International Innovative Research Journal of Engineering and Technology
ISSN NO: 2456-1983

International Conference on Emerging Innovation in Engineering and Technology
ICEIET-2017

Attack Awareness and Detection in Optical Networks using Zone based Hierarchial Link State Routing and Linear Network Coding

Dr.P.Boobalan[1], S.Salmon Raj[2], Rohit Peri[3], P.Praveen Kumar[4]

[1] Associate Professor,[2]Student Member/IT, Pondicherry Engineering College
boobalanp@pec.edu[1],salmonraj1713@gmail.com[2],rohitperi1995@gmail.com[3],ppravenn08@gmail.com[4]

Abstract— The use of optical networks has become increasingly important in supporting the rapidly growing and evolving global network traffic intensity in a cost-efficient manner. Due to which maintenance of security in optical network becomes a major priority. Due to the high data rates in optical networks which cause the physical-layer attacks. This attack can lead to financial losses to the clients or cause network-wide service disruption, possibly leading to huge data and revenue losses for network operators. Attacks which aim towards disruption of service generally involve insertion of malicious signals or power jamming which can propagate along configured connections causing serious damage. Conventional network survivability approach definitely has led to the detection of malicious node but not helped in it's removal .In this paper we have taken the characteristics of attack groups into consideration and make modifications to the dedicated path protection scheme by incorporating the concept of Zone Based Hierarchical Link State(ZHLS) routing with digital signature where zone network topology was established which help in detection of malicious node along the discovered path remove it and reconstructs the path. Further there was no occurrence of network traffic. To further strengthen the impact of reliability in optical transmission the concept of Linear Network Coding(LNC) was incorporated.

Keywords- Attack Groups, Malicious Signals, Network Traffic, Optical Transmission, Optical Networks, Physical Layer Attack

I. INTRODUCTION

We are witnessing the evolution of optical networks toward highly heterogeneous, flexible networks with a widening area of application. Optical networks have evolved from simple point to-point systems operating on a single wavelength with megabit per second rates over a few kilometres to ultra-long-haul multi terabit systems supporting over a 100 wavelengths per fibre and all-optical transmission schemes. As the bandwidth and reliability performance requirements of mission-critical applications increases, and the amount of carried data grows, issues related to optical network security becomes increasingly important.

Optical networks are vulnerable to several types of attacks at the physical layer, typically aimed at disrupting the service or gaining unauthorized access to carried data. Such security breaches can induce financial losses to clients or loss of privacy, or cause network-wide service disruption, possibly leading to huge data and revenue losses. Awareness of system weaknesses and possible attack methods is a prerequisite for designing effective network security solutions. As optical networks evolve, new and upcoming vulnerabilities must be identified and dealt with efficiency Due to ever increasing bandwidth demands, and new traffic requirements and models whose origin is primarily from the proliferation of cloud services, further enhancements in optical networking are more focussed towards increased dynamicity and flexibility.

Normally physical-layer attacks have been classified based upon the type of damage they cause: service disruption or eavesdropping. There are three types of attacks: 1) Signal insertion attacks, 2) Signal splitting attacks, and 3) Physical infrastructure attacks. Signal insertion attacks actually reduce the quality of transmission of legitimate connections by injecting harmful or malicious signals into the network, causing service degradation (or possibly service denial).Depending on the network topology ,architecture and optical components used, these attacks may propagate through the network, causing system-wide damage, and can appear spontaneously, potentially causing multiple restorations. It may disrupt individual or multiple connection which is traversing a link and typically cause signal degradation. Examples of such attacks are High-Powered Jamming Attacks, Amplifier Transient Attack, and Mixed Modulation Attack.Signal splitting attack are the attacks that split and remove part of a legitimate signal carried in the network for either eavesdropping or Signal degradation purposes. Such attacks may be difficult to detect and locate due to low losses incurred at the insertion point, going undetected by the network management system and/or raising alarms only downstream of the attacking point. It will breach privacy.

Examples of such attacks are tapping attacks and low power Qos attacks. Physical infrastructure attacks include all attacks that physically damage or tamper with the optical network infrastructure such as cutting a fibre, unplugging connections, or damaging optical components. These attacks typically persist until repaired and do not propagate through the network. They can disrupt all connections traversing the affected nodes/links They can often be modelled as single or multiple component faults and require efficient protection and/or restoration mechanisms. Examples of such attacks are Single component Attacks, Disaster like Attack, and critical location Attack.

This paper is more focused towards signal insertion attacks like power jamming, insertion of malicious signals and provide better network security against these attacks. Signal insertion attacks reduce the quality of transmission of legitimate connections by injecting harmful signals into the network, causing service degradation. Depending on the network architecture and optical components used, signal insertion attacks may propagate through the network, causing system-wide damage, and can appear sporadically, potentially incurring multiple restorations. In the existing system they have incorporated the characteristics of these attacks and developed a heuristic algorithm called as DPP (Dedicated Path Protection) scheme which will identify the malicious nodes or signals along the connection path and detects it. If malicious signal or node is not present along that path then that path is assumed to be attack protected. We have analyzed the recent developments in DPP schemes, future trends in optical networks .In this paper, we have taken the characteristics of attack groups into consideration and make modifications to the dedicated path protection scheme by incorporating the concept of ZHLS(Zone Based Hierarchical Link State) routing with digital signature where zone network topology was established which help in detection of malicious node along the discovered path remove it and reconstructs the path.Futher there is no network traffic. To further strengthen the impact of reliability in optical transmission the concept of LNC (Linear Network Coding) has been incorporated. LNC is capable of protecting from both the Jamming and eavesdropping, while addressing the issue of fault tolerance due to optical physical impairments

The paper is organized as follows: Section II describes the related works; Section III describes the overview of proposed system; Section IV is conclusion and finally followed by references in Section V

II. Related Works

This section examines the advances made in optical network technologies with a view to describe and explain the main challenges of this research study. The authors of [1] proposed efficient hybrid survivable schemes offering both high connection availability and low blocking probability. More specifically, they focused on a double link failure scenario and proposed a strategy in which both backup reprovisioning and path restoration are used on top of DPP.

Attack-awareness has been incorporated into the routing and wavelength assignment (WA) process in transparent optical networks to reduce the number of connections that can be affected by a single jamming attack in [2, 3]. Most of the studies [4] in the literature focusses on the issue of survivability to provide protection in the presence of such attacks.

In this they have developed a heuristic approach for survivable WA considering only signal degradation effects of power jamming inside optical switches. To minimize the overall damage of such attacks, the proposed heuristic also minimizes the in-band jamming attack radius of each lightpath. Comparison with generic path protection indicates that considering attacks in the planning process can a priori enhance connection security under high-powered jamming with efficient wavelength-link usage at a small trade-off with the number of wavelengths needed. But still it considers the only the attacking capabilities of the primary attacker, without taking into account the propagation of attacking potential among lightpaths.

The authors of [5] introduced the concept of AGs modelling the compound harmful effects from such attacks in both optical switches and fibres, and proposed a heuristic approach for attack-aware DPP which ensures all connections are attack protected. Furthermore, the proposed attack-survivable routing and wavelength assignment is aimed at reducing the maximum potential damage from these attacks, measured by an objective criterion called Attack Radius, as well as minimizing the number of used wavelengths to be resource-effective. In comparison with generic dedicated path protection without attack awareness, the proposed approach shows a significant enhancement of network survivability in the presence of attacks at a small trade-off of increased wavelength usage.

The authors of [6] investigated infinite jamming attack propagation to find an upper bound on the network vulnerability to such attacks.so they considered a more realistic scenario where crosstalk attacks can spread only via primary and/or secondary attackers and define new objective criteria for wavelength assignment, called the PAR (Primary Attack Radius) and SAR (Secondary Attack Radius),they also formulated the problem variants as integer linear programs (ILPs) with the objectives of minimizing the PAR and SAR values

The authors of [7] developed an ILP formulation for shared path protection again guaranteeing full attack-protection. The results of these studies suggested that obtaining full protection from attacks may increase considerable resource overhead. This indicates that schemes which maximize the degree of protection from attacks while using no extra resources compared to resource-minimizing approaches may represent more economically feasible solutions.

III. Overview of Proposed System

(*Attack Awareness and Detection in Optical Networks using Zone based Hierarchial Link State Routing and Linear Network coding*)

In the proposed approach first we have considered a set of nodes where the source and destination to nodes is assigned. And the communication with the nodes is done by sending packets. Further this packets are send in a two ray ground manner. That means it is a two way communication. Once the packet is sent search for malicious node will start along all the node paths. So through AA-DPP-H algorithm selection for best path will be done .If the best path is not found then it indicates that there is no presence of malicious node but if best path is found it automatically indicates the presence of malicious node. Once the malicious node is detected it must be removed along with the path in which it was detected so network topology will be designed into non overlapping zones and each zone will be having set of nodes.Now each zone will be having access points which will send packets and once this packets are sent the malicious nodes will be detected along with the path and that path will be removed and again it will be reconstructed. And in this eventually network traffic will be removed. Further to strengthen the network against the power jamming we will incorporate the concept of coding technique called LNC (Linear Network Coding).

In our proposed system we are using Fedora 14 version operating system that is installed in VMware in normal windows 10 operating system.A normal generic network simulation can be carried out in ns2 but since we are doing in optical networks. We
will be using a special patch called as OBS (Optical Burst Switching) patch.Optical Burst Switching (OBS) is an optical network technology that aims to improve the use of optical networks resources when compared to optical circuit switching (OCS).OBS is implemented using Wavelength Division Multiplexing (WDM), a data transmission technology that transmits data in an optical fibre by establishing several channels, each channel corresponding to a specific light wavelength.

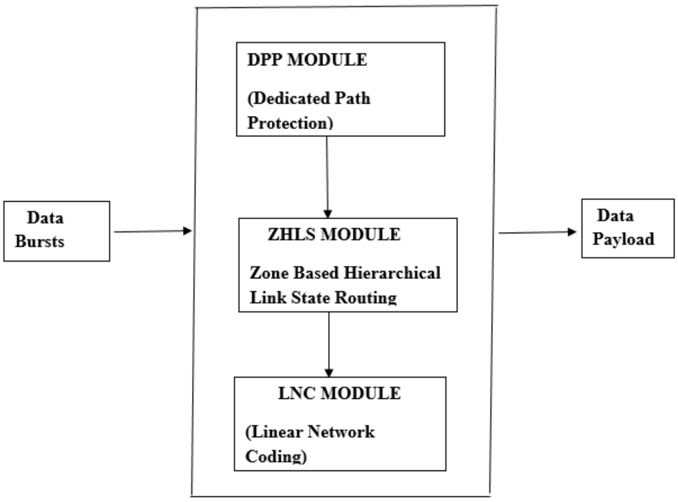

Fig.1 Overview of the proposed system

.

Optical Burst Switching is used in core networks, and viewed as a feasible compromise between the existing Optical Circuit Switching (OCS) and the yet not viable Optical Packet Switching (OPS). In OBS, packets are combined into data bursts at the edge of the network to form the data payload. Optical Burst Switching has several distinctive features: first, the packets are combined in the ingress (input) node, for a very short duration. This allows that packets that have the same constraints, e.g., the same destination address and maybe, the same quality of service requirements are sent together as a burst of data (therefore the term burst in the concept name). When the burst arrives at the egress (output) node, it is disassembled and its constituent packets routed to their destination.

While the burst is being assembled in the ingress node, or possibly, after the burst has been assembled, a control packet (or header packet), containing the routing information for that burst is sent to the network, ahead of the burst. The time that separates the transmission of the control packet and the transmission of the burst is termed the offset time, and it must be long enough to allow all the routers in the predicted path the burst will take, to be configured, and only for the time needed for the burst to cross the network. When the network nodes are configured, the burst departs the ingress node and travels through the network in an all optical form, using the circuit that was previously established by the control packet.

Another characteristic of OBS is that the routing information is transmitted in the Control Packet and is not part of the data burst itself. In fact, the burst crosses the intermediate nodes in the network using the pre-established and preconfigured circuit in an agnostic manner, i.e., the node does not need to interpret the data in the burst, and so, it does not need to know the format of the data in the burst. This is another special feature of OBS. Another distinctive characteristic of OBS is that the Control Packet will undergo optical to electronic to optical conversion at each intermediate node, and also optical to electronic conversion at the egress node, as to allow these nodes to be able to configure its optical switching devices. A final characteristic of OBS networks is that there is what is called a data and control plane separation, i.e., the channel that is used to transmit the control packets is specific and different from the channels that are used to transmit the data bursts.

Our system has three stages.

- Dedicated Path Protection (DPP).
- Zone Based Hierarchical Link State (ZHLS) Routing.
- Linear Network Coding (LNC)

A. Dedicated Path Protection:

Here the search for malicious node will be done along the path.And if it is found then it will make the network aware of the malicious node and this search will be going in an iterative manner till it finds that malicious node.

In this module the optical nodes will be created and placed randomly. During Setup, a network node receives the necessary neighbor discovery phase for discovering and updating one hop neighbors. Source node uses Alert protocol for traversing or searching the path in the network. It starts its searching from the source node and updates one hop neighbors and search continues to reach traffic free path between source node and destination. The traffic pattern tell us the deduce point-to-point traffic volume between each pair of nodes.

We need to discover the actual source or destination in order to discover the traffic pattern. Here probability distribution is used. Probability distribution calculates the probability of the data transmitted to neighboring node which provide an accurate estimation of a node as source or destination. This will help to discover the traffic pattern. Source node route the packets through more stable node to transfer packets to destination. The performance is analyzed through graphical result.

When selecting a path there are some path selection requirements Each link will be given risk ID's. Whether the link is already taken by a primary path. Whether the link is running a protection path. If so, the risk IDs of the primary paths are also known. If many protection paths share this link, the amount of data for this item is potentially large.The maximum number of shared protection paths the link supports. By lowering this number, we can decrease the amount of data for item. If it is desirable to cover node failure, network nodes can also be assigned risk IDs. Finally after all this the algorithm iteratively constructs a feasible solution and updates the incumbent solution if a more secure solution is found. The algorithm ends if a solution where all connections are attack protected is found or the maximal number of iterations is reached. Figure 2 shows the flow diagram for dedicated path protection.

B.Zone Based Hierachial Link State Routing:

The Zone-based Hierarchical Link State (ZHLS) routing is a one of the hybrid routing protocols which creates two routing tables named as inter zone routing table and intra zone routing table. In the earlier module only search for malicious node will be done but here we will be dividing the nodes into three zones which will be overlapping with each other in cluster form, each zone will be having an access point which will be controlling the distribution of nodes in the zones Now each zone will be having a channel header and at the center of the overlapping there will be access point which will communicate via channel header and they will be sending the hello packets. Now the malicious node will be detected along the path the node will be removed and the path will be reconstructed and the network will brought back to original and additionally the network traffic will be reduced.

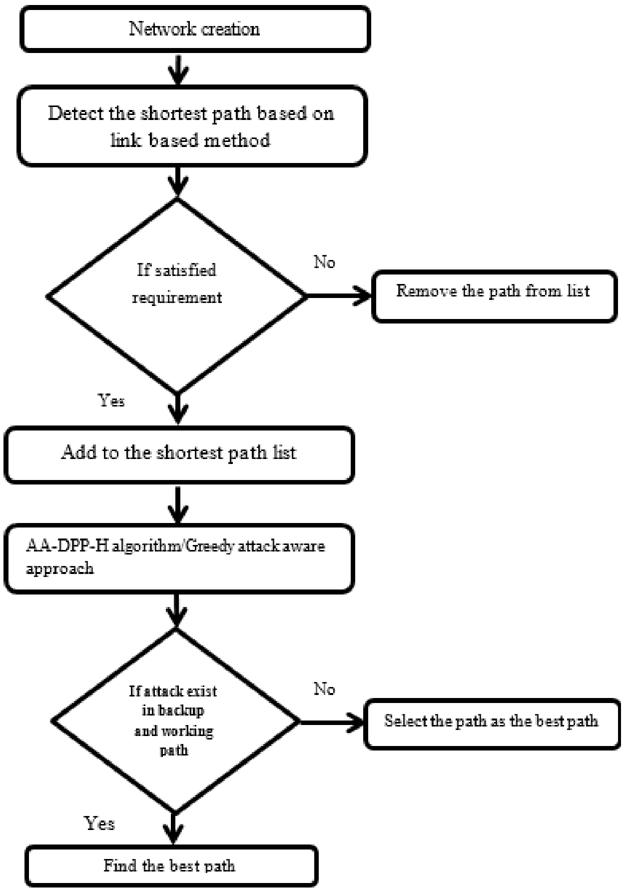

Fig.2 Flow diagram for Dedicated Path Protection

In this module a bi-level network topology arrangement is determined. Those are node level network topology and the zone level network topology prior to sending the data packets, the source primarily examines its intrazone routing table. The routing information exist in the system, if the destination node and source node is in the same zone .Otherwise, the source node initiates a locality request to remaining zone with the help of gateway nodes. Then, a gateway node of the zone where the destination node exist ,attains the locality appeal and responds with a locality reply encompassing of the zone ID of the destination. The zone ID and the node ID of the destination node are given in the header of the data packets initiated from the source node. At the time of packet progressing technique, intermediary nodes excluding nodes in the destination zone make use of inter-zone routing table, and an inter-zone routing table is employed when the packet reaches destination. Figure 3 shows the flow diagram for Zone based Hierarchical link state routing

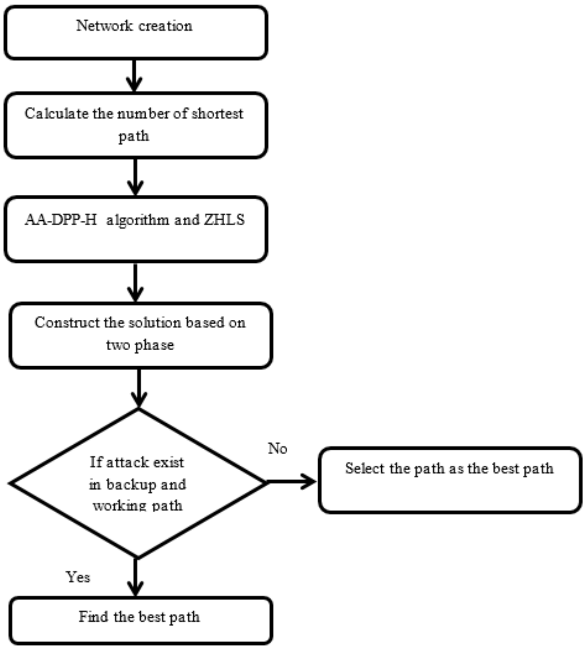

Fig.3 Flow diagram for Zone based Hierarchical link state routing

Correspondingly, there are two categories of link state packets (LSP) in the network topology which are defined. They are node level LSP and zone level LSP. The node level LSP comprises of a node ID of the adjacent nodes in the similar zone and the zone ID's of all the other zones in the network. A node occasionally transmits the node level LSP to every other node in the similar zone. Consequently, due to frequent node level LSP interactions, all nodes in a zone are similar to node level LSP. In ZHLS, the gateway node transmits the zone LSP all through system every time a virtual link is damaged or generated.

The network is divided into zones under ZHLS. A node is aware of its physical location by geolocation techniques such as GPS; then, it can determine its zone ID by mapping its physical location to a zone map, which has to be worked out at the design stage. The zone size depends on several factors such as node mobility, network density, transmission power, and propagation characteristics. The partitioning can be based on simple geographic partitioning or on radio propagation partitioning. The geographic partitioning is much simpler and does not require any measurement of radio propagation characteristics, whereas the radio propagation partitioning is more accurate for frequency reuse.

In proactive schemes, every node continuously maintains the complete routing information of the network. When a node needs to forward a packet, the route is readily available; thus, there is no delay in searching for a route. However, for a highly dynamic topology, the proactive schemes spend a significant amount of scarce wireless resource in keeping the complete routing information current. The link state routing is performed on two levels: local node and global zone levels. Unlike other hierarchical protocols, there is no cluster head in this protocol. The zone level topological information is distributed to all nodes. This "peer-to-peer" manner controls traffic bottleneck, avoids single point of failure, and simplifies mobility management. Since only zone ID and node ID of a destination are needed for routing, the route from a source to a destination can adapt to changing topology

C. Linear Network Coding:

Once the malicious node is found along the path and it is removed it is very important to ensure that networks never fell to such types of attacks again and again. Reliability of transmission
is very important to be maintained in optical networks. So inorder to strengthen the impact of reliability in optical transmission we will be using the concept of Linear network coding.

A number of effective solutions against jamming and eavesdropping attacks propose encryption and optimization of optical path disjointness; encryptions can effectively protect against eavesdropping, and path disjointness can make eavesdropping more difficult. However, the existing methods do not consider the case where the information is partially distorted, be it purposefully or as a side effect of that attack.

One of the effective methods to address this problem includes the Linear Network Coding (LNC). LNC can protect from both the jamming and eavesdropping, while addressing the issue of fault tolerance due to optical physical impairments. With LNC, the source combines the original data with random information or bit and design a network code that only the receivers are able to decrypt. The nodes can only decrypt packets if they have received a sufficient number of linearly independent information vectors or bits, which an eavesdropper might not be able to do.

LNC is also an erasure coding technique and thus can protect the source message also from random errors, and errors injected by the wire tapper via jamming attacks, which is significant in optical networks due to impairments. LNC can provide the so-called *r-secure coding,* whereby a wiretapper can eavesdrop any *r* channels in the network, without gaining any knowledge about the source message.

IV. CONCLUSION

As demand for optical networks is eventually increasing, the maintenance of it's security also becomes very crucial to ensure proper network operation. In this paper we have taken the characteristics of attack groups into consideration and make modifications to the dedicated path protection scheme by incorporating the concept of ZHLS (Zone Based Hierarchical Link State) Routing with digital signature where zone network topology was established which help in detection of malicious node along the discovered path remove it and reconstructs the path.

V. REFERENCES

[1] J. Ahmed, C. Cavdar, P. Monti, and L. Wosinska, "Hybrid survivability schemes achieving high connection availability with a reduced amount of backup resources," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 10, pp. A152–A161, Oct. 2013.

[2] N. Skorin-Kapov, J.Chen, and L.Wosinska,"A new approach to optical networks security: Attack aware routing and wavelength assignment,"IEEE/ACM Trans.Netw.,vol.18 ,no.3,pp.750-760,Jun.2010.

[3] M. Furdek, N. Skorin-Kapov, and M. Grbac, "Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation,"*IEEE/OSA J. Opt. Commun. Netw.*, vol. 2, no. 11, pp. 1000–1009,Nov. 2010.

[4] M. Furdek, N. Skorin-Kapov, and A. Tzanakaki, "Survivable routing and wavelength assignment considering high-powered jamming attacks," in *Proc. Asia Commun. Photon. Conf.*, 2011, pp. 1–7.

[5] M. Furdek and N. Skorin-Kapov, "Attack-survivable routing and wavelength assignment for high-power jamming," in *Proc. 17th Int. Conf. Opt. Netw. Des. Model.*, 2013, pp. 70–75.

[6] N. Skorin-Kapov, M. Furdek, R. Aparicio-Pardo, and P. Pavon-Marino, "Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms," *Eur.J. Oper. Res.*, vol. 222, no. 3, pp. 418–429, Nov. 2012.

[7] M. Furdek, N. Skorin-Kapov, and L. Wosinska, "Shared path protection under the risk of high-power jamming," in *Proc. 19th Eur. Conf. Netw. Opt. Commun.*, 2014, pp. 23–28.

[8] Marija Furdek,, Nina Skorin-Kapov, and Lena Wosinska, "Attack Aware Dedicated Path Protection in Optical Networks",IEEE/OSA Journal of Lightwave Technology ,Vol.34 ,no.4 , pp.1050-1061 ,Dec. 2015.

[9] K. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue,K Harasawa,Y.Nagasako, and A. Takada, "Security in photonic networks: Threats no. 21, pp. 3210–3222, Nov. 2011 .

[10] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska ,"Vulnerabilities and security issues in optical networks," in *Transparent Optical Networks , 16th International Conference on*, 2014, pp. 1–4.

[11] X. Chen, A. Jukan, and M. Medard, "Linear network coding and parallel transmission increase fault tolerance and optical reach," in *IEEE ICC*, 2015, pp. 5210–5215.

[12] M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Disaster survivability in optical communication networks," *Comput. Commun.*, vol. 36, no. 6, pp. 630–644, Mar. 2013.

[13] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3,pp. 725–736, Sep. 2011..

[14] R. Rejeb, M. S. Leeson, C. Mas Machuca, and I. Tomkos, "Control and management issues in all-optical networks,"*J. Netw.*, vol. 5, no. 2,pp. 132–139, Feb. 2010..

[15] R. Rejeb, M. S. Leeson, and R. J. Green, "Fault and attack management in all-optical networks," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 79–86, Nov. 2006.

[16] Y. Peng, Z. Sun, S. Du, and K. Long, "Propagation of all-optical crosstalk attack in transparent optical networks," *Opt. Eng.*, vol. 50, no. 8, pp. 085002.1–085002.3, Aug. 2011