Invited paper

Control Mechanism for All-Optical Components

Ridha Rejeb and Mark S. Leeson

Abstract—In this article, we give a brief overview of security and management issues that arise in all-optical networks (AONs). Then we present an outline of the multiple attack localization and identification (MALI) algorithm that can participate in some of the tasks for fault management in AONs. Consequently, we discuss a hardware-based control unit that can be embedded in AON nodes to accelerate the performance of the MALI algorithm. We conclude the article with a discussion concerning the applicability and implementation of this device in AON management systems.

Keywords— all-optical networks, fault and performance management, securing optical networks.

1. Introduction

Network management is an indispensable constituent of communication systems since it is responsible for ensuring the secure and proper operation of any network. Specifically, a network management implementation should be capable of handling the configuration, fault, performance, security, accounting, and safety in the network. However, network management for all-optical networks (AONs) faces additional challenges such as performance monitoring and ensuring adequate quality of service (QoS) guarantees in the network. Performance management is germane to successful AON operation since it provides signal quality measurements at very low bit error rates and fault diagnostic support. In particular, signal quality monitoring is difficult in AONs as the analogue nature of optical signals means that miscellaneous transmission impairments aggregate and can impact the signal quality enough to reduce the QoS without precluding all network services. This results in the continuous monitoring and identification of the impairments becoming challenging in the event of transmission failures.

The presence of a network management system (NMS) is essential to ensure efficient, secure, and continuous operation of any network. Specifically it handles the management of configuration, fault, performance, accounting, and security aspects, which are usually interlinked to one other. A key component in this system is performance management as it provides signal quality measurements at very low bit error rates and fault diagnostic support for fault management. Performance management is still a major complication for AONs, particularly, because signal quality monitoring in them is too difficult as the analogue nature of optical signals means that miscellaneous transmission impairments aggregate and can impact the signal quality enough to reduce the QoS without precluding all network services. This results in the continuous monitoring and identification of the impairments becoming challenging in the event of transmission failures. However, a simple and reliable signal quality monitoring method does not exist at present. Despite new methods for detection and localization of transmission failures having been proposed, no robust standards or techniques exist to date for guaranteeing the QoS in AONs. Therefore, the need for expert diagnostic techniques and more sophisticated management mechanisms that assist managing the proper function of AONs is highly desirable [1]–[7].

In this article, Sections 2 and 3 give a brief overview on the security and management issues that may arise in AONs. Section 4 introduces the control plane architectures taking into consideration still open and unsolved development issues. Section 5 presents an outline of the multiple attack localization and identification (MALI) algorithm [8] that can participate in some of the tasks for fault management in AONs. Section 6 discusses the efficiency of this algorithm focusing on its cost and complexity. Section 7 presents a hardware-based control unit [9] that can be embedded in AON nodes, in order to process the MALI's localization procedures in a real time fashion. Finally, in Section 8, we conclude the article with a discussion concerning the applicability and implementation of this device in AON management systems.

2. Security Issues in AONs

AONs are emerging as a promising technology for very high data rates, flexible switching and broadband application support. Specifically, they provide transparency capabilities and new features allowing routing and switching of traffic without any regression or modification of signals within the network. Although AONs offer many advantages for high data rate communications, they have unique features and requirements in terms of security and management that distinguish them from traditional communication networks. In particular, the unique characteristics of AON components and network architectures bring forth a set of new challenges for network security. By their nature, AON components are particularly vulnerable to various forms of denial of service, QoS degradation, and eavesdropping attacks. Since even short (in terms of duration) faults and attacks can cause large amounts of data to be lost, the need for securing and protecting optical networks has become increasingly significant [1], [2].

In the context of this work, a security *attack* is defined as an intentional action against the proper and secure functioning

of the network, whereas a *fault* is defined as an unintentional action against the ideal and secure functioning of the network. *Failures* are referred to as the faults and attacks that can interrupt the ideal functioning of the network. Security attacks upon AONs may range from a simple physical access to more complex attacks exploiting:

- the peculiar behaviors of optical fibers;
- the unique characteristics of AON components;
- the shortcomings of available supervisory techniques and monitoring methods.

Attacks can be classified as eavesdropping or service disruption [1]. In this scenario, they are different in nature ranging from malicious users (i.e., users inserting higher signal power) to eavesdroppers. Thus, attacks differ from conventional faults and should be therefore be treated differently. This is because they appear and disappear sporadically and can be launched elsewhere in the network. In particular, the attacker may thwart simple detection methods, which are in general not sensitive enough to detect small and sporadic performance degradations. Furthermore, a disruptive attack, which is erroneously identified as a component failure, can spread rapidly through the network causing additional failures and triggering multiple erroneous alarms. Security attacks therefore must be detected and identified at any node in the network where they may occur [2]. Moreover, the speed of attack detection and localization must be commensurate with the data transmission rate. Furthermore, transparency in AONs may introduce significant miscellaneous transmission impairments such as optical crosstalk, amplified spontaneous emission noise, and power divergence [3]. In AONs, those impairments accumulate as they propagate and can impact the signal quality so that the received bit error rate at the destination node might become unacceptable high.

3. Management Issues in AONs

Following from the previous sections, it is clear that network management for AONs faces additional challenges and still unsolved problems. One of the main premises of AONs is the establishment of a robust and flexible control plane for managing network resources, provisioning lightpaths, and maintaining them across multiple control domains. Such a control plane must have the ability to select lightpaths for requested *end-to-end* connections, assign wavelengths to these lightpaths, and configure the appropriate resources in the network. Furthermore, it should be able to provide updates for link state information to reflect which wavelengths are currently being used on which fiber links so that routers and switches may make updated routing decisions. An important issue that arises in this regard is how to address the *trade-off* between service quality and resource utilization. Addressing this issue requires different scheduling and sharing mechanisms to maximize resource utilization while ensuring adequate QoS guarantees. One possible solution is the aggregation of traffic flows to maximize the optical throughput and to reduce operational and capital costs, taking into account qualities of optical transmission in addition to protection and restoration schemes to ensure adequate service differentiation and QoS assurance. A control plane should therefore offer dynamic provisioning and accurate performance monitoring, plus efficient restoration in the network and most of these functions need to move to the optical domain. Connection provisioning, for example, should enable a fast automatic setup and teardown of lightpaths across the network thereby allowing dynamic reconfiguration of traffic patterns without conversion to the electrical domain [5]–[7].

Another related issue arises from the fact that the implementation of a control plane requires information exchange between the control and management entities involved in the control process. To achieve this, fast signaling channels need to be in place between switching nodes. These channels might be used to exchange *up-to-date* control information that is needed for managing all supported connections and performing other control functions. In general, control channels can be realized in different ways; one might be implemented *in-band* while another may be implemented *out-of-band*. There are, however, compelling reasons for decoupling control channels from their associated data links. An important reason for this is that data traffic carried in the optical domain is transparently switched to increase the efficiency of the network and there is thus no need for switching nodes to have any understanding of the protocol stacks used for handling the control information. Another reason is that there may not be any active channels available while the data links are still in use, for example, when bringing one or more control channels down gracefully for maintenance purposes. From a management point of view, it is unacceptable to teardown a data traffic link, simply because the control channel is no longer available. Moreover, between a pair of switching nodes there may be multiple data links and it is therefore more efficient to manage these as a bundle using a single separated out-of-band control channel [6].

4. Control Plane Architectures

The design of an optical network is an important and very practical issue. As stated above, a desirable architecture should feature, *inter alia*, flexible management, automatic lightpath protection and restoration, and the ability to compile an inventory. Moreover, network architectures should support the gradual introduction of new technologies into the network without time consuming and costly changes to embedded technologies. However, the network architectures currently used may be categorized in two main models, namely the *overlay model* and the *peer model*. Although both models consist essentially of an optical core that provides wavelength services to client interfaces, which reside at the edges of the network, they are intrinsi-

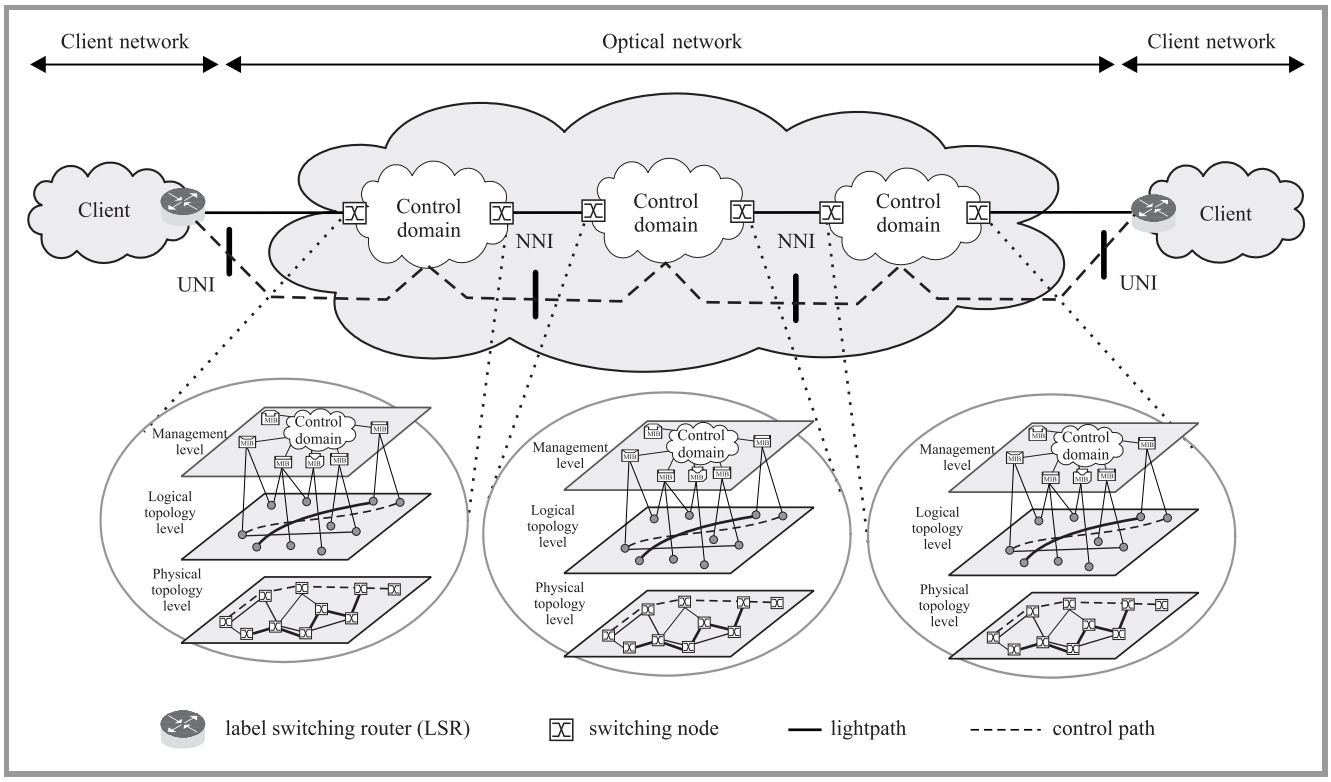

Fig. 1. Control plane management architecture.

cally different and offer up two key concepts for managing traffic flows in the network [10].

The overlay model hides the internal elements of the optical network and thus requires two separate, yet interoperable, control mechanisms for provisioning and managing optical services in the network. One mechanism operates within the core optical network and the other acts as the interface between the core components and the edge components which support lightpaths that are either dynamically signaled across the core optical network or statically provisioned without seeing inside the topology of the core. The overlay model therefore imposes additionally control boundaries between the core and edge by effectively hiding the contents of the core network.

The peer model considers the network as a single domain, opening the internal entities of the core optical network to the edge components making the internal topology visible and able to participate in provisioning and routing decisions. Whilst this has the advantage of providing a unified control plane, there are some significant considerations:

- The availability of topological information to all components in the network makes this model less secure.
- New standard control mechanisms are required since available proprietary ones cannot be employed.
- Additionally approaches for traffic protection and restoration are required.

Another model, known as the hybrid model, combines both the overlay and peer approaches, taking advantages from both models and providing more flexibility. In this model, some edge components serve as peers to the core network and share the same instance of a common control mechanism with the core network through the network-network interface (NNI). Other edge components could have their own control plane (or a separate instance of the control plane used by the core network), and interface with the core network through the user-network interface (UNI).

From a control plane point of view, the notion of the control domain is very useful. The control plane management architecture is presented in Fig. 1. The UNI is the interface between a node in the client network and a node in the core optical network. The NNI is the interface between two nodes in different control domains. The management information base is distributed among control domains, each of which has a partial knowledge of the global control information. A large optical network, as shown in Fig. 1, may be portioned into moderate control domains mainly for the following reasons [10]:

- To enforce administrative, management and protocol boundaries making them sufficiently reliable.
- To ensure rapid and accurate actions to be taken in response to failed conditions. For example, performing failure localizing processes in commensurate time.
- To increase the scalability of management functions and control planes.

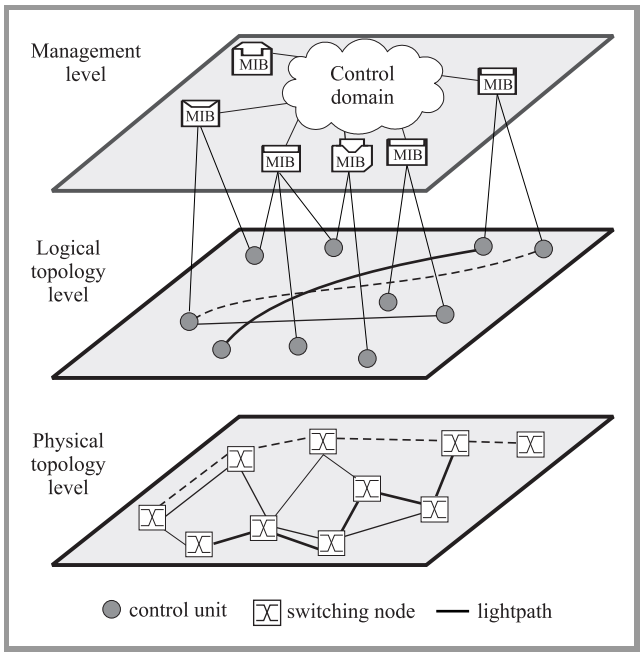

Fig. 2. The MIB distributed among element management systems.

The management information base (MIB) in a typical domain, as shown in Fig. 2, is distributed among its element management systems where each one has only a partial knowledge of the whole domain control and management information. However, there are still open and unsolved problems in the development of secure AONs that should be carefully addressed. One particular security issue is related to the UNI and NNI within the control plane employed. Consequently, the analysis of protocol stacks from a security perspective is an important prerequisite. Another issue related to network protection is a comparative study of the trade-off between network complexity and traffic restoration time.

5. The MALI Algorithm

This section presents an outline of the MALI algorithm that can participate in some of the tasks for fault management in AONs. The main task of the algorithm is to correlate multiple security failures and attacks locally at any AON node and to discover their tracks through the network. The MALI algorithm is distributed and relies on a reliable management system such as the link management protocol [11], since its overall success depends upon correct message passing and processing at the local nodes.

The key concepts of the MALI algorithm are based on the optical cross-connect (OXC) node model proposed in [8]. This model defines an OXC node as a 7-tuple $OXC = (F, W, D, S, M, \chi, \mu)$, where F, W, D, S, and M are nonempty component sets of fiber ports, supported wavelengths, wavelength demultiplexers, optical switches, and wavelength multiplexers, respectively. The main key functions of the OXC node model are represented by χ and μ. These are responsible for updating the connection and monitoring information of all established lightpaths that copropagate through the OXC node simultaneously. The model denotes the numbers of fiber ports and supported wavelengths by n and m, respectively. To identify the source and nature of detected performance degradation, the algorithm makes particular use of *up-to-date* connection and monitoring information of any established lightpath, on the input and output side of each node in the network. The required monitoring information can be correlated at local nodes or acquired from remote monitoring nodes [12].

The majority of the MALI algorithm comprises a generic localization procedure, which will be initiated at the downstream node that first detects serious performance degradation at an arbitrary lightpath on its output side.

A downstream node, which first notices serious performance degradation at a disturbed lightpath, raises an alarm, indicating that a failure has been detected on its output side. It then determines the set of lightpaths that share the same output fiber with the disturbed lightpath. For each of these, it determines the set of lightpaths that pass through the same optical switch at the same time. Hence, it delegates the localization process to the next upstream node when the status of a lightpath channel is nonzero on the input side of the node. Otherwise, it terminates the localization process for this lightpath and notifies the NMS that the disturbed channel is most likely to be affected in the current node.

An upstream node that receives the localization process with a disturbed lightpath starts the localization procedure from scratch and repeats all the steps when the channel status of the disturbed lightpath is nonzero on the output side of the node. Otherwise, it terminates the localization process and notifies the NMS indicating that the failure is most likely to be at the optical fiber link interconnecting both upstream and downstream nodes.

The localization procedure provides the NMS with state information about locations of possible disruption failures and attacks through the network. This information can be included as part of the failure notification. Once the origins of the detected failures have been localized, the NMS can then make accurate decisions (for example, which offender lightpaths should be disconnected or rerouted) to achieve finer grained recovery switching actions.

6. Cost and Complexity Analysis

Analyzing the cost and complexity of an algorithm has come to mean predicting the resources that the algorithm requires. Occasionally, resources such as memory, communication bandwidth, or hardware equipment are of prime concern, but most often it is ***computational time*** that we want to measure. The running time of the MALI's localization procedure is the sum of running times for each statement executed. For the worst-case, in which it is assumed

that an OXC node is fully loaded and that any lightpath can affect any other co-propagating lightpath of one form or another, it can be seen that the local running time of the localization procedure is of the order $O(m \cdot n)$. The major concern, however, is estimating the overall running time of the required recursive calls of the localization procedure when delegating the localization process to the next upstream nodes backwards through the network [9].

As stated in the previous section, the MALI's localization process is triggered immediately in the downstream node after detecting a failure. Then, it is delegated to certain upstream nodes involved in the localization process. As shown in Fig. 3, these nodes can be modeled as a rooted tree. The downstream node, which first notices the performance degradation on its output side, is referred to as the root node. The number of children of a node is called its degree. Thus, the maximal degree of any node is equal to the number of its input ports. The length of a localization path from the root node to an arbitrary node is called its depth in the tree. The height of a node in the tree is the number of links on the longest path from the node to a leaf. The height of the tree is the height of its root node and is equal to the largest depth in the tree.

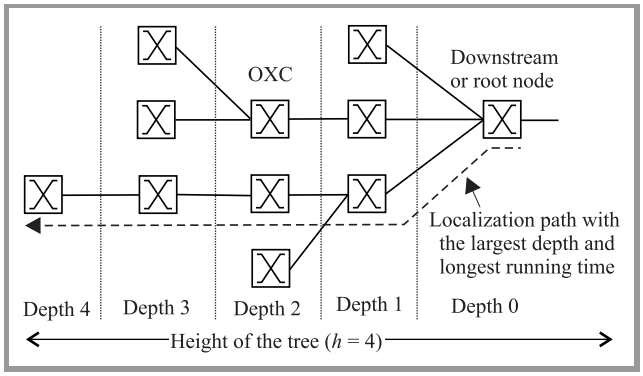

Fig. 3. Localization path tree.

Due to the distributed nature of the localization process it is expected that the localization procedure will be performed synchronously in all nodes of the same depth stage in the localization tree. Thus, the expected overall worst-case running time of the localization process is of the order $h \cdot O(m \cdot n)$, where h denotes the height of the localization tree. The height h is random since it depends on the distribution of upstream nodes involved in the localization process. Thus, it might impact the overall performance of the localization process particularly when it is becomes large [9].

7. Hardware Based Control Unit

In the previous section we saw that the local running time of the MALI's localization procedure is nonlinear, of the order $O(m \cdot n)$. However, to reduce the computational time required for running this procedure, it is reasonable to process some of computing steps in a parallel way. One of the significant conditions for running the localization procedure is that the computing steps required can be performed independently from each other. Since the localization procedure merely uses the current connection and channel state information at the input and/or output sides of the current node [8], it is not necessary to process it in a sequential way.

An optimal solution to solve this issue is to use a hardware-based control unit that can be embedded in AON nodes to process the localization procedure in a real time fashion. The device determines in *one-step* the set of established lightpaths that share the same output fiber with the disturbed lightpath at the same time. For each of these lightpaths, it checks the state of lightpaths that copropagate through the optical switch simultaneously. Hence, the computational time required is proportional to the *number of wavelengths* supported in the node.

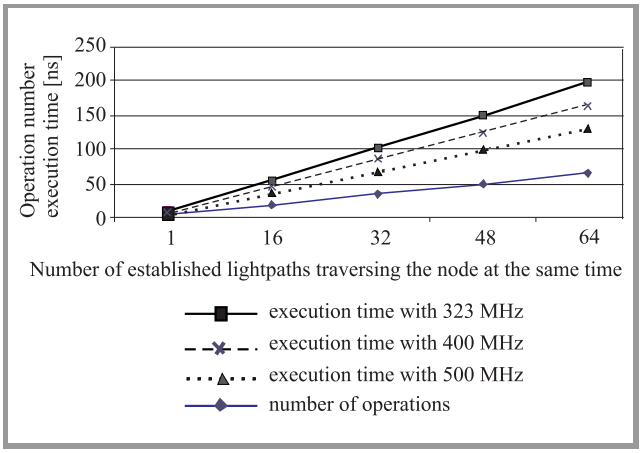

Fig. 4. Number of operation and execution time as a function of established lightpaths in 64×64-OXC node.

The performance evaluation of this approach is shown in Fig. 4. The internal design and simulation of this device was performed by a hardware simulation tool with a frequency of 323 MHz. The lower line shows the number of operations as a function of established lightpaths that share the same output fiber with the disturbed lightpath, whilst the upper plots the running time required for processing these steps. Both dotted lines are plotted with estimated values which are computed using higher frequences of 400 MHz and 500 MHz, respectively. The values are given by *time* $\sim$ *number of operation/frequency.* Both curves show unambiguously that the running time is decreasing as the frequency is increasing. Compared to the sequential approach, it is apparent that this method is more advantageous offering the benefit of reducing the running time required for processing the MALI's localization procedure. The resulting computational time is linear of the order $O(n)$, where n is the number of wavelengths supported in the node. Thus, it may ensure relaxation of the high cost and complexity of signal quality monitoring in AONs.

8. Conclusion

In this paper, we have presented a brief overview of the security and management issues that may arise in AONs. Then we have introduced the MALI algorithm that can be used for localizing the origins of multiple failures and security attacks upon AONs in a distributed manner. Consequently, we discussed a hardware-based control unit that can be embedded in AON nodes to process the MALI's localization procedures in a real time fashion. As a direct consequence, this device can participate in some tasks for fault management of AONs offering the benefit of relaxing the high cost and complexity of signal quality monitoring.

Although this approach may offer several benefits, there are several related issues that require further consideration. First, design concepts for the functional relationship between the hardware-based control unit and available management systems should be questioned. In particular, the development of efficient schemes for performance degradation resistant network control and management algorithms should be taken into consideration. Second, available and proposed control and management protocols that provision lightpaths within the network may be investigated and where necessary tailored to the control unit.

References

[1] M. Medard, S. R. Chinn, and P. Saengudomlert, "Node wrappers for QoS monitoring in transparent optical nodes", *J. High Speed Netw.*, vol. 10, no. 4, pp. 247–268, 2001.

[2] R. Bergman, M. Médard, and S. Chan, "Distributed algorithms for attack localization in all-optical networks", in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, USA, 1998.

[3] B. Ramamurthy *et al.*, "Impact of transmission impairments on the teletraffic performance of wavelength-routed optical networks", *J. Lightw. Technol.*, vol. 17, no. 10, pp. 759–764, 1999.

[4] C. Larsen and P. Andersson, "Signal quality monitoring in optical networks", *Opt. Netw. Mag.*, vol. 1, no. 4, pp. 17–23, 2000.

[5] C. Mas Machuca, I. Tomkos, and O. K. Tonguz, "Optical networks security: a failure management framework", in *Proc. Conf. ITCom. Opt. Commun. Multimed. Netw.*, Orlando, USA, 2003.

[6] 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, 2006.

[7] J. K. Patel, S. U. Kim, and D. Su, "A framework for managing faults and attacks in WDM optical networks," in *Proc. DARPA Inform. Survivab. Conf. Expos. DISCEX 2001*, Anaheim, USA, 2001, vol. II, pp. 137–145.

[8] R. Rejeb, M. S. Leeson, and R. J. Green, "Multiple attack localization and identification in all-optical networks", *Opt. Switch. Netw.*, vol. 3, no. 1, pp. 41–49, 2006.

[9] R. Rejeb, M. S. Leeson, and R. J. Green, "Hardware-based control unit for all-optical components", in *Proc. 10th IEEE Int. Conf. Transp. Opt. Netw. ICTON'08*, Athens, Greece, 2008, vol. 3, pp. 6–9.

[10] D. Saha, B. Rajagopalan, and G. Berstein, "The optical network control plane: state of the standards and deployment", *IEEE Commun. Mag.*, vol. 41, no. 8, pp. S29–S34, 2003.

[11] J. Lang, "Link management protocol (LMP)", RFC 4204, Oct. 2005.

[12] T. Wu and A. K. Somani, "Necessary and sufficient condition for k crosstalk attacks localization in all-optical networks", in *Proc. IEEE Globecom 2003 Conf.*, San Francisco, USA, 2003.

Ridha Rejeb is the Managing Director of the IAER Ltd. and an Assistant Professor at the Physics Institute, Faculty of Basic Sciences at the Esslingen University of Applied Sciences in Germany. He has more than 18 years of industrial experience in network and computer operating systems. He graduated in mathematics at the Stuttgart University of Applied Sciences in Germany. He received his M.Sc. degree in data communications systems from the Brunel University and his Ph.D. in engineering from the University of Warwick, UK. His major research interests include security in communication systems, resilience in transparent optical networks and information theory. He is an Associate Fellow in the School of Engineering, University of Warwick, UK. He is the Technical Program Chair of the ICTON-MW, member of the IEEE, editorial member of the Meditation Journal of Computers and Networks, and member of the CSNDSP technical committee.

e-mail: ridha.rejeb@iaer.eu
Institute for Advanced Engineering and Research
Felix-Wankel-Str. 4/1
73760 Ostfildern, Germany

Mark S. Leeson received a Ph.D. for work on planar optical modulators from the University of Cambridge, UK, in 1990 and then worked as a network analyst for a UK bank until 1992. Subsequently, he held academic appointments in London and Manchester before joining the University of Warwick, UK, in March 2000. He is an Associate Professor in the School of Engineering at the University of Warwick. His major research interests are optical receivers, optical communication systems, communication protocols, coding and modulation, ad hoc networking and evolutionary optimization. To date he has over 140 publications in these fields. He is a chartered member of the UK Institute of Physics, a senior member of the IEEE and a member of the UK EPSRC grants Peer Review College.

e-mail: mark.leeson@warwick.ac.uk
School of Engineering
University of Warwick
Gibbet Hill Road
Coventry, CV4 7AL, United Kingdom