# 期末大作业

网络空间安全学院 信息安全专业 1811494 刘旭萌

目录

[期末大作业 1](#_Toc75092872)

[设计背景 1](#_Toc75092873)

[当前结构的局限性 2](#_Toc75092874)

[加解密位置设定难 2](#_Toc75092875)

[数据压缩效率低 3](#_Toc75092876)

[设计新架构 3](#_Toc75092877)

[总览 3](#_Toc75092878)

[压缩加密层 4](#_Toc75092879)

[安全验证层 5](#_Toc75092880)

[通信流程 6](#_Toc75092881)

[结论 6](#_Toc75092882)

[参考文献 6](#_Toc75092883)

在设计TCP／IP网络协议和OSI标准通信模型的初期，网络设计者关心的问题是如何将数据从一台计算机有效和可靠的传输到另外一台计算机上去。**数据的安全性**在当时并没有提到议事日程。因此，TCP／IP通信协议和OSI标准通信模型没有内置的安全机制。当人们逐渐意识到这个设计缺陷之后，便想方设法在现有的框架内加入各种安全机制。但是，由于这些通信协议和通信模型不是为网络安全设计的，其体系结构也许并**不适用于新的安全功能**。为了从根本上纠正这一缺陷，网络设计者们开始研究如下课题：如果**从头开始设计网络通信协议，使其包含现有的安全机制及在未来能有效地加入新的安全功能**，网络体系结构应该怎样设计才是最好的。请同学们用word写下自己的看法和设计方案，不少于3000字，以自己学号命名上传到雨课堂。

## 设计背景

随着科技的高速发展，数据安全的重要性愈发展现，但目前最广泛使用的方式是在原有网络架构TCP/IP和OSI模型的基础上，添加各种网络安全协议。网络安全协议是营造网络安全环境的基础，是构建安全网络的关键技术。设计并保证网络安全协议的安全性和正确性能够从基础上保证网络安全，避免因网络安全等级不够而导致网络数据信息丢失或文件损坏等信息泄露问题。在计算机网络应用中，人们对计算机通信的安全协议进行了大量的研究，以提高网络信息传输的安全性。目前网络安全研究人员在链路层、网络层和传输层开发了相应的安全补充协议，期望在各个层次上分别达到保密性、完整性和不可抵赖性的安全目标。802.1X和EAP协议用于在链路层上实现发送方身份认证，IPSec和SSL分别在网络层和传输层利用密码技术实现了三个基本安全目标，802.11i协议族定义无线局域网WLAN的加密和完整性检测机制。

然而，由于在网络架构设计开发之初只考虑了数据传输的功能性，新添加的安全功能模块与原架构无论是在硬件上还是在软件上难免相互掣肘。为解决这一问题，本文设计了一种能够适用于新安全功能的网络架构，在该架构中，传输功能作为主要架构，安全功能作为选择模块。该架构支持目前各种流行的安全协议，并可以适应技术发展灵活调整其中的安全模块所使用的技术。

## 当前结构的局限性

### 加解密位置设定难

目前使用的TCP/IP结构（见图1）在传输过程中并没有使用任何加密技术手段，导致传输的数据极易被第三方劫持、篡改或窃取。在降低接收方对于数据信任程度的同时，大幅削减了数据沟通效率，所以急需一种方法对数据进行安全可靠传输。

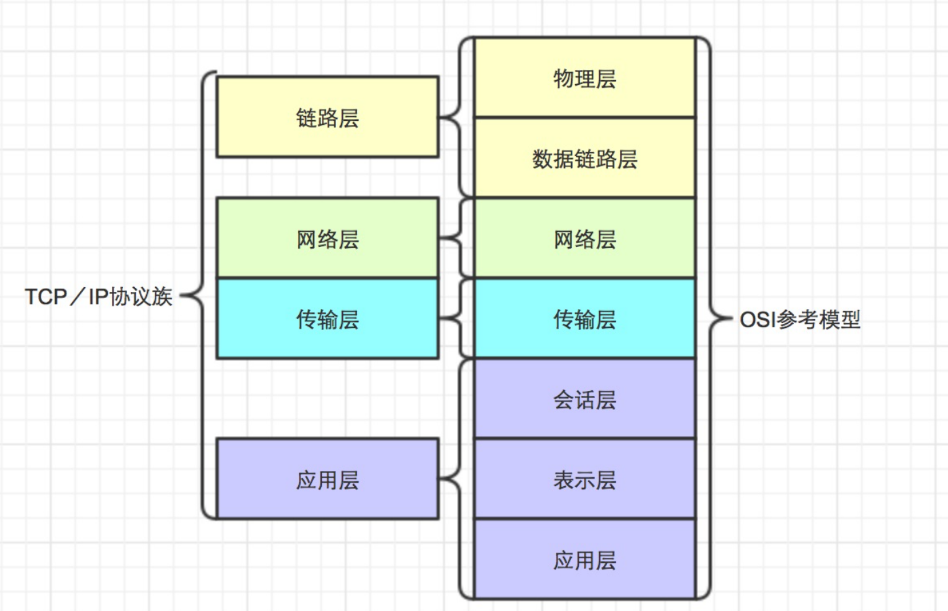


图1

若直接在原架构上添加加密功能，已知信息在各个层之间传递的过程中需要封装各种报头以达到各种功能，若加解密在应用层实现，应用层信息以密文方式出现，但在数据流经过传输层时会被封装传输层报头，在网络层会被封装网络层报头，这些封装报头均已明文的形式出现，其中就包括消息的源、目的IP地址，端口等各种信息。攻击者截获应用层加密信息后，虽然无法知晓消息的具体内容，但可以了解到发送、接收方的IP端口等信息，依旧可以根据这些信息进行流量分析，甚至是修改源、目的IP地址改变消息发送方向，也可以篡改加密信息内容导致接收方无法解密。若加密在传输层进行，链路层传输消息依然会出现明文IP报头，且TCP报头中存在部分需要在网络层校验的内容，而加密直接影响了校验，传输层加密甚至可能会直接影响到原本TCP/IP模型中的可靠传输功能，导致链路上出现大量错误数据报。若消息在链路层进行加密，攻击者无法获取消息中的任何内容，在最大程度上对数据内容进行加密。但是如此，无论是主机还是路由器，都需要对局域网内所有的消息先进行解密才能判断自己是不是该条消息的接收方，这个计算过程将消耗大量资源，尤其是在现有不改变原网络架构的情况下只能使用软件方式实现该加密方法，执行效率较硬件有较大差距，而目前大幅度使用硬件进行加密则设计到大量成本问题，和具有加解密功能链路层部件和不具有该功能部件之间的通信问题。所以目前，在网络架构的任一层进行加解密都无法被认为是最佳选择。

### 数据压缩效率低

目前数据在传输时不需要强制压缩，多为人为选择，且所有压缩工作都是由软件完成的。但是随着信息时代的到来，网络所需传输的数据量飞速增长，目前主要是靠增加传输带宽缓解这一问题，但是这种方法需要一定的经济成本，需要结合强制数据压缩方法。

## 设计新架构

为了解决上述提到的问题，本文提出了一种新的网络安全架构。

### 总览

图2

本方案在原有架构上进行改进，新增安全验证层、压缩层和加密层。其中安全验证层用于验证消息的可信度、进行算法可选择的加解密，目前验证可由数字签名相关技术实现，加密算法可由通信双方相互协商；压缩加密层将使用硬件实现相关逻辑，提升处理速率，功能为完成压缩步骤和基础加密过程。

### 压缩加密层

随着信息技术地高速发展，对于数据传输速率的要求不断增加，除了在带宽等技术方面的改进，数据压缩也能够很好地缓解信息爆炸带来的数据传输压力。在原先的网络体系结构设计中，压缩并没有作为一个必选项，而大多是在应用层甚至只是用户的个人选择。目前的数据压缩均由用户电脑完成，即由软件实现，而软件相较硬件更加灵活但处理速度慢。所以，若数据压缩成为必须功能，则应由硬件完成。前文分析到，在链路层进行相关加密可以最大限度地防止第三方截获数据，所以在该层对除原消息外所有新封装的报头进行加密。

#### 压缩算法：

使用硬件实现ZIP压缩算法的相关逻辑。ZIP算法原为传输层算法，是网络通信中广泛使用的数据压缩算法，它使用两个滑动窗口（见图3），分别称为基准窗和前视窗。两个窗口相邻，当窗口内数据处理完毕后同时前移，扫描整个文件，在移动中压缩数据。这个算法在执行地过程中将重复数据处理变换成相对距离+字符串长度，如图3所示，输入中前视窗中的“a loop”重复了基准窗中的数据，相对距离为17，字符串长度为7，所以将该部分重复数据用以0开始的二进制字符串表示，表示为017b7b

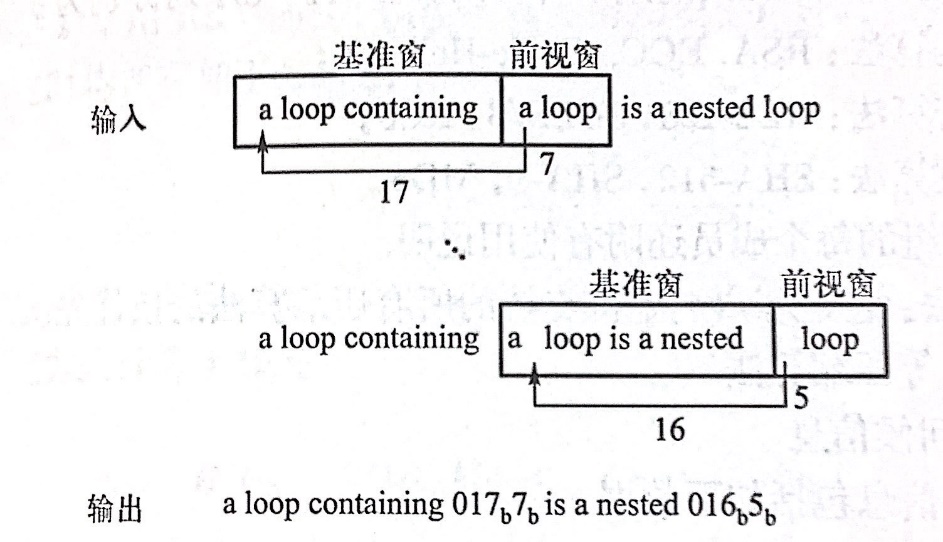


图3

现将该算法转换为链路层算法，使用硬件实现，当数据传输至链路层时，计算机将作数据报为01比特串进行识别，直接对硬件进行编程，完成两个窗口的识别功能。

#### 加密算法：

由于对链路层数据包进行加密可以最大限度地保证传输数据的安全性，所以将链路层数据加密设为必选项，必选项功能由硬件完成以提高效率。该部分加密功能专用集成电路（ASIC）技术，将加密算法制作成为硬件。由于技术的发展，密码强度需要不断提高，硬件由于其执行逻辑更改的不变性，本文设计该加密部件为可拆卸更换模式，即为该功能设计一个拱顶的输入输出标准，其内部执行逻辑可以以插卡方式更换。并且，由于硬件更新可能存在滞后现象，采用新算法的加密芯片应要支持就加密算法，保证新旧设备之间可以进行相互通信。

### 安全验证层

该层将完成对消息的签名，即用数据验证码或散列数据认证码作为数字签名，防止第三者伪造数据。目前最常用的方式是使用公钥密码系统和公钥证书，甲方为了认证一个即将送往乙方的数据M，首先求出数据的散列值，然后用其私钥将散列值加密得到，并用此作为为甲方对该数据的数字签名，甲方将数据和其数字签名以及甲方的公钥证书一同传送给乙方，乙方用公钥机构的公钥将甲方的公钥证书解密，得甲方的公钥，然后用其将解密的带，并验证是否而验证甲方数字签名的有效性。当然，签名方法需要根据使用场景进行相应变化，这也是使用软件方式完成数字签名功能的原因，因为它更加灵活。比如在电子交易的场景中，通常涉及三方参与，即卖家、买家与银行，这时就需要引入双重签名协议，其中卖家承担着将买家的购买消息转交至银行的功能，银行也需要根据卖家转发来的消息进行钱款移交并向卖家提供付款凭证。由于多方的参与需要更加复杂的签名流程。

除签名之外，对于一些需要较强保密性的数据，还需要使用额外的加密算法。目前的大部分加密算法均基于大整数分解的困难性或者离散对数分解的困难性，而随着计算机算力的加强，通过暴力计算破解特定位数的加密方法可行性日渐增加，所以每隔一段时间，加密算法就要进行一定地改进。或增加处理位数（原RSA加密中n一般取1024位，后随着计算能力的增强开始取2048位），或改进算法使加密流程更加复杂（如最开始的单层DES转向双层甚至三层DES）。密码算法需要根据技术发展请款灵活改进，故应使用软件方式实现。

### 通信流程

甲乙双方在建立连接时，首先进行三次握手建立连接，确定应用场景，互相商议交流数据是否需要深层次加密以及使用哪种加密算法和该算法的哪个版本，在应用层握手的过程中，链路层将自己支持的最高版本的链路加密算法版本号告知对方，商议双方可以接收的最新链路加密方法。握手成功，连接建立，双方互相确定对方的在线状态和签名加密方法。

传输数据过程中，应用层准备待传输数据，使用双方商议好的深层加密方法现对数据进行加密，然后进行可靠性签名。数据传输至传输层和网络层，分别封装相应报头，将数据传至链路层，在链路层完成相关功能后，使用ZIP算法对数据进行压缩，然后再使用公钥算法对压缩后的数据进行解密。接收方使用相反顺序处理消息，即先进行链路解密，解压缩，将数据通过网络层和传输层传至安全验证层。接收方对签名进行相关认证，然后对数据进行深层次解密，最后得到明文数据。

## 结论

本文设计了一个新的网络通信协议，为了提高新旧协议的兼容性，新协议中仍然具有原协议中的各个层，它支持现有的各种安全机制，并通过新增安全验证层和压缩加密层，支持新的安全机制的使用，添加了支持强制基础压缩和基础加密以及可选的数字签名和深层加密功能。增强了数据传输的安全性，提高了传输效率，缓解了拥塞问题。其中新增加的两个模块可以灵活选择各种算法，增强了该架构的可持续性。强制基础加密和压缩使用硬件逻辑实现，增加执行速度；可选安全验证模块使用软件实现，更加灵活，可以根据需要选择相应签名加密算法。

## 参考文献

《计算机网络安全的理论与实践》

<https://www.cnblogs.com/xumaojun/p/8544127.html>

<https://blog.csdn.net/pansaky/article/details/90641343>

<https://www.zhihu.com/question/324084095/answer/681603302>

<https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E5%8D%8F%E8%AE%AE/7296707?fr=aladdin>

https://www.cnblogs.com/Dio-Hch/p/12023165.html