An intrusion tolerant scheme of crosstalk attack based on multi-evidence trust model in multi domain optical networks

Qiwu Wu 1*, Fang Li 2, Lingzhi Jiang 2

1 College of Equipment Management and Support, Engineering University of PAP, Xi’an, 710086, China
2 College of Information Engineering, Engineering University of PAP, Xi’an, 710086, China

*Corresponding author’s e-mail: wuqiwu700@163.com

Abstract. In order to improve the survivability of multi-domain optical networks, an intrusion tolerant scheme of crosstalk attack based on multi-evidence trust model in multi domain optical networks was proposed. By collecting and processing evidence and classified crosstalk attacks, the reputation of nodes and links in the intra-domain and inter-domain were calculated, and the application framework of the multi-domain optical networks crosstalk attack tolerant intrusion scheme was proposed. The analysis and experimental results showed that compared with the typical tolerant intrusion scheme, this scheme had better tolerant intrusion capability when multi-domain optical networks suffer from crosstalk attack.

1. Introduction

In a multi-domain optical network, crosstalk attacks seriously threaten the availability, integrity, and confidentiality of information transmission throughout the network, which can result in failure to complete normal communication tasks [1, 2]. Therefore, how to maintain normal communication in a multi-domain optical network under crosstalk attacks is an important issue.

In recent years, invasion tolerance technology has been extensively studied by experts and scholars at home and abroad. In order to solve the problem that reliability and security depend on cluster heads in communication, the literature [3] proposed a clustering routing scheme with intrusion tolerance, but this scheme cannot solve the problem of crosstalk attacks. Aiming at the problem of poor tolerance capacity in the existing tolerance model, the literature [4] proposed a distributed tolerance model based on voting. Although this model can quantify the problem, it was not suitable for multi-domain optical networks. By analyzing various attacks in the optical network, the literature [5] proposed an effective measure that can ensure the normal operation of the network when attacked, but this measure was complicated and required high cost. In order to maintain good quality of service (QoS) and improve resource utilization, the literature [6] proposed an intrusion tolerance model that can deal with large-scale denial of service attacks, but this model had little effect in solving crosstalk attacks. The literature [7] proposed an intrusion tolerance scheme based on trust access control called Q-TI, but this scheme cannot be directly applied to multi-domain optical networks. The literature [8] proposed an intrusion tolerance scheme based on trust relationship called J-TI, which analyzed the intrusion tolerance capability of IP networks and achieved good results. However, this solution was still not applicable to multi-domain optical networks.
At present, there is no research report specifically aimed at crosstalk attack tolerance technology in multi-domain optical networks. Therefore, this paper took crosstalk attacks as the research object and designed crosstalk attack tolerance scheme based on the multi-evidence trust model in multi-domain optical network, which improved the survivability of optical networks.

2. Trust relationship
Generally speaking, the trust relationship mainly exists in the interaction between people. Therefore, the trust relationship plays an important role in social networks [9, 10]. The similarity between the multi-domain optical network and the social network in trust relationship is as follows:

Firstly, trust existed between two entities. Trust was the relationship between the believer and the trustee. The inter-domain and network entities in the domain were in a relationship of mutual trust before being subjected to crosstalk attacks. Secondly, trust is one-way. In a multi-domain optical network, the trustee sends a communication request, and the trustee responds to the request. Thirdly, trust is not transitive. That is, the node A trusts the node B and the node B trusts the node C, but the node A does not necessarily trust the node C. Fourthly, trust changes dynamically. In a multi-domain optical network, it is uncertain whether each network entity is attacked and when the attack occurs, and the trust value of each network entity gradually decays with time.

3. Intrusion tolerant scheme of crosstalk attack based on multi evidence trust model in multi domain optical networks

3.1. The overall structure
In order to improve the survivability of multi-domain optical networks, this paper took crosstalk attacks as the research object, established multi-domain optical network trust relationships, and proposed crosstalk attack tolerance scheme based on multi-evidence trust model in multi-domain optical network. The program consists of three main modules: evidence collection and processing, trust management, and trust database. The evidence collection and processing module mainly collects and processes crosstalk attack information in the optical network through the link management protocol (LMP). The evidence of crosstalk attacks mainly includes the power value measured by the power meter and the spectrum, waveform and eye diagram measured by the OSA. The main role of LMP is to discover in time when an attack occurs in the optical network, and quickly transmit the situation to the evidence collection and processing module for processing through the control plane. The trust management module realizes the conversion of the basic trust distribution function through the construction of the basic trust function. At the same time, the module submits the calculated, stored and updated trust values to the trust data management center in the trust database. The trust data management center has a direct trust storage table, an indirect trust storage table, and a comprehensive trust storage table. At the same time, the trust data management center stores the reputation of each network entity. The overall structure of an intrusion tolerance scheme based on the multi-evidence trust model is shown in Figure 1.

At the same time this article makes the following rule:

Rule 1: the relationship between the trust manager and the trustee is the relationship between giving and being believed.

Rule 2: between domains, PCE acts as a trust manager, and nodes in each domain act as trust managers; in the domain, the source node of the crosstalk attack is located as the trust manager, and the alarm message is sent as the trust manager.

Rule 3: the range of trust value is [0, 1], and each network entity has an initial trust value.

Rule 4: the trust value of each trust manager and trustee is calculated, stored and updated in the trust management module.

Rule 5: each node only maintains the trust information of its neighbouring nodes. At the same time, each trust table is not independent, they are combined with the routing table to spread out.
Rule 6: after the end of an optical communication cycle, the trust value of each network entity has been calculated. At the same time, before entering the next optical communication cycle, the trust data management centre stores and updates each trust storage table.

![Diagram of Trust Management Module](image)

**Figure 1. The overall structure of this scheme**

Through the above analysis, the tolerance conditions of the tolerance scheme are as follows:

**Condition 1:** When the reputation between the trust manager and the trustee is greater than the reputation threshold, normal communication is performed.

**Condition 2:** When the direct trust value (called Drui-j) calculated by the trust value between the trust manager and the trustee is greater than the initial trust value, normal communication is performed.

**Condition 3:** When the trust manager and the trustee, the comprehensive trust value (called Mrui-j) calculated by the trust value is greater than the initial trust value, normal communication is performed.

The above three intrusion tolerance conditions are independent of each other, but in the application process of the intrusion tolerance scheme, there will be a sequence, see the application framework in section 3.2 for details.

### 3.2. Application framework

The multi-domain optical network crosstalk attack tolerance scheme based on the multi-evidence trust model established in this paper has specific applications as follows:

**Step1:** When a crosstalk attack occurs in a multi-domain optical network, after accurately detecting and locating the source of the crosstalk attack, LMP quickly transmits the situation from the control plane to the evidence collection and processing module. Among them, the located network entity is the trustee, and the point of alarm information is the trustee.

**Step2:** Calculate the credibility between the believer and the trustee, if it is greater than or equal to the credibility threshold, meet the conditions for normal communication; if it is less than the credibility threshold, then transfer to the attack evidence collection and processing module.
Step3: The evidence collection and processing module classifies crosstalk attacks. Then the module inquires about the attack category and the degree of damage of the network entity and submits it to the trust management module, and then calculates the trust value.

Step4: When the Drui-j obtained by the trust calculation is greater than the initial trust value, it meets the intrusion tolerance conditions and communicates normally, and the trust value is stored and updated at the same time; when the Drui-j obtained by the trust calculation is not greater than their initial trust value, then Go to the trust database module.

Step5: Calculate the trust value of the believer and the trustee, and then get the comprehensive trust value Mrui-j between them. When Mrui-j is greater than the initial trust value, the intrusion tolerance condition is met and normal communication is performed; when Mrui-j is less than the initial trust value, the intrusion tolerance condition is not met and communication fails. At this time, LMP communicates through each PCE to recalculate its path.

4. Simulation

4.1. Network structure and Parameter settings

In order to verify the reliability and effectiveness of the multi-domain optical network crosstalk attack tolerance scheme based on the multi-evidence trust model, this paper uses VPI simulation software developed by VPI system to design and simulate optical fiber transmission systems. The simulation structure diagram is shown in the figure 2. This paper compares and analyzes the tolerance scheme proposed in this paper called D-TI, the tolerance scheme Q-TI proposed in literature [7] and the tolerance scheme J-TI proposed in literature [8]. The inter-domain routing protocol uses the Open Shortest Path First-Traffic Engineering protocol based on Traffic Engineering (OSPF-TE), and the signaling protocol uses the Resource Reservation Protocol-Traffic Engineering (RSVP-TE). The information transmission bit rate in the network is set to 40Gbit / s, the NRZ format signal with a duty cycle of 1, and the wavelength is set to 20. The Bit-rate Default is 40GHZ and the Sample Rate Default is 160e9bit/s. Fiber attenuation coefficient and dispersion is 0.2e-3dB/m and 2.0e-9s/m² respectively. The initial trust value is set to 0.5.

4.2. Experiment analysis

Figure 3 shows the comparison of simulation results before and after tolerance. Before and after the intrusion tolerance scheme with the multi-evidence trust model added, the quality of the eye diagram changes significantly. After adding the relevant program modules of the multi-evidence trust model's
intrusion tolerance scheme, the signal that had been attacked by crosstalk was cleared by the influence of the intrusion tolerance scheme. Therefore, the intrusion tolerance scheme in this paper can ensure the normal communication of multi-domain optical networks.

![Eye diagram before adopting tolerance scheme](image1)

![Eye diagram after adopting tolerance scheme](image2)

Figure 3. Comparison chart before and after tolerance

In the multi-domain optical network simulation environment of Figure 2, the relevant program modules of the D-TI scheme are added for experiments. At the same time, select OXC3 and OXC5 in D1 as the node A and node B of the experiment, select OXC8 in D2 as the node C of the experiment, and select OXC10 in D3 as the node D of the experiment. In the simulation experiment, it is assumed that the initial trust values of node A and node B are 0.9 and 0.6, respectively. If the attack strategy is adopted, a crosstalk attack occurs randomly in D1. The initial trust values of node C and node D are 0.5 and 0.4, respectively. If the attack strategy b is adopted, multiple crosstalk attacks randomly occur in the three domains.

![Tolerance under different strategies](image3)

Figure 4. Tolerance under different strategies

From the simulation results shown in figure 4, it can be seen that when strategy a is adopted, the node A with a high trust value suffers very little impact after being subjected to crosstalk attacks, and the node A still maintains a high level of trust. This is because it is a boundary node in D1, and it has almost no information interaction with other nodes in D1. However, when the node B is subjected to
crosstalk attacks, the impact is greater, but after a certain period of time, it can maintain a basic level of trust. This is because the node is a boundary node in D1, and there are more opportunities for information interaction with other nodes in D1. When strategy b is adopted, the border node C has more information interaction with the nodes and D3 in the domain. After being affected by multiple attacks, it gradually loses the possibility of tolerance. At this time, the PCE in the domain will redistribute routes for the link passing through the node. At the boundary the node D of D3, because it has less information interaction with the nodes and neighbours in the domain, even if the entire network has multiple crosstalk attacks, there is little impact on it. Therefore, when the node D adopts strategy b, normal information interaction can be maintained.

Acknowledgments
This work is supported by the National Science Foundation Project of P. R. China (No.61402529); the Natural Science Basic Research Plan in Shanxi Province of China (No.2020JM-361); the Young and Middle-aged Scientific Research Backbone Projects of Engineering University of PAP (No.KYGG201905); the Basic Research Foundation Project of Engineering University of PAP (No.WJY201920).

References
[1] Wagner, C., Eiselt, M., Grobe, K., Wei, J. L., Vegas Olmos, J.J., Tafur Monroy, I. (2016) Evaluation of Crosstalk Attacks in Access Networks Photonic Networks. In: 17. ITG-Symposium; Proceedings of, Leipzig, Germany, pp. 1-3.
[2] Monoyios, D., Manousakis, K., Christodoulou, C., Hadjiantonis, A., Vlachos K., Ellinas, G. (2016) Indirect crosstalk-aware routing and wavelength assignment in transparent optical networks with the use of Genetic Algorithms. In: 2016 18th International Conference on Transparent Optical Networks (ICTON), Trento, pp. 1-4.
[3] Kumar, W., Bhattacharya, S., Qazi, B. R., Elmirghani, J. M. H. (2012) An energy efficient double cluster head routing scheme for motorway vehicular networks. In: 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, pp. 141-146.
[4] Dai, Y. M., Wang, J. X., Yan-Wei, L.I. (2011) Distributed intrusion tolerant model based on voting and quantitative analysis. Application Research of Computers, 28:2242-2246.
[5] Feffer, A.L. (2015) Comprehensive security strategy for all-optical networks. M.D. Thesis, Massachusetts Institute of Technology, Massachusetts.
[6] Kwon, H., Kim, Y., Yoon, H., et al. (2017) Optimal Cluster Expansion-Based Intrusion Tolerant System to Prevent Denial of Service Attacks. Applied Sciences, 7:186-.
[7] Qin, H.W. (2009) Research on Theory and Application Technology of Network Intrusion Tolerance. M.D. Thesis, Nanjing University of Science and Technology, Nanjing.
[8] Ji, J.J. (2009) Research on Fault Tolerance and Tolerance of IP Network Based on Trust Relationship. M.D. Thesis, University of Electronic Science and Technology, Chengdu.
[9] Song, H., Pei, Q., Xiao, Y., Li, Z., Wang, Y. (2017) A Novel Recommendation Model Based on Trust Relations and Item Ratings in Social Networks. In: 2017 International Conference on Networking and Network Applications (NaNA), Kathmandu, pp. 17-23.
[10] Wang, J.L. (2017) Trust model with forgiveness scheme in social P2P system. M.D. Thesis, Dalian University of Technology, Dalian.