A Study on Cycle Attack by Multiaccess Interference in Multigranularity OCDM-Based Optical Networks

Shaowei Huang, *Student Member, IEEE*, Ken-Ichi Baba, Masayuki Murata, *Member, IEEE*, and Ken-Ichi Kitayama, *Fellow, IEEE*

***Abstract*—Previously, an optical code-division multiplexing (OCDM)-based network architecture was proposed to improve the wavelength utilization and to provide finer bandwidth granularities to users. By this technology, different channels using distinct optical codes (OCs) can be multiplexed onto the same wavelength, in which an OC is considered as the basic unit in lightpath provisioning. In the ideal case, multiaccess interference (MAI) inherent to the OCDM technology is assumed to be removed completely at intermediate nodes and cannot be propagated or accumulated along the lightpath. However, since no optical–electrical (O/E) or electrical–optical (E/O) conversion is allowed in transparent OCDM-based optical networks, the MAI cannot be removed completely at intermediate nodes with current all-optical regeneration techniques. As a result, the residual MAI may be propagated and accumulated along the lightpath and affect other active lightpaths carried by the same wavelength in the network. The affected active lightpaths may build unintended cycles along which the MAI is accumulated. Furthermore, this MAI keeps increasing when the lightpaths traversed by the cycle are active, which deteriorates the lightpath signal quality. Since this deterioration may eventually result in unacceptable signal quality and service disruption, the phenomenon caused by the MAI is termed as cycle attack in this paper. The explanations of the MAI propagation mechanism and the cycle attack problem are given. A depth-first search (DFS)-based algorithm is proposed to diagnose such cycle attacks under dynamic traffic conditions. The numerical results show that our DFS-based cycle attack diagnostic algorithm enables one to detect cycle attacks effectively, and the two-way resource reservation method associated with heuristic wavelength assignment is shown to mitigate the blocking performance degradation due to cycle attacks greatly with some proper wavelength and OC configuration.**

***Index Terms*—Attack, cycle, depth-first search (DFS), multiaccess interference (MAI), optical code-division multiplexing (OCDM), optical cross-connect (OXC), wavelength-routed optical network (WRON).**

I. Introduction

During the last few years, transparent optical networks (TONs) have attracted much interest because of their capability of accomplishing ultra-high-speed data transmission in the physical layer without optical–electrical (O/E) and electrical–optical (E/O) conversions [1]. However, as noises introduced by the transmission line or switching equipment cannot be removed completely at intermediate nodes, the signal quality suffers from degradation due to various impairments and becomes more vulnerable. The remaining noises may be propagated and accumulated along the lightpath and eventually damage other active lightpaths. Routing and wavelength assignment (RWA) problems taking into account the signal impairments due to polarization-mode dispersion (PMD), chromatic dispersion (CD), amplification spontaneous emission (ASE), etc., have been studied in [1]–[4], in which a connection request assigned a ligthpath with unsatisfactory signal quality is blocked. However, impairments like crosstalk impose more significant limitations on network design under actual traffic conditions, because lightpaths inserted and terminated dynamically may cause signal quality variation to other active lightpaths. This complicates the design of networks taking into account these impairments. The interband and intraband crosstalk models in transparent wavelength-routed networks (WRONs) were presented, and the RWA algorithms incorporating crosstalk were studied [5]–[7]. A connection requesting a lightpath that may cause unsatisfactory signal quality to other active lightpaths due to crosstalk is also blocked.

Potential security vulnerabilities arise in TON like those in computer security in general. Crosstalk in transparent WRON was termed an *attack* because it has attacking capabilities to other active lightpaths by deteriorating their signals [8]–[10]. A crosstalk attack model was presented to describe the behaviors that show how the intraband crosstalk is propagated in WRON [8], [9]. A new established lightpath may introduce the intraband crosstalk to those lightpaths sharing a link or node with it; the affected lightpaths may furthermore induce this attacking capability to other active lightpaths as well. However, attacking capabilities induced to those active lightpaths by a crosstalk attack can be neglected if optical switches with low crosstalk ratio, e.g., less than -35 dB, are employed. In such cases, the active lightpaths affected by the new one can be assumed to not have any attacking capabilities to other lightpaths [10].

We have presented the OCDM-based network architecture in [11] and [12]. In such a network, label-switched paths (LSPs) based upon the OCDM technology (OCDM-LSPs) can be multiplexed onto a single wavelength by distinct optical codes (OCs), and they can be discriminated by the optical correlation at intermediate nodes. The multiaccess interference (MAI) (crosstalk between the channels simultaneously sharing the same wavelength) is generated in the optical correlation, which is the dom-

Manuscript received May 8, 2007; revised December 14, 2007. Published August 29, 2008 (projected). This work was supported in part by the Japan Society for the Promotion Science.

S. Huang and K. Kitayama are with the Graduate School of Engineering, Osaka University, Osaka 565-0871, Japan (e-mail: huangshw@pn.comm.eng.osaka-u.ac.jp; kitayama@comm.eng.osaka-u.ac.jp).

K. Baba is with the Cybermedia Center, Osaka University, 567-0047 Osaka, Japan (e-mail: baba@cmc.osaka-u.ac.jp).

M. Murata is with the Graduate School of Information Science and Technology, Osaka University, Osaka 565-0871, Japan (e-mail: murata@ist.osaka-u.ac.jp).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2008.919483

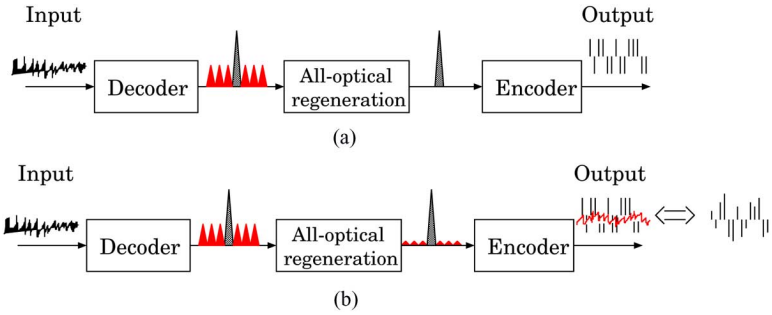

Fig. 1. (a) Ideal and (b) realistic all-optical regeneration at an intermediate node.

inant noise source from the network. Fig. 1(a) illustrates that the desired signal (peak) is generated and the MAI (sidelobe) is removed completely by the ideal all-optical regeneration techniques. In practice, optical thresholding techniques have been presented to suppress the MAI [14]–[17]. However, it is still difficult to remove the MAI completely with the current all-optical regeneration technologies. As illustrated in Fig. 1(b), the residual MAI will be also encoded and deteriorate the desired signal.

In general, an OCDM-LSP may traverse several nodes before reaching the destination in an OCDM-based network. Poorer optical correlation performance in the downstream nodes can be expected with the deteriorated encoded signal compared to the ideal case. The autocorrelation intensity peak to the maximum cross-correlation level ratio (so-called P/C ratio [18]) reflecting the signal quality decreases gradually along the route because of the MAI accumulation. The presence of an all-optical cycle in WRON using acoustooptic tunable filter (AOTF)-based cross-connects was reported, in which amplified spontaneous emission (ASE) or crosstalk oscillation could occur [19]. It emphasizes that this cycle problem cannot be neglected. Solutions by configuring the ATOF switches properly were given to eliminate such unintended cycles. In the OCDM-based networks, unintended cycles may also be built up and cause the MAI oscillation problem [20] because the residual MAI is propagated along the lightpaths in the network and could be looped back to form cycles. However, the mechanism building a cycle in our case differs from what was presented in [19], where the presence of all-optical cycles is limited to the particular device used for cross-connects (like AOTF-based cross-connect). In this paper, cycles are built not because of improper cross-connect configurations but because of dynamic traffic flowing throughout the network. It is a generic problem in incoherent/coherent OCDM-based networks if MAI cannot be removed completely, regardless of any particular technology or device used in the encoding, decoding, and regeneration processes. Therefore, the phenomenon caused by the MAI is considered one of the most distinguished features in transparent OCDM-based optical networks and should be taken into account while dealing with dynamic traffic. The P/C ratios of the lightpaths traversed by the cycle may suffer from a dramatic decrease along the unintended cycles and eventually results in unacceptable signal quality to those lightpaths. In this paper, this phenomenon is termed as *cycle attack*.

The rest of this paper is organized as follows. We explain the MAI propagation mechanism and the cycle attack problem in Section II. A depth-first search (DFS)-based algorithm is proposed to diagnose cycle attacks under dynamic traffic conditions, and a two-way resource reservation method associated with heuristic wavelength assignment is described in Section III. In Section IV, an overview of the simulation model is given. In Section V, simulations are performed to evaluate the influence of the cycle attack problem.

II. Cycle Attack by MAI Propagation in OCDM-Based Networks

In this section, the MAI propagation mechanism is first described, and the cycle attack problem due to this propagation is explained.

A. MAI Propagation Mechanism

Fig. 2 shows the MAI propagation mechanism at intermediate nodes. Each node is an OCDM optical cross-connect (OXC) described in [11], in which wavelength conversion is not considered. As described in [11], after being separated by a wavelength de-multiplexer, OCDM-LSPs 1 (solid line) and 2 (dashed) carried by wavelength λ are discriminated at the decoder by the optical correlation at Node A. In the ideal case shown in Fig. 1(a), the MAI can be removed completely, and only the decoded autocorrelation peak "1" of OCDM-LSP 2 will be encoded and forwarded to the downstream node. But with the realistic all-optical regeneration, the MAI introduced by OCDM-LSP 1 cannot be removed completely and is also encoded and propagated along OCDM-LSP 2. For example, in coherent OCDM systems using the binary phase-shift keying (BPSK) approach for encoding, the amplitude of OCDM-LSP 2 at the output port of the decoder at Node A is the summation of the decoded signal (peak) itself and the MAI component originated by OCDM-LSP 1. As shown in Fig. 2, the amplitude of OCDM-LSP 2 after encoding at Node A fluctuates because of the MAI component.

There is a possibility that OCDM-LSP 2 and OCDM-LSP 3 are carried by the same wavelength encounter at Node B and are switched to the same output port as illustrated in Fig. 2. As explained above, the signal at the output port of Node B is the summation of the amplitude of OCDM-LSP 3, OCDM-LSP 2, and the MAI from OCDM-LSP 1. Thus, the amplitude of OCDM-LSP 3 is also influenced by the MAI from OCDM-LSP 1, or, in other words, OCDM-LSP 3 is attacked and the MAI attacking capability from OCDM-LSP 1 is induced to OCDM-LSP 3 from OCDM-LSP 2. Using the

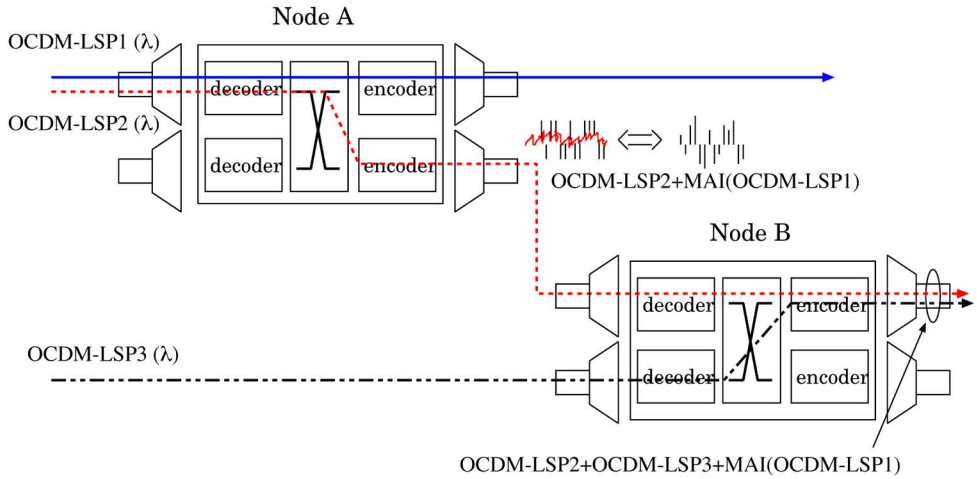

Fig. 2. MAI propagation mechanism.

terminology defined in [9], if OCDM-LSP 1 is taken for an original attack flow (OAF), OCDM-LSP 2 and OCDM-LSP 3 can be regarded as secondary attacked flows (SAFs). Note that this MAI propagation phenomenon only occurs among the OCDM-LSPs carried by *the same wavelength*. Therefore, there exist n independent MAI propagation layers in a network with n wavelengths.

The MAI propagation mechanism is outlined as follows: 1) the residual MAI is regarded as the attacking source; 2) attacking capability can only be induced to other active lightpaths carried by the same wavelength as OAF; 3) a lightpath is considered to be only attacked if it traverses the same link with the attacked flows.

B. Cycle Attack due to MAI Propagation

In OCDM-based optical networks, signal quality is mainly determined by the performance of optical correlation carried out at decoders. If there is any residual MAI, the encoded signal of the desired signal will be deteriorated and result in poorer correlation performance in downstream nodes. As described above, the MAI can be propagated through the network lightpath by lightpath, unintended cycles may be built, and the MAI is looped back. If the MAI is looped back, the P/C ratios of the active lightpaths traversed by the cycle will suffer a dramatic decrease because of the MAI accumulation and eventually result in unacceptable signal quality. For example, for a 511-chip superstructured fiber Bragg grating (SSFBG) OCDM system, a signal with P/C ratios not able to provide crosstalk lower than -19.4 dB is considered unacceptable [21]. Therefore, the cycle attack problem cannot be neglected in the design of OCDM-based optical networks.

An attacking capability propagation prober, namely, $\mathrm{ACPP}_{k\to l}^{i\to j}(\lambda)$ with a Boolean value is proposed to serve as an indicator for attack propagation of a wavelength λ in the direction from $\mathrm{link}_{i\to j}$ to $\mathrm{link}_{k\to l}$. The value of $\mathrm{ACPP}_{k\to l}^{i\to j}(\lambda)$ can be easily obtained by using the information maintained by the routers. If an outgoing $\mathrm{link}_{k\to l}$ includes a lightpath ID that can match any from the incoming $\mathrm{link}_{i\to j}$ at a node, $\mathrm{ACPP}_{k\to l}^{i\to j}(\lambda)$ in that direction is set to "1"; otherwise $\mathrm{ACPP}_{k\to l}^{i\to j}(\lambda)$ is set to "0." Fig. 3(a) shows the case before a new OCDM-LSP is inserted. OCDM-LSPs 1 (solid line) and 2 (dotted line) are active lightpaths carried by the same wavelength λ. OCDM-LSP 1 and 2 can be treated as the OAF and SAF, respectively. All the links traversed by OCDM-LSP 1 and 2 are attacked; thus, $\mathrm{ACPP}_{5\to 6}^{4\to 5}(\lambda)$, $\mathrm{ACPP}_{6\to 1}^{5\to 6}(\lambda)$, and $\mathrm{ACPP}_{1\to 2}^{6\to 1}(\lambda)$ are set to "1." The arrows illustrated in Fig. 3(b) indicate the attacking capability propagation direction. If new OCDM-LSP 3 is to take the route along $1 \to 2 \to 3 \to 5 \to 6$, OCDM-LSP 2 will induce the attacking capability from OCDM-LSP 1 to OCDM-LSP 3

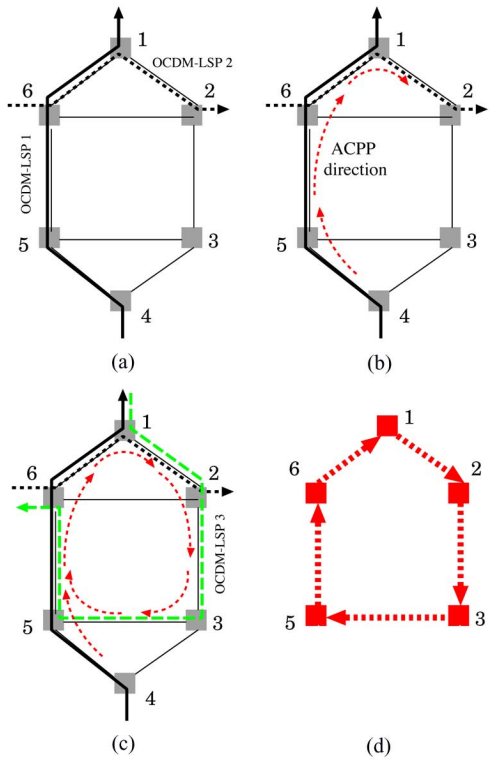

Fig. 3. Cycle attack by MAI propagation. (a) A network with active lightpaths; (b) MAI propagation before new lighpath insertion; (c) MAI propagation after new lightpath insertion; and (d) harmful cycle created by OCDM-LSP 1, 2, and 3.

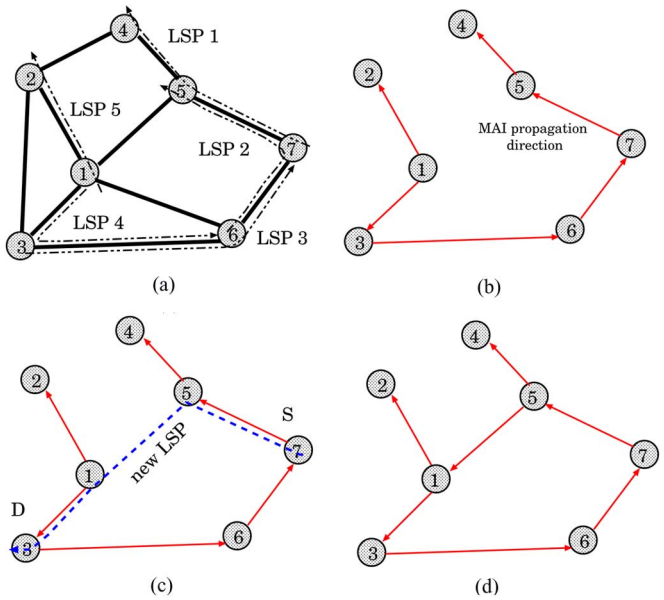

Fig. 4. Logical topology creation and its updating to λ layer. (a) Physical topology with active lightpaths; (b) logical topology reflecting the MAI propagation; (c) new lightpath insertion; and (d) updated logical topology after new lightpath insertion.

because OCDM-LSP 3 and 2 traverse the same $\text{link}_{1\to 2}$. Therefore, $\text{link}_{2\to 3}$, $\text{link}_{3\to 5}$, and $\text{link}_{5\to 6}$ are also attacked and the corresponding $\text{ACPP}_{2\to 3}^{1\to 2}(\lambda)$, $\text{ACPP}_{3\to 5}^{2\to 3}(\lambda)$, and $\text{ACPP}_{5\to 6}^{3\to 5}(\lambda)$ are set to "1." From Fig. 3(c), it can be observed that the MAI attacking capability originating from OCDM-LSP 1 is looped back to itself along the $\text{link}_{5\to 6}$, because OCDM-LSP 3 and 1 traverse the same $\text{link}_{5\to 6}$. This loopback results in MAI accumulation along the cycle $1 \to 2 \to 3 \to 5 \to 6 \to 1$ shown in Fig. 3(d). Consequently, as described above, the P/C ratios of these three OCDM-LSPs suffer a dramatic decrease and result in unacceptable signal quality.

The above explanations also reveal that if any cycle attack is caused by the insertion of the new lightpath, the created cycle includes at least one link traversed by this new lightpath. This gives a very important implication for diagnosing the unintended cycle attacks under dynamic traffic conditions. In the following section, a cycle attack diagnostic algorithm taking into account this hint is proposed.

III. DFS-Based Cycle Attack Diagnostic Algorithm

The difficulties in attacking diagnosis stem from the localization of the attacking source in WRON [9]. But as with what is described in the previous section, *a cycle at least includes one of the links the new lightpath traverses*. This means the unintended cycle attacks are possible to detect along the new lightpath.

A. Algorithm Description

A DFS-based algorithm commonly used to traverse a graph is applied to resolve the cycle attack diagnosis problem in this paper. Hereafter, it is named the DFS-based cycle attack diagnostic algorithm. Because cycle attacks only occur where the MAI is propagated, logical topology information reflecting how the MAI is distributed in the network is required. Fig. 4 illustrates how the logical topology is interpreted by the MAI propagation and how it is updated after a new lightpath insertion. Fig. 4(a) illustrates the physical topology with active lightpaths, and Fig. 4(b) shows the logical topology obtained from Fig. 4(a) with the MAI distribution information in which the arrows represent the MAI propagation directions. It has to be clarified that the MAI propagation direction is different from the ACPP direction because it only provides the information on whether a link has MAI or not, and not whether the MAI is propagated from one link to another. From Fig. 4(b), it can be observed that the logical topology is a directional graph and may have fewer edges than the physical topology. If a new connection request is supposed to take the route $7 \to 5 \to 1 \to 3$ as shown in Fig. 4(c), the MAI from this new OCDM-LSP will be introduced to $\text{link}_{7\to 5}$, $\text{link}_{5\to 1}$, and $\text{link}_{1\to 3}$. Fig. 4(d) illustrates the updated logical topology taking into account the newly attacked links. This logical topology is used as the graph in the algorithm and appears in the adjacent-list representation.

Based upon this logical topology information [see Fig. 4(d)], the cycle attack diagnosing procedure is performed to check and locate the unintended cycle attacks. It begins from the source node of the new lightpath [see Fig. 5(a)]. A stack called *NStudy* is introduced to record the nodes under study in the algorithm. The *basic principle* is if a node appears twice in NStudy, the algorithm returns a "cycle existing" message. Similar to the traditional DFS algorithm, the order in which our algorithm discovers the edges and vertices in the graph depends entirely on the order in which the edges appear in the adjacent lists. Although a different order may lead to a different search dynamic, our DFS-based algorithm has the same essential property of diagnosing unintended cycles. For simplicity, no priority is set while choosing the neighbor of a node to traverse, i.e., one neighbor node 4 of node 5 is chosen to be visited first [see Fig. 5(b)]. If there is not any outgoing link, the node stacked in *NStudy* will be popped out. As illustrated in Fig. 5(c), node 4 is popped out from *NStudy* and the algorithm goes back to node 5. The dashed line represents backtracing in the DFS algorithm. From the lightpaths shown in Fig. 4(a) and (c), we can observe that the MAI is not propagated from $\text{link}_{5\to 1}$ to $\text{link}_{1\to 2}$; thus, node 2 is not traversed in the algorithm. With this procedure, a cycle can be detected in Fig. 5(g) and (h) because node 7 appears twice in *NStudy*. However, it is not necessary to be a cycle attack. Only if the MAI is propagated from $\text{link}_{6\to 7}$ to $\text{link}_{7\to 5}(\text{ACPP}_{7\to 5}^{6\to 7}(\lambda) = 1)$, that is, if the MAI is looped back, *a harmful cycle* (cycle attack) message is generated in the algorithm [see Fig. 5(g)]. Otherwise, if there is no MAI propagation from $\text{link}_{6\to 7}$ to $\text{link}_{7\to 5}(\text{ACPP}_{7\to 5}^{6\to 7}(\lambda) = 0)$, as illustrated in Fig. 5(h), the cycle is regarded as a harmless cycle that will not cause service disruption.

B. Two-Way Resource Reservation Method

Since unintended cycle attacks may occur at new OCDM-LSP insertion, they must be detected in the OCDM-LSP establishment. Resource reservation protocol traffic engineering (RSVP-TE) [22] has been presented to allow the establishment of LSPs taking into account network constraint parameters such as bandwidth and wavelength continuity. In this paper,

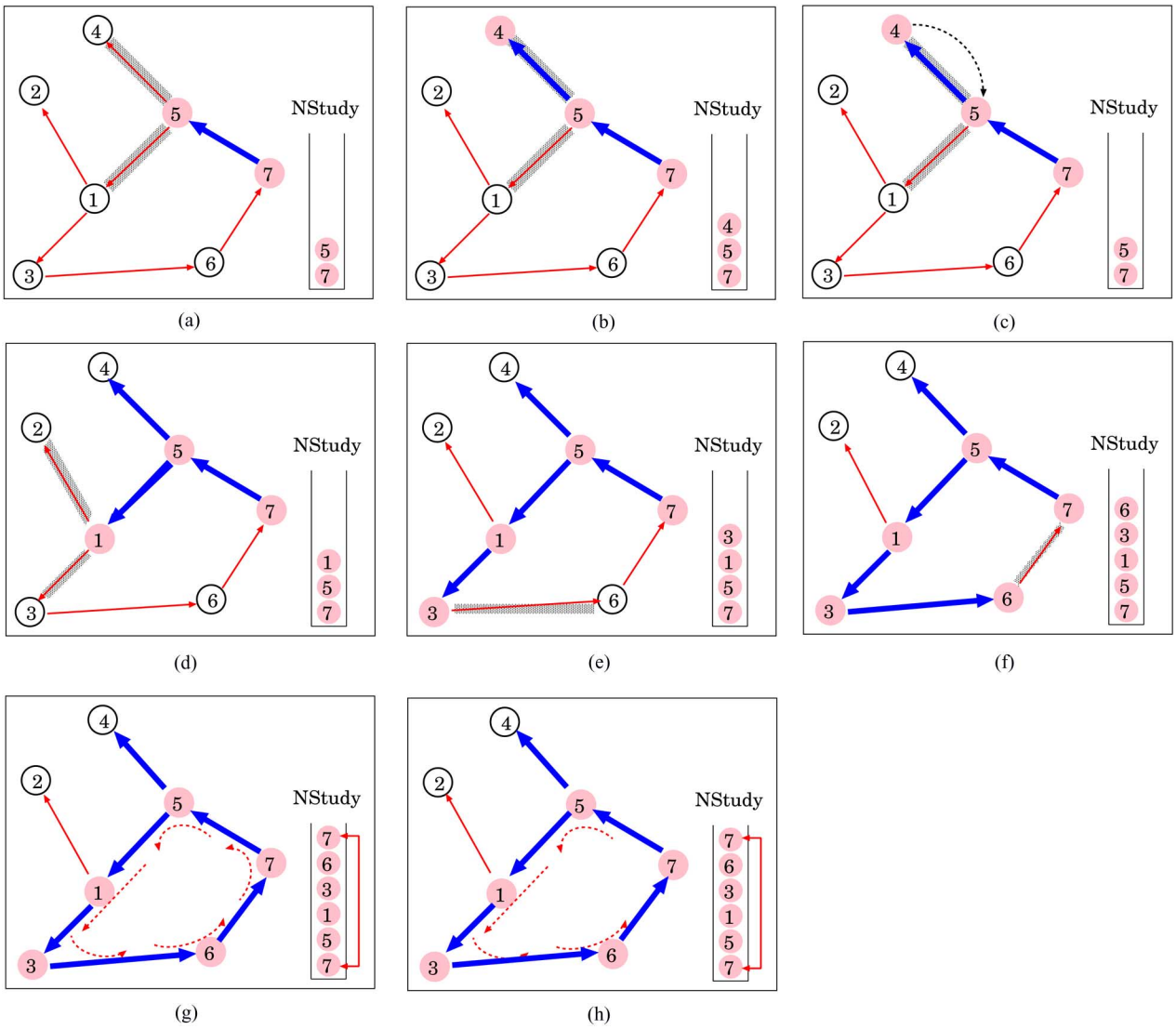

Fig. 5. Principle of the DFS-based cycle attack diagnostic algorithm. Thin arrows are the MAI propagation directions. Thick arrows correspond to edges traversed in the algorithm. Shaded edges are the candidates to be traversed in the algorithm. Dotted arrows are the ACPP directions. (a)–(f) traversing edges of the logical topology; (g) harmful cycle is detected; and (h) harmless cycle is detected.

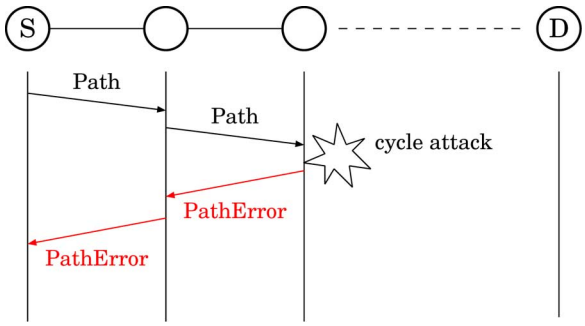

Fig. 6. Two-way resource reservation taking into account cycle attacks.

we deploy a two-way resource reservation method taking into account the unintended cycle attacks in the OCDM-LSP establishment.

First, a route is computed, and a wavelength as well as an OC is preassigned to the new connection request. As illustrated in Fig. 6, before launching the real traffic, a "Path" message is sent along the precomputed route. The DFS-based cycle attack diagnosing procedure described above is performed at each intermediate node. If no cycle attack is detected in the current traversed link, the "Path" message is passed to the next node along the route; otherwise, a "PathError" message is sent back to inform the source node a cycle attack. Two cases are considered when a "PathError" message is received: 1) block it without other attempts and 2) try another setting up attempt. The explanations of these two cases are given in the next section.

The pseudocode of the DFS-based cycle attack diagnostic algorithm associated with the two-way resource reservation method is given in the Appendix.

IV. Overview of Simulation Model

The simulation model is illustrated in Fig. 7. It mainly consists of the following three submodules to deal with dynamic connection requests.

1) To an initiated connection request, the routing procedure is first executed, where the common shortest path algorithm

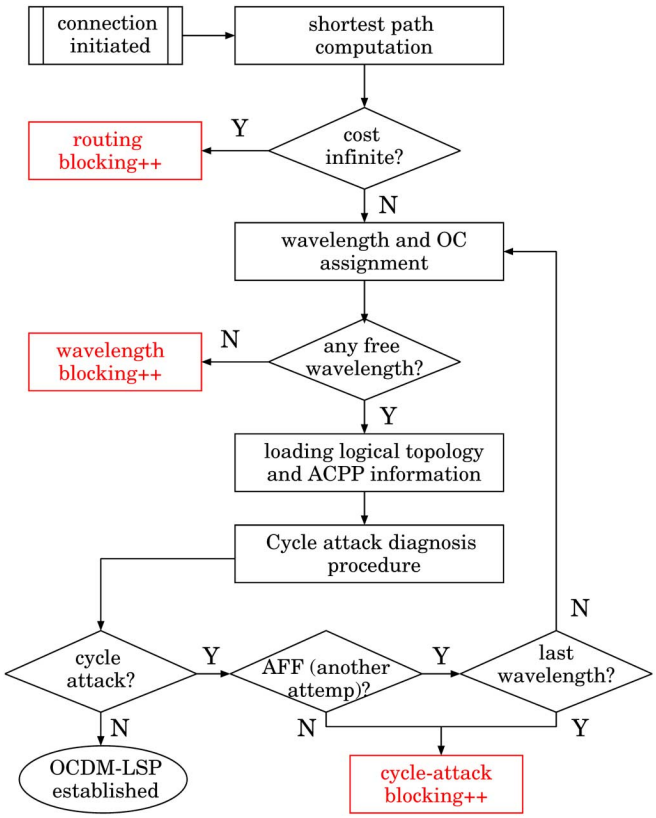

Fig. 7. Simulation model taking into account cycle attacks.

(Dijkstra) is deployed to compute the route. It incorporates a cost function of each link, which defines the ratio of total channels and free OCDM channels. Therefore, a link with more free OC channels is preferred. If there is not any available route from the source to the destination (infinite cost), the connection request is announced *routing blocking*.

2) The wavelength and OC assignment processes follow the routing process. As described in Section II, the presence of cycle attack is restricted to the lightpaths carried by the same wavelength, and the OC assignment has no contribution to the cycle attack impact on blocking performance. Hence, only the first-fit scheme is used for OC assignment for simplicity reasons. That means a free OC with a lower sequence number will be selected first. Regarding the wavelength assignment, three schemes are considered. The first two are common first-fit (FF) and random (RND) schemes. A free wavelength with a lower sequence number is selected in FF or a free wavelength is randomly selected in RND. The third one is a heuristic wavelength assignment approach called advanced first-fit (AFF), which will be described later. Wavelength conversion is assumed not to be allowed along the route. Thus, the connection request will be announced *wavelength blocking* if there is no available wavelength from source to destination.
3) After the routing and wavelength/OC assignment, an OCDM-LSP setting up attempt is performed by using the two-way resource reservation method described above. The logical topology and ACPP information are loaded to perform cycle attack diagnosis along the precomputed route. If a "PathError" message indicating cycle attacks is received, in FF and RND wavelength assignment schemes, the connection request will be blocked immediately and all the assigned resources are released. However, in the AFF scheme, another setting attempt will be carried out with the next available wavelength with the lowest number. Only if no wavelength can avoid the unintended cycle attacks along the precomputed route, the connection request is announced *cycle-attack blocking*. In the next section, AFF is demonstrated significantly to mitigate the blocking performance degradation due to the cycle attacks greatly.

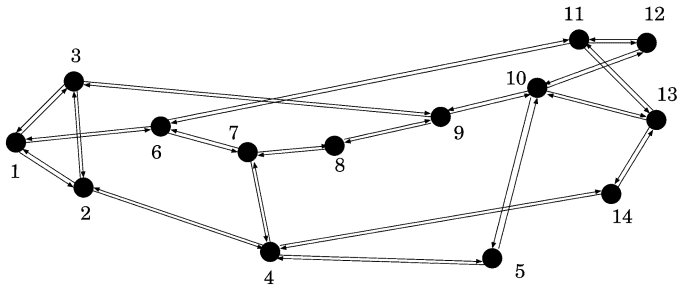

Fig. 8. NSF network.

V. Numerical Results

A. Simulation Description

Simulations are conducted to validate the DFS-based cycle attack diagnostic algorithm with a six-node network shown in Section II and the 14-node National Science Foundation (NSF) network shown in Fig. 8. Each directional fiber has L wavelengths ($L = 1, 4, 6, 8, 40$, etc.) and N OCDM channels per wavelength ($N = 1, 2, 4, 5, 10, 40$, etc.). Connections arriving at the network have a rate of λ, which is Poisson distribution, and an exponential service time of $1/\mu$ (μ is the service rate). λ/μ is defined as the network offered load in our simulations. The ideal regeneration case is referred to as the *ideal case* and the realistic regeneration case is referred to as the *cycle-attack case*.

B. Performance Evaluation

a) Impact of Cycle Attack With Different Wavelength and OC Combinations: Fig. 9(a)–(d) illustrates the blocking performance for both ideal case and cycle-attack case with different wavelength and OC combinations. As described in [12], OC conversion provided by the OCDM technology benefits the blocking performance. Therefore, in networks not allowing wavelength conversion, a combination with more OCDM channels per wavelength and fewer wavelengths is expected to outperform one with fewer OCDM channels per wavelength and more wavelengths. Comparing Fig. 9(a) and (d), it can be observed that, in the ideal cases of FF and RND, the combination (one wavelength, 40 OCs) equivalent to a pure OCDM network yields the best, and the combination (40 wavelengths, one OC) equivalent to a pure WDM network yields the worst among the four combinations.

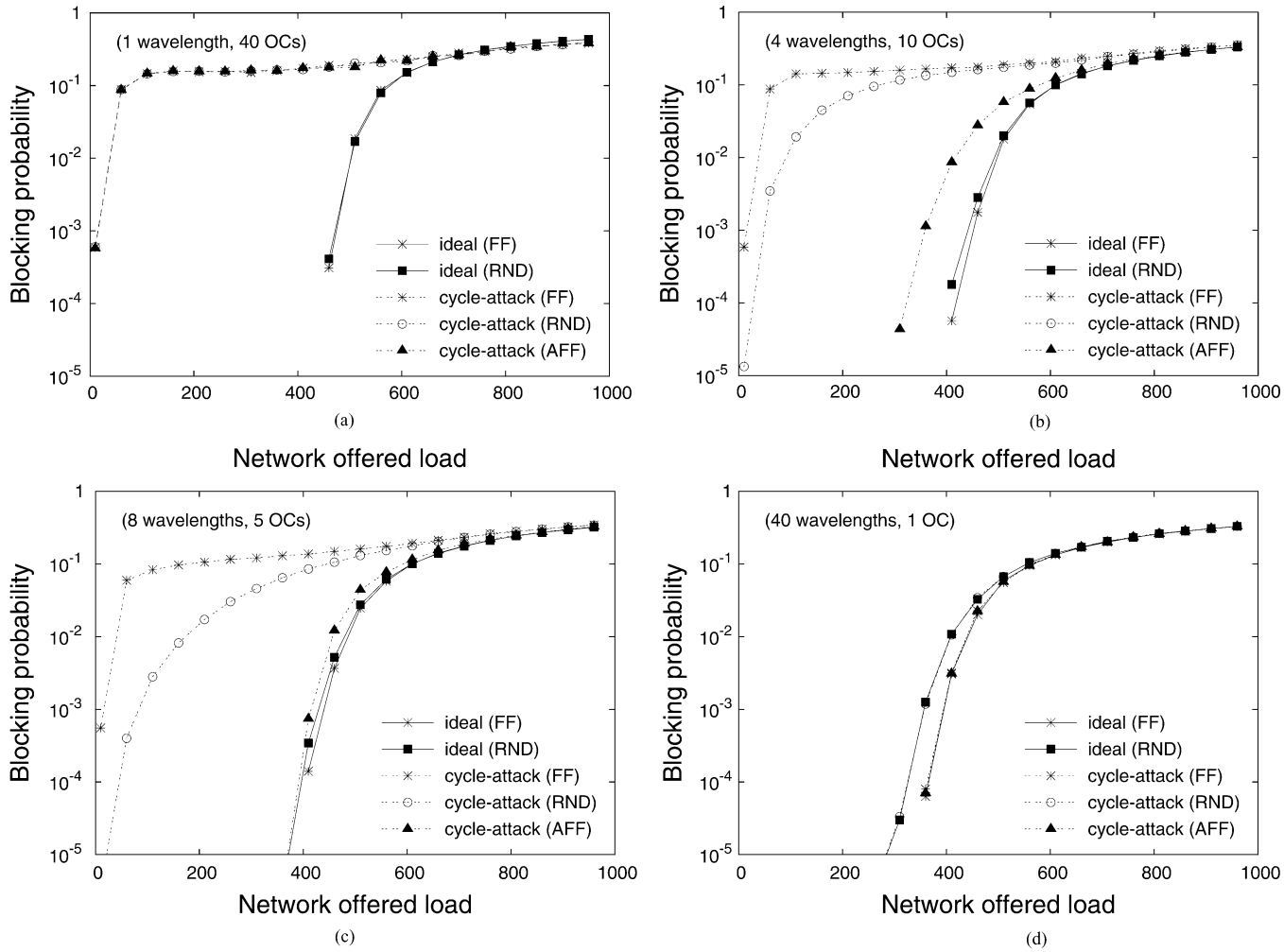

Fig. 9. Blocking versus network offered load for different wavelength and OC combinations with NSF network: (a) (one wavelength, 40 OCs) pure OCDM network; (b) (four wavelengths, ten OCs) hybrid OCDM-WDM network; (c) (eight wavelengths, five OCs) hybrid OCDM-WDM network; (d) (40 wavelengths, one OC) pure WDM network.

However, the cycle-attack case is more complicated. First, it suffers worse blocking performance than the ideal case; because the connection requests building, unintended cycle attacks are blocked [see Fig. 9(a)–(c)]. This indicates that the DFS-based algorithm is able to detect the cycle-attack blockings successfully. Since combination (40 wavelengths, one OC) is equivalent to a pure WDM network, there are no cycle attacks and the cycle-attack case performs the same as the ideal case [see Fig. 9(d)]. Secondly, from Fig. 9(a)–(c), a decrease of blocking probability is observed in the cycle-attack case when the number of wavelengths is increased. This effect is evident to RND and AFF of the cycle-attack case because the availability of more wavelengths increases the probability to assign a wavelength without cycle attacks. In particular, the combination (eight wavelengths, five OCs) using AFF achieves the blocking performance very close to the ideal case. This property is completely different from what has been observed from the ideal case because more wavelengths and fewer OCDM channels in the ideal case result in worse blocking performance. This is considered as a distinguished finding in transparent OCDM-based optical networks.

Another important finding is that the AFF of the cycle-attack case with the combination (eight wavelengths, five OCs) [see Fig. 9(c)] provides better blocking performance than the pure WDM network [see Fig. 9(d)] despite the unintended cycle attacks. The main reason for this improvement is because OC conversion in the combination (eight wavelengths, five OCs) helps to relieve the impact of wavelength continuity constraint in pure WDM networks. Therefore, it can be concluded that the OCDM technology can be still considered the promising alternative to provide finer bandwidth granularity even with the realistic all-optical regeneration techniques.

b) Impact of Cycle Attack on Granularities: Fig. 10 illustrates the blocking probability with respect to the number of OCDM channels per wavelength. Both the ideal and the cycle-attack cases achieve better blocking performance with an increase of OCDM channels per wavelength because the network capacity is enlarged. Moreover, the cycle-attack case is outperformed by the ideal case because of cycle-attack blockings. In the cycle-attack case, AFF behaves differently from FF and RND and enables a very fast decrease in blocking probability with an increase of OCDM channels per wavelength. Increasing the OCDM channels is observed not to help to decrease the blocking probability in FF and RND. This is because a connection request will be blocked in FF and RND by unintended

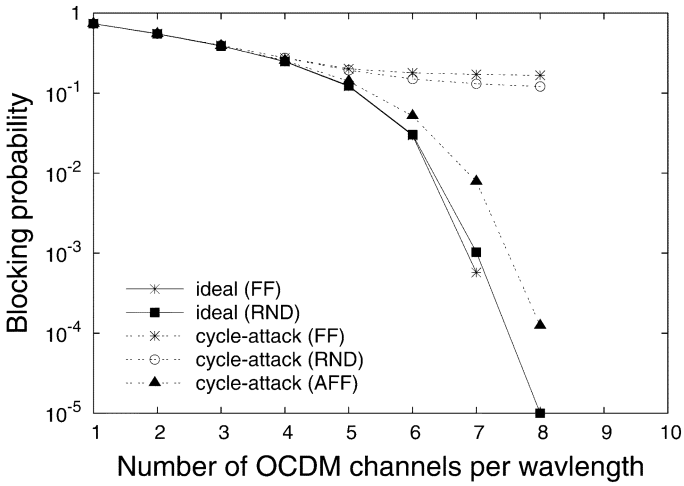

Fig. 10. Blocking versus number of OCDM channels per wavelength. NSF network, six wavelengths per fiber, $\rho = 460$.

cycle attacks even though there are available wavelengths and OCs along the route, as described in the simulation model in Section IV.

c) Blocking Percentages by Different Constraints: In the simulation model, three blocking constraints have been described: *insufficient capacity (routing blocking), wavelength continuity (wavelength blocking),* and *cycle attacks (cycle-attack blocking)*. In this section, we investigate the impact of different blocking constraints with different wavelength assignment schemes in terms of percentage of total blocking. Percentages of routing, wavelength continuity, and cycle attack blockings are expressed as *per(routing), per(wavelength)* and *per(cycle-attack)*, respectively. Thus, we have per(routing) + per(wavelength) + per(cycle-attack) = 1.

Figs. 11 and 12 illustrate the blocking percentages of different blocking constraints in the NSF network and a six-node network. In the case of the NSF network, it can be observed that *per(routing)* is very small (smaller than 10^{-4}) and wavelength continuity and cycle-attack blockings are dominant. A tendency that *per(wavelength)* increases but *per(cycle-attack)* decreases with an increase of network offered load in all wavelength assignment schemes is observed from Fig. 11. The main reason is that high network offered load increases the difficulty of reserving the same wavelength from the source to the destination in large-scale networks. Consequently, the connection requests are blocked in wavelength assignment before entering the cycle-attack diagnosing process. However, as illustrated in Fig. 11(c), AFF has less influence on the total blockings, and a 10–20% decrement in *per(cycle-attack)* is achieved comparing to FF and RND [see Fig. 11(a) and (b)].

In the six-node network, different behaviors from the NSF network are observed (see Fig. 11). First, the routing constraint becomes one of the dominant blocking factors instead of the wavelength continuity constraint because links in the six-node network are more easily to be filled up with lightpaths. Secondly, opposite tendencies of *per(routing)* and *per(cycle-attack)* are observed in Fig. 12(c) compared to Fig. 11(c), in which *per(routing)* decreases and *per(cycle-attack)* increases with an increase of network offered load. AFF succeeds in avoiding

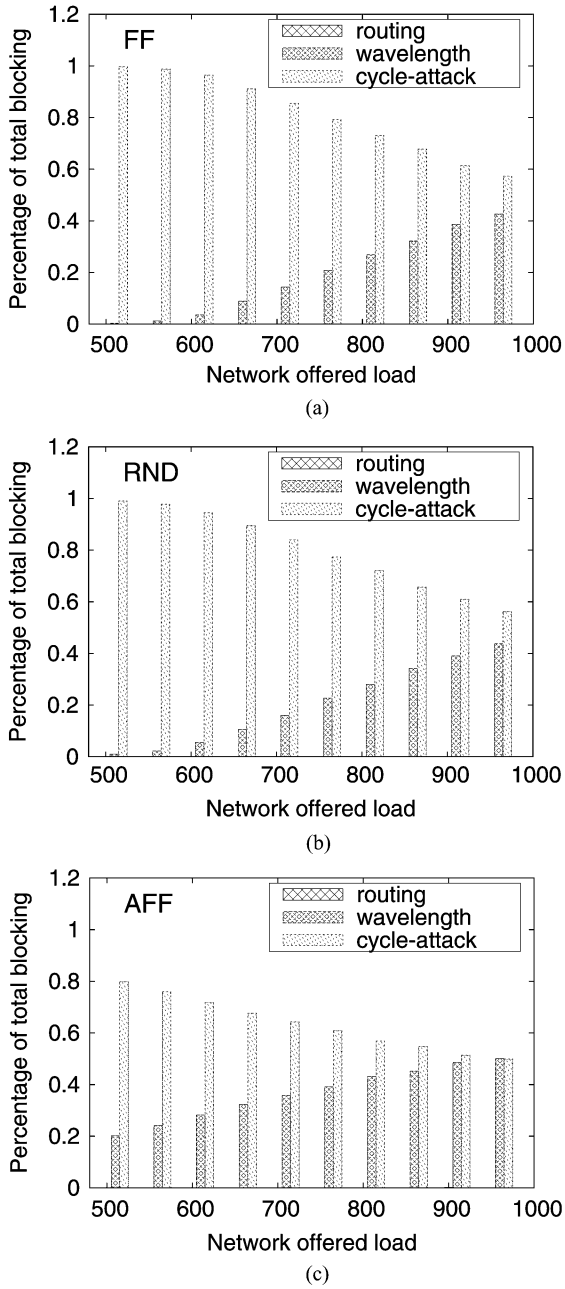

Fig. 11. Percentage of total blocking versus network offered load. The NSF network is configured with (eight wavelengths, five OCs). (a) FF (first-fit); (b) RND (random); (c) AFF (advanced first-fit).

cycle attacks by multiple setup attempts under low network offered load conditions, and routing blocking becomes dominant. However, under higher network offered load conditions, cycle attacks become the dominant factor causing blockings. This implies that cycle attacks are difficult to avoid in a small network when traffic increases, and the effect of wavelength assignment is diminished.

Finally, a summary of the numerical results is given. AFF is a simple but efficient method to mitigate the blocking performance degradation due to cycle attacks. With some configuration, e.g., (eight wavelengths, five OCs), OCDM-based optical networks can perform better than WRON even with realistic all-optical regeneration techniques. However, cycle

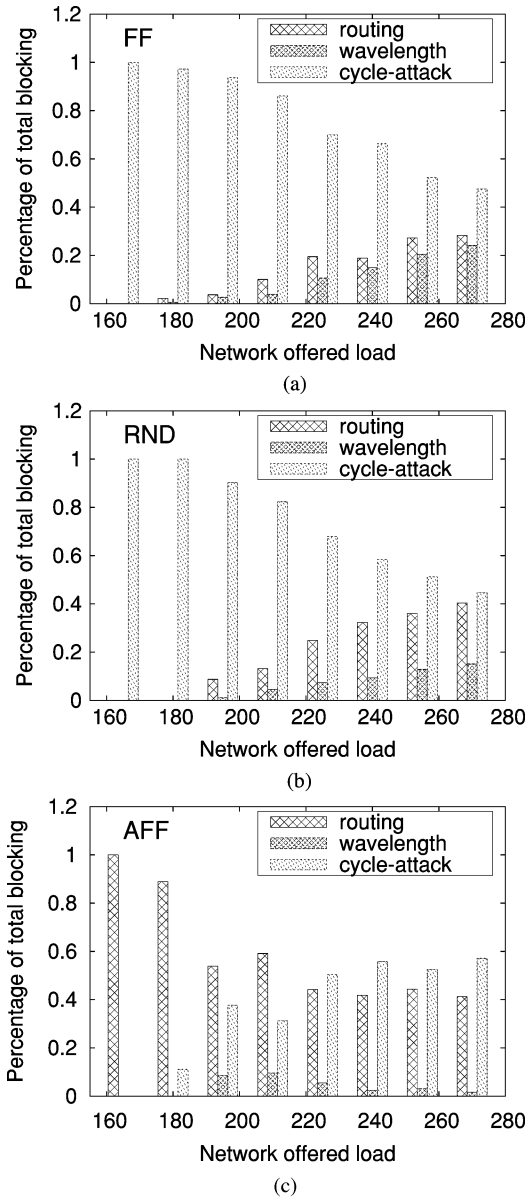

Fig. 12. Percentage of total blocking versus network offered load. The six-node network is configured with (eight wavelengths, five OCs). (a) FF (first-fit); (b) RND (random); (c) AFF (advanced first-fit).

attacks remain the dominant factor of blocking when network offered load is high in both large (e.g., NSF) and small (e.g., six-node) networks.

VI. Conclusion

The MAI propagation mechanism in transparent OCDM-based optical networks has been explained and the cycle attack problem due to the MAI propagation studied. A DFS-based algorithm for diagnosing such cycle attacks also has been proposed. An approach for mitigating the blocking performance degradation due to cycle attacks has been considered from the wavelength assignment perspective. Numerical results have shown that wavelength assignment schemes have great impact on the blocking performance. The proposed AFF can mitigate the impact of cycle attacks effectively, substantially improving the overall performance of the network when compared to FF and RND schemes.

There are still many open topics left in the transparent OCDM-based optical networks, which need further discussions. For example, using AFF wavelength assignment to avoid unintended cycle attacks along the precomputed route may suffer from a long delay for data transmission if multiple attempts are performed. One possible solution to reduce this LSP establishment delay is to prepare a cycle-attack-aware route for each connection request. How to find an available wavelength having the highest probability not causing cycle attacks and potential congestion for future connection requests are the important issues; the other possible solution is to divide the network into different lambda layers and create a spanning tree for each lambda layer before dealing with any connection request. This is considered as the most efficient way to enable OCDM-LSP establishment without any delay due to cycle attacks. In this method, how to create the spanning tree for each lambda layer and the selection of a lambda layer are the main issues.

Appendix A
Pseudocode of DFS-Based Cycle-Attack Diagnostic Algorithm

In this Appendix, we give the pseudocode of our DFS-based cycle-attack diagnostic algorithm.

Algorithm DFS-Based Cycle-Attack Diagnosis

Input:

G: graph provided by the logical topology;

L: precomputed lightpath;

NStudy: stack for recording traversed vertice.

Output:

Msg: cycle attack identification.

```
// two-way resource reservation method
diagnosis_path(lightpath L)
{
  stack NStudy = empty
  for each node x along the precomputed lightpath L
  {
    checked_node++// counter for checked node
    dfs_cycle_attack(G, x, checked_node)
    if Msg is cycle attack
      call is blocked and return
  }
}
```

```
// cycle attack diagnosis
dfs_cycle_attack(graph G, x, checked_node)
{
   list neighbor = empty
   search(x)
   while (size of NStudy is not equal to checked_node)
   {
      remove w from the beginning of neighbor
      if w not yet visited
      {
         add w to NStudy
         search(w)
      }
      // difference from the traditional DFS algorithm
      else
      {
         if the MAI is looped back// ACPP along the cycle
         should be checked.
            Msg is set cycle attack and return Msg
      }
   }
}
// search neighbors of a given node
search(vertex v)
{
   visit v
   for each edge (v, w)
      add w to the beginning of neighbor
}
```

It mainly consists of three parts: diagnosis_path(lightpath L) is the implementation of the two-way resource reservation method, dfs_cycle_attack(graph G, x, checked_node) is implementation of the cycle-attack diagnosing procedure with xth node along the precomputed route, and search(vertex v) is the implementation of finding the adjacent nodes. Graph G is the logical topology obtained from the MAI distribution information mentioned in Section III. The difference from the traditional DFS algorithm can be observed in dfs_cycle_attack(graph G, x, checked_node), in which a "cycle attack" message will be generated if a node is visited twice and a harmful cycle is built.

ACKNOWLEDGMENT

S. Huang would like to thank the ICOM Electronic Communication Engineering Promotion Foundation and the Japan Society for the Promotion Science.

REFERENCES

[1] J. Stand, A. Chiu, and R. Tkach, "Issues for routing in the optical layer," *IEEE Commun. Mag.*, vol. 39, pp. 81–87, Feb. 2001.
[2] R. Sabella, E. Iannone, M. Listanti, M. Berdusco, and S. Binetti, "Impact of transmission performance on path routing in all-optical transport networks," *IEEE J. Lightw. Technol.*, vol. 16, pp. 1965–1972, Nov. 1998.
[3] B. Ramamurthy, D. Datta, H. Feng, J. P. Heritage, and B. Mukherjee, "Impact of transmission impairments on the teletraffic performance of wavelength-routed optical networks," *J. Lightw. Technol.*, vol. 17, no. 10, pp. 1713–1723, Oct. 1999.
[4] R. Cardillo, V. Curri, and M. Mellia, "Considering transmission impairment in wavelength routed networks," presented at the Opt. Netw. Design Model. (ONDM) 2005 Conf., Milan, Italy, 2005.
[5] Y. Pointurier, M. Brandt-Pearce, T. Deng, and S. Subramaniam, "Fair routing and wavelength assignment in all-optical networks," presented at the IEEE/OSA Opt. Fiber Conf. (OFC), Anaheim, CA, Mar. 5–10, 2006.
[6] Y. Pointurier, "Cross-layer design in all-optical networks incorporating crosstalk effects," Ph.D. dissertation, Univ. of Virginia, Charlottesville, VA, 2006.
[7] T. Deng, S. Subramaniam, and J. Xu, "Cross-aware wavelength assignment in dynamic wavelength routed optical networks," in *Proc. IEEE Broadband Netw. (BROADNETS)*, San Jose, CA, 2004, pp. 140–149.
[8] M. Medard, D. Marquis, and S. R. Chinn, "Attack detection methods for all-optical networks," presented at the Netw. Distrib. Syst. Security Symp., San Diego, CA, 1998.
[9] T. Wu and A. K. Somani, "Cross-talk attack monitoring and localization in all-optical networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 6, pp. 1390–1401, Dec. 2005.
[10] G. Liu and C. Ji, "Resilience of all-optical network architectures under in-band crosstalk attacks: A probabilistic graphical model approach," *IEEE J. Sel. Areas Commun.*, vol. 25, pp. 1–16, Apr. 2007.
[11] S. Huang, K. Baba, M. Murata, and K. Kitayama, "Variable-bandwidth optical paths: Comparison between optical code-labeled path and OCDM path," *J. Lightw. Technol.*, vol. 24, pp. 3563–3573, Oct. 2006.
[12] S. Huang, K. Baba, M. Murata, and K. Kitayama, "Architecture design and performance evaluation of multi-granularity optical networks based on optical code division multiplexing," *OSA J. Opt. Netw.*, vol. 5, no. 12, pp. 1028–1042, Dec. 2006.
[13] D. J. G. Mestdagh, *Fundamentals of Multiacess Optial Fiber Networks*. Norwood, MA: Artech House, 1998.
[14] J. H. Lee, P. C. Teh, Z. Yusoff, M. Ibsen, W. Belardi, T. M. Monro, and D. J. Richardson, "A holey fiber-based nonlinear thresholding device for optical CDMA receiver performance enhancement," *IEEE Photon. Technol. Lett.*, vol. 14, pp. 876–878, Jun. 2002.
[15] X. Wang, N. Wada, T. Hamanaka, K. Kitayama, and A. Nishiki, "10-user, trulyasynchronous OCDMA experiment with 511-chip SSFBG en/decoder and SC-based optical thresholder," presented at the 2005 Conf. Optical Fiber Communication (OFC'05), Anaheim, CA, 2005, paper PDP33.
[16] K. Li, W. Cong, V. J. Hernandez, R. P. Scott, J. Cao, Y. Du, J. P. Heritage, B. H. Kolner, and S. J. B. Yoo, "10 Gbit/s optical CDMA encoder-decoder BER performance using HNLF thresholder," presented at the 2004 Conf. Opt. Fiber Commun. (OFC'04), Los Angeles, CA, 2004.
[17] Z. Jiang, D. S. Seo, S.-D. Yang, D. E. Leaird, A. M. Weiner, R. V. Roussev, C. Langrock, and M. M. Fejer, "Four user, 2.5 Gb/s, spectrally coded O-CDMA system demonstration using low power nonlinear processing," presented at the 2004 Conf. Opt. Fiber Commun. (OFC'04), Los Angeles, CA, 2004.
[18] X. Wang, K. Matsushima, A. Nishiki, N. Wada, F. Kubota, and K. Kitayama, "High-performance optical code generation and recognition using 511-chip 640-Gchip/s phase-shifted superstructured FBG," *Opt. Lett.*, vol. 30, no. 4, pp. 355–357, Feb. 2005.
[19] J. Iness, B. Ramamurthy, and B. Mukherjee, "Elimination of all-optical cycles in wavelength-routed optical networks," *J. Lightw. Technol.*, vol. 14, pp. 1207–1217, Jun. 1996.

[20] S. Huang, K. Baba, M. Murata, and K. Kitayama, "Impact of MAI noise cycle attack on OCDM-based optical networks and its diagnostic/mitigation algorithm," presented at the IEEE Global Commun. Conf. 2007, Washington, DC, Nov. 2007.
[21] K. Kitayama, X. Wang, and N. Wada, "OCDMA over WDM PON—Solution path to gigabit-symmetric FTTH," *J. Lightw. Technol.*, vol. 24, no. 4, pp. 1654–1662, Apr. 2006.
[22] RSVP-TE: Extensions to RSVP for LSP Tunnels. IETF Request for Comments RFC 3209, Dec. 2001.

Shaowei Huang (S'06) received the B.E. degree from the Department of Electrical and Electronics Engineering, Nankai University, Tianjin, China, in 2002 and the M.E. and Ph.D. degrees in electrical, electronics, and information engineering from Osaka University, Osaka, Japan, in 2006 and 2008, respectively.

He is now with the Department of Electrical, Electronics, and Information Engineering, Osaka University.

Dr. Huang received a fellowship from the Japan Society of Promotion Science in 2007.

Ken-Ichi Baba received the B.E., and M.E. degrees in information and computer sciences and the D.E. degree from Osaka University, Osaka, Japan, in 1990, 1992, and 1995, respectively.

He was a Research Associate with the Education Center for Information Processing, Osaka University, until 1997. He became an Assistant Professor with Electronic and Photonic Systems Engineering, Kochi University of Technology, Kochi, Japan, in 1997. He has been an Associate Professor with the Cybermedia Center (then Computation Center), Osaka University, since 1998. His research interests include broadband communication networks, computer communication networks, and photonic network systems.

Masayuki Murata (M'89) received the M.E. and D.E. degrees in information and computer sciences from Osaka University, Osaka, Japan, in 1984 and 1988, respectively.

He is a Professor in the Graduate School of Information Science and Technology, Osaka University. In 1984, he joined Tokyo Research Laboratory, IBM Japan, as a Researcher. In 1987, he joined Osaka University. He has published more than 400 papers in international and domestic journals and conferences. His research interests include computer communication network architecture and performance modeling and evaluation.

Dr. Murata is a member of the Association for Computing Machinery, The Internet Society, the Institute of Electronics, Information and Communications Engineers of Japan, and the Information Processing Society of Japan.

Ken-Ichi Kitayama (S'75–M'76–SM'89–F'03) received the B.E., M.E., and Dr. Eng. degrees in communication engineering from Osaka University, Osaka, Japan, in 1974, 1976, and 1981, respectively.

In 1976, he joined the NTT Electrical Communication Laboratory. In 1982–1983, he spent a year as a Research Fellow with the University of California at Berkeley. In 1995, he joined the Communications Research Laboratory (presently, National Institute of Information and Communications Technology), Tokyo. Since 1999, he has been a Professor with the Department of Electrical, Electronic and Information Engineering, Graduate School of Engineering, Osaka University. His research interests are in photonic networks, optical signal processings, OCDMA systems, and radio-over-fiber communication systems. He has published more than 220 papers in refereed journals and has received more than 30 patents. He is an Associate Editor of *Optical Switching and Networking*.

Prof. Kitayama is a Fellow of the Institute of Electronics, Information and Communications Engineers (IEICE) of Japan. He is a member of the Editorial Board of IEEE PHOTONICS TECHNOLOGY LETTERS and IEEE TRANSACTIONS ON COMMUNICATIONS. He received the 1980 Young Engineer Award from the Institute of Electronic and Communication Engineers of Japan, the 1985 Paper Award of Optics from the Japan Society of Applied Physics, the 2004 Achievement Award from IEICE, and the 2007 Shida Rinzaburoh Award.