International Journal of Computer Applications Technology and Research
Volume 5– Issue 6, 403 - 411, 2016, ISSN:- 2319–8656

Comparative Study of Optic Fibre and Wireless Technologies in Internet Connectivity

Onu Fergus U.
Department of Computer Science,
Ebonyi State University, Abakaliki – Nigeria

Ikporo Stephen C.
Department of Computer Science,
Ebonyi State University, Abakaliki – Nigeria

Abstract: Most of the activities going on in the world today demand information and data sharing in one form or the other. Consequently, the Internet and its connectivity has gradually become a household concern. The connection to the Internet requires physical transfer of signal (data/information) from one point to another. This can either be through physical medium (wire) or through the air (wireless). This paper a comparative study of Fiber Optics and Wireless Technologies in Internet connectivity seeks to identify which of the two technologies is better for signal transmission in terms of bandwidth utilization, performance, reliability, cost effectiveness, resilience, and security. The study adopted the use of secondary sources for the sourcing of materials. A lot of journal articles, research publications, testbooks, white papers and many more were critically studies and comparatively analysed. It was clear that both media have hitches and challenges. The study showed that although initial cost of acquisition is an inhibitive factor for fibre optic connection, unlimited bandwidth delivery and high Quality of Service (QoS) placed Fiber optics above wireless connectivity in their overall performance.

KEYWORDS: Internet connectivity, quality of service, wireless technology, Bandwidth utilization, Channel Resilience.

1.0 INTRODUCTION

Communication is as old as man himself. Right from creation, man needed to communicate with one another and with their environment. Communication can be verbally or through signs and symbols. This communication no matter the form (verbal or through signs and symbols) is usually through a medium. The medium alone is not the network. The network is the combination of the medium and the communicating devices (active or passive). In every part of the world, leaders and decision makers have recognized the important role which Information and Communication Technology (ICT) has to play in connecting people and as such ICT stimulates and drives employment, economic growth and social development both in the developed and developing countries. For this singular reason, efforts are being made in every part of the world to accelerate the spread of ICT access across all regions.

Despite the improved and substantial investment made in ICT infrastructure in some parts of the world especially Africa in recent years, focus has been on the improvement of the mobile infrastructure and access. Appreciable gaps in the backbone networks are yet to be addressed. This fact has made the effective high-speed Internet services needed for important key business, government and consumer applications continue to be either unavailable or very expensive. In Africa, the cost of broadband Internet access on the average is about three times higher than what is obtainable in Asia, where significant broadband infrastructure investments have been made [1].

The development of broadband access promises an increased economical development. This requires state-of-the-art network connectivity to be realized. Systems like video conferencing, distance education, academic research and remote surgeries, all require large amount of bandwidth, speed, efficiency, great reliability and security. These factors are some of the demands placed on telecommunications networks today [2].

Understanding the best medium to use when trying to transmit information (signal) from one point to another can make such connectivity an easy one. But in the reverse case, this choice can be very troublesome since one needed to understand the performance of the network in terms of the factors such as: bandwidth, performance, reliability, cost efficiency; resiliency, redundancy, and security, which must be considered during Internet connectivity. Generally, [3] categorised network transmission media into guided and unguided groups. Fibre optics belongs to the category of guided media while wireless technology belongs to undguided media family [3] continued.

Most of the recent generations of emerging wireless communication standards utilize improved modulation techniques to squeeze more bandwidth out of available frequency. However, the total bandwidth achieved by wireless technologies, especially the ones using the unlicensed spectrum, are still of magnitude behind what is possible with Fiber optics. Where most unlicensed wireless setups can deliver bandwidths of multiple megabits per second the most advanced Fiber optic connections can deliver multiple gigabits per second, [4].

Ethernet protocol yields gigabit transfer rates and it is increasingly deployed over long distance. With wireless technologies, flexibility in upstream/downstream bandwidth is provided, but high QoS is more difficult to guarantee if bandwidth is shared between users. As a general rule and in application, better QoS is expected from a Fibre optic connection as it provides a dedicated link between two points [4].

This comparative study of optic fiber and wireless technologies in network interconnectivity adopts a methodological technique by considering a set of requirements which include: Application requirements; Technological requirements; Policy and regulatory requirements; Operations and maintenance requirements. The importance of each requirement and each criterion depends on the context of the application. The decision to adopt an optic fiber-based or wireless-based technology for network interconnectivity depends heavily on the evaluation of

these requirements for each technology in the context of the application domain, [5].

With the level of broadband penetration in recent years in all parts of the world, interest has shifted from apenetration to Internet accessibility and efficiency to users. Government and corporate organizations at various levels have made tremendous effort in bringing Internet connectivity to people. In each case, the best medium to achieve this goal of ensuring that people have access to Internet has always been a problem. While some always opt for Fiber optics cable, many others always choose to use wireless connection. This has lead to people trying to fuse the two by using Fiber over Wireless (FoW), and others have tried using Fiber-Wireless (Fi-Wi), [22].

2.0 LITERATURE REVIEW

2.1 Overview of Communication System

Communication system is the system responsible for the transmission of information from one point to another. Communication system can be analogue or digital. Figure 1 shows the block diagram of a typical communication system. The source as represented in figure 1 can generate either analogue signal (eg. speech, audio, image and video), digital data such as text or multimedia data. Information from the source is passed to the source encoder which generates binary data. The generated binary data is modulated to generate waveforms for transmission over the channel. The channel is subjected to various types of impairments (eg. noise) due to its open nature. At the receiver, the whole process is reversed so as to finally restore the original source information, [26].

The communication system can be wired or wireless. Wireless communication deals with the transmission of signal through low-energy radio frequency waves using open air, transmitter and receiver as the media. While wired communication system involves the transmission of signal through wire with the aid of transmitter and receiver. Wired communication system can be through Twisted Pair cable (shielded or unshielded), Coaxial cable or Fiber Optics cable, [24].

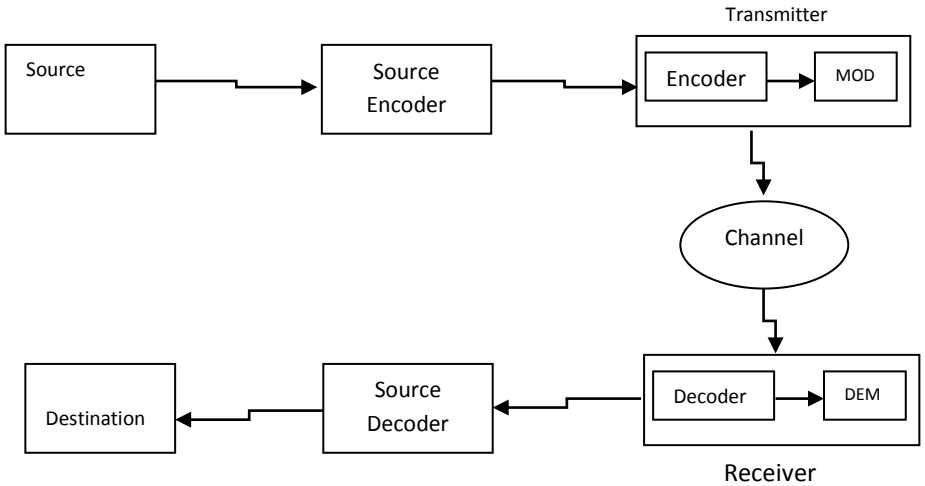

Figure 1: Block Diagram of general communication System

2.2 Wireless Communication System Trends and advancement

This involves the transmission of message signal from one point to another using an open air, transmitter and receiver as the media. This message signal is transmitted to the closest antenna site and delivered by radio signal to another wireless node or receiver, [24]. Wireless communication can be implemented through Wireless Local Area Network (WLAN), Wireless Fidelity (Wi-Fi) etc. The introduction of wireless communication was dated back to 1800s by M.G. Marconi, when he successfully established a radio link between a land-based station and tugboat, [25]. This was succeeded by the invention of Amplitude Modulation (AM) for music broadcasting in 1906 by Fessenden, and in 1933, Edwin H. Armstrong invented Frequency Modulation (FM), [26].

Wireless system advanced rapidly in the last two decades. Wireless communication systems migrated from first-generation (1G) which used narrow-band analogue signalling for voice transmission in 1980s to the second generation (2G) narrow-band systems of 1990s, which used digital communication technique with TDMA, FDMA or CDMA. 2G was deployed for the transmission of voice signal operating on Global System for Mobile Communication (GSM) 900MHz with GPRS 56kbps to 114kbps. 2G also witnessed invention of Global System for Mobility (GSM), Personal Digital cellular (PDC), etc, [4].

Currently, different wireless technologies (eg.GSM, CDMA and TCDMA) were deployed throughout the world for 2G, 2.5G and eventually 3g networks. Despite 2.5G networks offering a higher data rate f 144kbps which was far higher than 2G. It was also used to deliver basic data services like text message. However, 2.5G does not allow for the download of images or even browse a website from PDA, [4].

According to [6], as the limitation of 2G increases, the conception of 3G became more pronounced. The design and deployment of 3G network was aimed at overcoming all the deficiencies of the 2G and 2.5G technologies as it offers more advanced and innovative services such as high-bit rate and broadband for multimedia service.

3G system should be able to prove roaming capabilities and as well be able to make information services instantly available, [7].

3G technology uses digital communication technique that involved transmission of voice signal as well as multimedia services. The Universal Mobile Telecommunication System (UMTS), which is a 3G cell phone technology, was developed into 4G technologies.

4G technology (which is another level in wireless communication) is developed to provide a comprehensive IP solution, where voice, data, and streamed multimedia could be given to user on "anytime" "anywhere" basis, and at a higher data rate than the previous generations. 4G technology is considered to complete the cycle of technological advancements in wireless communications, with features that will permit a much faster velocity in data transfer and wider area coverage than with the current 3G technology, [4].

The earlier wireless systems composed of a base station with a high-power transmitter and covered a significantly large geographic area. Each of the base station served only small number of users and was also very costly. The major technical problem with it was the lack of compatibility in the system as only few were able to communicate with the public switched telephone network (PSTN).

However, today, there have been significant increases in the number of base stations with low-power radio transmitters, which now cover a large geographic area. This is the reason for the proliferation of mobile systems around the globe.

Presently, wireless services have witnessed four stages of progression ranging from simple communication, high-speed downloading, high-speed downloading and uploading, to real-time latency-sensitive services, which are all enabled by the wireless technology. Apart from the multimedia services such as speech, audio, video, and data, the pervasive use of wireless communication could also be used in healthcare, home automation, etc, [4].

2.3 Security Issues in Wireless Communications Systems

Security concern in wireless communication refers to various threats that expose transmitted signals to unauthorised attacks thereby reducing their integrity and confidentiality. In combating this, more sophisticated measures have been taken to ensure that confidentiality and integrity of transmitted information via the wireless media are not compromised. This includes the measures for prevention of unauthorised access or damage to information transmitted over wireless networks. Security issues with wireless communication systems can be grouped into four major components like: physical security, network security, communication security and administrative security. The physical security deals with protection of all facilities where the communication system components are housed. Network security ensures the protection of the system's hardware, software and associated interfaces. The communication security ensures confidentiality and integrity of information transmitted over the air waves. Finally, the administrative security involves the use of procedural control to ensure the confidentiality, integrity and availability of communication systems, [8].
According to [9], [6], [10], and [11], some of the security issues relating to wireless network are summarised as follows:

- **Eavesdropping on Non-Secured Channels:** This is the act of illegitimate interception and reception of information transmitted over a wireless communication system. It is the attack against the confidentiality of data being transmitted over the network. This is possible because it is easy for the network signal to be received outside the vicinity of the valid users. Hence, attackers can hijack the signal over the air from a certain distance, [9].
- **Electromagnetic Interference (EMI):** This occur due to the signal fading and disruption of wireless signals as a result of too long a distance between the transmitter and the receiver, atmospheric conditions or metallic surfaces, which reflect the radio waves and also due to obstacles in the line-of-sight, [10].
- **Overloading of Bandwidth:** This is caused by piggybacking, which is an access to someone else's wireless connection by another within the sphere (area) of the wireless connection without the consent and knowledge of the main subscriber. It can cause service violations, direct attack on ones computer and illegal activities by malicious users, [6].
- **Wireless Sniffing:** This is the invasion of sensitive information like password, bank account numbers, credit card details, etc, using sniffing tools on an unsecured network with an unencrypted traffic. When a network is unsecured, sensitive communication or transactions on them are always at risk.
- **Denial of Service (DoS):** This is the flooding of the network with either valid or invalid messages by the wireless intruders using powerful transceivers enough to cause interference effects on the Wireless LAN (WLAN). They usually cause the WLAN not to be able to communicate using the radio path. DoS causes network interruption and prevent data transmission. This in turn enables malicious attackers observe the recovery of the network and record the codes as they are being re-transmitted by valid user using cracking devices that will aid such attacker to break the security and gain unauthorized access to the system, [11].
- **Spoofing and Session Hijacking:** This is when an attacker impersonates the identity of a valid user to illegitimately gain access to privileged data and resources in the network. This is always the case as 802.11 networks do not authenticate the source address, which is the Media Access Control (MAC) address of the frame. Spoofing can be eliminated by ensuring proper authentication and access control mechanism of WLAN, [11].
- **Traffic Redirection:** This is the manipulation of the MAC address as well as the IP address of a particular wired station by an attacker in order to change the traffic route o f a particular computer to the of the attacker. Others include: Rogue Access Point and Caffe Latte Attack, etc, [10].

2.4 Security Measures with the Wireless Communication

According to [10], 802.11b provided the following security features in wireless network.

- **Service Set Identifier (SSID):** This is the process of ensuring that all devices that require access to a particular WLAN are configured with the same SSID. It is added on the header of the packet sent over the WLAN and are verified by the Access Point. This ensures that clients cannot communicate with a particular access point unless both have same SSID configurations. However, SSID provides little security because it is more of a network identifier than a security feature, [10].

- **Wired Equivalent Privacy (WEP):** This is the standard encryption mechanism for wireless networking. It is an algorithm that is used to protect wireless communications from eavesdropping and modification. It also prevents unauthorized access to a wireless network. WEP relies on secret key shared between a wireless station and an access point which is used to encrypt data packets before they are transmitted and an integrity check is used to ensure the packets are not modified in transit, [13].
- **Media Access Control (MAC) Address Authentication:** Here, the access point is configured to accept association and connection requests from only those modes whose MAC addresses are already registered with it. This provides for additional security layer, [10].

2.5 Wired Communication System

Wired communication refers to the transmission of signals from one point to another through physical media (wire. Wired media is also called guided media [4]. The three identified guided media are Twisted Pair (shielded or unshielded), Coaxial or Fiber Optic Cables.

Twisted Pair Cables (TP): Twisted pair cable is a multi-core (eight) cables twisted into four pairs. Two of the pairs carry the positive or true voltage and are considered tip (T1 to T4), while the other two pairs carry the inverse of voltage grounded and are called ring (R1 to R4). Twisted pair cables are of two categories namely **shielded twisted pair (STP)** and **unshielded twisted pair (UTP).** UTP is the commonest type of cable, but has a problem of crosstalk. STP has sheath for each pair of cables to prevent the interference caused by the crosstalk. TP cable can only reliably connect network segments of not more than 100meters [4].

Coaxial Cable: This consists of a center copper conductor core, a plastic insulating material, a metallic braided sheath, and an outer plastic sheath. The core conducts the data, while the remaining layers provide insulating and protection against signal interferences which might corrupt the transmitted data. A single Coaxial cable has a diameter range of 1 – 2.5cm. It can be used to transmit over a longer distances and support more stations on a shared line than twisted pair, [8]. Coaxial cable has two classes namely: Thinnet (10Base2) and Thicknet (10Base5). **Thinnet or 10Base2** is more flexible than thicknet, hence it is easier to work with. It uses British Naval Connectors (BNC) to attach thinnet cable using T connectors, barrel connectors and terminators. **Thicknet (10base5)** is rarely used today because it is difficult to install and has slow transmission speed [8]. Coaxial cable no matter the type can reliably connect segments of about 185meters.

Fiber Optic Cable: Figure 2 shows a sample optic fibre cable. It is a flexible thin filament of glass (silicon glass) that can accept electrical signals and covert them into optical (light) signals which are reconverted to electrical signals at its destination. They are non-metallic and hence not susceptible to interferences like electromagnetic interference (EMI), radio frequency (RF) or lightning. They are typically smaller and lighter in weight and are practically impervious to outdoor atmospheric conditions. Fiber optic networks are the backbone of the Internet and our enterprise communications infrastructure and can transmit data, video and other applications. They can transmit up to 62 miles before the signals need to be regenerated [19]. The structure of the cable consists of concentric sections shown in figure 2:

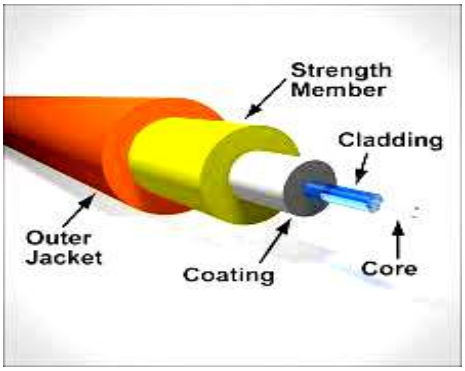

Figure 2: A Sample Optic Fiber cable. [Source: 14].

The Core: The core is the innermost (center) section of the wire and consists of one or more very thin strands, or fibers with a diameter range of 8 to 100µm. It is always made up of glass or plastic. They are the carrier of the optical data signal from the transmitting end to the receiving end.

The Cladding: This is the protective polymer which surrounds the core. The interface between the core and the cladding acts as a reflector to confine light that would otherwise escape the core. It is made up of material that is of lower index of refraction than the core. This is why light is reflected back into the core and the data continues to travel without a loss of light.

The Buffer: This is also carried the coating which helps protect the fiber from physical and environmental damage. It is commonly made of a gel material or a thermoplastic material. The coating is normally stripped away from the cladding to allow termination to an optical transmission system during installation.

The Amor: This layer is usually metallic, rigid, weather proof, and very strong. It serves as physical security measure against outside forces or manipulations.

The Jack: This is the outer layer and always orange in colour. It serves as protection against contaminants, moistures, abrasion, crushing and other environmental dangers, [14].

Fiber optics converts packets of data-images, texts, video, and emails into a stream of light (optical signal). The cable carries the light signal from the transmitter to the receiver, which uses photodiode or photocell to detect the light, and then converts it back to an electrical signal. When the distance increases and becomes longer, an optical regenerator is usually used to boost and regenerate the weakened signal.

Fiber optic cable carries significantly smaller amount of fibers, usually between 2 and 48 fiber strands per bundle and have two cores, as shown in figure 4 below. Generally, one core is used for transmission (TX) and the other core for Reception (RX), [14].

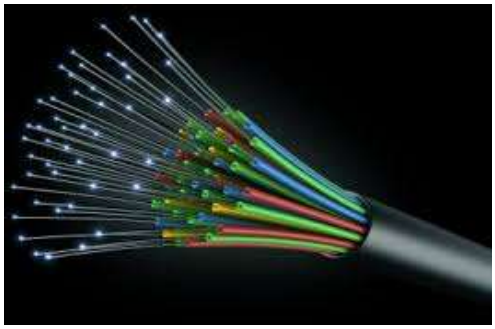

Figure 4: Sample of Optic Fiber with several strands of fiber. [Source: 14].

The signal transmission through Optic fiber is of two modes: Single Mode and Multi Mode;

Single Mode: This is used to transmit signal in longer distances, 50 times more than the multi mode. It has core of between 8-10 micrometer and has a technology that uses powerful laser diode and can transmit with wavelength of 1300/1550nm and a transmission speed range 10GE/1GE/100mbps and a distance of up to 40kmor more. It only has one mode of transmission and costs more than multi-mode, but it is less susceptible to signal attenuation and distortion from overlapping light pulses. The core here is always small, about 9 microns, and also has small numerical aperture (NA).

Multi Mode: This is used to transmit in short and medium distances. It has technology that uses less powerful Light Emitting Diode (LED) which can transmit infrared laser light of wavelengths, 850nm/1300nm. It has core of diameter usually 50, 62.5, or 100 meters with transmission speed of up to 10gbps/1Gbps/100mbps and distance of between 300 meters and 4km. As the name implies, transmission occurs in more than one mode as light waves are dispersed through the cable. Multi-mode fiber can be used with less expensive connectors and LED transmitter, making it more economical choice for application with shorter distances and lower bandwidth demands, [17].

2.6 Security Issues with Fiber Optics

The security issues in fiber optics is basically grouped into: Physical Layer Security and Data Layer Security.

Physical Layer Security: this deals with the physical detection and intrusion to the cable which does not involve significant data interruption. This is why it is not of any advantage to post the fiber optics communication infrastructures on the Internet as it can provide roadmap and bring attention to the fiber optic communications' vulnerabilities. Once an intruder gains access to the cable, the actual tap can easily be done that ever thought or imagined. The intruder can use any available commercial items such as laptop, optical tap, pocket Sniffer Software or even optical/electrical converter to do virtually detectable tap on the cable.

Another physical layer security concern can come from the unintended attackers. This happens when someone unintentionally attacks the cable thereby causing a tap or cut on the cable. Once a successful tap is made, the cable is exposed such that packet sniffer software can be employed to filter through the packet headers.

Data Layer Security: This occurs when the intruder through any tap on the cable tamper with the data being transmitted on the cable. With the cable already tapped, the filter can be applied to the data allowing specified IP addresses, MAC addresses or DNS information to be gathered and then stored or forwarded to the intruding parties' various tools and mechanisms, including other optical connections, links, wireless, another wavelength or other resources, [20]. When the intruder has successfully used an unobtrusive method to retrieve data directly from the fiber optic cable, the need for accessing the company's network will not be necessary. Hence the problem on how to get over firewalls, IDS and IPS will not occur. The only possible problem to the intruder would be when the transmitted data are encrypted. Though depending on the encryption method used, it may still be a matter of time before the intruder breaks the encryption and have their way. Others include;

Optic fiber Splicing: This is the most detectable fiber optical disruptions of data as the cables are cut, thereby allowing for disruption of data transmission. When this type of data interruption/disruption is detected, or noticed, a technician or repair person can be sent out to find the source and fix it.

Optic Fiber Bending or Clamping: This occurs when the cables are tapped without piercing them or disrupting the flow of data. This mainly happen when the cable is bent or clamped in a précised way that can form a micro-bends. When micro-bends or ripples are introduced, photons of light can leak out thereby allowing the intruders' receiver to capture enough of these escaped (leaked) photons of light to have viable data, [20]. This is mostly more pronounced on lowers speed data rates than higher data rates.

According to [20], every signal leak of less than 0.1dB contains all the information being transmitted by each photon. Hence, once the signal is captured, the intruder can use an optical fibre network analyzer to determine the communications protocol and to decipher the information. As far as, there is no disruption or indication of interference with the users' communication the tap is virtually undetected.

This method of tapping fiber cable without actually touching the cable physically, injects additional light into the fiber plant and analyzer, the underlying optical signal protection, an end- user may never notice that their data has been intercepted. Again, another security concern is when intruder gain access to the cable before the first switching center. Detection can go unnoticed even as optical tapping requires less complex and expensive equipment in the local cable and access loops, [20].

2.7 Security Measures in Optic Fiber Communication.

There are some security counter measure in fiber optics communication. These include:

Fibre optic Secure Link: This is used to sense the physical infrastructure disturbance. It uses technology that can concurrently make use of a fibre optic communication cable as a tampering- alert, or integrity- testing sensing cable. It monitors in real-time, any physical disturbance such as clamping or bending. One key advantage this technique is that, it is not necessary for optical losses to occur in order for the technique to sense disturbances, (15).

Encryption Method: This method deals with the encryption of all data being transmitted. This method ensures that a strong encryption with long codes is employed. It also allows for end user to use physical method that can change the light signals as it simultaneously identifies illegal attacks, [16]. Encryption method can also be achieved using photons to encrypt the data. In this method, when a transmitter sends photons that are specifically directed at given intervals through a fiber optic cable, the receiver then analyzes the arrival of the photon at the given intervals. When a matching segment of the transmission pattern advertised on a separate wave length by a transmitter is received, the receiver will then utilize the" key" and authenticate the unlocking of data from the stream. Because of the weakness of the light beam passing through the cable, any alteration would be immediately observed, and any intruder snooping on injecting would inevitably disturb the photon patterns. When this happens, the receiver's device would detect the change in pattern, ending the transmission and sounding the alarm, [17].

Opterna's FiberSentinel System: This uses Wave Sense intrusion prevention technology, artificial intelligence, and optical digital signature recognition to monitor fiber connections. It reportedly detects all physical intrusions and immediately cancels all transmissions. At the time of intrusion detection, this continuous real time monitoring system will switch the data transmission to an alternate fiber path and alerts the network operator, [18].

Oyster Optics Security Solution: This provides optical security, monitoring, and intrusion detection solution that is protocol independent. The system uses a secure phase modulation of the optical signal to impress data on the optical carrier. If data is intercepted, the intruder will not be able to access the captured data unless he/she has Oyster Optics' receiver that is synchronized to the transmitter at power up. This provides a unique transmitter and receiver by using a non-pseudo-random manufacturing process that cannot be replicated. This system can reroute data transmission to a backup system whenever an intrusion is detected. It can be implemented as a stand-alone device or at the transceiver card level, [20].

2.8 How Fiber Optics Communications Work

Fiber Optics technology converts electrical signals carrying data to light and sends the light through transparent glass fibers about the diameter of a human hair. The efficiency of fibre optics is a product of the Index Of Refraction (IOR) and Total Internal Reflection concept. This concept indicated that since fiber is light based, data travels at the speed of light. The speed of light in a vacuum is 186,000 miles per second. When the light is travelling through a medium, the speed is different to it is travelling through a vacuum. The index of refraction is always gotten by dividing the speed of light in a vacuum by the speed of light in a medium. By definition, the IOR of a vacuum has a value of 1. The typical IOR for the core is 1.48 and 1.46 for the cladding. This indicates that light travels slower in the medium, as the IOR gets larger, [21].

The total internal reflection plays key role in the success transmission of data. Total internal reflection occurs when light ray travelling from in one material hits a different material and reflects back in the original material without any loss of light. The core and cladding inside a fiber optic cable work in this manner. The IOR of the core is higher than that of cladding, so when the light from the core hits the cladding, it is reflected back to the core and the data continues to travel. For the total internal reflection to occur, the IOR for the core must be higher than the cladding, [22].

The fibre optics cable's efficiency is also highly enabled by its critical angle. The light of fiber optic must enter through this critical angle. The critical angle of fibre optic is always given by:

$$QC = \cos^{-1}(n2/n1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Where

n1 is the IOR for the core and
n2 is the IOR for cladding.

E.g. given that n1 is 1.48 and n2 is 1.46, then the critical angle of the given fiber cable,

$$QC = \cos^{-1}(n_2/n_1)$$

$$= \cos^{-1}(1.46/1.48)$$

$$= \cos^{-1}(0.9864864864865)$$

$$= 9.43000^{o}, \text{ [source: 20].}$$

If the angle of incidence is greater than the critical angle, then there will be no angle of refraction. This means that if the light entering the cable hits the core –to – cladding interfaces at an angle greater than the critical angle, it will be reflected back to the core. But if it hits at an angle less than the critical angle, attenuation occurs and the full signal will never reach the receiver.

Attenuation in fibre optics occurs when there is loss to optical power as the light makes its way down the cable. If the light hits impurities in the glass, it will scatter or be absorbed. Extrinsic attenuation may be caused by microbending or macrobending, [21].

Fibre optics use very thin strands of glass or plastic to transmit communication signals. Because they are light based, and data transmitted through them at the speed of light, and they are capable of handling vast amount of data in a much shorter time than copper cable. These light signals use various colours of light (frequencies) as carriers of data. Each colour of light can have multiple hues (sub-frequencies) as separate carriers also, and can carry information for thousands of miles. One strand of fibre carries as much information as 1000 copper cables, making it more efficient and cost effective method of transmitting data over long distances, [19].

2.9 How Wireless Communications Work.

Wireless communication converts data it transmits into electromagnetic waves for broadcasting. Wireless broadband connects homes or business to the internet using a radio link between the customer's location and service provider's station. Wireless technology uses long-range directional equipment to provide broadband service in remote and urban areas with an external antenna being needed. Wireless broadband can be fixed or mobile. The fixed wireless broadband allows the users to access the internet from a fixed point and often require a direct line of sight between the transmitter and the receiver e.g. Wimax802.16d, while the mobile wireless include the Wi-Fi network. Wireless Local Area Network (WLAN) provides wireless broadband access over shorter distances and are often used to extend the reach of wire line or fixed wireless broadband connection within home, organization and campus environment.

Wi-Fi networks use unlicensed devices to provide internet and can be designed for private access for home, or business, or public Internet access as ''Hotspots'' such as campuses, hotels, airports, city parks e.t.c. The Wi-Fi operates at the frequency band of 2.4GHz or 5GHz and support services close to what wired LANs offer (eg. Ethernet). A Wi-Fi enabled device such as a personal computer, mobile phone, etc can connect to the Internet if they are within the range of wireless network connected to Internet. The coverage of one or more interconnected to access point (Hotspot) can be for few rooms or for many square miles covered by access points with overlapping coverage.

Wi-Fi technology can be deployed in mesh configuration, (wireless mesh network) which allows for continuous connection and reconfiguration around broken or blocked paths by ''hopping'' from node to node until the destination is reached. Wi-Fi networks range by design. A typical wireless router using 802.11b or 802.11g with a stock antenna might have a range of 32m (120ft) indoors and 95m (300ft) outdoors. In general, Wi-Fi performance decreases roughly quadratically as distance increases at constant radiation levels. However, by using directional antennas within Line Of Sight (LOS), outdoor ranges can be improved. The Wi-Fi technology can be enhanced and extended by the use of; high gain and MIMO antennas and protocol hacking.

MIMO and High Gain Antennas: A long range Wi-Fi for wireless Metropolitan Area Network uses high gain outdoor directional antennae to establish point-to-point links between fixed points in the system. Using dual antennas with orthogonal polarities along with a 2 x 2 MIMO chipset effectively enable two different carriers' signals to be sent and received along the same long distance path. High gain antenna may be of many designs, but all transmission of narrow signal beam over distance of several kilometres, usually nulling out nearby interference

sources. Another way to extend range is by using power amplifier, commonly known as "range extender amplifiers", which supply around ½ watt of power to the antenna. This amplifier can give more than five times the range of an existing network.

Protocol Hacking: This involves modifying the standard IEEE 802.11 protocol stacks to make them more suitable for long distance, point-to-point usage. This has the risk of breaking interoperability with other Wi-Fi devices and suffes inference from transmitters located near the antenna.

Packet Fragmentation is also used to improve throughput in noisy/congested situations.

3.0 DISCUSSION

This comparative study of fibres optics and wireless technologies in internet connectivity has been presented under two broad topics viz: the similarities and differences between fibre optics and wireless technologies.

Differences between Wireless and Optic Fibre Technologies.

This study presented the difference between Wireless and Optic Fibre Technologies under nineteen (19) key factors as presented in table 1.

Table 1: comparism of wireless and optic fibre technologies

S/	Factor	Optic fibr technology	Wireless technolog
1.	Bandwidth	Bandwidth is bett utilized	Bandwidth is share
2.	Quality of Service (QoS	QoS is better fibre optic	QoS is not as good as in fibre
3.	Efficiency	Fibre is more efficien	Wireless is efficient as fibre
4.	Installation cost	Cost of installing fibre is quiet higher than wireless.	Here wireless has a decisive advantage over fibre
5.	Operation Co	There is recurring costs beyond the installation costs	The extra cost aft installation is less in wireless.
6.	Maintenance Cost	Maintaining connection in fibre cost higher	To maintain connection in wireless is lower
7.	Build–Out Strategies	Adding new access points amounts to extra cost.	New access points can always be added with little or no extra cost.
8.	Network Scalability	Scalability depends on the initial plan of the network	Scalability depends on the load on the base stations and the backhaul
9.	Interference	Fiber uses light waves which is affected by EMI	Wireless uses unlicensed spectrum which is affected by EMI
10	Data Security	Data interception is highly low if not impossible in fiber	Data interception is inherent in wireless technologies.
11	Mobility and Interoperabili	Fiber has interoperability problem because of the wire.	Wireless allows for mobility and interoperability with other devices.
12	Network Coverage	Fiber optics can provide higher network coverage of about 40km or more	Wireless signal degrades with distance and hence can cover a distance of 30 miles.
13	Transmission Speed	Fiber can transmit with a speed as much as 10GE/100m bps	Wireless can transmit with a speed of 30mbps at maximum.
14	Application Support	Fiber can be employed in all layers of a network including access, distribution and backbone	Wireless can only be used as business application and not as a backbone.
15	Health Hazar	Fiber is safer as the light signals transmitted by them are fully contained within the fiber coating with no electromagnetic field or hazardous radiation coming out from them	Wireless technology predisposes people to several diseases like radio frequency sickness, radio wave sickness, microwave sickness, carcinogen, Alzheimer's disease, multiple sclerosis, autism, diabetes, asthma, ADHD, cardiac rhythm and function etc.
16	Environmenta friendliness,	Microwave radiation from wireless can cause reproductive, navigational and health problems for birds, bees, bats and other terrestrial animals. Also too much exposure to Wi-Fi and radiation from antennas causes and barks fissures.	Fiber can cause trending and land breaking, tar cutting, destruction of commercial trees etc especially during installation.
17	Energy Efficiency Mgt.	Fiber optic has better energy efficiency because it uses substantially less energy and does not expose wildlife and vegetation to	Wireless is less energy efficient and can expose wildlife and vegetation to radiation.

		radiation.	
18	Legal and Regulatory Issues	Fiber has legal/regulatory issues pertaining rights of way and pole attachments.	Wireless providers face legal/regulatory issues of unlicensed and licensed spectrum.

4.0 CONCLUSION

This research shows that optic fibre and wireless technologies are complementary to each other. Fiber is always an essential supporting infrastructure for wireless and its real strength lies closer to the core of the network than at the edges. The ultimate goal of any connectivity option should be to have ubiquitous, differentiated network where users can choose the delivery technology that best suits their needs.

Fiber optics provide high data rate in gigabyte per second with good quality link, but it is always expensive when compared to other technologies, and susceptible to many physical (though accidental) attacks. When there is budgeting constraints, wireless technologies, especially WiMax are suitable for implementing a MAN but with a limited data rate of not more than 30 megabyte per second and smaller number of users. The choice of which technology to adopt is definitely and highly depend on the consideration, constraints and priority of the user. For instance, if there is budget or funding constraints the choice of wireless connectivity wiould be favoured, but if there is enough fund, fibre optics is by far a better choice as it provides better quality of service, better bandwidth management and greater number of users.

Both fiber and wireless technologies despite their advantages are still faced with several security issues. Wireless communication network battle with security issues like eavesdropping, wireless sniffing, Denial of Service (DoS), Traffic Redirection, Rogue Access Point, Bandwidth overloading, Electromagnetic Interference, etc, while fibre optics technology have high labour cost, high legal and regulation issue, fiber cut and tapping, etc to contend with.

It is worthy to mention that where users are low and funding is the case including rural areas with difficult terrain; wireless technology is the way to go. However, when there is funding problem and the number of user are high with the network coverage expected to be quite large; fiber optics technology is the answer.

In terms of security of the network, the wireless is inadvertently subjected to various vulnerabilities and security issues. Fiber optics on the other hand always has physical attack and accidental security issues associated with it. Hence, it is almost impossible to have a perfect secured network.

Therefore, the notable practice when making the choice of which technology to implement is always for the need of the user to be placed side by side with the user's priority and constraints.

5.0 REFERENCES

[1.] ARC Electronics. "Brief Overview of Fiber Optic Cable Advantages over copper". The basics of fiber optic cable- an unpublished tutorial. from *http//www.arcelect.com/fibercable.htm* assessed 12/12/2015.

[2.] http://www.businessweek.com/magazine/content/11_09/b4217033849315.htm

[3.] Onu, F. U., Ugwu, I. O. and Okpara C., (2007) Fundamentals of Computer Studies revised edition Copy craft int'l company Ltd. Abakaliki Nigeria pp 224-246.

[4.] http://www.wirtel.co.uk/article_africa_2005_q3_001_alvarion.htm

[5.] Bruno Puzzolante, G. R.c (2006). Nationwide Implementation of a WiMax Mobile Access Network.

[6.] Khan, F., (2009). LTE for 4G Mobile Broadband: Air Interface Technologies and Performance.

[7.] ISO, (2005). "Information Technology-Security Techniques-Code of Practices for Information Security Management.

[8.] Moore, L., (2006). Wireless Technology and Spectrum Demand: Advanced Wireless Services. Congressional Report for Congress.

[9.] Homeland Security, (2006). "Wireless Communication Security"

[10.] Hamid, R. A., (2003).Wireless LAN: "Security Issues and Solutions".

[11.] Sing, G., (2012). Security Issues in Wireless Local Area Network (WLAN).

[12.] US-CERT, (2008). " Using Wireless Technology Securely a government organization". http://www.us-cert.gov/reading_room/home-network-security/> (2014).

[13.] Miller, K. S., (2001). Facing the Challenges of Wireless Security. Technology News **17**

[14.] SANS Institute (2003). An overview of Wireless Security Issues.

[15.] Sovoboda, E., (2005). Code Breakers Stumped by Photon-based System: *Discovery*. **33**

Vol. **26** No. 1.

[16.] Tapanes, E. and Carroll, D., (2010). "Securing Fiber Optics Communication Link against Tapping". Foptic Secure Link- White paper. Available at http/www.fft.com.au/products assessed on 21/12/2015.

[17.] Snawerdt, P., (2002). Phase-Modulated Fiber Optic Telecommunications System.

[18.] Book, E., (2002). "Info-Tech Industry Targets Diverse Threats. Fears of Network Vulnerability fuel market for improving security systems". http://www.americantechsupply.com/fiberopticsecurity.htm.

[19.] Fiber Optic Association, (2004). "Understanding Fiber Optic Communications" available at http:www.thefoa.org/ppt assessed on 12/1/2016.

[20.] Oyster Optics, Inc., (2003). Securing Fiber Optic Communication against Optical Tapping.

[21.] "White Paper on optical taps and various solutions" available at http:www.oysteroptics. com/index resources.html assessed on 3/1/2016.

[22.] Alwayn Virek., (2004). "The Physics behind fiber optics and Fiber Technologies, availabe at

http/www.ciscopress.com/articles/article.asp retrieved on 22/12/2015.

[23.] Corning Incorporated, (2005). "Basic Principles of Fiber Optics", *Corning Cable System:* availabe at http://www.corningcablesystems.com/web/college/fiber tutorial.nsf/apprin?OpenForm retrieved on 11/11/2015.

[24.] Connect Africa Summit 2007, Kigali, Rwanda; availabe at http//www.itu.int/ITU-D/connect/Africa/2007/summit/pdf/s2_background.pdf retrieved on 23/11/2015.

[25.] Finke II, L. G., (2000). "Wireless Communication: A modern Necessity". *Journal of Information Technology* **63**, (*5*).

[26.] Chuah, M., and Zhang, Q., (2006). Design and Performance of 3G Wireless Network and Wireless LANs. USA: Springer.

[27.] Du, K., and Swamy, M. N. S., (2009). Wireless Communication System: From RF Subsystems to 4G Enabling Technologies. London: Cambridge University press.

[28.] Chen, L. and Zheng, L., (2012). "A concentrated-grant-based bandwidth allocation algorithm for Ethernet passive optical networks," in Proceedings of the Symposium on Photonics and Optoelectronics (SOPO '12), pp. 1–4.