中文核心期刊

一种光传送网的加密和密钥传送策略

唐世庆[1,2],孙以泽[1],王 琦[2],黄 蕾[2]
(1.东华大学 机械工程学院,上海 201620;2.上海贝尔股份有限公司,上海 201206)

摘要:介绍了一种基于 FPGA 实现的光传送网络加密策略,利用 ITU-T 标准 G.709 光数据单元(ODU*k*)帧结构中的预留开销字节传递密钥报文,将含有密钥的以太网包插入实验(EXP)开销字节。通过先进先出缓存器(FIFO)预存含有密钥的以太网包,以及采用寄存器控制发送包的方案。通过仿真和网络测速验证了该策略可以有效减少密钥传送延迟。

关键词:光传送网;加密;密钥;FPGA
中图分类号:TN948　　**文献标识码**:A　　**文章编号**:1002-5561(2018)04-0010-04
DOI:10.13921/j.cnki.issn1002-5561.2018.04.003

Scheme of encryption and key transport in optical transport network

TANG Shiqing[1,2], *SUN Yize*[1], *WANG Qi*[2], *HUANG Lei*[2]
(1. College of Mechanical Engineering, Donghua University, Shanghai 201620, China; 2. Shanghai Bell Co., Ltd., Shanghai 201206, China)

Abstract: This paper proposes an encryption scheme based on FPGA in optical transport network. The reserved overhead bytes are used to transmit the key message in the optical channel data unit (ODU*k*) frame structure of ITU-T G.709 standard, and the ethernet packets of encryption key can be inserted into the Experimental (EXP) overhead byte. The ethernet packets with the encryption key are prestored in the buffer of first in first out(FIFO), and the packets are sent by the register control. The scheme that reduces latency time has been verified by the simulation and the network test.

Key words: OTN; encryption; key; FPGA

0 引言

企业和个人数据大规模迁移至云端,数据安全至关重要。未经加密的互联网通信不再安全可靠,所有通信应该有条件地进行加密。常见的网络加密方案有路由网关加密方法、中心密钥服务器和物理层加密方法等。运用网关加密方法会增加成本和延迟,中心密钥服务器也会显著增加系统投入和维护成本。而物理层加密方法通过光传送网(OTN)对光学层端至端进行加密是一种低延迟、与业务无关的解决方案,可以有效地利用宝贵的网络资源。

本文介绍基于 FPGA 实现的 OTN 的物理层加密方法,此方法可以有效地减少密钥报文的传送延迟时间,且通过网络边缘的密钥交换算法,可省去中心密钥服务器,降低客户投入和运行成本。本方案适用于多个运营商,密钥可在光信道数据单元(ODU)服务的源端和宿端自动交换[1]。

收稿日期:2017-09-22。

作者简介:唐世庆(1974-),男,博士,主要研究方向为光传输产品芯片设计与验证。

1 OTN 加密和密钥传送

1.1 加密算法

数据加密是通过加密算法或加密密钥将明文转变为密文,终端用户则通过解密算法和解密密钥将密文恢复为明文。两种常见的加密算法分为对称加密算法和不对称加密算法。对称加密有多种算法,因为它的效率很高,所以被广泛使用在很多核心加密协议中。目前,最流行的对称加密标准是高级加密标准(AES),该标准由美国国家标准与技术研究院(NIST) 在 2001

年发布。AES 的区块长度固定为 128bit，密钥长度可以是 128bit、192bit 或 256bit，例如最常用、最安全的标准 AES-256 采用 256bit 密钥长度[2]。本文使用伽罗瓦/计数器模式（Galois/Counter Mode, GCM）的 AES-256 加密结构，其结构图如图 1 所示。GCM 模式 AES-256 结构带有 128bit 伽罗瓦消息验证码（Galois Message authentication Code Mode, GMAC）认证标签，基本算法取 128bit 分组加密。密钥在模块间或两个及以上的实体间建立，这是一种分布式对称密钥。

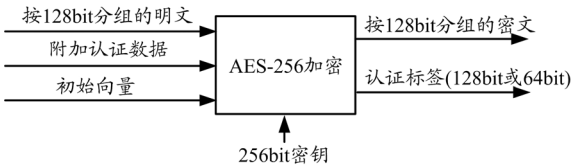

图 1 GCM 模式 AES-256 结构图

1.2 OTN 加密

由 ITU-T G.709 标准定义的 OTN 是一个多业务、多速率聚合层，它能够支持几乎所有客户类型和协议的复用、传输和交换，包括以太网、光同步数字传输网（SONET/SDH），以及 1~100Gb/s 数据速率的光纤通道等。相比于第二层（L2）和第三层（L3）加密，对 OTN 第一层（L1）进行加密，能提供高效的、低延迟的安全传送解决方案，并在服务类型、速率和网络体系结构等方面有很高的灵活度，因此这种加密方式对网络运营商极具吸引力。

光信道传送单元（OTU*k*）的帧结构如图 2 所示。OTU 的加密，即对图中光信道净荷单元（OPU*k*）进行加密。加密模式选择 GCM 模式 AES-256。当前密钥和下一个密钥通过一个 OTN 开销通道发送到远端。在远端，密钥与本地版本相比较，如果匹配，可以进行密钥切换。一旦确认密钥匹配，本地软件提前几帧设置密钥会话终结。当密钥会话期满时，密钥切换发生。每帧加密数据在 OPU*k* 自动发送。GCM 认证标签随 ODU*k* 的保留字节每一帧（64bit）或每两帧（128bit）自动发送。认证增加了安全性，阻止了企图解密的攻击。在大多数情况下，认证标签随净荷一起从源端发到目的地。在目的地，要在解密净荷之前使带内认证标签生效。如果标签不正确，目的地则忽略此业务。

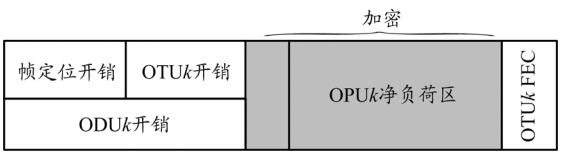

图 2 加密的 OTU*k* 帧

1.3 在 ODU*k* 上传送密钥信息

关于密钥交换和传送，目前还没有相关标准。ITU-T G.709 定义了 ODU*k* 开销中的 EXP 字节和其它一些保留字节。通过这些保留字节，安全信道可以在 ODU 通道甚至边界建立。本文采用 EXP 开销字节传送密钥信息，因此密钥的传送没有增加额外的带宽消耗。

在 ODU*k* 开销上传送密钥的系统结构如图 3 所示。节点 A 是近端网元，节点 B 是远端网元。节点 A、B 通常由一个设备控制器和至少一个线路控制器组成。在节点 A 端，带虚拟局域网（Virtual Local Area Network, VLAN）标签的以太网包用来承载来自设备控制器的密钥信息，通过以太网交换芯片和开销预处理 FPGA，在 OTN 开销处理芯片中将密钥信息插入 EXP 开销字节。在节点 B 端，OTN 开销处理芯片从 OTU4 中提取 EXP 字节中的密钥信息，通过开销预处理 FPGA 和以太网交换芯片，带 VLAN 的以太网包将接收到的密钥信息送到设备控制器。线路控制器直接与以太网交换芯片相连接。以太网交换芯片通过运行在机架之间的内部局域网（Internal Local Area Network, ILAN）标签与其它线路控制器和设备控制器相连接。物理（MAC）地址在网元中是唯一的，按机架和槽位分配。在网络中可能有重复的 MAC 地址，因此需要用 VLAN 加以区分。在每个节点的设备控制器或线路控制器与开销预处理 FPGA 之间都有一个 VLAN。EXP 字节在 100G OTU4 条件下速率带宽为 13.702MHz，因此，以太网交换芯片和开销预处理 FPGA 连接采用百兆媒体独立接口（Medium Independent Interface，MII）。

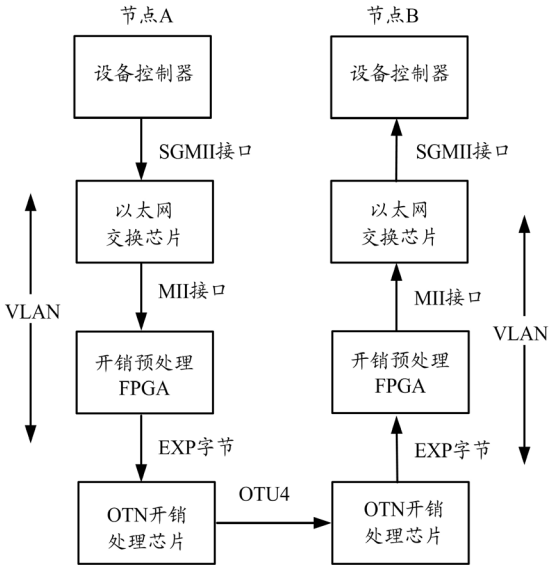

图 3 在 ODU*k* 开销上传送密钥的系统结构图

设备控制器和以太网交换芯片连接为千兆媒体独立接口(Gigabit Medium Independent Interface,GMII),余下带宽可用于传送其它业务。

输入开销预处理 FPGA 的以太网包格式如图 4 所示。由目的地址字段、源地址字段、标签协议标识字段、标签控制信息字段、类型字段、物理和数据通道标识码字段、数据字段以及帧校验序列字段组成。目的地址字段为 6 字节,指示目的 MAC 地址。源地址为6字节, 指示源 MAC 地址。标签协议标识字段为 2 字节,值为 0x8100。标签控制信息字段为 2 字节,包括用户优先级(3bit)、规范格式指示器(1bit)和 VLAN 标识(12bit)。类型字段为 2 字节。物理和数据通道标识码字段为 5 字节,由 3 字节物理通道标识和 2 字节错误校正码(Error Correcting Code, ECC)标识组成。数据字段最大长度是 256 字节,最小长度是 37 字节。帧校验序列字段为 4 字节。

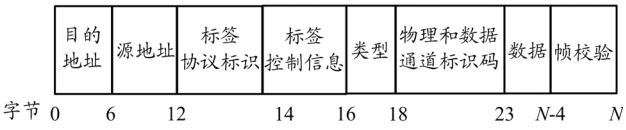

图 4 输入开销预处理 FPGA 的以太网包格式

输入 OTN 开销处理芯片的以太网包格式采用高级数据链路控制 (High-level Data Link Control, HDLC)帧格式。HDLC 帧格式如图 5 所示,包括开始标志、信息字段、帧校验字段和结束标志。开始标志和结束标志均为 8bit 标志码“01111110”。因为此链路为点到点,所以没有使用 HDLC 的地址字段。HDLC 净荷为 96 字节,包括信息字段和帧校验字段。HDLC 的帧校验字段需要使用循环冗余校验 (Cyclic Redundancy Check, CRC)编码器,会对从开始标志之后的第一个净荷字节开始,到最后一个净荷字节做 CRC 计算。16bit CRC 计算基于多项式 $X^{16}+X^{12}+X^5+1$, 每一帧初始值为 0xffff。2 字节 CRC 校验值插入 HDLC 信息字段之后的帧校验字段。先插入低字节,再插入高字节。

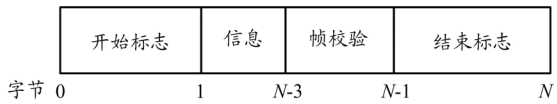

图 5 输入 OTN 开销处理芯片的 HDLC 帧格式

为保证标志码的唯一性,同时兼顾帧内数据的透明性,HDLC 编码器在发送端逐比特监视开始标志和结束标志之间的 HDLC 净荷, 当发现有连续 5 个“1”出现时,HDLC 编码器会在连续 5 个“1”后面插入 1 个填充比特“0”。在接收端,HDLC 解码在接收的数据流中搜索标志码“01111110”,搜索以比特为粒度,因为不能确保标志字节在接收数据中正好是固定的字节边界,标志字节可以在接收数据比特流的任意比特位置起始。假如,接收到 1 个标志码“01111110”,后面紧跟着的又是一个标志码“01111110”或者多于 6 个连续 “1”,HDLC 解码器认为这是一个有效的 HDLC 帧,指示为帧起始。接着搜索其后的比特流,当发现 5 个连续“1”出现后,则删除其后的 1 个比特“0”,由此恢复为原来的比特流。在两个标志码之间的整个帧需要按此过程检查和恢复。

1.4 密钥报文快速传送实现

传统的密钥报文传送方法由设备控制器和线路控制器的软件发送, 本文用 FPGA 寄存器控制 FIFO 发送密钥报文的方案取代传统方案,大大减少了密钥报文的传送延迟时间。寄存器控制 FIFO 发送密钥报文方案如图 6 所示。在密钥报文发送方向,软件通过 FPGA 寄存器接口向发送密钥 FIFO 写密钥报文数据,并写该报文的长度。当软件向发送控制寄存器写“1”时,发送密钥 FIFO 中的密钥报文全部发送出去,当报文发送完毕,发送控制寄存器置“0”。发送密钥 FIFO 至少能装载一个报文。在密钥报文接收方向,接收密钥 FIFO 存储接收到的密钥报文,当一个 96 字节报文被接收,会发出一个中断。当软件检测到该中断,则将接收控制寄存器比特置“1”,接着读取接收密钥 FIFO 中的报文数据,当软件读取完一个接收报文,将接收结束指示寄存器置“1”,表示一个密钥报文读取完毕。软件继续检测中断,若仍有中断,继续读取接收到的密钥报文,直至所有密钥报文读出。密钥报文最大包长是固定长度,接收密钥 FIFO 至少能装载两个报文, 由于接收密钥 FIFO 接收到一个密钥报文后会立即产生中断并被软件读出,因此即使在大数据量处理情况下,也不会出现 FIFO 溢出情况。

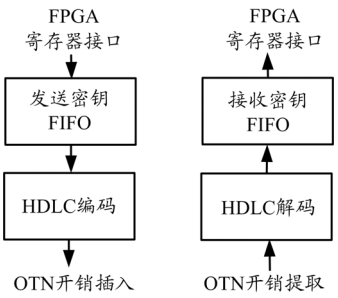

图 6 寄存器控制 FIFO 发送密钥报文方案

2 测试结果

本文对所提出的策略进行仿真, 仿真结果如图 7 所示。其中,igmii_txclk_mac 是 FIFO 控制的发包时钟信号,igmii_txd_mac 是 FIFO 控制的发包数据信号,ig-

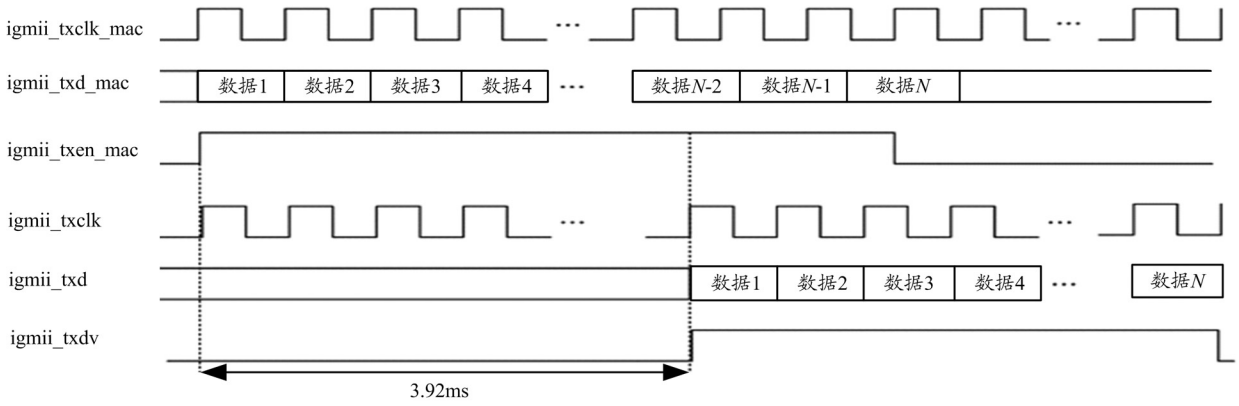

图 7 通过寄存器控制 FIFO 减少延迟时间的仿真波形

mii_txen_mac 是 FIFO 控制的发包使能信号。而 igmii_txclk 是软件控制的发包时钟信号，igmii_txd 是软件控制的发包数据信号，igmii_txdv 是软件控制的发包数据使能信号。从仿真结果可以看出，采用 FPGA 寄存器控制 FIFO 发送密钥报文，与采用设备控制器或线路控制器软件发送密钥报文的方式相比较，延时会减少 3.92ms。

3 结束语

OTN 加密的优势在于它支持灵活、可扩展的业务交付模型，而无需牺牲网络延迟、效率等，并有能力支持各种各样的业务和客户类型。本文提出的基于寄存器控制 FIFO 的密钥发包解决方案可以加速密钥报文传送，减小在线路控制卡中的密钥传送延迟。同时寄存器配置执行方式有益于增加软件灵活性、简化网络管理以及增强安全设备可靠性。另外，本方案还利用兼容协议的 EXP 字节提供密钥通信服务，保障密钥传送安全，减少成本，提高竞争力。

参考文献：

[1] ITU-T. Interfaces for the optical transport network: G.709/Y.1331-2012 [S]. Switzerland: ITU-T, 2012.

[2] IEEE. Local and metropolitan area networks - Media Access Control (MAC) Security-Amendment 1: Galois Counter Mode - Advanced Encryption Standard-256 (GCM-AES-256) Cipher Suite: IEEE 802. 1AEbn-2011 [S]. New York: IEEE, 2011.

[3] IEEE. Local and metropolitan area networks: media access control (mac) Security: IEEE Std 802. 1AE-2006[S]. New York: IEEE, 2006.

[4] IEEE. Local and metropolitan area networks. Bridges and Bridged Networks: IEEE Std 802. 1Q-2014[S]. New York: IEEE, 2014.

[5] ISO. Information technology-Telecommunications and information exchange between systems-High-level data link control (HDLC) procedures: ISO/IEC 13239-2002[S]. Switzerland: ISO, 2002.