International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 5 Issue 7|| July 2016 || PP. 36-41

Review of the Security Challenges of Fiber Optics Technologies in Network Connection in Nigeria and the Countermeasures.

Ikporo, Stephen Chibueze[1], Ogbu, Nwani Henry[2]
[1]*Department Of Computer Science, Ebonyi State University, Abakaliki – Nigeria*
[2]*Department Of Computer Science, Ebonyi State University, Abakaliki – Nigeria*

Abstract: *The increasing number of people who transfer data from one place to another daily demands that the telecom industries develop a sophisticated strategy to guaranty quality data transferred without compromise or interception. Some of these industries in a bid to meet up with this demand employ any means of data transfer possible to them. Internet connectivity requires physical transfer of data from one place to another. This can be achieved either through wire or wirelessly. Connection through wire could be by UTP, Coaxial or Fiber Optics. Experience showed that wired is more advantageous when considering bandwidth utilization, performance, reliability, resiliency and security, many people are toeing this way and fiber optics their major choice. Fiber optics can be bundled as cable and used for data transmission through which light propagates with little attenuation, which makes it advantageous for long distance communication. The massive choice of fiber optics of recent has increase the security challenges bedevilling it, as it is now the prime target of network attackers. This has increased its vulnerability. Fiber optic is experiencing some security issues like splicing, clamping, cutting and tapping in developing countries like Nigeria. The paper tries to evaluate the security challenges bedevilling the optic fiber*

Keywords: *Network, Bandwidth technology in Nigeria so as to propose possible countermeasures. , Fiber Optics, Internet Layer Security, Attenuation.*

I. Introduction

The high economical development associated with the broadband build up and development requires state-of-the-art broadband connections to be realized. Systems such as video conferencing, distance education, academic research and remote surgeries, all demand large amount of bandwidth, speed, efficiency and great reliability.

Notwithstanding the substantial and improved investment already made in ICT infrastructure in some parts of the world especially Africa in recent years, much focus has always been on the improvement of the mobile network infrastructure and access with appreciable gaps still remaining in the backbone networks. This has led to a very high expensive or non unavailability of effective high-speed Internet services needed for important key business, government and consumer applications. Where available, the cost of broadband Internet access is on the average, three times higher than what is obtainable in other part of the world, where significant broadband infrastructure investments have been made.

Data transmission is made possible by the combination of the medium and the active devices that make up the network. Most of the recent generations of emerging wireless communications standard utilize improved modulation techniques to squeeze more bandwidth out of frequency. In practice, there is a trade off between frequency and data-carrying capacity, such that as we lower the frequency, we lose total bandwidth. However, the total bandwidth achieved by wireless technologies, especially the ones using the unlicensed spectrum, are still orders of magnitude behind what is possible with Fiber. Whereas most unlicensed wireless setups can deliver bandwidths of multiple megabits per second, most advanced Fiber optic connections can deliver multiple gigabits per second.

The downstream bandwidth in mbps, the upstream bandwidth, as well as the Quality of Service (QoS) are all important factors for the sustainability of a connection for a particular application. In application, Fiber optic connection provides better QoS because of the dedicated link it provides between two communicating points.

II. Literature Review

Fiber Optics is a flexible thin filament of glass (silicon glass) that can accept electrical signals as input and covert them into optical (light) signals which are reconverted to electrical signals at its destination. They are non-metallic and not susceptible to interference, such as electromagnetic interference (EMI), radio frequency (RF) or lightning. It does not conduct electricity, which means that fiber can be installed in many more types of areas that are prone to such interferences. They are typically smaller and lighter in weight and are practically impervious to outdoor atmospheric conditions. Since there is no radiation from fiber, it is hard to tap than copper, and with no issues of grounding, shorting or crosstalk of cables. They carry much more information than conventional copper wire and are generally not subjected to retransmission of signals. 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 can be regenerated (boosted), [8].
Optical fiber (or "fiber optic") is the medium and the technology which transmits information as light pulses along a glass or plastic strand or fiber. Optical fiber carries much more information than conventional copper wire and is in general not subject to electromagnetic interference and the need to retransmit signals. Most telephone company long-distance lines are now made of optical fiber. Transmission over an optical fiber cable requires repeaters at distance intervals, [4].
It has a cylindrical shape and consists of concentric sections: the Core, the Cladding, the Buffer, the Amor and the Jacket as shown in the figure 1 below.

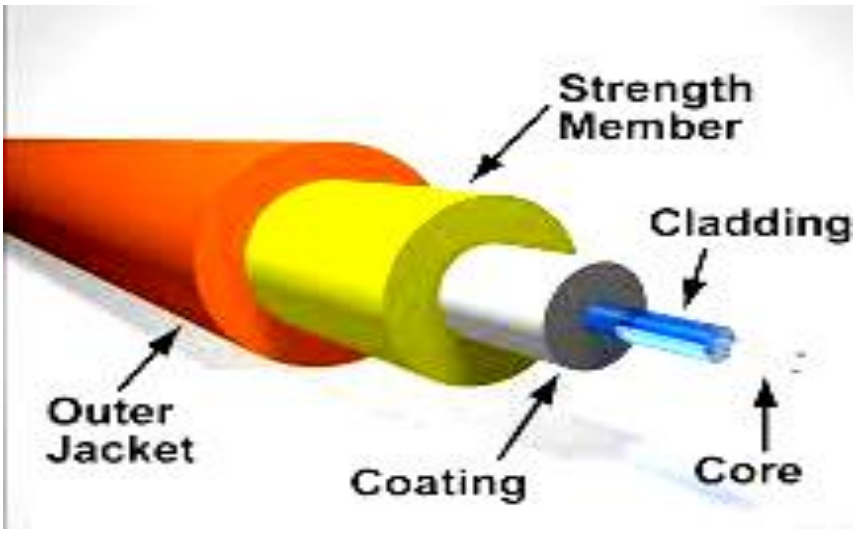

Figure 1: A Sample Optic Fiber cable.
Source: thorlabs.com.

- **The Core:** This 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:** Cladding 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, [10].

The glass fiber requires more protection within an outer cable than copper. For these reasons and because the installation of any new cabling is labor-intensive, the security of optic fiber need not be compromised. Fiber can be deployed as single mode fiber and used for longer distances or multimode fiber and used for shorter distances
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 2 below. Generally, one core is used for transmission (TX) and the other core for Reception (RX), [10].

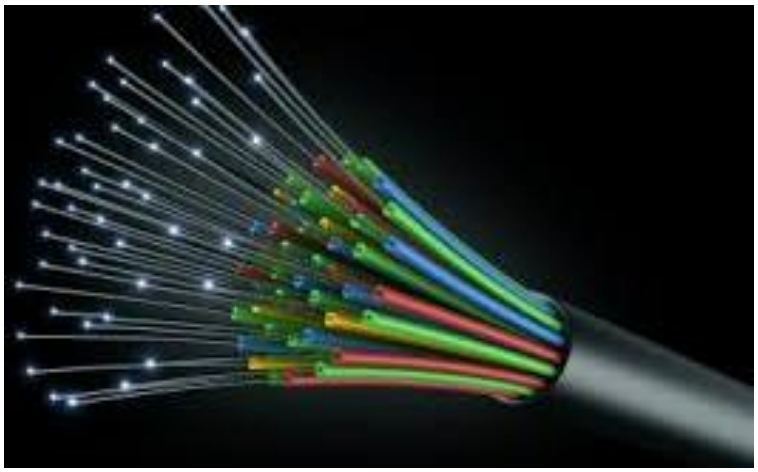

Figure 2: Sample of Optic Fiber with several strands of fiber.
Source: tele-source.com.

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, [6].
- **The Technology Of Fiber Optics:** Fiber Optics technology converts electrical signals carrying data to light and sends the light through transparent glass fiber 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, [11].

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, [11].

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 $QC = Cos^{-1}(n2/n1)$. 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,

$QC = Cos^{-1}(n2/n1) = Cos^{-1}(1.46/1.48)$

$= Cos^{-1}(0.9864864864865) = 9.43000^{o}$, [11].

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, [10].

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, 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, [4].

Security Issues With Fiber Optics

Before now, many researchers had opined that fiber is almost as easy to tap as copper. Today, there are millions of miles of fiber cable spanning across the globe with unimaginable amount of data being transmitted across them daily including sensitive government data, personal, organisation, financial and medical information. The security of these fiber cables have been a subject of discourse to many researchers. The security in fiber optics is basically grouped into: Physical Layer Security and Data Layer Security, [6].

- **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, packet 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, [4]. 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 includes;
- **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, [4]. This is mostly more pronounced on lowers speed data rates than higher data rates.

According to [4], 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, [4].

III. Security Measures In Optic Fiber Communication.

There are some measures deployed as security counter measure in fiber optics communication. These includes,

- **Foptic 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 to using this technique is that, it is not necessary for optical losses to occur in order for the technique to sense disturbances, [12].
- **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, [14].

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, [6].

- **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, [7].
- **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, [4].

IV. Conclusion

Fiber serves as an essential supporting infrastructure for wireless and other network and has real strength lies closer to the core of the network than that at the edges. It provides high data rate in gigabyte per second with good quality link, but it is always expensive when compared to other technologies. However, in recent times Fiber optics has been subjected to many security challenges which made them to be susceptible to many physical attack and accidents which include; fiber cut and tapping, fiber clamping and fiber splicing, etc.

References

[1]. Aikaterini, A. V., Security of IEEE 802.16 Royal Technologies, (2006).

[2]. ARC Electronics, "Brief Overview of Fiber Optic Cable Advantages over copper". The basics of fiber optic cable- an unpublished tutorial, (2015). URL: http//www.arcelect.com/ fibercable.htm.

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

[4]. Fiber Optic Association, (2004). "Understanding Fiber Optic Communications". URL:

[5]. http:www.thefoa.org/ppt.

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

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

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

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

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

[11]. Oyster Optics, Inc., Securing Fiber Optic Communication against Optical Tapping. "White Paper on optical taps and various solutions", (2003). available at http:www.oysteroptics. com/index resources.html assessed on 3/1/2016.

[12]. Alwayn Virek., "The Physics behind fiber optics and Fiber Technologies, (2004). Available at http/www.ciscopress.com/articles/article.asp retrieved on 22/12/2015.

[13]. Corning Incorporated, "Basic Principles of Fiber Optics", Corning Cable System, (2005). Available at http://www.corningcablesystems.com/web/college/fibertutorial.nsf/apprin? Open Form retrieved on 11/11/2015.

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

[15]. Sovoboda, E., Code Breakers Stumped by Photon-based System: (2005). Discovery. 33. Vol. 26 No. 1.