中文核心期刊

EPON 系统中安全服务策略分析及改进(本期优秀论文)

徐 鹏[1],胡国荣[1],张 迅[2]
(1.中国科学院 微电子研究所,北京 100029; 2.巴黎高等电子研究所 电子工程系,巴黎)

摘要:从以太网无源光网络(EPON)潜在隐患入手,分析窃听、拒绝服务、伪装及窃取服务等安全风险,提出一种基于 ECC 公钥数字证书的认证方案。同时,引进了基于 CCM 方式的数据认证加密方案,并在 OMNeT 环境中仿真该认证及加密方案,并与其它现有方案进行对比分析。从结果可知,该认证方案具有低延时特性,且满足不可否认性等安全性问题。

关键词:安全;以太网无源光网络;认证方案;椭圆曲线密码;高级加密算法
中图分类号:TP391　　文献标识码:A　　文章编号:1002-5561(2013)01-001-04

Analysis and improvement of secueity services schemes in EPON system

XU Peng[1], *HU Guo-rong*[1], *ZHANG Xun*[2]
(1.Institute of Microelectronics,Chinese Academy of Sciences, Beijing 100029,China; 2. Electronics Engineering, ISEP,Paris)

Abstract:This paper firstly analyze various types of potential network structure targeted attacks in Ethernet passive optical network, EPON, such as passive monitoring,denial of service (DoS),masquerading,and theft of service (ToS).Basing on the analyzing results,an authentication scheme based on ECC public algorithm and CCM-AES additional authentication encryption method will be illustrated.And then relevant simulation results are following.Ultimately,a comparison between this paper indicated authentication and encryption scheme and other works gives in order to measure the performance.From the comparison,the results demonstrate the efficiency of the indicated security schemes which also meet the security condition of non-renouncement.

Key words: security; enter net passive optical network (EPON); authentication scheme; ECC; AES

0 引言

作为网络互通的主要部分,接入网技术的发展瓶颈已严重制约了高速网络的发展及提升空间。以太网无源光网络(EPON)系统,结合了以太网成熟的、普及的网络技术以及无源光网络的高速性,在工业界将视为 FTTx 系统改造中的主要技术被纳入规划或已经实施。同时,在学术界,EPON 系统将做为向下一代光网络(Next Generation PON, NGPON)系统中的过渡技术,在 NGPON-I 系统以及下一代 OFDMA PON 的研究中起到基石作用。

收稿日期:2012-09-26。
基金项目:Sino-France XU Guangqi Project:26223NK(法国学人徐光启项目:26223NK)资助。
作者简介:徐鹏(1987-)男,硕士研究生,主研方向为数字通信芯片设计、计算机通信系统安全。

EPON 技术中引入的点到多点(P2MP)是核心技术之一,由于其结构的特殊性及下行传输媒介的传播特性,不可避免地引入了较为普遍的网络安全威胁。由于简单的 LLID 滤除方式,使下行广播通道数据能被任何想窃听的组织或个人在混杂模式下访问,如此而来就造成了被动监听,拒绝服务攻击等问题,所以安全方案将是 EPON 正常通信的基础保证。

本文首先从 EPON 的结构出发,引出潜在的安全威胁,然后再在网络安全服务基本保证的基础上提出基于 ECC 的数字证书认证方案以及 CCM-AES 认证加密策略,最后分析比对结果。

1 EPON 系统简介

典型的 EPON 系统是一个有光线路终端(OLT)、光网络单元(ONU)以及光分配网络(ODN)组成,为单纤双

向系统。采用 TDMA 多址接入方式避免了数据冲突而引入的损耗。

1.1 MPCP

MPCP 协议是 MAC 控制子层的主要部分,用于实现一个可控制的网络配置,如 ONU 的自动发现和注册、测距以及上行接入等。为了完成点对多点的控制功能,引入 5 个新的 MPCP 控制帧:GATE、REPORT、REGISTER_REQ、REGISTER 以及 REGISTER_ACK。这 5 个 MPCP 控制帧采用标准的以太网帧格式,同时由于它们在 EPON 中分别被赋予不同的用途。其中,GATE 和 REPORT 用于带宽分配机制和测距,GATE、REPORT、REGISTER_REQ、REGISTER 以及 REGISTER_ACK 用于自动发现和注册机制[1]。

自动发现与注册机制是保证 OLT 和 ONU 之间能够正常通信的关键技术之一,用于完成 ONU 向 OLT 的注册。在 GATE/REPORT 机制中,ONU 端等待 OLT 发出的 GATE,然后通过 REPORT 向 OLT 报告自己的状态,并请求自己所需要的带宽。

1.2 DBA

为了提高上行传输的带宽利用率,在 OLT 中 MAC 控制层上引入动态带宽分配算法模块,负责动态分配合适的时隙给对应的 ONU。目前,EPON 系统中的 DBA 可以分为静态统计复用类算法(IPACT 及其扩展算法)、QoS 保证算法(BGP 及其扩展算法)以及去中心类算法三种。

2 安全威胁分析

EPON 网络中的安全隐患包括窃听、拒绝服务、伪装和窃取服务等[2]。

①窃听。EPON 中,只要将其中一个注册过的 ONU 的工作方式设置为混杂模式,就可以在下行方向进行窃听。攻击者所要做的是将基于 LLID 的过滤规则失效即可。同时,所有窃听者(ONU)都是被动进行的,OLT 无法察觉。

②拒绝服务。EPON 系统中的拒绝服务攻击时通过扰乱敏感数据(包括 MAC 地址和 LLID 编号)来实现的。伪造假冒的 REPORT MPCPDU 请求过大的带宽,造成有缺陷的 DBA 算法分配大量的系统资源给非法用户,而其它用户却处于“挨饿”状态。

③伪装和窃取服务。EPON 网络中的初始伪装攻击是基于被动监测的,在此期间,恶意用户收集目标设备(ONU)信息,包括 LLID 数目、MAC 地址和 RRT 等。这些信息用来对恶意 ONU 进行伪装,主要通过操纵每个传输数据帧(MAC 以及 LLID 地址)中的敏感数据,达到伪装目的。

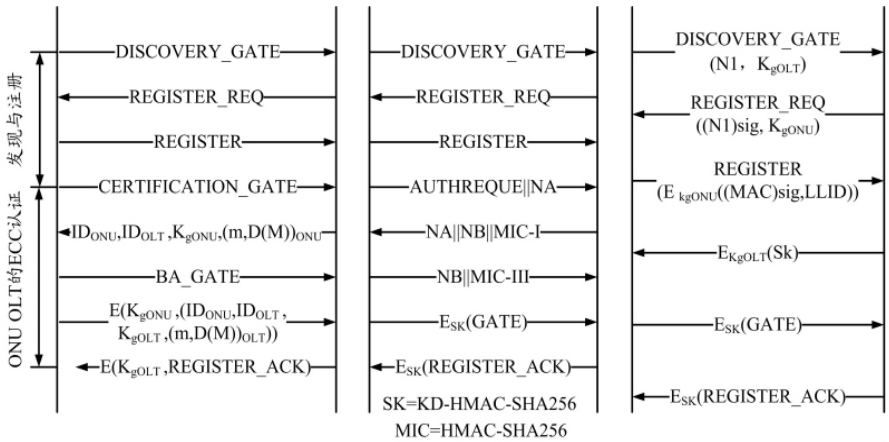
3 安全服务

在现有的关于 EPON 系统的安全方案中有基于搅动密码机制的方案[3],有基于 AES 加密方案的机制,有基于 RADIUS 认证方案的复杂安全策略[4],同时还有基于 IPSec 安全协议的方案[5]。其中不仅包括了数据加密方案,同时不乏有认证策略。

3.1 认证方案

EPON 系统中对 OLT 的认证,主要是为了防止 ODN 或者其他非法 OLT 冒充合法 OLT 与其它网络中的 ONU 进行正常通信;对 ONU 的认证主要是用来防止 EPON 中的自动发现和注册过程中 ONU 自动分配 LLID 的问题以及非法入侵的 ONU 假装合法 ONU 发送数据的问题。认证过程的选择主要在认证完成后和在注册完成前进行,然而,文献[5]提出了一种基于注册过程的认证方式,其过程是在 REGISTER_REQ 帧中携带认证密钥。

文献[6]和文献[4]分别提出了基于公钥密码以及对称密码的认证方案,它们都完成于 ONU 的注册过程中,图 1(a)和图 1(b)分别描述了两种认证方案。



(a) 基于 ECC 加密的认证方案(I) (b) 基于挑战响应的认证方案 (c) 基于 ECC 加密的认证方案(II)

图 1 各类认证方案比较

文献[6]是采用对称密钥体系中“挑战响应”的方式来进行认证方案的,借助于 HASH 函数以及 AES 加密方案以及 SHA256 哈希函数,完成了基于随机数的挑战策略,从实现目标方面,确实完成了 OLT 以及 ONU 双方的认证。但是,其实现过程中设计四次

HMAC-SHA256 计算生成消息认证码(MIC),提前预设值共享密钥,和两次 KD-HMAC-SHA256,不论存储敏感消息、计算消耗还是传输数据流等方面都有缺陷。而方案[4]中,认证过程在注册请求之后进行,整个过程在公钥体系中进行,而且在认证过程完成后也未确定用来进行数据加密的会话密钥。

图 1(c)是在分析了以上两种认证方案的基础上提出的基于 ECC 公钥体系的认证策略。选择 ECC 算法的原因是公钥密钥体系可以很好地实现加密和数字签名等机制。相对于 RSA 算法,ECC 有更高的安全性及较短的密钥长度。

本认证方案可归纳为如下:

①OLT 发送 Discovery GATE 帧,其中在 Pad 域中添加 20 字节 (160 位)OLT 的公钥 KgOLT 以及 4 字节的 N1 随机数。此处,数据发送为广播形式。

②ONU 收到 GATE MPCPDU 帧后,将随机数 N1 用自己的私钥做签名,然后协同 20 字节 ONU 的公钥作为 REGISTER_REQ 帧中内容发送给 OLT。

③OLT 收到注册请求后,析取出 ONU 的公钥,同时用公钥解密收到的签名部分,如果正确得到随机数 N1,可说明 ONU 的认证通过;否则,中断认证。正确接收到 REGISTER_REQ 帧并析取出相关数据域后,OLT 将分配 LLID 给相应 ONU,并将分配好的 LLID 用 ONU 的公钥加密,同时将 ONU 的 MAC 地址用 ONU 公钥加密后,再用 OLT 的私钥签名后第二次用 ONU 的公钥加密,并将加密后的数据发送给 ONU。

④ONU 收到 REGSITER 控制帧后,用自己的密钥进行解密,并得到相应 LLID 以及用 OLT 私钥签名过的 ONU-MAC 地址,然后通过存于自身的 OLT 的公钥验证是否是 OLT 自签名。如果是则将数据中另一项 (MAC)K_{gONU} 用自己的私钥解密,并验证 OLT 发送的 MAC 地址是否与自身 MAC 地址匹配,如果匹配则 OLT 是合法的;否则,反之。ONU 通过对 OLT 的认证之后,通过附加消息发送会话密钥 Sk 给 OLT,该消息可以用 OLT 的公钥加密,也可以不用,理由取决于 E-PON 上行信道传输的相对安全性。

⑤收到会话密钥传输消息之后,OLT 将用继续完成 GATE 的发送,此时用会话密钥加密数据帧以及确认 GATE 帧中的 Payload 域;使用第三步中生成的 (LLID)K_{gONU} 来生成新的 LLID 来填充前导码中的相关区域;将确认 GATE 帧发送给 ONU。

⑥ONU 收到 REGISTER 以及确认 GATE 数据帧之后,发送 REGISTER_ACK 帧,注册过程完成。

3.1.1 认证约束条件及安全性

信息安全伴随着计算机网络、信息系统的发展而存在的,只有在一定的约束条件下存在相对安全的安全方案,我们就可以说是安全算法。本方案中我们规定的约束条件如下:

①OLT 和 ONU 各自预存有数字证书;双方证书是可以被权威结构认证的;此过程在仿真中是通过网络建立而产生公私钥对而实现的。

②光分路器(ODN)是安全的(该假设在文献[2]中对 PSC 结构的介绍)。

③OLT 单元中预存的各 ONU 映射表 (用于存贮 LLID,MAC,K_{gONU} 以及 Sk)是安全不可泄漏的。

3.2 加密方案

目前 EPON 系统的加密基本定位于数据链路层。同时,密钥管理又是影响数据保密性的一个关键因素,所以在本小节,我们主要对比分析了数据加密方案,然后讨论密钥的管理问题。

3.2.1 数据加密方案

EPON 链路层中数据加密方面的工作主要集中在基于 AES 的 CRT 和 CBC 模式的数据加密[7][8]以及三重搅动加密的方案[3]。三重搅动算法使用三个级联搅动器,增加密钥数量,采用时域关联的异或运算,运算成本较低。但相对于 AES 算法,攻击者仍有较高的概率可以获得密钥。文献[2]中详细描述了 AES-CRT 的加密模式及密钥产生、计数器使用及加解密模块的统一性问题,并详细分析了其加密过程。在本文中,我们基于现有方案,提出基于 CCMP 的加密方案。

CCMP 是基于 CCM 的 AES 加密方案,它可以提供数据保密、认证、完整性以及重放保护等服务。CCM 是 IETF 定义的一种用于块密码的通过模式,它有 M 和 L 两个参数,分别表示 MIC 和 CCMP 的长度。CCM 方案要求每一次会话都有一个临时密钥,同时用一个 48 位长的包数(PN)作为随机数。关于 CCMP 的详细内容可以参看[9]。

3.2.2 密钥管理问题

在 EPON 的链路层安全方案中设计到的密钥管理问题主要有:初始会话密钥建立以及密钥更新。通过第 3.1 节中认证方案的描述可知,在 ONU 成功完成一次发现注册之后,它就和 OLT 建立了一个用于加密初始密钥,现在重点考虑密钥更新及密钥同步问题。密钥的更新包括认证过程中的数字证书的更新以及加密数据所用的加密密钥的更新。数字证书及公钥的更新即可由 OLT 发起并发送新的证书,也可由 ONU 发

起并将其公钥附加与发给 OLT 的消息帧中。然而，会话密钥的发起可以用由 OLT 和 ONU 完成，但会话密钥的产生由 ONU 完成，并上传到 OLT(基于上行链路的相对安全性假设)。完成密钥更新后的首要问题就是协同新密钥的使用时间，该过程是由 OLT 中密钥生效时间确定的。

4 数据对比及结果分析

数据比对主要用来分析认证过程中的交互方案及认证各过程所需时间；加密方案主要考虑加密相同长度的字符串的延时。图 2 中，方案 1 代表本文中改进的认证方案，它基于 ECC 的加密签名机制；方案 2 的仿真结果是开放的 EPON 网络结构，其中不包含加密及认证方案；方案 3 为文献[6]中提到的认证方案；方案 4 为文献[4]中提到的方案。从图 3 可知，即使在没有加密认证方案时，4 个 ONU 的认证过程也要使用约 50ms(仅为仿真结果)的时间，从而取得 ONU 的全注册。分析可知，相对于数据处理来说，在网络上完成 OLT 与 ONU 交互会加大注册的延时，这是因为不仅 OLT 或 ONU 都得相应相关协议处理流程，还有上行时隙的分配以及传输延迟等问题。文献[6,4]中，八步交互在 ONU 节点较多时会出现较大的注册延时以及注册时期发生的较多碰撞。而本文中的方案在不降低安全性的前提下，较大程度地缩短了注册所耗时间，且在较多 ONU 同时注册时也不会发生较多的碰撞。

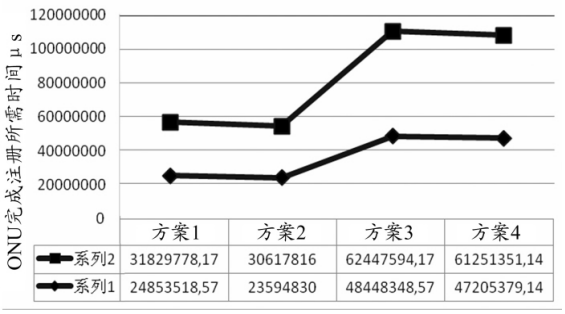


图 2 认证方案的仿真结果

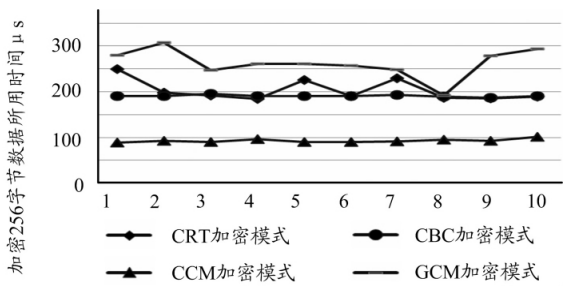


图 3 加密方案的比对

加密方案的选择还是基于 AES 高级加密算法的不同模式。CCM 模式的 AES 加密方案不仅能提供数据保密性服务，同时还能起到认证的作用，结合基于 ECC 方式的认证方式，可构成双因子认证。在本仿真中，只是用 CCM 的数据加密方案，并比对各种方案在加密 256 字节数据时所耗时间，可以发现，CCM 模式的加密方案有着较其它模式更快的速度。

5 结束语

本文首先分析了 EPON 通信系统中面临的各种安全威胁，针对存在威胁提出了在 EPON 的注册发现过程中，加入了公钥的分发，以及基于数字签名验证方案，并通过在上行信道中传输由 ONU 生成的会话密钥完成初始密钥交换过程。数据加密方面，在 AES 算法的基础上提出了基于 CCM 模式的加密方案，并在加密速度等方面进行了与其它方案的比对。从结果分析来看，相对于文献[10,11]中的方案，本方案不仅在认证方面取得高效率的输出，同时在数据加密上也得到了较好的结果。但是，由于采用基于 ECC 的公钥加密及认证方案，所以在处理时间上相对于基于对称密码的“挑战响应”方案较慢。

参考文献：

[1] IEEE.802.3[S].IEEE, Standard 2005.

[2] KRAMER G.Ethernet Passive Optical Networks [M]. New York: McGraw-Hill, 2005.

[3] HAJDUCZENIA M,PEDRO R M,SILVA J A .On EPON Security Issues [J].IEEE Commun.Surveys & Tutorials,1st Quarter,2007,9(1):68–83.

[4] KIM J.Authentication and Privacy in EPON [C]. IEEE802.3ah Ethernet in the First Mile, 2002.

[5] MURAKAMI K, FUJIMOTO Y, YOSHIHARA O.Authentication and Encryption in EPON[C].IEEE802.3ah Ethernet in the first mile, 2003.

[6] GOFF Y L,FRANCE Telecom,YUKIHIRO Fujimoto,et al. Encryption Layer Comparison[C],IEEE 802.3ah Ethernet in the first mile,2003.

[7] 王荣，王慧鑫，王浩，等.EPON 系统中认证与加密机制研究[J].光通信技术，2012,36(6): 17–20.

[8] 赵丹.EPON 安全认证与入侵检测系统研究[D].苏州：江苏大学硕士学位论文，2008.

[9] 孟玉.EPON 系统安全保密技术研究[D].武汉邮电科学研究院，2005，(18–16):32–38.

[10] 徐伟亮，范红.利用 AES 算法实现 EPON 下行流量加密技术[J].光通信技术，2004,28(2):26–28.

[11] 苏振宇，寿国础，胡怡红.EPON 三重搅动加密算法及安全性分析[J].光通信技术，2007,31(10):20–22.

[12] IEEE.IEEE Standard for Broadband over Power line networks: Medium Access Control and Physical Layer Specifications [M]. IEEE Std 1901-2010, 30, December 2010.