文章编号:1005-0523(2013)04-0035-05

基于改进的AES算法的EPON安全方案研究

殷爱菡,王胜凯

(华东交通大学信息工程学院,江西 南昌 330013)

摘要:提出了一种基于改进的AES-128算法的加密方案。该方案在AES-128算法的密钥扩展阶段引进时间戳,然后对EPON的下行方向的数据进行加密,同时利用时间戳的同步实现密钥的动态更新和同步,从而保证传输数据的实时性和安全性。实验结果证明了该方案的可行性和有效性。

关键词:EPON;AES-128;下行数据;时间戳

中图分类号:TN915 **文献标志码**:A

EPON(ethernet passive optical network,以太无源光网络)作为下一代宽带接入网的重要解决方案之一[1],能满足庞大业务流对带宽的需求,但由于EPON点对多点的拓扑结构,采用标准以太网数据包,并且广播发送下行数据[2-4],因此存在非常严重的安全隐患。目前对下行数据加密多采用RSA(rivest shamir adleman)加密算法[5],将AES(advanced encryption standard,高级加密标准)和ECC(elliptic curve cryptosystem,椭圆曲线密码系统)相结合的算法[6],或者直接利用AES的计数器模式加密[7]。但这些传统的加密方法很难同时满足业务的安全性和实时性要求,且会增加额外的成本并严重影响网络的整体性能。因此,这里提出了一种基于时间戳的AES加密方案,该方案可有效利用时间戳的动态更新和同步实现密钥的更新和同步,从而保证数据传输的实时性和安全性。

1 AES-128密钥扩展

AES作为对称加密算法代表,具有安全性强,效率高等优点,能够满足实时性数据传输要求。它是一种对称加密算法,由字节代换、行移位、列混合和加轮密钥进行循环变换所形成[8]。该方案选择了AES-128算法,它需要经过10轮变换形成,加密原理如图1所示。

首先,输入的明文与主密钥进入加轮密钥模块完成异或操作后将结果按顺序依次执行字节代换、行移位、列混合和加轮密钥这4种变换,此4种变换为一轮,然后依次执行9次轮变换,第10轮中不执行列变换,最后直接输出结果,即为明文被加密后得到的密文。

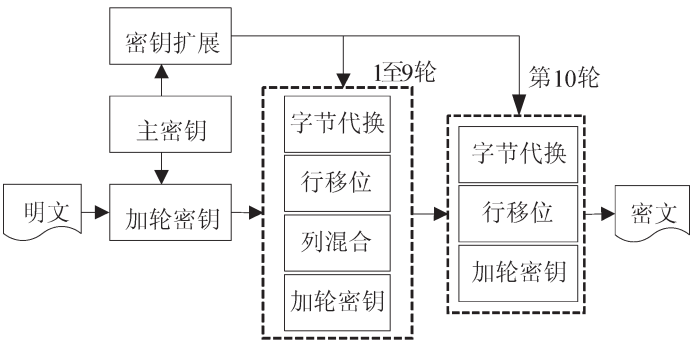

图1 AES-128加密机制
Fig.1 Encryption mechanism of AES-128

收稿日期:2013-05-31

基金项目:国家自然科学基金项目(61262079)

作者简介:殷爱菡(1963-),女,教授,博士,研究方向为光通信技术。

AES-128加密过程中,需要用到10次轮密钥,为了保证加密过程的可靠性,这10个轮密钥都是不相同的,但都是相关的,都是通过对初始密钥进行密钥扩展得到的[9],密钥扩展的过程如图2所示。

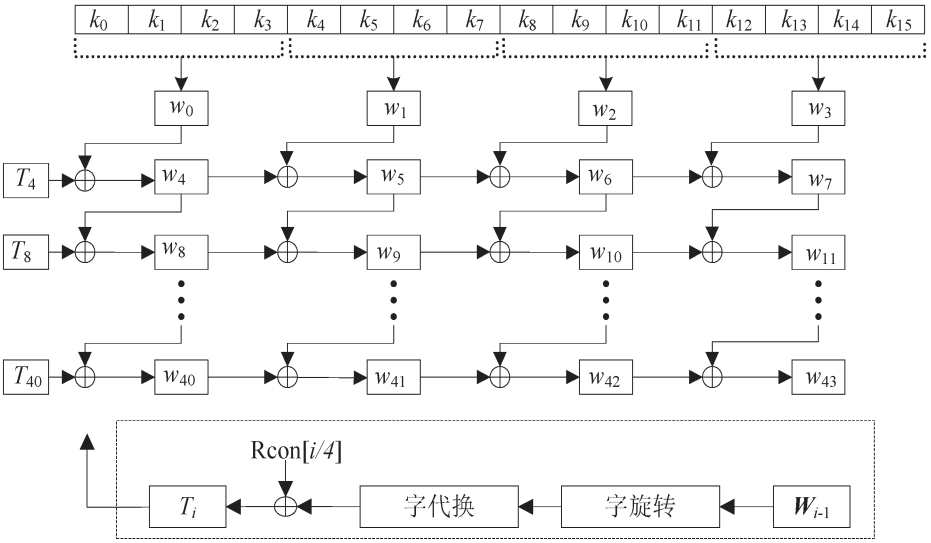

图2 AES-128密钥扩展过程

Fig.2 Key expansion of AES-128

密钥扩展的过程如下:

1) AES-128共128 bit,即16字节($k_0 \sim k_{15}$),得到第一个字 $\boldsymbol{W}_1=(w_0, w_1, w_2, w_3)$;

2) 其余的字($\boldsymbol{W}_i$,其中 $i=1\sim11$)根据满足的条件不同,由如下的方法得到:

a.当满足条件 $i \bmod 4 \neq 0$ 时,$\boldsymbol{W}_i=\boldsymbol{W}_{i-1}\oplus\boldsymbol{W}_{i-4}$;

b.当满足条件 $i \bmod 4 = 0$ 时,$\boldsymbol{W}_i=T_i\oplus\boldsymbol{W}_{i-4}$,这里 T_i 是一个临时字,是把字旋转和字代换应用于 $\boldsymbol{W}_{i-1}$,并把结果和轮常数Rcon[i/4]进行异或得到。

2 时间戳的提取和同步

由于OLT(optical line terminal,光线路终端)是根据自己的本地时钟为ONU(optical network unit,光网络单元)安排时隙,因此,为了避免冲突,ONU的时钟必须与OLT的时钟保持一致。最简单的方法就是将OLT的时钟直接发送给ONU,然后ONU刷新自己的本地时钟,而传递时钟就需要利用存放在IEEE 802.3MAC控制帧中的时间戳,表1为MAC控制帧的组成,其中时间戳占4个字节。EPON系统测距时,下行的时间戳存放在OLT发给ONU的Gate控制帧中,上行的时间戳在ONU发给OLT的Report控制帧中,因此,我们可以在系统测距过程中提取到时间戳。

表1 MAC控制帧结构

Tab.1 Constructure of MAC control frames

名称	前导码	目的MAC	MAC类型Ox8088	MAC控制帧类型	时间戳	数据信息	FCS纠错码
大小	8字节	6字节	2字节	2字节	4字节	40字节	4字节

OLT有个本地时钟计数器,该计数器对时间颗粒进行计数。当OLT发送MPCP(muti-point control protocol,多点控制协议)帧时,它就将本地时钟计数器的值,即绝对时钟插入到时间戳中。ONU端也有具有同样功能的计数器,无论何时接收到来自OLT端的MPCP帧,都会用这个帧携带的时间戳来刷新自己的本地时钟,以达到同步的目的。

3　基于时间戳的AES-128算法

这里提出的改进方案是在AES的密钥扩展阶段引进时间戳，让密钥跟随时间动态更新和同步，保证密钥的安全，使得窃密者无法篡改被加密的数据信息。

由于在列混合变化，状态矩阵需要与一个常数矩阵相乘来得到新的状态矩阵，而此常数矩阵是特定的，加入时间戳会导致无法解密，字节代换、行移位和加轮密钥只是对状态矩阵进行线性变化，因而也无法在其中加入时间戳。考虑到密钥扩展过程只是进行了简单的字节运算，加入时间戳，可以让密钥跟随时间动态更新和同步，所以在此过程中引入时间戳是可行的。

如图3所示，在密钥扩展过程加入了时间戳，使得扩展密钥和时间相关，能够随着时间的变化而动态更新，确保EPON下行数据的安全。

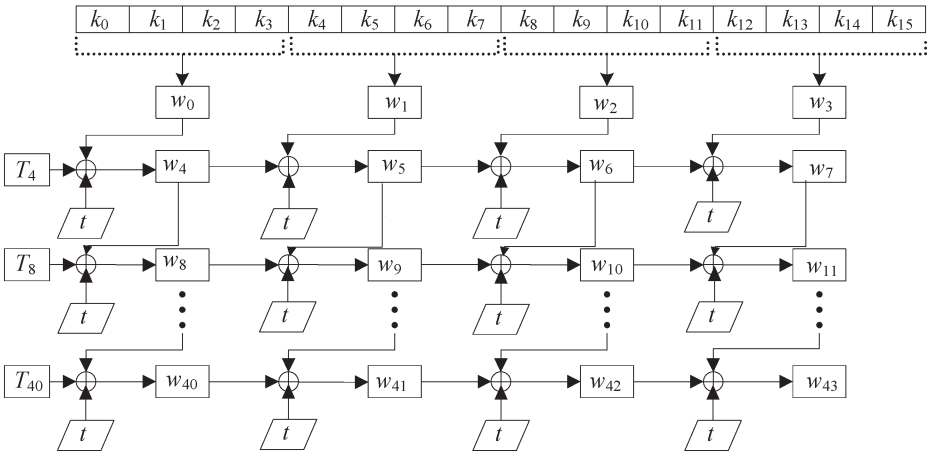

图3　基于时间戳的方案

Fig.3　Scheme based on timestamp

加入时间戳以后，密钥扩展过程可描述为

1）第一个字（w_0，w_1，w_2，w_3）还是由（k_0~k_{15}）组成；

2）其余的字由如下的方法得到：

a. 当满足条件$i \bmod 4 \neq 0$时，$\boldsymbol{W}_i = \boldsymbol{W}_{i-1} \oplus \boldsymbol{W}_{i-4} \oplus t$；

b. 当满足条件$i \bmod 4 = 0$时，$\boldsymbol{W}_i = T_i \oplus \boldsymbol{W}_{i-4} \oplus t$，这里$T_i$是一个临时字。

在AES-128算法中引进时间戳后，由于在下行数据传输过程中，密码密钥的发送和接均与时间相关，同时OLT和ONU使用了相同的扩展方案，所以加/解密过程都是可行的。不发送初始密钥，这样有效避免了密钥泄露的危险。同时，密钥通过时间戳进行同步和更新，使得系统的安全得到了保证。

4　结果分析

1）复杂性分析。提出的方案是基于成熟的AES-128算法，因此可以抵抗大多数已知的攻击类型。AES-128算法是对称加密算法中最好的一种，它简单的设计结构使得加密速度非常的快，而且消耗也很低。本方案只引入了时间戳，增加的运算只有模运算，应该说简单的模加运算不会对加密速度产生影响，也不会引入更多的复杂性。

事实上，通常情况下$t > 2^8$，增加的复杂度可以通过公式（1）体现：

$$\Delta f\left(n_{\mathrm{b}}\right) = N_{\mathrm{k}} N_{\mathrm{r}} \log t = 4 \times 10 \times \log t = 40 \log t \tag{1}$$

其中：n_{b}是指输入的需要加密的数据长度；N_{k}是密码密钥的长度；N_{r}是循环的轮数。与原始的AES-128算法的复杂性相比，增加的这点复杂度是完全可以忽略不计的。

2）平均性能分析。首先将基于时间戳加密方案的网络平均时延和平均吞吐量与原来的AES算法和

未加密的情况进行比较。

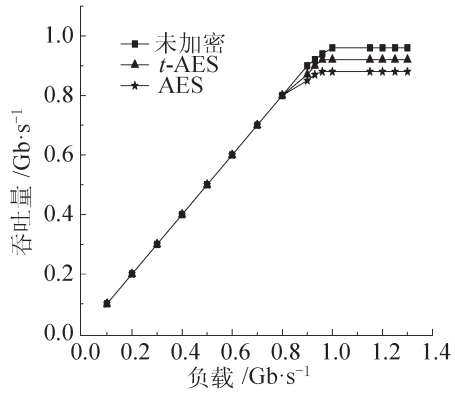

图4 平均吞吐量比较

Fig.4 Comparison of average throughput

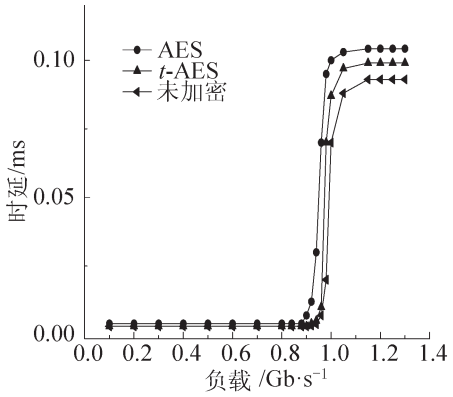

图5 平均时延比较

Fig.5 Comparison of average time delay

从图4和图5中可以看出，与传统的单独AES算法加密相比，时间戳的方案降低了时延并提高了吞吐量，且时延和吞吐量都是在负载达到1之后才会恶化，而采用原来的AES加密方法在负载达到0.9的时候就已经开始恶化了。因为原来的AES算法虽然结构比较简单，但是其密钥需要通过信道传输，占用了一定的带宽，因此，使得系统的带宽利用率降低，导致了时延的增加和吞吐量的降低。而时间戳的方案不需要通过信道传输密钥，性能自然比原来的AES算法优越。

3）具体性能分析。为了能够更加直观的看出性能的变化，我们将吞吐量和时延随着仿真时间的变化情况与原始的AES加密算法进行了对比分析，如图6和图7。

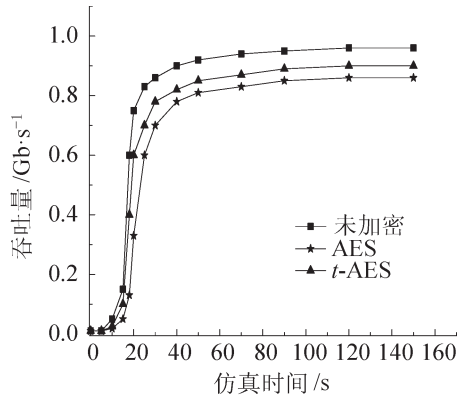

图6 吞吐量比较

Fig.6 Comparison of throughput

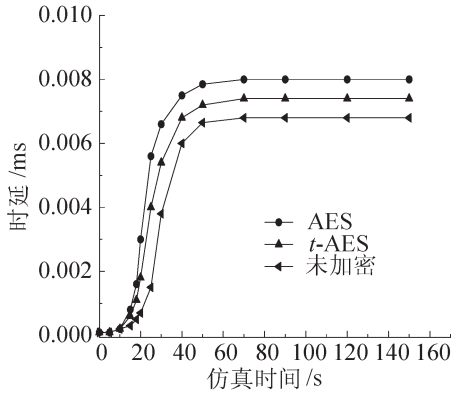

图7 时延比较

Fig.7 Comparison of time delay

我们将仿真时间设为160 s，大概在19 s时系统开始传送数据，在19 s到20 s的一秒时间里，吞吐量和时延急剧增加，并在20 s后逐渐趋于稳定，到40 s时，二者都达到了最大值，吞吐量为0.93 Gb·s^{-1}，时延为0.008 ms。

通过对比我们可以发现基于时间戳的方案要比原始的加密方案有更大的吞吐量，但时延与未加密和原始算法相比有略微的增加。但是，在接入网中规定的最大传播时延不能超过0.1 ms，而这里的传播时延最大才0.008 ms，远小于0.1 ms，就算是在网络负载恶化的情况下，其平均时延也才0.1 ms。且时间函数加密方案的密钥是随着时间动态更新的，安全性比其他任何方法都高。因此，在保证EPON系统业务高安全性的前提下，在网络允许的范围内，牺牲这一点微小的延时和吞吐量还是可以让人接受的。

5　结束语

为了解决EPON的AES-128加密方案中密钥无法动态更新而导致下行数据容易被窃取并篡改的问题，新方案在AES-128算法的密钥扩展阶段引入了时间戳，使得密钥可以随着时间戳动态更新和同步。分析表明该方案是可行的，特别是对第三类在安全方面有较高要求的业务来说是非常适用的。

参考文献：

[1] 殷爱菡，刘方仁. 以太无源光网络中光网络单元注册的FPGA实现[J]. 华东交通大学学报，2011，28(2)：19-23.

[2] ZHANG LINCONG，LIU YEJUN，GUOLEI，et al. Energy-saving scheme based on downstream packet scheduling in Ethernet passive optical networks [J]. Optical Fiber Technology，2013，19(2)：169-178.

[3] GU WEN，VERMA PRAMODE K，KARTALOPOULOS STAMATIOS V. A Unified Security Framework for Wi-MAX over EPON access networks [J]. Security and Communication Networks，2011，4(6)：685-696.

[4] BERISA T，FOULI K，MAIER M，et al. Adaptive grant extension in OC-Enhanced PONs [J]. Communications Letters IEEE，2011，15(4)：458-460.

[5] AIHAN Y，YANYAN C，FAN W，et al. Research and implementation of EPON system encryption security[C]// Magdy Bayoumi. International Conference of China Communication. USA：Scientific Research Publishing，2010：78-81.

[6] FU ZIYI，LI ZONGJIE. Study of authentication and encryption scheme in EPON[C]//Proc International Symposium on Electronic Commerce and Security Workshops,USA：Scientific Research Publishing，2010：8-10.

[7] SARWARUL C，MARTIN M，Security issues in integrated EPON and next-generation WLAN networks[C]// Bayoumi. Consumer Communications and Networking Conference. Las Vegas，NV：Conference Publications，2010：1-2.

[8] GONG JIN，WENYI LIU，HUIXIN ZHANG. Multiple lookup table-based aes encryption algorithm implementation [J]. Physical Media，2012，25(2)：842-847.

[9] BEHROUZ A FOROUZAN. 密码学与网络安全[M]. 马振晗，译. 北京：清华大学出版社，2009：175-203.

Research of the EPON Security Scheme Based on Improved AES Algorithm

Yin Aihan，Wang Shengkai

（School of Information Engineering，East China Jiaotong University，Nanchang 330013，China）

Abstract：A new encryption scheme based on improved AES algorithm is proposed in the Ethernet Passive Optical Network（EPON）. In this scheme，AES-128 algorithm is combined with timestamp in the process of key expansion for encrypting downstream data in EPON. Accompanying the dynamic update and synchronization of keys，the extraction and synchronization of timestamp are released to achieve the real time and security. The simulation results indicate the validity and feasibility of this scheme.

Key words：EPON；AES-128；downstream data；timestamp