penetrate walls. Yet, there is no frequency allocation problem for infrared media transmission because it does not require a licence (Salous et al. 2016).

WLAN standards

WLAN users have many options when looking for network gear. Many products conform to the 802.11 series wireless standards, also known as Wi-Fi technologies (Han 2008). Other wireless technologies include Bluetooth, HomeRF and HiperLAN, designed for specific networking applications. According to Microsoft (2003), the IEEE 802 standards define two separate layers for the data-link layer of the OSI model. The first is the LLC layer, and the second is the MAC layer. As shown in Figure 2, the IEEE 802.11 wireless standard defines the specification of the physical layer and the MAC layer that communicate up to the LLC layer. The components of the 802.11 architecture fall under the physical layer or MAC layer.

Wi-Fi is the popular name for the wireless Ethernet 802.11b standard for WLANs (Lehr and McKnight 2003). Wireline LANs emerged in the early 1980s as a way to connect PCs, terminals, and other distributed computing devices to share resources and peripherals such as printers, access servers, or shared storage devices. The most popular LAN technology was the Ethernet (Sadeghi, Barraca, and Aguiar 2017). Over the years, the IEEE approved the succession of Ethernet standards to support higher capacity LANs over a diverse array of media. The 802.11x family of Ethernet standards are used for wireless LANs, where Wi-Fi LANs operate using an unlicensed spectrum in the 2.4 GHz band.17. The current generation of WLANs support up to 11 Mbps data rates within 100 metres of the base station. WLANs are deployed in a distributed way to offer last-hundred-metre connectivity to a wireline backbone corporate or campus network (Ji 2017; Mykhalevskiy and Horodetska 2019).

Typically, WLANs are implemented as part of a private network, whereas the base station equipment is owned and operated by the end-user community as part of the corporate enterprise, campus, or government network. In most cases, the use of the network is free to end-users; that is, it is subsidised by the community as a cost of doing business, such as corporate employee telephones. Although each base station can only support connections over a 100-metre range, it is possible to provide continuous coverage over a wider area by using numerous base stations. Several corporate businesses and university campuses have deployed such contiguous WLANs (Rudenkova 2020; Siunduh 2013). However, WLAN technology was not designed to support high-speed hand-offs associated with users moving between base station coverage areas (i.e., the problem solved by mobile systems).

In the last two years, a number of service providers have started offering Wi-Fi services for a fee in selected local areas such as hotels, airport lounges, and coffee shops. In addition, Gast (2005) states that there is a growing movement of so-called "FreeNets", where individuals or organisations are providing open access to subsidised Wi-Fi networks, in contrast to WLANs that are principally focused on supporting data communications. However, with the growing interest in supporting real-time services such as voice and video over internet protocol (IP) networks, it is possible to support voice telephony services over WLANs.

Research Methodology

Philosophical Grounding

A research methodology is a systematic approach that is used to evaluate data collected through a specified data collection process. The research method is important to identify, select, process, and analyse the information derived from the study. Research activity is typically directed by specific fundamental and philosophical assumptions about what constitutes proper research, and which research methods are applicable for the development of knowledge in a given study (Creswell 2015). For this reason, this study was based on the epistemological assumption, and focused on obtaining findings that investigate the usefulness, impact and benefits of Wi-Fi technologies on campuses. Thus, the study included students, and academic, non-academic and casual staff as active users of the internet service being offered at UJ campuses.

Research Approach

This study followed a quantitative research method, and a document analysis was deemed suitable as it promoted a strategy of inquiry to uncover new knowledge on a topic about which little is known. Quantitative research is useful in achieving research objectives by identifying a problem, questions, and gaining a better understanding of a phenomenon. In line with this statement and considering the nature of the problem that the study attempted to solve, a questionnaire was used as data collection technique, supported by the document analysis. The study also complied with ethical academic research standards; to that end, relevant ethical permission was obtained, and voluntary

participation, anonymity, and confidentiality were ensured throughout the research process.

Stratified random sampling was employed, using shared attributes as the strata for diploma, undergraduate and postgraduate students. The study targeted students, and academic, non-academic and casual staff members across UJ's four campuses, namely, the Bunting Campus, the APK Kingsway Campus, the Soweto Campus, and the Doornfontein Campus. UJ was deemed a suitable study area because of its location, mode of education delivery, and the provision of ICT services and infrastructure. After administering the questionnaire, a response rate of 82.9 per cent ($n = 178$) was recoverable and recorded. The questionnaire took between 10 and 15 minutes to complete.

Results and Discussion

This section analyses the results and presents a discussion of responses in relation to the research objectives, which were to explore the effectiveness, impact and usefulness of WLANs in a higher education environment to promote and support effective learning engagements, and to enhance quality education delivery and students' academic success. The aim was also to establish the potential benefits of using Wi-Fi technology at university campuses and student residences.

Demographics

The demographic discussion begins with a presentation of the variables. These results were organised in frequency tables and figures. The respondents' background information, such as highest education level, occupational status, and campus setting, was cross-tabulated in Table 1. These campuses were selected based on their location, mode of education delivery and infrastructure.

In Table 1, a cross-tabulation analysis was performed on the respondents' highest education level, occupational status, and campuses with major access to the university's Wi-Fi network. The results show that all students across a range of qualifications, and academic, non-academic and casual staff have Wi-Fi access across several delivery sites. The majority of the respondents who accessed the university Wi-Fi network were students, based on their learning engagements and curriculum activities that needed to be performed. Conversely, academic, non-academic and casual staff use the Wi-Fi network for administrative and related purposes.

Table 1: Cross-tabulation of the highest education level, occupation status, and campus where respondents often access Wi-Fi networks

Highest education level (only indicate the highest)			**APK %**	**APB %**	**DFC %**	**SWC %**	**TOTAL %**
National diploma	Occupation status	Student	95.8	69.6	77.8	40.0	78.7
		Academic staff	4.2	13.0		20.0	8.2
		Non-academic staff		13.0	22.2	40.0	11.5
		Casual staff		4.3			1.6
	Total		100.0	100.0	100.0	100.0	100.0
Bachelors' degree	Occupation status	Student	26.3	72.7	27.3	69.2	46.3
		Academic staff	47.4	9.1	27.3	15.4	27.8
		Non-academic staff	26.3	18.2	36.4	15.4	24.1
		Casual staff			9.1		1.9
	Total		100.0	100.0	100.0	100.0	100.0
Postgraduate diploma or Honours degree	Occupation status	Student	37.5	77.8	58.3	88.9	65.8
		Academic staff	25.0	11.1	33.3		18.4
		Non-academic staff	37.5	11.1	8.3	11.1	15.8
	Total		100.0	100.0	100.0	100.0	100.0
Master's degree	Occupation status	Student		60.0		66.7	45.0
		Academic staff	100.0	20.0	75.0	22.2	40.0
		Non-academic staff		20.0	25.0	11.1	15.0
	Total		100.0	100.0	100.0	100.0	100.0
PhD	Occupation status	Student			100.0	100.0	60.0
		Non-academic staff		100.0			40.0
	Total			100.0	100.0	100.0	100.0
Total	Occupation status	Student	58.5	68.0	50.0	70.3	61.8
		Academic staff	26.4	12.0	26.3	13.5	19.7
		Non-academic staff	15.1	18.0	21.1	16.2	17.4
		Casual staff		2.0	2.6		1.1
	Total		100.0	100.0	100.0	100.0	100.0

APK = Auckland Park Campus; APB = Auckland Park Bunting Campus;
DFC = Doornfontein Campus; SWC = Soweto Campus

Authentication, Wi-Fi Access and Usage

A Wi-Fi network is deemed open when the WEP and WPA security protocols are not used. An open network gives users unrestricted access to the internet, library catalogues, and web pages with course information. The only limitation to accessing this type of network is the geographical distance from the APs. Cisco (2011), and Scarfone and Dicoi (2007) state that open wireless networks increase usability simply because students and employees do not need to remember passwords to authenticate their devices. It also allows short-term guests easy internet access without the need for new user accounts and provides the public with effortless access to online catalogues maintained by university libraries.

In the context of this study, this is not the case; the university uses WEP and WPA security protocols (RF Wireless World n.d.). Hence, the wireless campus networks offer restricted access to a particular service, and access to university information systems

requires user login credentials. It has been advised that sensitive personal information should not be available on open wireless networks (Sevtsuk 2009). To that end, any wireless network that is providing sensitive information will require the use of a strong password to authenticate users who want to access such sensitive information. 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 purposes. The advantage of this method is that it ensures that users can get adequate network access quickly and easily. It also uses familiar mechanisms and generates minimal user support requirements (Abdelkarim 2006; Siunduh 2013).

As reflected in Table 2, the respondents were asked to indicate what is required for students, academic staff, non-academic staff, and guests to gain access to the campus Wi-Fi networks. Of the $n = 178$ respondents who took part in the study, 68 (38.2%) stated that in order for a student to access the Wi-Fi network, they require a user ID and password, and 60 (33.7%) suggested that for an employee to gain access, they are required to use their user ID and password. When it comes to guest users, 50 (28.1%) respondents suggested that a UJ guest user will require a user ID and password.

Table 2: Authentication mechanism to gain access to Wi-Fi networks on campuses and residential areas

Itemised	**Frequency**	**Percentage**
UJ-registered student with user ID and password	68	38.2
UJ employees/staff with user ID and password	60	33.7
UJ-allowed guest with user ID and password	50	28.1
Total	$N = 178$	100.0

Table 2 reflects the basic and general principles of an authentication mechanism that either allows a user to access the campus Wi-Fi network or denies a user to access the campus Wi-Fi network. In this case, all users go through the ICS department to attain configurations that enable their devices to connect wirelessly to the campus network. When users are authenticated to use the wireless university network, the ICS department can track their activities on campus and in residential areas. Analyses from many network sessions and activities can be combined to build user profiles. This allows the university to prevent security breaches on the network that can lead to negative publicity.

Therefore, mandatory authentication of all users is introduced to prevent successful cyberattacks and to deflect criticism away from the ICS department. Furthermore, it is fundamental to note that the majority of the respondents indicated that they had basic access to the university Wi-Fi network both on campus and in student resident areas. They also reported that they were quite familiar and aware of the location and areas on

campus in which Wi-Fi hotspots were situated. Figure 3 demonstrates the way in which the students, academic staff, non-academic staff, and guests access the university Wi-Fi network across all campuses.

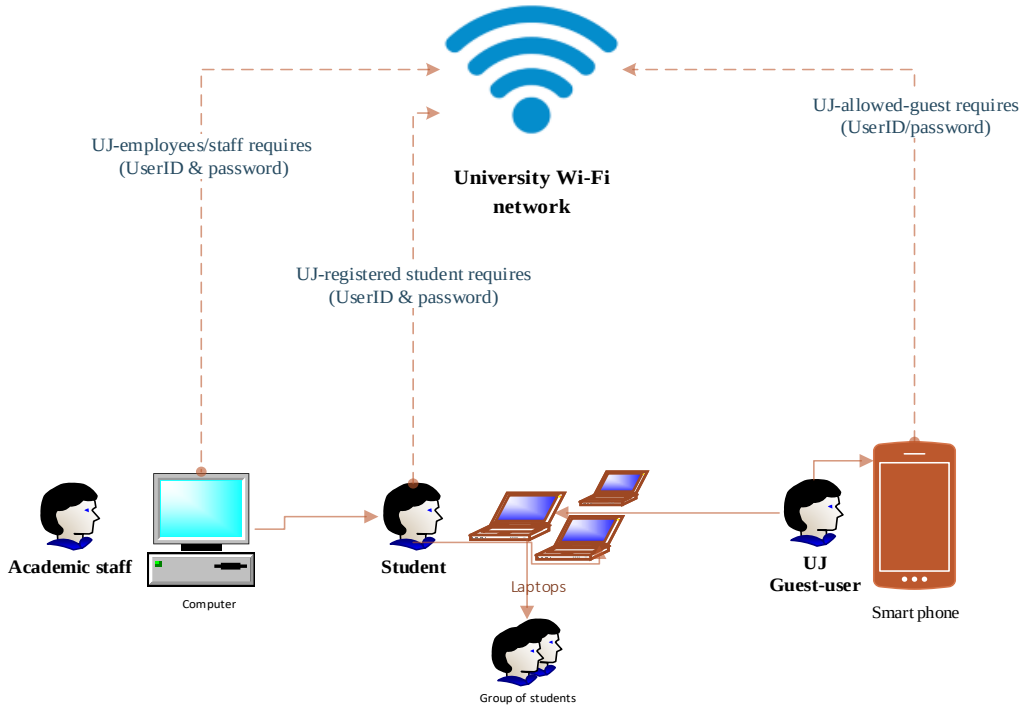

Figure 3: User authentication and requirements

The affordability of WLANs is critical for HEIs to provide internet services to the university community; this allows the teaching and learning environment to work efficiently (Ji 2017; Siunduh 2013). Wi-Fi hotspots and APs are useful in providing quality service and promoting students' learning engagement at various campus locations. The usefulness and advantage of hotspot coverage are that students can choose to navigate from one point on campus to another, using their technological devices and smartphones while simultaneously transmitting data (Table 3). The library has become one of the key APs as a centre for research, teaching, learning and socialising. Drozdenko et al. (2017) and Cisco (2008) sustained that APs provide connectivity or serve as a link between wired networks and Wi-Fi-capable devices such as mobile phones, laptops, computers, and personal digital assistants. APs are generally situated in large buildings on university campuses, including libraries, lecture halls, auditoriums, and student cafeterias. Several APs are employed to provide desirable access through wider coverage WLANs.

Table 3: Cross-tabulation of areas or locations with strong Wi-Fi presence on campus, and the devices used to access the university Wi-Fi network

Itemised		**Laptop %**	**Smart phone %**	**Desktop %**	**Notepad/ iPad/tablet %**	**Other %**	**Total %**
When using the UJ Wi-Fi network, in which areas or locations do you experience a stronger Wi-Fi presence than any other area?	Library	10.7	11.2	3.9	3.4		29.2
	Lecture hall	2.8	5.1	2.8	1.7		12.4
	Cafeteria	8.4	5.1	6.2	3.4	1.1	24.2
	University building	1.1	3.9	2.8	2.2		10.1
	Parking area	3.4	2.8	3.9		0.6	10.7
	Bus terminal	3.4	1.7	2.2	1.1		8.4
	24-hour study area	1.7	3.4				5.1
Total		31.5	33.1	21.9	11.8	1.7	100.0

Ji (2017) and Drozdenko et al. (2017) found that the Wi-Fi networks on campuses have several benefits. These benefits relate to the flexibility of Wi-Fi networks compared to wired networks, since they are not limited by cables. The $n = 178$ respondents confirmed there are several places or locations in which students, academic staff, non-academic staff, and guests access the campus Wi-Fi network. This platform allowed the users to access or receive information at any network coverage point in real time.

The campus Wi-Fi network also has an element of good scalability. Users can add one or more APs to effectively expand the network and meet the needs of specific applications and installations. It was reflected in Table 3 that students, academic, non-academic and casual staff use various gadgets or devices to access the university Wi-Fi network across all campuses and in several locations. The results also indicated areas on campuses with strong Wi-Fi presence or signals, deemed to be hotspots. Of the respondents, 29.2 per cent reported the library to have the strongest Wi-Fi presence. In support of these findings, the document analysis report from the university's ICS department (2012) stated:

> In order to be able to achieve excellence, access to resources must be provided equally to all 4 campuses. To address a network connectivity problem that had been prevalent at the Soweto Campus for a long time due to on an unreliable connection going via Baragwanath hospital, a bypass was commissioned which has returned stability of the Soweto Campus connection to 100%.
>
> In 2012, the rollout of Wi-Fi covering all four (4) libraries, 26% of all lecture venues, communal areas in all student residences and selected open areas in all campuses. Wi-Fi rollout has enabled UJ's ubiquitous connectivity strategy and established a foundation for the implementation of e-Learning services. The availability of Wi-Fi connectivity

also implies less congestion at the computer labs as students are now able to connect their Wi-Fi enabled devices from the many hotspot areas across UJ.

The following section reflects how often students and staff use the university's Wi-Fi network across all spheres of the campuses and student residences.

Figure 4 demonstrates the statistics on the users of the network and how frequently they use it. The results show that approximately 81 (45.5%) respondents frequently use the Wi-Fi network several times daily, 26 (14.61%) respondents indicated they use the Wi-Fi network infrequently each day, and 3 (1.69%) respondents often went a whole day without accessing the Wi-Fi network either at campus or at their residence. The document analysis provided by the university ICS department supports these findings, which demonstrate a series of Wi-Fi ratio trends.

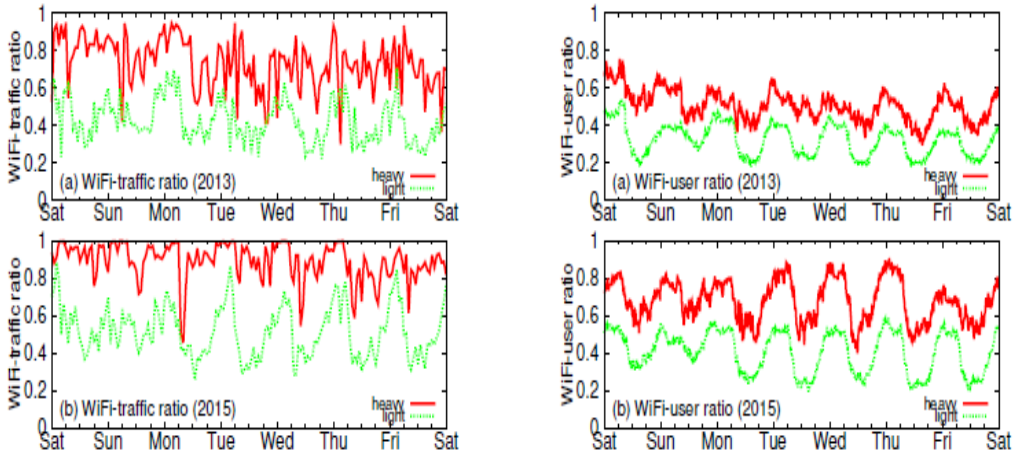

Figure 4: Wi-Fi ratio

The document analysis report revealed users' traffic patterns on daily activity. The essence of this analysis is to demonstrate the impact Wi-Fi networks have on campuses and in residential areas based on light users and heavy users. The report indicates that daily Wi-Fi traffic increases every year across all campuses, and there is a disparity in how often users use the university's Wi-Fi networks. The illustrations in Figure 4 suggest the daily traffic activities from midnight per user per day.

In addition, the report also reflects that users currently download more information through Wi-Fi networks compared to preceding years. Therefore, light users initially overlooked the significance of Wi-Fi, but as students progressed in their studies and their behavioural and usage patterns changed, reflecting increased online activities. This change in their behaviour and usage enabled ICS to monitor their Wi-Fi traffic ratio and Wi-Fi user ratio. The Wi-Fi traffic ratio describes users' Wi-Fi download activities against their total download activities at hourly intervals. This indicates that most online

activity entails downloads through the university's Wi-Fi network. Conversely, the Wi-Fi-user ratio describes the number of users linked to Wi-Fi networks in an hourly interval. Thus, a ratio that is nearly 1.0 implies that, at a specific time, most users are using the university's Wi-Fi network.

The report further suggests Wi-Fi traffic upsurges, indicating an increase in the use of Wi-Fi networks. Moreover, the report illustrates that the Wi-Fi traffic ratio differs based on daytime trends, and the Wi-Fi signal has been found to be much stronger between 23:00 and 02:00 and weaker on weekday afternoons. The number of users has been found to peak between 21:00 and 02:00, whereas 10:00 to 18:00 reflects off-peak times. The report confirms that Wi-Fi networks are increasingly being overloaded, since the Wi-Fi-traffic ratio has been growing from 0.58 in 2013 to 0.71 in 2015. It was also determined that the Wi-Fi-user ratio increased from 32 per cent in 2013 to 48 per cent in 2015. Thus, light users ultimately realised the benefits of using the university's Wi-Fi network.

Respondents' Perceptions of the University's Wi-Fi Network

The respondents recognised that the university's Wi-Fi network is reliable, accessible and supportive; they claimed that it encourages uninterrupted learning (Figure 5). Furthermore, they also indicated that Wi-Fi offers them affordable engagement in their respective studies. According to Raman and Chebrolu (2007), a Wi-Fi network is not only cost-effective in its implementation and tools, but also in its operation in a licence-free continuum. Some respondents reported that the university's Wi-Fi network is effective and free since no charges are imposed on students for accessing the network.

The results in Table 4 reflect that the respondents had numerous reasons for using Wi-Fi on campus. Of the $n = 178$ respondents, 39 (21.9%) used the Wi-Fi network for browsing and surfing online contents or information, and 25 (14%) used the network for research purposes, followed by those respondents who used the Wi-Fi network for shopping (13.5%), entertainment (12.9%), social networking (11.2%), downloads and gaming (8.4%), online transactions (11.2%) and e-learning (6.7%). Although the respondents' use of the Wi-Fi network differed, the results suggest that Wi-Fi networks across all campuses are being used to browse and surf for online content and information. It also includes shopping, researching, entertainment, networking, gaming, discussions, e-learning, downloading, checking emails and performing academic tasks.

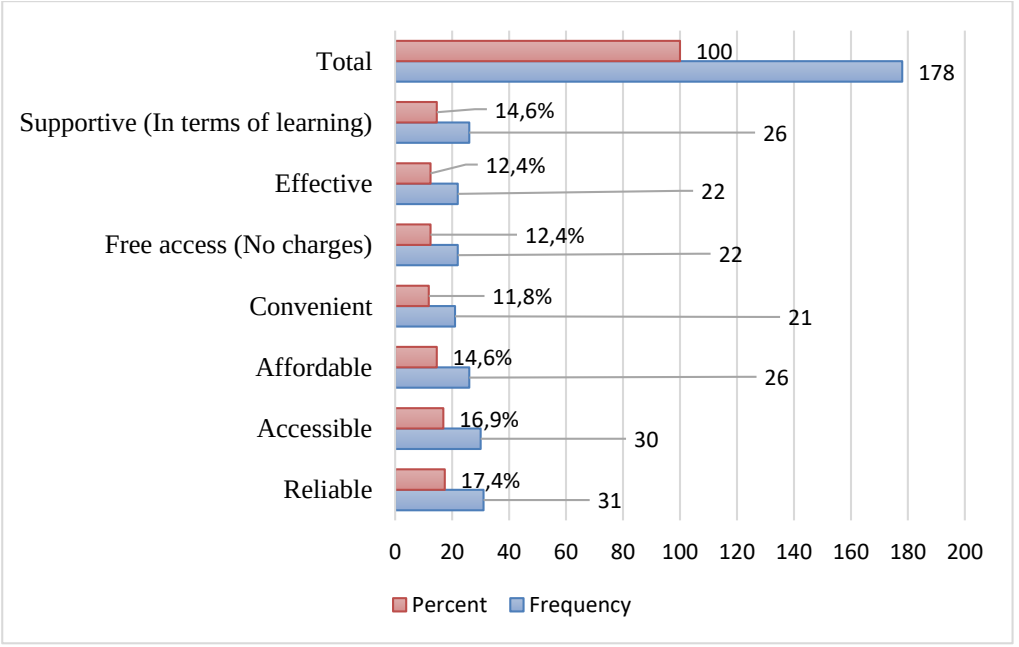

Figure 5: Respondents' perceptions

Table 4: Wi-Fi use and purpose

Itemised	Frequency	Percentage	Cumulative percentage
Browsing (i.e., online contents or information)	39	21.	21.9
Research	25	14%	36
Shopping	24	13.5	49.4
Entertainment	23	12.9	62.4
Social networking (e.g., Facebook, WhatsApp, Instagram)	20	11.2	73.6
Downloads and gaming	15	8.4	82
Online transactions (purchase)	20	11.2	93.3
E-learning	12	6.7	100.0
Total	*N* = 178	100.0	

Several benefits may be associated with the use of a university Wi-Fi network, and WLANs are being incorporated to its maximum capacity by universities worldwide. Benefits include easier access for users, and ICS departments can benefit from decreased physical cabling requirements. Table 5 illustrates that Wi-Fi networks on

university campuses make today's campuses more flexible by offering new connectivity features and freedom of movement, and by expanding areas of support. Table 5 further reveals that the respondents felt they benefit significantly since WLANs enable collaborative and interactive learning. Without the use of an on-campus Wi-Fi network, it would have been impossible for students to collaboratively learn and interact with fellow students. Others shared that they could easily and swiftly communicate with their lecturers through the Wi-Fi connection. Easy and affordable access to educational content at any given time and place was also made possible by on-campus Wi-Fi networks. Fong and Wong (2017) aver that Wi-Fi gives us the flexibility and convenience of not being tied to a fixed location. Also, more and more electronic devices such as mobile phones, cameras, gaming devices, television and entertainment equipment are now Wi-Fi enabled.

Table 5: Benefits associated with the university Wi-Fi network

Itemised	**Frequency**	**Percentage**	**Cumulative percentage**
Enables collaborative and interactive learning	75	42.1	42.1
Promotes student management	35	19.7	61.8
Easy access to educational content	24	13.5	75.3
Advanced flexibility	33	18.5	93.8
Establishes an approach conducive to learning	11	6.2	100.0
Total	*N* = 178	100.0	

Table 5 illustrates that having a Wi-Fi network at universities and across all campuses means leveraging Wi-Fi-enabled devices and platforms for educational goals and purposes. Nonetheless, keeping abreast with technological advancements could pose a few challenges for educational institutions. Ultimately, the affordability and accessibility of Wi-Fi connections on campuses play an essential role in universities delivering effective and engaging learning experiences, as indicated by the respondents. Educators can facilitate classes through various means by offering all-inclusive interactive learning engagements and task activities on connected platforms, leverage online podiums to share assessments, and create a communal agenda. Also, by ensuring the affordability of Wi-Fi networks across all campuses, the university has been able to guarantee a fast, reliable and secure data network, to provide pervasive connectivity to the community, to facilitate virtual student experiences and engagement, to offer a searchable online institutional repository, and to deliver IT service excellence.

Optimal Performance and Security

Security has continuously been a significant concern related to Wi-Fi networks. The dangers of using different technological devices and the associated privacy concerns related to information being transferred over the network are growing exponentially.

Therefore, there is a need to protect the university's Wi-Fi network from being attacked (Ji 2017). WLANs use service set identifiers for their security, and users use them to join WLANs. Some WLANs enter the MAC APs to control the access of devices. Both of these methods are regarded as insufficient solutions to security challenges (Ji 2017). According to Siunduh (2013), there are also challenges in the use of ICT services and wireless networks, and the security of the information systems. Internet use among the university community depends on the degree of wireless network coverage on campuses, the availability of relevant IT-enabled services, and security measures implemented on wireless networks. A balance needs to be reached between the ease of access and the levels of security.

Various campuses have implemented different kinds of security configuration on their wireless networks to meet the security requirements of these networks. In this section, the study explores the extent to which respondents agreed with the concerns associated with campus security. The respondents were asked to indicate under what conditions they would consider using the university's Wi-Fi network. The majority indicated that they would consider using the network if it is secured, fast and reliable. This implied that when appropriate security measures are implemented, users feel that they are protected while using the Wi-Fi network in an open space. In line with this finding, the researchers tried to establish whether there were specific security concerns associated with UJ's Wi-Fi network that needed to be dealt with, based on the respondents' feedback (see Table 6).

Table 6: Foreseeable security concerns associated with the university's Wi-Fi network

I think the security concerns associated with the university W-Fi networks should be dealt with for the following reasons	**SD %**	**D %**	**NAD %**	**A %**	**SA %**
To avoid a security bridge	15.7	17.4	15.7	40.4	10.7
To safeguard the privacy of personal details	3.6	7.2	18	50	21.2
To prevent being hacked and impersonated	10.2	12.5	5.3	32	40
To reduce online dangers owing to public spaces	6.7	8.4	14.6	36	34.3
For monitoring and control mechanisms	3.9	10.7	15.7	51.1	18.5

SD = strongly disagree; D = disagree; NAD = neither agree nor disagree; A = agree; SA = strongly agree

With the extensive distribution of Wi-Fi networks these days, it is becoming easy for hackers or attackers to disguise their true personality by arbitrarily hopping onto open wireless networks to carry out malicious attacks and leave without being noticed or apprehended. Most existing wireless network infrastructure may not keep logs of

network activities by default, making it more difficult to acquire imperative network hints that may lead to future forensic inquiries on a suspected malicious network occurrence. In this instance, a malicious hacker who intends to cause harm may aimlessly pick an open Wi-Fi network, expediently join the AP of any network, upload or download malicious files through the AP, then close the session. The process takes mere minutes to accomplish. It is therefore critical to consider the foreseeable security concerns raised.

The itemised list presented in Table 6 illustrates the areas of concern the respondents felt the ICS department ought to further improve on, to ensure Wi-Fi network users across all campuses are not compromised. It is suggested that if these areas of concern are dealt with, network users can use the network freely, without being fearful of security bridges. It also assures users that their confidential information and personal data are protected. The concern of being hacked and the threats associated with it will be reduced, bearing in mind that the network runs in public spaces or domains, and may be exposed to online dangers. The respondents felt that the ICS department should implement monitoring and control mechanisms to help manage access, grant privilege, and revoke access to the Wi-Fi network when necessary.

Strategy for Improvement

Studies have shown that inadequate Wi-Fi presence, access control and monitoring, inadequate bandwidth and unstable service quality continue to be a major challenge and concern that frustrate universities' Wi-Fi network users (Fong and Wong 2017). The respondents were asked to suggest the best possible tactics to improve the university's Wi-Fi network across all campuses, and the results are given in Table 7.

Table 7: Strategy for improvement

What are your suggestions for improving the on-campus WLAN services?	**SD %**	**D %**	**NAD %**	**A %**	**SA %**
The ICS department should have network management tools that provide real-time visibility and analytics	9.6	19.1	20.2	47.2	3.9
The ICS department should identify areas on campuses with high activity and improve Wi-Fi hotspot presence	15.2	23	10.1	50	1.7
The ICS should ensure that access is optimised, without compromising quality, reliability and availability	12	17	5	40	26
The ICS department should ensure that Wi-Fi access privileges are revoked from academic and non-academic staff and students who may have completed their studies or left their jobs	21.3	9.6	6.7	37.1	25.3

SD = strongly disagree; D = disagree; NAD = neither agree nor disagree; A = agree;
SA = strongly agree

The respondents collectively recommended that the university's ICS department consider some of these recommendations as a strategic move to enhance the Wi-Fi network services. They were of the opinion that these sets of recommendations are strategic initiatives that create a platform for transforming teaching, learning and improving efficiency. The respondents felt these recommendations could help increase budgets for the deployment of wireless campus network infrastructure to improve internet coverage on campuses.

Findings

The article probed the effectiveness and usefulness of WLANs in higher education environments to promote effective learning engagements. Over the years, it has become evident that the use of ICT has fundamentally revolutionised and shaped our mode of education delivery through affordable Wi-Fi networks. The findings suggested that Wi-Fi network access on university campuses has great benefits, as the implementation of the WLANs in HEIs provides students with digital affordability, competencies, and confidence levels that allow them to overcome ICT challenges. More importantly, the provision of appropriate WLANs supports online programme delivery that enhances students' learning engagement and development. Wi-Fi on university campuses is nothing new, and UJ recently increased its wireless hotspot coverage, allowing students to connect from anywhere on the four campuses without having to visit the computer labs.

The university's document report shows that the use of university Wi-Fi networks on campuses have increased over the years as more students have embraced the benefits of Wi-Fi network-aided laptops, smartphones, desktop computers, notepads, iPads, tablets, and other devices. Moreover, the number of Wi-Fi network users at popular hotspot coverage points – such as the library, lecture hall, cafeteria, university building, parking area, 24-hour study area and bus terminal – appeared to have increased as more users are starting to realise the benefits, convenience and flexibility that Wi-Fi offers.

According to the UJ web content report that was published on 4 March 2013, along with the ICS department's report of 2012, and the Faculty of Engineering and the Built Environment (FEBE) Annual Report of 2016, the Executive Director of ICS, Mr Andile Swartbooi, mentioned that UJ has been overseeing the installation of additional Wi-Fi, which officially began in 2010. The ongoing process was accelerated in 2011 to cover all four campuses in terms of libraries, student centres, large lecture venues and communal areas in all the student residences. Several marked external hotspots were also located at strategic areas across the four campuses. The findings represented in Table 3 confirmed this statement. The respondents mentioned that they had Wi-Fi network access and connectivity across several sites located across all campuses. The executive director further outlined a few key benefits from the Wi-Fi network expansion and said that Wi-Fi allows students to gain access to online resources from anywhere on campus, which also helps to alleviate overcrowding at student computer labs. According to Mr Swartbooi (UJ 2013),

> Students can use a variety of devices, ranging from laptops to tablets and smartphones and many other electronic devices to connect to the UJ Wi-Fi network.

It was also evident that UJ decided not to charge for the wireless internet access, but there is a need to ensure that students use the internet service responsibly. The ICS has continued to work on policies that will promote the responsible use of the Wi-Fi service. The policy will ensure that the internet is treated as an educational tool, where restrictions will apply to using the service reasonably for teaching, learning and research purposes. Table 2 and Figure 3 support this claim as the respondents were asked to indicate what is required in order to gain access to the university's Wi-Fi network. The majority of the students mentioned that a user ID and password are required to be granted access to the Wi-Fi network. Mr Swartbooi (UJ 2013) said:

> While, students would probably agree that the Wi-Fi is a bonus, with students no longer having to queue or walk to the labs at night, it would be great to see if academic performance will improve overall.

In support of this claim, the respondents were asked whether the use of Wi-Fi networks could aid in improving their learning experience, engagement, and overall academic performance. The respondents confirmed that they use the Wi-Fi network to browse for online content and knowledge; some revealed that they use it for research activities, shopping, entertainment and socialising. The majority of the respondents claimed that they use the Wi-Fi network for educational purposes.

As part of the bigger UJ ICT strategy, the Wi-Fi access is an indication of UJ's continuous efforts in striving to be seen as a university of stature and as a reputable institution of higher learning. Students will have a better chance at succeeding in their academics by giving them the access to the information they need wherever they are.

Conclusion and Recommendations

Even as Wi-Fi network technology continues to gain prevalence in HEIs and is globally recognised, the principal technology is constantly changing to improve efficiency and enable data-intense applications and multifaceted experiences on wireless technology. The study offered a detailed introduction, research objectives and research problem. The literature review provided an extensive overview of the processes involved during the implementation of WLANs. Moreover, the discussion included the benefits of its use, Wi-Fi's role in improving easy access to education, learning enthusiasm, increased educational opportunities, and quality education. Subsequently, the quantitative research method and epistemology assumption were discussed, and a clear argument of the research processes, approaches, and the theories that were used in the study was provided. The discussion also focused on the access to and use of ICT by students and staff members across four UJ campuses.

The respondents acknowledged that the university's Wi-Fi network is reliable, accessible and supportive. They also reflected that it encourages uninterrupted learning and allows them to access affordable learning contents. However, a few security concerns were raised, and areas for improvement were mentioned. It was recommended that the university's management consider ICT as a strategic platform for transforming teaching, learning and improving efficiency; management should therefore increase its budgets for the deployment of wireless campus network infrastructure to increase internet coverage on campuses. The security concerns raised in this study should not be ignored, although not all the mentioned issues were a major challenge – some of the issues related to security and performance optimisation have also been dealt with appropriately. Hence, the ICS department should ultimately consider implementing necessary solutions, promoting optimal usage, partnerships, and resources so HEIs can provide efficient ICT services and high-quality education. The provision of ICT infrastructure in HEIs promotes a digitally enabled environment that can help students access learning materials online on their personal devices from any location. Therefore, improved ICT infrastructure will enable collaborative and interactive learning, promote student management, and offer easy access to learning content – irrespective of location – by advancing flexibility and creating an atmosphere that is conducive to learning.

Acknowledgements

This research acknowledges the financial support received from the National Research Foundation (research grant: 120730) in advancing and articulating this article.

References

Abdelkarim, R. 2006. "Security in Wireless Data Networks: A Survey Paper." Accessed 20 April 2017. http://www.cs.wustl.edu/~jain/cse574-06/ftp/wireless_security/index.html.

Akhtar, A., and S. C. Ergen. 2018. "Directional MAC protocol for IEEE 802.11 Ad-Based Wireless Local Area Networks." *Ad Hoc Networks* 69: 49–64. https://doi.org/10.1016/j.adhoc.2017.10.009.

Alexandra, G. 2015. "Getting Familiar with Wi-Fi Channels? WLAN Back to Basics." Accessed 26 March 2020. http://boundless.aerohive.com/experts/WLAN-Channels-Explained.html.

Bradley, M. 2017a. "Wireless Standards 802.11a, 802.11b/g/n, and 802.11ac." Accessed 1 April 2020. https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553.

Bradley, M. 2017b. "What Hardware is Required to Build a Wireless Network?" Accessed 1 April 2020. https://www.lifewire.com/required-to-build-wireless-networks-816542.

Cisco. 2008. “Authentication Types for Wireless Devices.” Accessed 25 April 2019. http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthentiationTypes.html.

Cisco. 2011. “Wireless LAN Controller Web Authentication Configuration Example.” Accessed 20 April 2019. http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlansecurity/69340-web-auth-config.html.

Creswell, J. W. 2015. *A Concise Introduction to Mixed Methods Research*. Thousand Oaks: Sage.

Crow, B. P., I. Widjaja, J. G. Kim, and P.T. Sakai. 1997. “IEEE 802.11 Wireless Local Area Networks.” *IEEE Communications Magazine* 35 (9): 116–26. https://doi.org/10.1109/35.620533.

Ding, A. X., and W. Dan. 2012. “The Security Experience of Wireless Local Area Network at Ningbo University.” In *Advanced Materials Research*, Vol. 488, 1603–1608. Trans Tech. https://doi.org/10.4028/www.scientific.net/AMR.488-489.1603.

Dixit, S., and A. Pandharipande. 2007. “New Directions in Networking Technologies in Emerging Economies.” *IEEE Communications Magazine* 45 (1): 92–95. https://doi.org/10.1109/MCOM.2007.284543.

Drozdenko, B., M. Zimmermann, T. Dao, K. Chowdhury, and M. Leeser. 2017. “Hardware–Software Codesign of Wireless Transceivers on Zynq Heterogeneous Systems.” *IEEE Transactions on Emerging Topics in Computing*. https://doi.org/10.1109/TETC.2017.2651054.

FEBE Annual Report. 2016. Web content. Faculty of Engineering and The Built Environment. https://www.uj.ac.za/faculties/febe/Pages/annual-report.aspx.

Fong, K. K. K., and S. K. S. Wong. 2017. “Wi-Fi Adoption and Security in Hong Kong.” *International Business Research* 10 (8): 129–48. https://doi.org/10.5539/ibr.v10n8p129.

García Pineda, M., S. Sendra, C. Turró Ribalta, and J. Lloret. 2011. “Users Macro and Micro–Mobility Study Using WLANs in a University Campus.” *International Journal on Advances in Internet Technology* 4 (1): 37–46.

Gast, M. 2005. *802.11 Wireless Networks: The Definitive Guide*. O’Reilly Media.

Han, Y., 2008. “The Study of Students’ Perceptions of On-Campus Wireless Local Area Networks (WLANs) Usage.” PhD thesis, Unitec Institute of Technology.

Hassan, W. H. W., H. King, S. Ahmed, and M. Faulkner. 2018. “Enhancement Techniques of IEEE 802.11 Wireless Local Area Network Distributed Coordination Function: A Review.” *ARPN Journal of Engineering and Applied Sciences* 13 (3): 1053–62.

Information and Communication System. 2012. “Annual Report.” Accessed 23 July 2018. https://www.uj.ac.za/Pages/Search.aspx?k=ICS%20annual%20reeport#k=ICS%20annual%20report.

Jacob, S. M., and B. Issac. 2008. “Mobile Technologies and its Impact – An Analysis in Higher Education Context.” *International Journal of Interactive Mobile Technologies* 2 (1).

Ji, M. 2017. “Designing and Planning a Campus Wireless Local Area Network.” Bachelor’s thesis, South-Eastern Finland University of Applied Sciences.

Khorov, E., A. Kiryanov, A. Lyakhov, and G. Bianchi. 2018. “A Tutorial on IEEE 802.11 Ax High-Efficiency WLANs.” *IEEE Communications Surveys and Tutorials* 21 (1): 197–216. https://doi.org/10.1109/COMST.2018.2871099.

Kowsar, M. M. S., and S. Biswas. 2017. “February. Performance Improvement of IEEE 802.11 n WLANs via Frame Aggregation in NS-3.” In *International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 1–6. IEEE. https://doi.org/10.1109/ECACE.2017.7913039.

Lee, C. C. E., S. W. Y. Leow, and X. J. Kong. 2020. “The Use of Mobile Technologies for Learning in Higher Education: Students’ Readiness.” *SEARCH Journal of Media and Communication Research* 107–27.

Lehr, W., and L. W. McKnight. 2003. “Wireless Internet Access: 3G vs. Wi-Fi?” *Telecommunications Policy* 27 (5–6): 351–70. https://doi.org/10.1016/S0308-5961(03)00004-1.

McCormick, D. K. 2017. “IEEE Technology Report on Wake-Up Radio.” In *An Application, Market, and Technology Impact Analysis of Low-Power/Low-Latency 802.11 Wireless LAN Interfaces*, 1–56. IEEE.

Microsoft. 2003. “How 802.11 Wireless Works.” Accessed 28 April 2017. https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx.

Mohd Ali, A., M. J. Sibley, and I. Glover. 2017. “WLAN 802.11 e Evaluation Performance Using OPNET.” *International Journal of All Research Education and Scientific Methods* 5 (1): 35–38.

Murad, M., and A. M. Eltawil. 2020. “Performance Analysis and Enhancements for In-Band Full-Duplex Wireless Local Area Networks.” *IEEE Access* 8: 111636–52. https://doi.org/10.1109/ACCESS.2020.3001876.

Mykhalevskiy, D. V., and O. S. Horodetska. 2019. “Investigation of Wireless Channels According to the Standard 802.11 in the Frequency Range of 5 GHz for Two Subscribers.” *Journal of Mechanical Engineering Research and Developments* 42 (2): 50–57. https://doi.org/10.26480/jmerd.02.2019.50.57.

Raman, B., and K. Chebrolu. 2007. “Experiences in Using Wi-Fi for Rural Internet in India.” *IEEE Communications Magazine* 45 (1): 104–110. https://doi.org/10.1109/MCOM.2007.284545.

RF Wireless World. n.d. “WEP vs WPA vs WPA2.” Accessed 2 April 2019. http://www.rfwireless-world.com/Terminology/WEP-vs-WPA-vs-WPA2.html.

Rudenkova, M. 2020. “802.11 Wireless LAN Using ns-3.” Paper presented at the 2020 Inforino, 14–17 April, Moscow, Russia.

Sadeghi, R., J. P. Barraca, and R. L. Aguiar. 2017. “A Survey on Cooperative MAC Protocols in IEEE 802.11 Wireless Networks.” *Wireless Personal Communications* 95 (2): 1469–93. https://doi.org/10.1007/s11277-016-3861-0.

Salous, S., V. Degli Esposti, F. Fuschini, R. S. Thomae, R. Mueller, D. Dupleich, K. Haneda, J. M. M. Garcia-Pardo, J. P. Garcia, D. P. Gaillot, and S. Hur. 2016. “Millimeter-Wave Propagation: Characterization and Modeling toward Fifth-Generation Systems. [Wireless Corner].” *IEEE Antennas and Propagation Magazine* 58 (6): 115–27. https://doi.org/10.1109/MAP.2016.2609815.

Scarfone, K., and D. Dicoi. 2007. “Wireless Network Security for IEEE 802.11a/b/g and Bluetooth.” Accessed 1 April 2018. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.6200&rep=rep1&type=pdf.

Sevtsuk, A. 2009. “Mapping the MIT Campus in Real Time Using Wi-Fi.” In *Handbook of Research on Urban Informatics: The Practice and Promise of the Real-Time City*, 326–338. IGI Global. https://doi.org/10.4018/978-1-60566-152-0.ch022.

Siunduh, E. S. 2013. “Analysis of the Effect of Wireless Campus Networks on Internet Usage in Kenyan Universities.” Master’s research project, University of Nairobi.

UJ (University of Johannesburg). 2013. “Wi-Fi Access a Huge Benefit for UJ Students.” Accessed 10 June 2018. https://www.uj.ac.za/newandevents/Pages/Wi-Fi-access-a-huge-benefit-for-UJ-students.aspx.

Valkanis, A., A. Iossifides, P. Chatzimisios, M. Angelopoulos, and V. Katos. 2019. “IEEE 802.11 Ax Spatial Reuse Improvement: An Interference-Based Channel-Access Algorithm.” *IEEE Vehicular Technology Magazine* 14 (2): 78–84. https://doi.org/10.1109/MVT.2019.2904101.

Wang, Y., M. Li, and M. Li. 2017. “The Statistical Analysis of IEEE 802.11 Wireless Local Area Network-Based Received Signal Strength Indicator in Indoor Location Sensing Systems.” *International Journal of Distributed Sensor Networks* 13 (12): 1550147717747858. https://doi.org/10.1177/1550147717747858.

Yaqoob, I., I.A. T. Hashem, Y. Mehmood, A. Gani, S. Mokhtar, and S. Guizani. 2017. “Enabling Communication Technologies for Smart Cities.” *IEEE Communications Magazine* 55 (1): 112–120. https://doi.org/10.1109/MCOM.2017.1600232CM.