引用本文：刘林：软件定义光网络的轻量级安全交互机制[J]. 光通信技术，2019，43(2)：42–45.

软件定义光网络的轻量级安全交互机制

刘 林

（国网辽宁省电力有限公司 大连供电公司，辽宁 大连 116011）

摘要：互联网新业务的迅猛发展对基于 OpenFlow 的软件定义光网络(SDON)提出了更高的安全性要求。对互联网多业务背景下 SDON 所面临的通信安全挑战进行了分析，提出了一种 SDON 的轻量级安全交互机制。该机制充分利用光网络现有的 OpenFlow 协议进行安全扩展加强，建立面向多业务的端到端可信连接，并以一般的 SDON 应用为典型场景对多业务 SDON 的轻量级安全信令交互进行仿真验证。仿真结果表明：该机制能有效提高 SDON 对多业务交互的安全性以及业务连接建立的成功率。

关键词：软件定义光网络；安全交互；可信连接；OpenFlow 协议

中图分类号：TN929.1　**文献标识码**：A　**文章编号**：1002-5561(2019)02-0042-04

DOI：10.13921/j.cnki.issn1002–5561.2019.02.010　**开放科学(资源服务)标识码(OSID)**：

Lightweight secure interaction mechanism for software defined optical network

LIU Lin

(Dalian power supply company, State Grid Liaoning Electric Power Co., Ltd., Dalian Liaoning 116011, China)

Abstract: With the rapid development of new Internet services, OpenFlow-based software defined optical network (SDON) requires higher security. This paper analyzes the communication security challenges faced by SDON under the background of internet multi-service, and proposes a lightweight security interaction mechanism for SDON. This mechanism makes full use of the existing OpenFlow protocol of optical network for security extension and enhancement to establish end-to-end trusted connection for multi-service. The lightweight security signaling interaction of multi-service SDON is simulated and validated in a typical SDON application scenario. Simulation results show that the mechanism can effectively improve the security of SDON to multi-service interaction and the success rate of service connection establishment.

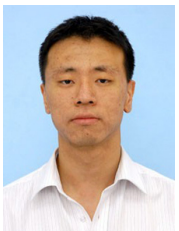
Key words: software defined optical network; security interaction; trusted connection; OpenFlow protocol

0 引言

目前基于软件定义网络(SDN)的思想，众多研究者提出了多种信息通信新型架构，如软件定义光网络(SDON)架构。SDON 主要分为数据转发平面、控制平面和应用平面[1–5]。控制平面和数据转发平面互相分离。控制信道与数据平面的数据传输信道相互独立，通过控制平面的信令协议交互，实现对数据传输业务连接的高效控制。因此，控制平面的可信连接技术受到了广泛重视。可信连接是指在光传送网技术体制的基础上，建立具备节点可信度、带宽和优先级保障的业务连接，确保数据传输业务的端对端安全。文献[6]针对当前光网络架构中存在协议安全性不足，提出了一种可信网络连接协议模型并进行安全论证，但该模型过于复杂，难以适应大规模光网络扩展的需要。文献[7]基于动态邻接信任熵，提出了一种安全路由算法，但是该算法在路由过程中所考虑的安全性因素较为单一，难以满足不同颗粒度业务的需求。文献[7,8]分别提出了多种可信网络的评价模型，但均未对 SDON 的协议交互安全性进行深入研究。为此，本文提出一种 SDON 的轻量级安全信令机制。

收稿日期：2018–09–29。

作者简介：刘林(1982–)，男，硕士研究生。主要研究方向是电力通信技术、软件定义光网络技术。负责完成的电力行业科技项目 4 项，获省部级科技进步奖 2 项、中国电力企业联合会信息化成果奖 6 项。



1 SDON 的通信安全分析

在互联网多业务的复杂背景下，SDON 的通信安

全问题具有一定的复杂性，更容易受到涉及光网络的所有层面的安全攻击。以 OpenFlow 为典型的信令协议用于光通道创建、拆除和修改等操作的具体执行[8-10]。通过 OpenFlow 信令交互能够完成 SDON 的资源按需分配，所以信令协议是 SDON 的关键技术之一[11-13]。由于 OpenFlow 信令协议的开放性，在一定程度上增加了 SDON 的安全风险，具体表现在以下几方面：

①窃听攻击：当控制平面进行 OpenFlow 的协议交互时，攻击者可能截获这些协议信息，破解出消息的内容，作为发动安全攻击的第一步。

②阻塞攻击：当 SDON 中非法网元生成大量的光连接请求，触发 OpenFlow 协议发起光连接的控制和交互信息，导致光网络负载剧增而阻塞率劣化。

③消息篡改：网络攻击者利用截获到的协议消息进行伪造，破坏业务连接的建立，引起正常的光连接失败并提高光网络的阻塞率。

④重放攻击：网络攻击者将截获到的协议消息进行复制，多次反复传送该消息，破坏正常的协议交互过程。

⑤通信量攻击：攻击者在一定的技术条件下有可能通过消息交互的流量，获取到协议交互的模式，包括光通信节点的标识以及协议消息交互过程。

综上所述，SDON 由于其集中控制平面技术的开放性，面临着一定的安全威胁。随着 SDON 的推广和网络安全技术的发展，对 OpenFlow 的安全交互技术研究将为面向互联网多业务的光网络提供重要的安全保证。

2 基于 OpenFlow 的轻量级安全交互机制

针对上述安全威胁，本文引入改进数字签名和消息反馈方法，在控制器节点与光交换机节点之间的 OpenFlow 协议交互过程中，给出了无需第三方参与的轻量级认证方法，从而完成数据传输之前的端到端可信连接的安全建立。

2.1 轻量级安全交互原理

本文提出的 SDON 轻量级安全交互机制是在 OpenFlow 协议的基础上进行安全增强。该安全交互机制引入非第三方参与的安全身份认证加密生成地址(CGA)算法，通过对光交换节点的身份认证，在保证光交换节点与控制器节点(CN)身份合法性的基础上完成两者的安全认证，最终实现 SDON 端到端可信连接的建立。SDON 的协议安全交互系统如图 1 所示。

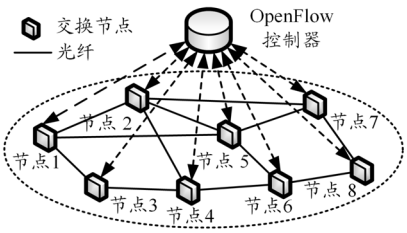


图 1 SDON 系统架构

该系统仍采用 SDN 的典型架构，由 1 个 OpenFlow 控制器和多个支持 OpenFlow 协议的光交换节点组成。所有的控制器和光交换节点内部都集成了 CGA 算法模块，负责对接收到的 OpenFlow 协议消息进行攻击检测与解密，以及对发送的 OpenFlow 协议消息进行加密。

2.2 轻量级安全交互流程

SDON 中，OpenFlow 协议的安全交互主要涉及控制器和光交换节点之间对 OpenFlow 协议信息的处理。本文基于增强的 OpenFlow 信令协议，在信令交互过程中，利用攻击预防和入侵检测的原理，对 OpenFlow 消息中的固定参数进行数字签名保护。具体流程描述如图 2 所示。

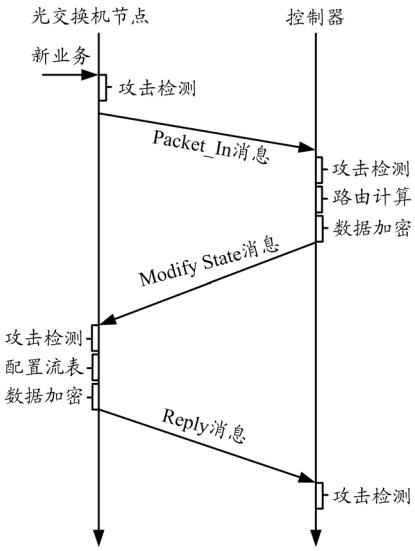


图 2 安全信令的交互过程

步骤 1：光交换节点收到来自业务终端的连接请求，生成 Packet-In 消息上报给控制器。

步骤 2：控制器接收到 Packet-In 消息，触发攻击检测。若检测通过，则用自身的私钥进行解密；若检测出安全攻击，则判断该光交换节点存在安全威胁，转到步骤 7。

步骤 3：控制器调用路由模块计算出光路由。

步骤 4：控制器将路由的相关参数信息封装在 Modify-State 消息的流表项中，并将光路径标识(Path-Id)、业务流表项或组表项(Flow/Group Entries)等可变值对象封装在该消息中，之后使用本节点的私钥对该消息中的 Path-Id 值、业务流表或组表项(Flow/Group Entries)等调用 CGA 算法进行加密。

步骤 5：光交换节点收到来自控制器的 Modify-State 消息后，首先触发攻击检测。若检测出安全攻击，

则通过告警信息上报控制器；若检测通过则用自身的私钥进行解密，生成 Reply 消息；对波长标签等固定值对象进行数字签名，封装在 Reply 消息中，之后向控制器发送该 Reply 消息。

步骤 6：控制器收到 Reply 消息后，同样先进行攻击检测。若攻击检测通过，数据平面的光交换节点通过已经建立的这条光路径传输业务数据，否则判断该光交换节点存在安全威胁，转到步骤 7。

步骤 7：控制器记录本次安全攻击，取消业务连接请求，并统计 SDON 的安全威胁程度，如果威胁程度高于阈值则触发 CGA 算法模块进行密钥更新。

2.3 安全性与复杂度分析

本文提出的安全信令机制中，安全性主要包括 4 个方面：完整性保护、内部攻击防护、重放攻击防护和伪造消息防护。

①完整性保护：通过对消息中不变对象的消息摘要进行数字签名及验证，检测来自外部和内部的消息篡改攻击，实现对信令消息的完整性保护。

②内部攻击防护：对重要可变对象采用反馈比较的方法，防止重要 QoS 参数被非法节点恶意篡改，保证实际光连接与业务请求的一致性。

③重放攻击防护：通过在信令消息中引入序列号，防范节点对信令消息的重放攻击。

④伪造消息防护：通过引入基于数字签名的消息认证方法，以确保信令消息本身的准确性。

假设整个网络有 n 个节点，其集合为 $\{N_1,N_2,\cdots,N_n\}$，N_s 为源节点，N_d 为目的节点；若光网络中的各节点均符合信令交互所需的保密性、完整性和可用性等要求，并提供端到端可管可控的安全服务，则 $SC(N_s,N_d)=\{N_s,\cdots,N_d\}$ 为节点 N_s 与 N_d 之间的安全连接（Security Connection，SC）。DSC 表示在节点 N_s 和 N_d 间满足安全度、阻塞率和时延要求的安全连接的度量。

$$DSC(N_s,N_d,V_{SC},V_B,V_D)=w_1\times\sum_s^d\frac{1}{V_{SC,i}}+w_2\times\sum_s^d\frac{1}{V_{B,i}}+w_3\times\sum_s^d\frac{1}{V_{D,i}} \quad (1)$$

其中，$V_{SC,i}$ 为节点 i 的综合安全度，$V_{B,i}=(1-P_{block})$ 为阻塞率满足度（阻塞率为 P_{block}），$V_{D,i}$ 为时延满足程度；w_1、w_2 和 w_3 分别为安全度、阻塞率和时延对应的权重，且满足 $(w_1+w_2+w_3)=1$ 的限制条件；s、d 分别为源节点、目的节点的 id 号。

复杂度是考量光网络信令机制的另一个关键指标。在协议复杂度方面，安全交互机制与原有 OpenFlow 协议消息以及交互过程保持整体一致性，无需额外的信令消息，只对信令消息进行轻量级的安全性扩展；在时间复杂度方面，引入了攻击检测与加解密处理，安全交互的时间复杂度为 $O(N)$，其中 N 为光通路所经过的平均节点数，虽然信令的安全处理时延会略有增加，但这对于安全等级要求较高的光网络，该时间复杂度在可接受范围内。

3 仿真结果与分析

为了验证所提出的安全交互机制，本文以支撑互联网的长距离光网络作为典型应用场景，从阻塞率、业务连接建立时延 2 个方面，对具有安全信令机制的 SDON 和不具有安全信令的 SDON 进行仿真评估。仿真环境采用 NS2 网络仿真软件构建，网络规模为包含 32 个节点的光网络，由于密集波分复用（DWDM）光网络的引入，利用单模光纤的带宽以及低损耗的特性，采用多个波长作为载波，允许各载波信道在光纤内同时传输。仿真环境中的连接请求到达模型采用泊松过程，流量分布采用均匀分布模型，即时间 t 内的连接请求服从泊松分布，业务强度采用归一化负载强度表示，其含义为各输入端口业务平均到达速率。

$$P_n(t)=\frac{(\lambda)^n}{n!}e^{-\lambda t} \quad (2)$$

在泊松分布下，参数 λ 为负载强度，其取值可采用均匀分布或非均匀分布，λ^{xy} 表示为输入端口 x 到输出端口 y 的流量，如式（3）所示。

$$\lambda^{xy}=\begin{cases}\lambda\left(Q+\dfrac{1-Q}{N}\right), & x=y\\ \lambda\left(\dfrac{1-Q}{N}\right)\end{cases} \quad (3)$$

其中，Q 为不均衡指数，Q 越大，流量分布越集中。仿真环境中的连接保持时间 T 满足指数分布，θ 为常数。

$$P(T\leqslant t)=\frac{1}{\theta}e^{\frac{t}{\theta}} \quad (4)$$

在光网络系统中分别采用安全交互机制与传统的非安全交互机制进行仿真，仿真结果如图 3、图 4 和图 5 所示。

从图 3 可以看出，当链路的波长数分别设置为 8 和 16，随着业务连接请求数目（负载）的增加，2 种波长配置模式的连接阻塞概率都在上升；但是随着波长数目的增加，平均连接阻塞率有了明显的改善。

从图 4 可以看出，随着安全攻击次数的增长，传统机制的阻塞率明显高于安全交互机制。在传统的信令机制下，对信令过程的安全攻击会导致信令处理的

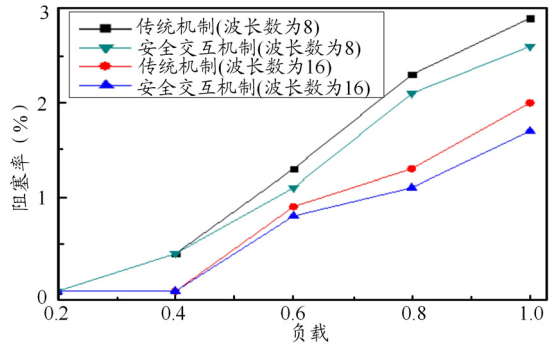


图 3 阻塞率比较

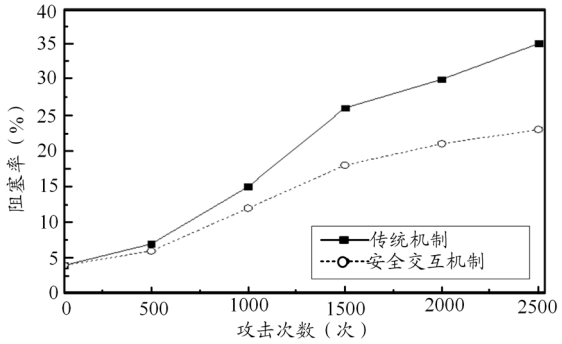


图 4 安全攻击情况下的阻塞率比较

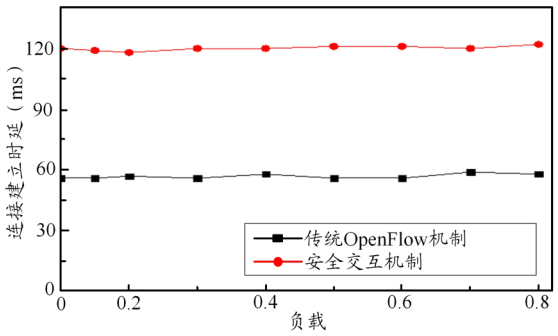


图 5 业务连接建立时延比较

混乱和波长资源非法占用，造成业务连接建立失败。而本文所提出的信令安全机制能较好地防范安全攻击所引发的业务连接阻塞。

从图 5 可以看出，安全交互机制的平均时延大于传统机制，这是因为业务连接请求规模的增大，密钥更新涉及的节点数增多，从而需要的处理时延也随之增加。这也是安全交互机制为了提高信令的安全性所付出的代价。

4 结束语

为了提高 SDON 对互联网多业务一般应用场景的支持能力，本文提出了一种 SDON 轻量级安全交互机制。该机制充分利用光网络现有的 OpenFlow 协议进行扩展加强，设计了以建立端到端的可信连接。仿真结果表明：本文所提出的安全交互机制能有效提高 SDON 对互联网业务交互的安全性，并保证了业务连接的成功率。

参考文献：

[1] SAMADI P, WEN K, XU J, et al. Software-defined optical network for metro-scale geographically distributed data centers [J]. Optics Express, 2016, 24(11): 12310–12320.

[2] YIN Y, WEN K, GEISLER D J, et al. Dynamic on-demand defragmentation in flexible bandwidth elastic optical net-works [J]. Optics Express, 2012, 20(2): 1798-1804.

[3] FURDEK M, WOSINSKA L, GOŚCIEÑ R, et al. An overview of security challenges in communication networks [C]// Inter-national Workshop on Resilient Networks Design and Modeling. International Workshop on Resilient Networks Design and Modeling 2016, Sept 13–15, 2016, Halmstad, Sweden. Halmstad: IEEE, 2016.

[4] WANG P, XU H, HUANG L, et al. Minimizing Controller Response Time Through Flow Redirecting in SDNs [J]. IEEE/ACM Transactions on Networking, 2018, 26(1): 562–575.

[5] GONG L, ZHU Z. Virtual Optical Network Embedding (VONE) Over Elastic Optical Networks [J]. Journal of Lightwave Technology, 2013, 32 (3): 450–460.

[6] AZODOLMOLKY S, PETERSEN M N, FAGERTUN A M, et al. SONEP: A Software-Defined optical Network emulation platform [C]// International Conference on Optical Network Design and Modeling 2014, May 19–21, 2014, Stockholm, Sweden. Stockholm: IEEE, 2014: 216–221.

[7] ZHANG J, ZHAO Y, JI Y. Software-Defined Optical Network Technique Evolution and Innovative Application [J]. In-formation & Communications Technologies, 2016(1): 10–16.

[8] CHEN M, SHOU G, HU Y, et al. Enabling Software-Defined Optical Networks based on OpenFlow Extension [C]// Opto-Electronics and Communications Conference 2015 (OECC 2015), June 28 –30, 2015, Shanghai, China. Shanghai: IEEE, 2015: 1–3.

[9] BAI Huifeng, ZHOU Ziguan, SONG Yanbin. Research on the multicast mechanism based on physical-layer-impairment awareness model for OpenFlow optical network[J]. Optoe-lectronics Letters, 2016, 12(3): 212–215.

[10] YANG H, ZHANG J, ZHAO Y, et al. Time-aware Software De-fined Networking for OpenFlow-based Datacenter Optical Networks[J]. Network Protocols & Algorithms, 2014, 6(4): 77–84.

[11] LI H, LIU Y. OpenFlow-based adaptive adjust-ment of optical path resources in dynamic optical net-works [J]. Optical Switching & Networking, 2016, 22(11): 105–116.

[12] CAO X, YOSHIKANE N, TSURITANI T, et al. Dynamic Open-flow-Controlled Optical Packet Switching Network [J]. Journal of Lightwave Technology, 2015, 33(8): 1500–1507.

[13] ISHIDA S, NISHIOKA I. Software-defined packet optical transport networks offering multiple services [C]// Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference 2013 (OFC/NFOEC 2013), March 17 –19,2013, Anaheim, USA. Anaheim: IEEE, 2013: 1–3.