A security optical tree establishment protocol based on distributed path computation element in multi-domain optical networks

Yang Zhou¹, Qiwu Wu²*, Lingzhi Jiang¹

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

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

Abstract. How to build a secure optical tree through signalling mechanism in multi domain optical network is an important problem. To solve the problem, a security optical tree establishment protocol based on distributed Path Computation Element (PCE) in multi-domain optical networks was proposed. The protocol used a distributed PCE architecture. By expanding the optical network control plane and integrating multiple security mechanisms, the new signaling process of establishing a multicast optical tree was designed. The analysis and experimental results showed that, the protocol performed better performance in a malicious environment compared with the typical layered PCE-based protocol.

1. Introduction

In the multi-domain optical network multicast process, the wavelength channel between the source node and multiple destination nodes is called the multicast optical tree, and the signalling protocol is mainly used to maintain the connection of the optical tree. How to safely establish and maintain a multicast optical tree is critical [1].

For the establishment of multi-domain optical network security multicast tree, some research results have been made at home and abroad. In RFC 5520 [2] and RFC5920 [3], it analyzed the security requirements for the establishment of cross-domain optical paths in multi-domain optical networks and proposed security defense techniques. However, neither of them considered the method of establishing multicast trees. Literature [4] proposed a secure optical path establishment protocol with better performance than RSVP-TE signaling protocol, but it was only suitable for unicast. Literature [5] adopted the method of parallel calculation of each PCE under the layered PCE architecture. This scheme called pH-PCE greatly reduced the delay of road construction, but it was only applicable to unicast and did not consider security factors. Literature [6] proposed a fast optical path providing mechanism based on layered PCE architecture, which can provide a faster solution for establishing inter-domain paths, but this solution was only applicable to unicast and was not applicable to distributed architecture. Literature [7] proposed a hierarchical distributed topology discovery (HDTD) protocol based on hierarchical PCE. This protocol preserved the confidentiality of the domain while maintaining an abstract topology within the domain, but it lacked a security mechanism and was not applicable to distributed architecture. Literature [8] proposed a lightweight security signaling mechanism for multi-domain optical networks of energy Internet. It considered the security issues...
faced in multi-domain optical networks and improved existing signaling protocols, but it cannot be directly applied to the establishment of cross-domain multicast trees for multi-domain optical networks under the distributed PCE architecture.

Therefore, the current research results were mostly based on the layered PCE architecture, which did not consider the cross-domain road construction safety factors, and was only applicable to unicast solutions. There was no multi-domain optical network multicast security construction scheme under the distributed PCE architecture. Therefore, based on the previously proposed in literature [9] and various security mechanisms, this paper proposed security optical tree establishment protocol based on distributed architecture PCE in multi-domain optical network (DA-PCE).

2. Design of Multicast Security Establishment Mechanism

In this paper, the security plane of the multi-domain optical network was expanded first. As shown in Figure 1, the security-expanded multi-domain optical network control plane includes nine main units and three databases. The specific functions of the nine main units are as follows.

The information management unit is the centre for the converging and processing of various types of information on the control plane, and is mainly responsible for processing business information sent from other units. The security service unit mainly provides various security services such as message encryption and decryption, identity authentication, data source authentication and digital signature. The node control unit is mainly responsible for providing interface services for each node of the optical network, so that the nodes can communicate through the normal interface. The PCE unit receives the calculation request from the nodes, it performs path calculation based on the topology and resource information retained in the traffic engineering database (TED). The OSPF traffic engineering (OSPF-TE) unit is responsible for the release of TE information in the optical network domain, and updates and maintains the information in the TED. The resource reservation protocol TE (RSVP-TE) unit implements the RSVP-TE protocol. It configures the resources of the nodes based on the RSVP messages between the nodes, and finally realizes the establishment of a point-to-multipoint multicast tree. The link manager protocol (LMP) unit is the monitor of the entire network status, and it is mainly responsible for collecting the on-off status of optical links and the reservation of interface resources. When there is dangerous behaviour in the network, the unit immediately informs the OSPF-TE unit. The trust management unit is based on the LCT model [10]. It first calls the trust database to make a security judgment on the behaviour of each node and PCE. At the same time, when the node or PCE needs to query trust value data, it provides current and historical data query services. The key management unit applies the key management scheme in literature [9], which calls the key database to complete the generation, distribution and update of the key.

Figure 1. Safely expanded control plane
3. Security optical tree establishment protocol based on distributed PCE in multi-domain optical networks

3.1. Protocol ideas and related extensions

The DA-PCE protocol is a secure light tree establishment protocol that calculates the multicast tree in parallel and configures the wavelength in parallel in each domain under the distributed PCE architecture. In this protocol, the source node PCE plays a coordinated control role similar to the parent PCE in pH-PCE. The nodes in the domain report the link resource status in real time by starting the OSPF-TE unit, and then coordinate with each other through the PCE of each domain to calculate the route that meets the security constraints. Then the protocol uses RSVP-TE protocol for wavelength configuration, and finally realizes the safe establishment of multicast optical tree.

The DA-PCE protocol extends the PCEP communication protocol with a total of 6 types of PCEP messages. The Calculation message is generated by the source domain PCE, instructing each domain PCE to start path calculation based on this message. The Resource message is generated by the PCE in each domain and contains detailed topology and available wavelength information in each domain. The Available resource message is generated by the source domain PCE. The source domain PCE screens the topology information and wavelength information to obtain routing and wavelength information that meets the constraints. The Configuration success message is generated by the head node of each domain path segment, indicating that each domain has completed wavelength configuration. The Establish failure message is generated by the PCE in the source domain, indicating that the multicast light tree establishment failed. The Establish success message is generated by the PCE in the source domain, indicating that the multicast light tree is successfully established.

In order to simplify the description of the protocol flow of DA-PCE, this article defines the following 12 function modules. The F_Authen (A) module represents the identity authentication of node A. The F_Sig(A) module represents the digital signature using the private key of node A. The F_Ver(A) module represents the use of node A’s public key to verify the digital signature. The F_Session key module indicates that the shared session key is used for message encryption or decryption. The F_SC module indicates source authentication of messages. F_PCE module represents the use of an autonomous domain layer group key for message encryption or decryption. F_RA represents the use of routing algorithms to calculate routes. The F_Wave module indicates wavelength selection through RESV message reservation. The F_Instruction module indicates that the PCE of the source domain generates the calculation message. The F_Path-Key module represents the encryption related path. The F_Error indicates that multicast tree establishment failed.

3.2. Protocol process

This article uses Figure 2 as an example to describe the multicast tree-building process of the DA-PCE protocol in detail. There are four domains and four PCEs in Figure 2. The source node is 1 and the destination nodes are 8 and 10. The sequence number of the specific steps of the DA-PCE protocol process has been marked in Figure 2, the steps are as follows:

Step1: After receiving the multicast request \( R = \{ m_1, m_2, m_0 \} \), the source node 1 calls the F_Authen \(( m_1) \) and F_Session key modules.

Step2: PCE1 judges that the destination nodes \( m_2 \) and \( m_0 \) are not in D1. At this time, PCE1 calls F_Session key and F_Authen (PCE1) and sends it to the remaining PCEs. PCE1 finds that the domains of \( m_2 \) and \( m_0 \) are D3 and D4.

Step3: PCE1 calls F_Authen (PCE1), F_SC, F_Session key and F_RA to get an optimal abstract multicast tree \( T'_m(m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9, m_0) \), and then PCE1 calls F_PCE encryption and sends the loose path to PCE2, PCE3 and PCE4.
Step 4: PCE2, PCE3, and PCE4 call F_PCE to decrypt the loose path. They detect the loose paths and available wavelengths in their respective domains. Finally, PCE1 gets path $m_1$-$m_2$-$m_3$, PCE2 gets path $m_4$-$m_5$-$m_6$, PCE3 gets path $m_7$-$m_8$, and PCE4 gets path $m_9$-$m_{10}$. Then each PCE calls F_Wave for wavelength selection, calls F_Path-Key to generate a Calculation message, and finally calls F_PCE to encrypt the message and sends it to PCE1, waiting for PCE1 to uniformly configure resources.

Step 5: PCE1 calls F_PCE and F_Path-Key. PCE1 splices the PCRep sent from each PCE and calls F_Wave for wavelength selection, and then PCE1 calls F_Path-Key to encrypt the spliced path to obtain $T_{\text{PSK}}(m_1, m_4, m_5, m_7, m_9, m_{10})$. The path and the assigned wavelength are integrated into the Available resource message, the message is sent to the remaining PCEs. The remaining PCEs complete the path and wavelength configuration of the optical tree establishment.

Step 6: The path and the assigned wavelength are integrated into the Available resource message, F_PCE is called and the message is sent to the remaining PCEs. The remaining PCEs complete the path and wavelength configuration of the optical tree establishment. Each domain PCE calls the F_Group and F_Sig modules to send the message to the PCC and each branch node, and each node starts to check the path and available wavelength.

Step 7: The head nodes $m_1$ and $m_5$ of each sub-LSP call their respective F_SC, F_Group, and F_Ver (PCE), and then add the routing and wavelength information of the sub-LSP obtained in the PATH message. They finally call F_Group to encrypt the message and send it to the downstream node.

Step 8: When the downstream node gets the PATH message, it calls F_Group and F_SC to obtain the routing and wavelength information of the sub-LSP, and then judges the available wavelength. If the wavelength is available, the node calls F_Group and continues to send the message to the downstream node. If the wavelength is not available, the node calls F_Error.

Step 9: After the sub-LSP tail nodes $m_1$, $m_5$ and $m_{10}$ get the PATH message, they first call F_Group and F_SC to obtain the routing and wavelength information of the sub-LSP to generate a RESV message. The nodes passing on the reverse path call F_Group and F_SC to decrypt the RESV message, and then configure the wavelength according to the requirements of PCE1. After the wavelength configuration is completed, F_Group is called to encrypt the RESV message and continue to transmit to the head node of each sub-LSP. If an error occurs during this period, F_Error is called.

Step 10: Each child LSP head node $m_1$ and $m_5$ call F_Group and F_SC. If the wavelength configuration is successful, it means that the child LSP path configuration is successful, and a
Configuration success message is generated immediately, and the head node calls F_Session key and F_Authen \((m_1 \text{ or } m_3)\) Send to PCE1 and PCE2. If the wavelength configuration fails, F_Error is called.

Step11: PCE1 and PCE2 call F_Authen \((m_1 \text{ or } m_3)\), F_SC after receiving the message. If the message is correct, PCE2 calls F_PCE and F_Authen (PCE2) to send the message to PCE1.

Step12: PCE1 calls F_Authen (PCE2), F_SC and F_PCE. If PCE1 has collected all the Configuration success message at this time and has not received the RESV-ERROR message, an Establishment success message is generated. If a RESV-ERROR message is received, F_Error is called.

Step13: PCE1 calls the F_Session key module and sends the message to the source node, at which point the wavelength configuration is complete.

Step14: \(m_1\) calls F_Session key and F_SC, and then starts to transmit data to \(m_4\) and \(m_6\), and the establishment of the multicast light tree is completed.

4. Algorithms analysis

The DA-PCE protocol can resist various security threats including: message tampering, forgery and replay attacks, identity forgery attacks. The security of the protocol key depends on the discrete logarithm problem of elliptic curves and the irreversible one-way hash function. The delay of establishing the DA-PCE protocol multicast tree is composed of the multicast tree calculation delay, wavelength configuration delay, and path confirmation delay. All three are statistical constants, so the complexity of the establishment time of the protocol multicast tree is \(O(N)\). At the same time, the DA-PCE protocol does not increase the number of additional signaling and uses the flooding method to update the information in the TED, so the message complexity of the DA-PCE protocol is \(O(N^3)\).

5. Simulation

5.1. Network structure and Parameter settings

In order to verify the effectiveness of the DA-PCE protocol, this article uses NS-2 for experiments. Two types of protocols under the typical layered PCE architecture, the PH-PCE protocol in [5] and the HDTD protocol in [7], were selected as the comparison objects. At the same time, based on the optical network simulation system SPSP-NA [11] developed and designed by the research group, this paper writes the relevant modules of the three protocols. The network topology of the experiment is shown in Figure 3. Each domain has 20 nodes and 29 communication links. The network topology of HDTD protocol and PH-PCE protocol needs to be added with parent PCE. The time for the parent PCE to calculate the boundary node and the loose path is 25ms, and the average rate of the path request message in the experiment follows the Poisson distribution.

![Figure 3. Experimental simulation diagram](image)

5.2. Experiment analysis

Under the condition that the network load is 60Erl and the number of domains is 8, the data packet delivery rate of the three protocols in environments with different proportions of malicious nodes is shown in Figure 4. The experimental results show that as the proportion of malicious nodes increases, the data packet delivery rate of the three protocols decreases to varying degrees. The performance of
the PH-PCE protocol and the HDTD protocol is poor. This is because neither protocol supports the security mechanism. When malicious nodes increase in the network, normal nodes cannot identify malicious nodes, resulting in data packets being discarded by malicious nodes. The DA-PCE protocol uses a variety of security mechanisms to effectively monitor the malicious behaviour of nodes. Once the node's trust value is lower than the set threshold, the DA-PCE protocol will shield these nodes in routing and choose trust High-value nodes and paths, therefore, in a malicious node environment, the performance of the DA-PCE protocol is better.

Figure 4. Data packet delivery rate under different proportions of malicious nodes

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] Gao, T., Li, X., Guo, B., Yin, S. and Huang, S. (2018) A Shared Segment Protection Approach for Distributed Sub-Tree Based Optical Multicasting Scheme in Elastic Optical Datacenter Networks. In: 2018 Optical Fiber Communications Conference and Exposition (OFC), San Diego, CA, pp. 1-3.
[2] Bradford, R., Vasseur, J., Farrel. A. (2009) Preserving Topology Confidentiality in Inter-Domain Path Computation Using a Path-Key-Based Mechanism. http://datatracker.ietf.org/doc/rfc5920/.
[3] L. Fang, Ed. (2010) Security framework for mpls and gmpls networks. https://datatracker.ietf.org/doc/rfc5520/.
[4] Zhou, X.W., Wu, Q.W., Wang, J.P., Wang, L.N., Sun, Y. (2009) An efficient ASON secure optical path establishment protocol. Acta Photonica Sinica. 38:2071-2076.
[5] Wang, Z.W. (2012) Research on Cross-domain Parallel Road Construction Method of Optical Network Based on Layered PCE. M.D. Thesis, Chengdu University of Electronic Technology, Chengdu.
[6] Song, Y., Zhou, Z., Chen, Y. (2016) Hierarchical path-computation-element based lightpath control in multi-domain software defined optical network. In: 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI). IEEE, pp.52-55.
[7] Choi, J.S., Li, X. (2017) Hierarchical Distributed Topology Discovery Protocol for Multi-Domain SDN Networks. IEEE Communications Letters. 21:773-776.
[8] Cao, Y.D., Wang, W., Zhang, Y.L., Wang. J.S. (2018) Lightweight Security Signaling Mechanism in Optical Network for Smart Power Grid. In: 2018 IEEE International Conference on Computer and Communication Engineering Technology (CCET). Beijing, pp.110-113.
[9] Zhou, Y., Wu, Q.W., Jiang, L.Z. (2019) A group key management scheme based on distributed path calculation unit in multi-domain optical network. Computer Application. 9:167-171.

[10] Liu, Z.Q. (2017) Research on Key Problems of Trust Modeling in Mobile Distributed Environment. M.D. Thesis, Xidian University, Xian.

[11] Wu, Q.W., Wang, Q. Jiang, L.Z. (2014) Research and Implementation of ASON Secure Routing Simulation Platform Based on NS-2. Optical Communication Research.10:4-6.