Source based Security Issues in WDM Systems

A. Antwiwaa, A. Kumar, A. K Jaiswal
Department of Electronics and Communication Engineering, Sam HigginBottom University of Agriculture Science and Technology, India

Article Info

Article history:

Received Mar 28, 2017
Revised Jun 6, 2017
Accepted Jun 20, 2017

Keyword:

Adversary
Attack
Clone
Security
Source based

ABSTRACT

The issue of security has become a bigger heddle for all telecommunication companies to climb in this era where information hungry customers are increasing daily. Unauthorized users are finding novel ways of accessing information of others and thereby attacking the requisite legitimate users' information accounting to security threats. In this work, two forms of WDM system attacks will be considered. These attacks include a clone source based attack where the adversary tries to replicate the transmitted signal of the legitimate user by transmitting at the same wavelength and power and the different wavelength source based attack where the adversary transmit at a wavelength different from that of the legitimate user thereby creating interaction effects igniting security issues. Finally, a simulation of the outcome will be considered and the resulting output will be analyzed.

Corresponding Author:

Anita Antwiwaa,
Department of Electronics and Communication Engineering,
Sam Higgin Bottom University of Agriculture Technology and Science,
211007, Allahabad, Rewa Road, India.
Email: anitaantwiwaa@yahoo.com

1. INTRODUCTION

Wavelength division multiplexing (WDM) has the capability of transmitting onto a single optical fiber multiple number of signals with different wavelength. Different information channels can be added or extracted at different location by employing the services of add/drop multiplexer. This adds flexibility to the WDM system [1-3].

WDM system upon its numerous advantages also faces a lot of security threats. Security has become a major concern to today's telecommunication. Companies are striving to find ways of protecting the integrity of the data of their customers. Amidst all strives, data theft has increased exponentially within the years. Several review literatures in [4-8] have discussed some theoretical methods which can be used to detect some attacks which an attacker can inflict upon the infrastructure of an all optical network. The attacks considered include traffic analysis, data delay, service denial, eavesdropping, quality of service degradation and spoofing. Attacks has been categorized into 3 types [9-11] namely direct attack where the attacker aims at the transmission network, optical amplifiers and optical transmission to cause jamming, gain competition and fiber cut respectively. The attacker can also aim at certain network elements to cause indirect cross talk, unauthorized access through the use of add/drop ports and intentional crosstalk propagation from preceding blocks and this is known as indirect attack. The last category is where the anomalies caused by the significant changes in the quality of signal mimic an adversary but they are actually not an adversary. This is called pseudo-attacks. Figure 1 represents a direct attack where the intruder's signal has affected other legitimate users who do not share common physical components via cross talk [9].

This work will consider a source based attack (SBA) where the attacker capitalizes on the input source within a particular network.

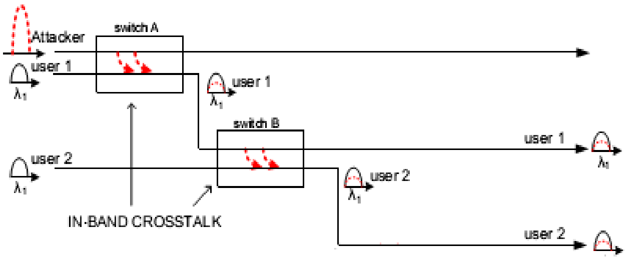


Figure 1. Direct attack via in-band cross talk.

2. OVERVIEW OF WDM

The increase of the demand for data has called for an increase in the data carrying capacity of the network as well as an increase in the speed and the quality of service of the network. There is therefore a need for a technology which can utilize the existing devices by making use of the channel. WDM multiplexes multiple optical carrier signals onto a single fiber via the use of different optical wavelengths.

Figure 2 represents a WDM system which transmits and receives five different wavelengths. Increasing the number of wavelengths of the channel can lead to decrease in channel spacing. The decrease in the channel spacing breeds four-wave mixing (FWM) and cross phase modulation (XPM) which is triggered by impairments due to non-linearity of the fiber [12]. These impairments affects the overall performance of the system and create loopholes for security vulnerabilities of the network.

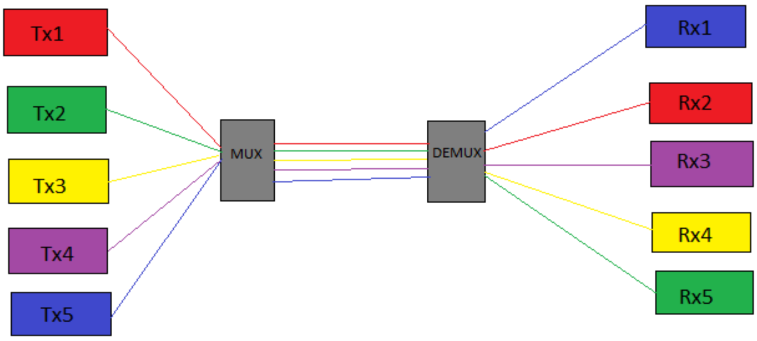


Figure 2. WDM system with five transmitters and five receivers

3. EXISTING ATTACKS AND ITS EFFECT ON WDM SYSTEMS

There are various forms of attacks that can effect a WDM system. Some of these attacks have adverse effect on WDM systems to the extent of causing service distruption. These attacks will be reviewed in this section.

Attacks was studied under three categories [8] by considering All optical Network (AON). These attacks includes In-band Jamming method where the attacker interfer with the signal to reduce the effeciency of the network thereby causing service distruption. The second method considered was an out-of-band jamming method where the attacker reduces the efficiency of the communication signal component via making use of the leaky components or cross-modulation effect to cause service disruption. Finally, the author considered an unauthorized observation where the crosstalk leaking from adjcent signal is listened by the attacker using a shared resources in order to access the information transmitted. This method leads to eavesdropping.

Another form of attack is as a result of the expliotatation of the characteristics of the various components in WDM system [9]. Some of the components considered were the optical fiber and the amplifiers. Tapping was performed by explioting the non-linearities of the fiber using a cross-phase modulation and Raman effect which has the tendency of causing amplification or attenuation of signal on one wavelength by the adjacent wavelength. It was deduced that an attacker can take advantage of the crosstalk effects and propagate a malicious signal unto the fiber which can decrease the quality of service. Gain compensation was also used as a means of attack by injecting a signal with different wavelength into the fiber during the pumping stage and the injected signal will be amplified indiscriminately with the orignal signal causing denial of service.

Timing analysis attack is also another form of attack which considers the side channels of a network and it entails the total time involved to complete a critical action [13]. A type of attack considered was Bernstein's timing attack were the security key was identified by comparing the cipher text which is achieved by the server time stamping and encrypting it using servers key and adding time stamp with the server's received ciphertext.

These existing attacks affects the WDM system adversely but they all make use of the non-linearity effect of WDM channel. The next session discusses novel form of attack in WDM system which does not utilize the vulnerabilities of WDM non-linearities.

4. SOURCE BASED ATTACK

Fiber network was considered as very secured but intruders are constantly working hard to access unauthorized information from the network. In this section, we propose two novel form of attacks which can affect the performance of the WDM system. A WDM network has several transmitters which operates at different wavelengths. The output of the transmitters are multiplexed onto a single channel. At a point in time if a particular transmitter is free, an adversary from within the network can capitalized on that idle period and attack the network. This adversary can pretend to be a legitimate user by transmitting information at a particular wavelength. The wavelength can go a long way to create interference with the ongoing transmission depending on the wavelength transmitted by the intruder. This can cause the signal strength to reduce thereby causing a denial of signal as well as creating four-wave mixing effect and cross phase modulation effect as a result of the nonlinear effect in the medium. This form of attack can be termed as source based attack (SBA). In the SBA attack, an adversary can act as a clone transmitter by transmitting information of the same wavelength, power, phase, amplitude etc. Since the clone and the legitimate signals are the same, after multiplexing, it will be very difficult for the receiver to distinguish between the two signals hence putting the legitimate user's signal at risk. The adversary can also transmit a signal at a wavelength and power either higher or lower than the legitimate user.

The channel condition will determine the absence or presence of nonlinear effects and these effects can create security vulnerabilities thereby putting the legitimate user's signal at risk. Figure 3 represents a simulation of a WDM SBA at a distance of 631.72Km with 0.2dB/Km fiber attenuation. Section IV will discuss the simulation results obtained from the WDM SBA diagram in Figure 3.

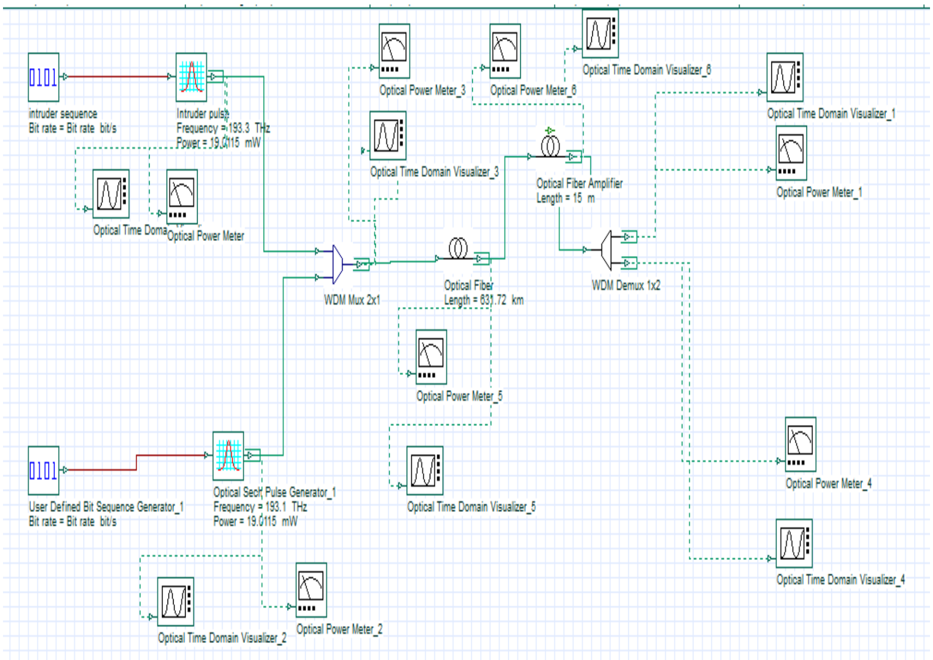


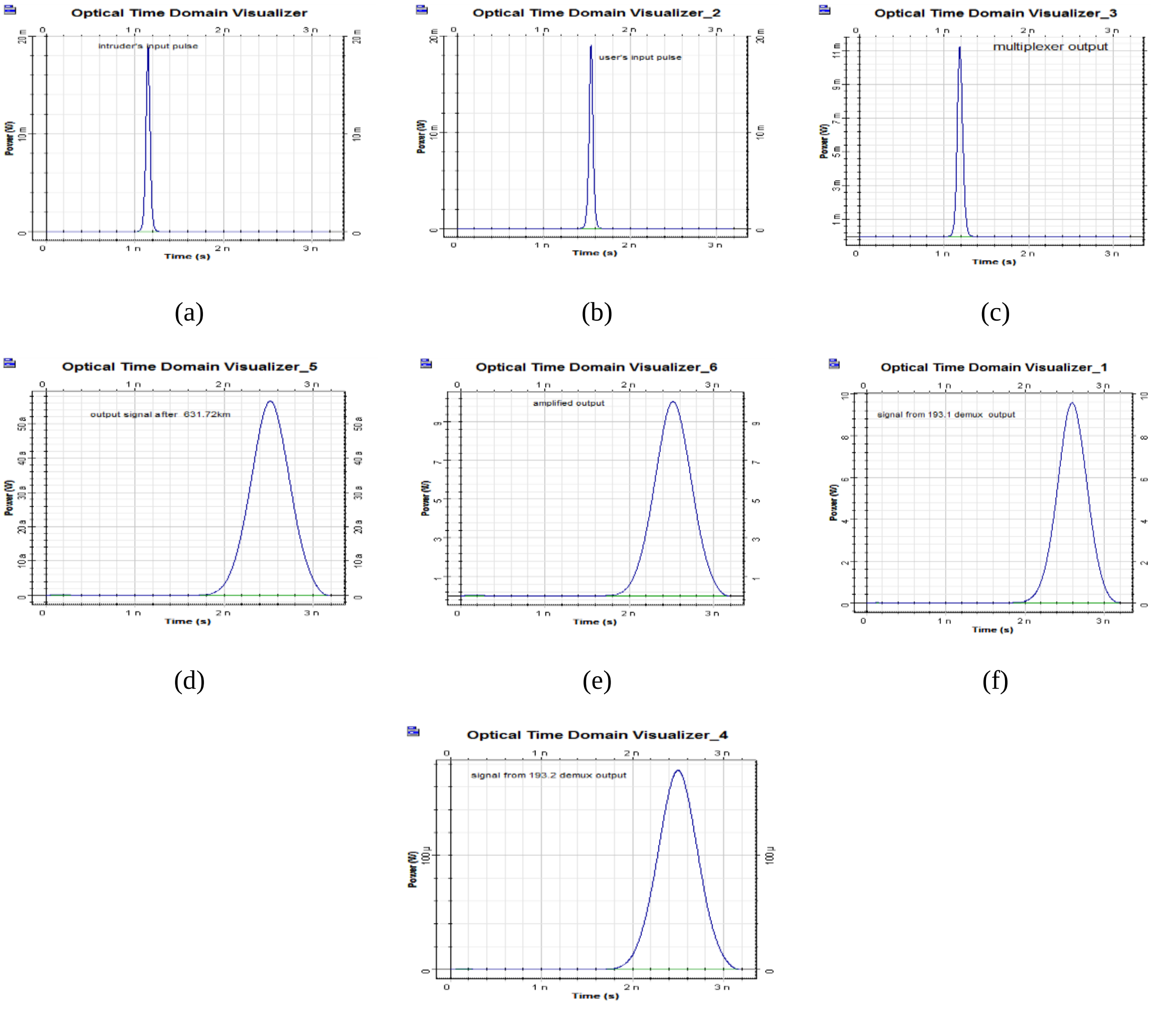
Figure 3. Simulation of WDM SBA at fiber length of 631.72Km

5. WDM SBA SIMULATION RESULTS

The WDM SBA simulation step up consist of two optical sources, a 2x1 WDM multiplexer , an optical fiber length of 631.72Km with 0.2dB/Km attenuation, 15m length optical amplifier and a 1x2 WDM demultiplexer with a 193.1 and 193.2THz output ports.

5.1. Clone Source based Attack (CSBA)

The adversary mimic the characteristics of the legitimate user and attack the WDM system by using the same frequency of operation and the input power as that of the legitimate user. The adversary used the same wavelength and power as that of the legitimate user. The adversary acts like a clone user. The wavelength used was 193.1THz and input signal power of 19.00115mw. The results are shown in Figure 4(a) to 4(g). Figure 4(a) and 4(b) represents the signal of the adversary and the legitimate user respectively. Both users are transmitting at the same wavelength and power but different bit sequence assuming that the frequency of transmission is known to the adversary but the bit sequence is unknow. The generated signals are multiplexed resulting in the output of Figure 4(c). The multiplexed output shows that the multiplexer sees both signals as the same signal since they have the same wavelength and power. This cause a power decrease from initial 19.00115mW to 11.000mW which is about 57.8% decrease. The adversary and the legitimate user's signal are added up by the multiplexer to produce a single pulse and transmitted along the channel.



(a)

(b)

(c)

(d)

(e)

(f)

(g)

Figure 4. (a) Input signal transmitted by the adversary, (b. Signal transmitted by the legitimate user, (c) Multiplexed output of both the user's and adversary signal, (d) Signal after travelling for 631.72km, (e) Amplified signal, (f) Demultiplexed signal at port 193.1 THz, (g) Demultiplexed signal at port 193.2THz

Due to the effect of the various channel impairments, the multiplexed signal has suffered a drastic decrease in signal power after 631.72Km as shown in Figure 4(d). Moreover, the signal has been affected by pulse broadening effect. The mixing of these two signals with different bit sequences can lead to service deniel and disruption because of the presence of channel interference and will result in a significant change in the demultiplexed bit sequence thereby causing a change in the bit sequence of the legitimate user. Eavesdropping is a possible occurrence because of the effect of pulse broadening which can cause a crosstalk in the adjacent channel. The decreased signal power is then amplified and the outcome of the amplification is shown in Figure 4(e). The amplified signal output is demultiplexed by 1x2 demultiplexer with 193.1 and 193.2 THz wavelengths. The output is shown in figure 4f and 4g respectively. The output results shows that both signals are the same. The resultant output signal is affected by pulse boardening effect which will eventually affect the pulse sequence.

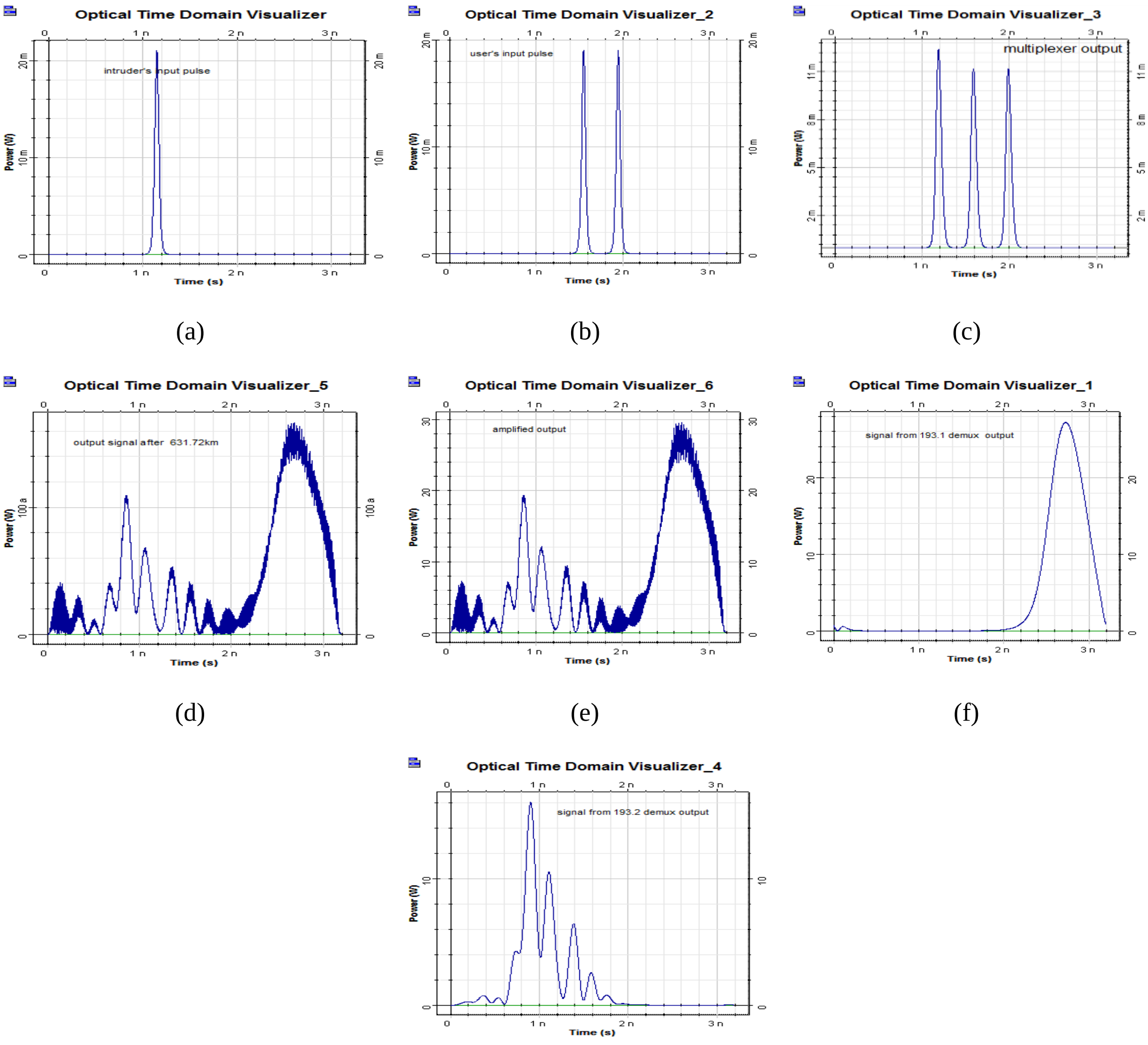
Comparing the clone based attack with the existing attacks reviewed in section 4, this attack has the capability of producing all the existing forms of attacks and has a serious implication on the network.This shows that, a clone based source attack has a crucial effect on the security of the legitimate user's signal. The adversary can easily intercept the legitimate user's signal in CSBA thereby causing a service disruption, eavesdropping and service denial. These bring the network to a compromise and the integrity of the resutant signal wil be at stake.

5.2. Different Wavelengths Source Based Attack (DWSBA)

This type of attack assumes that the adversary does not know the operating wavelength of the legitmate user, therefore a different wavelegth was used by the adversary. In this work the adversary and the legitimate user's wavelengths were 193.1 and 193.2THz respectively. The adversary's 193.1THz and the legitimate user's 193.2THz transmitted signals are represented in Figure 5(a) and 5(b) respectively. Both users have different bit sequence but the same power. The multiplexed ouput is represented in Figure 5(c). Since they are of different wavelength the are copropagating in the channel and they are easily distinquishable. The impairments in the channel has caused signals to interact with each other. This interaction has triggered a fourwave mixing effect and a pulse broadening effect. The outcome is represented in Figure 5(d) where multiple pulses have evolved and spectrum to has widden. This FWM effect has caused the adversary's signal to interact with the legitimate user's signal. The decreased in signal power with time demands an amplification. Figure 5(e) represents the amplified signal after 631.72Km. The resultant output signal is separate by the 1x2 demultiplexer according the wavelength at the port. The adversary's signal output was detected by the 193.1 THz port and it is shown in figure 5f that the signal received has been affected by pulse broadening and also carried some information belonging to the legitimate user.

The legitimate user on the other hand has been adversly affected by interaction which has ignited a FWM effect. This has caused the signal to degrade greatly. The security of the legitmate user has been compromised because the transmited signal was not received and the adversary has succeeded in intercepting the original signal. FWM effect has distorted the signal completely and the legitimate user's signal now contains part of the adversary's signal. This can cause a service disruption , denial of service as well as eavesdropping. Since the adversary now have access to part of the information of the legitmate user, tapping attack which is aimed gaining unauthorized access to the data and using it for traffic analysis can also be performed by the adversary.

Comparing this attack to the existing attacks reviewed, it has the capability of causing serious treat to the WDM system by causing a denial of service, service disruption, eavesdropping and traffic analysis.



(a) (b) (c)

(d) (e) (f)

(g)

Figure 5. (a)Adversary's input signal at 193.1THz, (b) Legitimate user's input signal at 193.2 THz, (c) Multiplexed output of the adversary and the user's signal, (d)Transmitted signal output, (e) Amplified output signal, (f) Output signal from 193.1 demultipler output, (g) Output signal from 193.2 demultiplexer output port.

6. CONCLUSION

A compromised network has a great impact on the network users and the network operators as well. This undermines the security of the ongoing communication. Confidentiality between communicating parties is very essential in telecommunication. Unauthorized uses are working to find ways and means to access vital information of users. An important loophole in WDM system is the WDM source based attack. WDM source based attack has a great impact on WDM signals. In the presence of channel impairments, the signals suffers from various non-linearity issues which degenerates into various security issues.

The clone source based attack adversely affects the security of a WDM system since the adversary mimics the legitimate user and operates with the same wavelength and power of the legitimate user. This makes it difficult for the receiver to differentiate between the actual signal and the legitimate signal since both signals are the same. It has the capability of producing a service deniel, service disruption and eavesdropping attacks. This makes it this attack a more serious issue of concern. The adversary succeeds in intercepting the legitimate signal thereby affecting the authentication and confidentiality of the received signal.

The DWSBA also causes the signals to be affected by non-linearity effects like pulse broadening and FWM which creates room for security vulnerabilities in WDM. The adversary operates within a frequency which is different from that of the legitimate user. The operating frequency can be either higher or lower than that of the legitimate user. These generated frequencies can either overshadow or drain the legitimate uses signal thereby causing low quality of service, denial of service, eavesdropping and traffic analysis. These attacks has adverse recursions on the transmitted signal therefore methods of detecting and isolating CSBA and DWSBA should be considered in the future works.

REFERENCES

[1] J. M. Senior, S. D. Cusworth, *"Devices for Wavelength Multiplexing and Demultiplexing"*, Optoelectronics, IEEE Proceedings, vol. 136, no. 3, pp. 183- 202, 1989.

[2] E. GerdKeiser, "A Review of WDM Technology and Applications", *Optical Fiber Technology*, vol. 5, pp. 339, 1999.

[3] S. S. Bujari, "A survey on simulation of MEMS optical switch for WDM applications", *World Journal of Science and Technology*, vol. 2, no. 10, pp. 39-43, 2012.

[4] M. M´edard, D. Marquis, S. R. Chinn, *"Attack Detection Methods for all-Optical Networks"*, in Proc. of Network and Distributed Systems Security Symposium, Session 3, paper 2, San Diego, California, 1998.

[5] M. P. Fok, P. R. Prucnal, "All-Optical Encryption based on Interleaved waveband switching modulation for optical network Security," *Opt. Lett*., vol. 34, pp. 1315–1317, Apr. 2009.

[6] M. P. Fok and P. R. Prucnal, "Low-Latency Nonlinear Fiber-based Approach for Data Encryption and Anti-Jamming in Optical Network", presented at the 2008 *IEEE/LEOS Annual Meeting*, Newport Beach, U.S., Nov. 2008, Paper ThG 3.

[7] M.P. Fok, Wang Z., Deng Y, Prucnal P.R. (2011), "Optical Layer Security in Fiber-Optic Networks", *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 3, (September 2011), pp. (725-736), ISSN 1556-6013

[8] M. Médard, D. Marquis, R. A. Barry, Finn S.G. (1997), "Security Issues in All-Optical Networks", *IEEE Network*, vol. 11, no. 3, (May/June 1997), pp. 42-48, ISSN 0890-8044.

[9] M. Furdek, N. Skorin-Kapov, M. Bosiljevac, Z. Sipus, *"Analysis of Crosstalk in Optical Couplers and Associated Vulnerabilities"*, in Proc.33rd Int. Convention (MIPRO), May 2010, pp. 461–466.

[10] J. K. Patel, S. U. Kim, D. H. Su, S. Subramaniam and H.-A. Choi, *"A Framework for Managing Faults and Attacks in WDM Optical Networks"*, Proc. of the DARPA Information Survivability Conference and Exposition, Anaheim, California 2001.

[11] N. M. Yazdani, M. S. Panahi, E. S. Poor, "Intelligent Detection of Intrusion into Database using Extended Classifier Systems", *IAES/IJECE*, vol. 3, no. 5, October 2013, pp. 708-712.

[12] A. M. Adel Saleh, Jane M. Simmons, "Technology and Architecture to Enable the Explosive growth of the Internet," *IEEE Communications Magazine*, pp.126-132, Jan., 2011.

[13] D. R. Rani, S. Venkateswalu, "Security against Timing Analysis Attack", *IAES/IJECE*, vol. 5, no.4, August 2015, pp. 759-764.

BIOGRAPHIES OF AUTHORS

Anita Antwiwaa received her B.E in 2009 from All Nations University, Ghana in Electronics and Communication Engineering and M.Tech. in 2012 from SRM university, India in Communication Systems Engineering. She is currently a PhD candidate in Sam HigginBottom university of Agriculture Technology and Sciences, India in Electronics and Communication. She was a lecturer in All Nations University, Ghana from 2012 to 2014 and her research interest are in the areas of Fiber optics security, Cryptography and coding theory. Ms. Antwiwaa is a member of IEEE, IOP, NSBE and IET Ghana.

Anil Kumar is Asst. Prof. at SHIATS-DU Allahabad. He obtained B. (MMMEC, Gorkhpur) in ECE, M.Tech. (IIT BHU Formerly I T B.H.U.) in Microelectronics Engineering, and PhD from SHIATS-DU India. He guided various projects & research at undergraduate & postgraduate level. He published many research paper in different journals. He has more than 10 years teaching experience and actively involved in research and publications. His area of interest includes Antenna, microwave, artificial neural network and VLSI.

A.K. Jaiswal is Prof. and Head of ECE-Department at SHIATS-DU Allahabad. He obtained M.Sc. in Electronic & Radio Engineering from Allahabad University in 1967. He guided various projects & research at undergraduate & postgraduate level. He has more than 40 years Industrial, research and Teaching experience and actively involved in research and publications. His area of interest includes Optical Networks and satellite communication.