|  |
| --- |
|  |
| 校园无线身份认证密码协议分析 |
| [南开大学密码学实验案例] |
|  |
| **汪定 编著** |
|  |

|  |
| --- |
|  |

# 实验概述

目前，校园网已经成为了高校校园的一种基础设施，为学校师生提供网络接入，以满足教学、科研、管理和信息服务需求。校园网用户数量，尤其是流动用户的数量，较之从前有了很大的增长，校园网提供的业务形式也有很大程度上的增多，用户的接入方式也多样化，面临着复杂的信息安全问题，威胁高校师生的隐私及信息安全。

如果不采用身份认证机制，将导致很多问题[1]。例如，由用户PC的系统漏洞引发的病毒传播和网络攻击、非法用户访问内部敏感信息和有限的资源等。特别地，随着无线接入用户的增多，由于无线WLAN的开放性和移动性带来的固有诸多安全隐患，使得用户在认证过程中用户认证信息，如用户名，密码，证书等，很容易被泄露；用户在身份认证通过后的网络通信信息也面临着同样的安全威胁。因此，对大量的用户进行高效的管理，部署一种符合校园网LAN/WLAN环境的安全接入认证解决方案，已经成为运行整个校园网必须解决的问题。

在这个实验中，我们将**分析校园无线身份认证密码协议**，了解当前校园网的认证方式，对认证过程及其安全性进行简单的分析说明。

# 目 录

[实验概述 2](#_Toc14600)

[目 录 3](#_Toc14480)

[第一章 基础知识 4](#_Toc19750)

[1.1 当前研究 4](#_Toc13577)

[1.2 802.1x认证技术 5](#_Toc11997)

[第二章 协议分析 16](#_Toc6598)

[2.1 实验目的 16](#_Toc646)

[2.2 实验原理 16](#_Toc1235)

[2.3 实验内容和步骤 20](#_Toc19325)

[2.4 实验报告和要求 20](#_Toc31761)

[第三章 拓展部分 22](#_Toc13324)

[参考文献 23](#_Toc17889)

# 第一章 基础知识

课时：1.5课时。

## 当前研究

为了确保校园网的安全，高校采取认证方式对网络用户进行身份验证，常见的以太网接入认证方式有PPPoE，Web/Portal及802.1x。其中，PPPoE（PPP over Ethernet）于1998年后期问世，被广泛应用于窄带网中，将其应用于宽带以太网，是传统PSTN窄带拨号接入技术在以太网接入技术的延伸。PPPoE在校园网这一实际应用场景中虽然有稳定、容易接受的优点，但它的缺点却更为突出，比如PPP到Ethernet封装效率低，在认证发现阶段有大量的广播严重影响效率，同时组播开展困难等，而解决这些问题势必带来更高的建设成本和更大的维护工作量[2,3]。Web/Portal认证则是一种基于HTTP/HTTPS协议的接入认证方式，是基于业务类型的认证，用户通过使用Web浏览器来访问网络，不需要特定的客户端, 支持各种不同类型的终端接入，因而对用户来说非常方便，也大大减少了网络运营商的网络维护工作。但也具有建网成本高、安全性差、用户连接性差和认证前分配IP地址导致的浪费地址资源等缺点[3,4]。

802.1x通过对认证方式和认证体系结构进行优化，有效地解决了传统PPPoE和Web/Portal认证方式带来的问题，消除了网络瓶颈，减轻了网络封装开销，降低了建网成本，实现认证和业务分离，具有高灵活性和强的可扩展性；通过具体的EAP认证方式，可提供强加密方法的无线客户端和服务器之间双向认证，并生成保护无线传输的动态加密密钥[5]，具有可靠的安全性，是一种全新的、更为安全的校园网接入认证解决方案[6]。目前大多数高校采用802.1x的认证方式。

## 802.1x认证技术

自主学习本节剩余内容（1.5课时），结合IEEE 802.1x技术标准，了解WiFi连接过程，理解802.1x认证系统基本概念和常见攻击方法，指出协议存在的各种安全漏洞，改进现有协议，或设计新的安全高效的协议。

### 1.2.1 802.1x协议体系结构

802.1x 协议起源于 802.11 协议，它的一个基本认证机制是扩展认证协议（EAP），它是一种基于端口的网络访问控制方法[1]，正是它的这一特性，使其可应用于无线与有线的环境。802.1x协议的出现的主要目的是为了解决局域网（特别是无线局域网）用户的接入安全问题[7]。在它出现之前，无线局域网（WLAN）的安全主要采用MAC地址绑定，无线通信协议802.1b中有线对等保密（WEP）等方法。但经过实际检验，这些方法根本不足以保护无线网络用户信息的安全。802.1x协议的出现，极大的增强了无线网络的安全性。

802.1x协议体系结构由三部分构成[8]：客户端系统(Supplicant System)，认证系统，即设备端(Authenticator System)，认证服务器系统(Authentication Server System) ，如图1所示：

客户端系统

EAPOL

LAN/WLAN

认证系统

非受控

端口

受控

端口

客户端系统

PAE

认证系统

提供的服务

认证系统

PAE

认证服务器

认证服务器

图1 802.1x协议体系结构

客户端系统指用户终端及安装在其上的一个客户端软件，用户通过启动客户端软件发起 802.1x协议的认证过程。认证系统指支持 802.1x协议的网络设备，如交换机或AP。认证服务器系统通常是RADIUS服务器，它对客户的身份进行实际认证，然后通知认证系统是否允许客户端接入网络[9]。

认证系统的端口访问实体PAE通过不受控端口与客户端系统的端口访问实体PAE进行认证，二者之间运行EAPOL协议；认证系统的PAE与认证服务器之间运行可扩展认证协议 EAP，EAP帧中封装了认证数据，将该协议承载在其他高层次协议中，如 Radius，以便越复杂的网络到达认证服务器。认证系统每个物理端口内部有受控的服务端口(Controlled Port)和非受控的认证端口(unControlled Port)。非受控端口始终处于双向连通态，主要用来传递 EAPOL协议帧，可保证随时接收Supplicant发出的认证EAPOL报文。受控端口只有在授权状态下连通，用于传递网络资源和服务。受控端口在非授权状态下，根据受控方向的不同，可能单向连通，也可能双向断开[10]。

### 1.2.2 802.1x通信实体协议栈

以EAP-MD5为例，描述 802.1x的通信实体协议栈。EAP-MD5是一种单向认证机制，可以完成网络对用户的认证，但认证过程不支持加密密钥的生成；EAP-TLS是一种双向认证机制，通过用户和服务器的双向认证，可提供更高的安全性。基于EAP-MD5的802.1x认证系统通信实体协议栈如图2所示：

EAP-MD5

EAPoL

MAC

PHY

EAP

EAPoL

RADIUS

IP

MAC

PHY

MAC

PHY

UDP

EAP-MD5

RADIUS

UDP

TP

MAC

PHY

客户端

认证设备

RADIUS

图2 基于EAP-MD5的802.1x认证系统功能实体协议栈

### 1.2.3 EAP在802.1x中的层次

802.1 认证系统使用EAP(Extensible Authentication Protocol)协议完成客户端、设备端和认证服务器三者之间认证信息的交互。EAP是PPP(Point to Point)认证中的一个通用协议，其特点是EAP在链路控制阶段(Link Control Protocol，LCP)不选定认证机制，而是把这一步推迟到认证阶段，这样就允许认证系统在确定某种特定认证机制前请求更多的信息，还可以采用一个后端服务器来实际实现各种认证机制，认证系统仅仅需要传递认证信息。局域网中802.1x技术结合EAP认证，可以允许申请者和认证者之间采用灵活的方案进行认证，并且对将来出现的更先进合理的认证技术具有很好的兼容性，以满足无线局域网安全需要。

802.1x中引入可扩展认证协议EAP，但标准中并没有指定具体采用何种身份认证方法，而实际上EAP只是一种封装协议，它支持多种认证机制的灵活选择，允许高层使用不同的身份认证协议，如MD5，TLS和TTLS等[7]。

EAP-MD5支持客户端到服务器之间的单向认证，安全性一般。但因其实现和使用都较简单，加之它提供了一般场合下足够的安全性，是目前比较受欢迎的一个标准。

在各EAP认证类型中，TLS安全性最高，支持双向认证，是一个IETF标准，是客户端和 RADIUS服务器上最受欢迎的一个标准。TLS不仅需要在服务器端安装证书，而且在各个客户端上也要安装客户端证书。TLS在采用强加密方法的客户端和服务器之间提供双向认证，并生成保护无线传输的加密密钥，具有强度更高的安全性。因此TLS适合于对安全性有很高需求的场合。

EAP在802.1x中应用的层次如图3所示[11]。

TLS

MD5

Other

TTLS

Extensible Authentication Protocal

(EAP)

EAPOL

802.11

wireless Lan

802.5Token

Ring

802.3

Ethernet

PPP

**Eap**

**Layer**

**Data Link**

**Layer**

**Authentication**

**Layer**

图3 EAP在802.1x中的层次

### 1.2.4 802.1x协议认证流程

802.1x的认证流程如图4所示[7]，具体过程如下：

Authentication Server

Authenticator

Supplicant

EAP-Logoff

Logoff

Authentication failure

Authentication success

Radius-Access-Reject

EAP-Failure

Radius-Access-Accept

EAP-Success

Radius-Access-Request

EAP-Response/Auth

Radius-Access-Request

Radius-Access-Challenge

EAP-Request/Auth

EAP-Request/Identity

EAPOL-START

EAP-Response/Identity

EAPOL

图4 802.1x的认证流程

1. 客户端向接入设备发送一个EAPoL-START报文，开始802.1x认证接入。
2. 接入设备向客户端发送EAP-Request/Identity报文，要求客户端将用户名送上来。
3. 客户端回应一个EAP-Response/Identity给接入设备的请求，其中包括用户名。
4. 接入设备将EAP-Response/Identity报文封装到RADIUS-Access-Request报文中，发送给认证服务器。
5. 认证服务器产生一个Challenge，通过接入设备将RADIUS-Access-Challenge报文发送给客户端，其中包含有EAP-Request/MD5-Challenge。
6. 接入设备通过EAP-Request/MD5-Cha11enge发送给客户端，要求客户端进行认证。
7. 客户端收到EAP-Request/MD5-Challenge报文后，将密码和Challenge做MD5算法后的Challenged-Password，在EAP-Response/MD5-Challenge回应给接入设备。
8. 接入设备将Challenge，Challenged Password和用户名一起送到RADIUS服务器，进行认证。
9. RADIUS服务器根据用户信息，做MD5算法，判断用户是否合法，然后回应认证成功败报文到接入设备。若认证成功，则携带协商参数及用户的相关业务属性给用户授权；若认证失败，则流程到此结束。
10. 如果认证通过，用户通过标准的DHCP协议(或DHCP Re )，通过接入设备获取规划的IP地址。
11. 如果认证通过，接入设备发起计费开始请求给RADIUS用户认证服务器。
12. RADIUS用户认证服务器回应计费开始请求报文．用户上线完毕．

此外，EAPoL可选择地支持在认证通过后在客户端和接入设备之间传输密钥信息，该功能通过EAPoL-Key报文进行四次握手来实现[7]，具体内容详见节2.2.1。

### 1.2.5 Radius协议

RADIUS: Remote Authentication Dial In User Service，远程认证拨入用户服务，由RFC2866定义，是目前实现AAA功能应用最广泛的协议[12]。其最初设计用来管理使用串口和调制解调器的大量分散用户。RADIUS 协议规定了NAS与RADIUS 服务器之间如何传递用户信息和记账信息。RADIUS 协议的认证端口是1812 ，计费端口是1813。RADIUS服务器负责接收用户的连接请求，完成验证，并把传递服务给用户所需的服务信息返回给NAS。NAS和RADIUS之间的验证信息的传递是通过密钥的参与来完成的。用户的密码加密以后才在网络上传递，以避免用户的密码在不安全的网络上被窃取。RADIUS通过建立一个唯一的用户数据库，存储用户名，用户的密码来进行验证; 存储传递给用户的服务类型以及相应的配置信息来完成授权。

由于RADIUS协议简单明确，可扩充，因此得到了广泛应用，包括普通电话上网、ADSL上网、小区宽带上网、IP电话、VPDN（Virtual Private Dialup Networks，基于拨号用户的虚拟专用拨号网业务）、移动电话预付费等业务。

（1） Radius工作原理

Radius认证网络拓扑总体结构如图5：



RADIUS服务器

远程用户

NAS

校园网络

图5 RADIUS认证简图

如上图所示，Radius认证体系包含三个部分，客户机，网络接入服务器（NAS），Radius服务器[7]。客户机就是请求上网的电脑或者工作站。NAS，一般是交换机或者AP，控制用户上网的具体执行者。Radius服务器储存客户的认证信息，此信息可以判定用户是否合法。NAS与Radius服务器之间有一个共享密钥，用来保存两者之间传递的信息的机密性。NAS与客户机通过普通局域网协议交互，NAS与Radius之间通过Radius协议交互。

Radius认证流程如下：客户端用户通过局域网接入NAS，NAS向RADIUS服务器使用Access-Require数据包提交用户信息，包括用户名、密码等相关信息，其中用户密码是经过MD5加密的，双方使用共享密钥，这个密钥不经过网络传播；RADIUS服务器对用户名和密码的合法性进行检验，必要时可以提出一个Challenge，要求进一步对用户认证，也可以对NAS进行类似的认证；如果合法，给NAS返回Access-Accept数据包，允许用户进行下一步工作，否则返回Access-Reject数据包，拒绝用户访问；如果允许访问，NAS向RADIUS服务器提出计费请求Account-Require，RADIUS服务器响应Account-Accept，对用户的计费开始，同时用户可以进行自己的相关操作。其具体流程图如下：

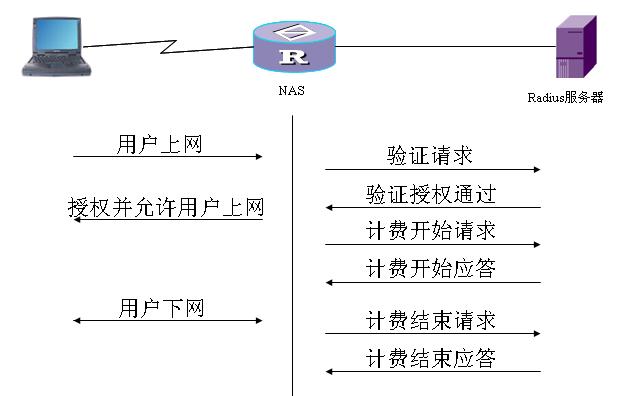


图6 Radius认证流程简图

（2）Radius中的认证方式

Radius协议支持多种认证方式。主要有密码验证协议（PAP），挑战握手验证协议（CHAP），微软挑战握手验证协议（MSCHAP，MSCHAP2），LDAP认证，Kerberos认证，EAP系列认证协议等。

前几种协议中，PAP，CHAP协议过于简单，安全性不够。Kerberos协议基于对称密码体制，能提供很强的安全性，但部署管理较为复杂。

EAP系列认证协议是可扩展认证协议，它是802.1x协议体系的基本认证机制，它提供了一个认证框架，在其框架范围上又可以运行多个不同安全级别的认证协议，其支持的比较成熟的认证协议主要有EAP-MD5，EAP-SRP，EAP-SIM，EAP-AKA，EAP-TLS，EAP-TTLS，EAP-PEAP。其中EAP-AKA，EAP-SRP主要应用于无线网络的数据完整性校验或者手机网络。

### 1.2.6 面临的安全威胁

然而，802.1x协议仍存在一定的安全缺陷，面临拒绝服务攻击、会话劫持、中间人攻击等安全威胁。例如，攻击者可通过伪造网络数据，如EAPOL-Logoff、EAP-Failure等实现拒绝服务攻击[13]，还可在上述拒绝服务攻击基础上，冒充合法的认证者或客户端实现会话劫持。Wang等人[14]在2012年系统地分析了802.11i无线局域网络中中间人攻击的攻击框架和有效攻击的条件，并以EAP-TTLSv0为例进行了说明。Vanhoef等人[15]在CCS’17介绍了攻击者可以利用协议设计或实现过程中存在的缺陷，诱骗受害者重新安装已经在使用的密钥，严重影响通信安全，后面所要分析的四次握手就容易受这种密钥重装攻击（Key Reinstallation Attack）的攻击。因此，研究无线身份认证密码协议，分析其安全性并针对安全漏洞进行改进意义重大。

但是，同学们也需要注意，即使形式化安全证明方法也不是万能灵药，因为形式化方法也存在一系列问题，如无法刻画一些现实安全目标、证明过程容易出错、安全假设容易脱离实际且往往滞后、严重依赖于协议分析者的攻击经验等等。因此，对协议进行启发式分析，仍是十分重要的。

# 第二章 协议分析

课时：2.5课时。

## 2.1 实验目的

使用抓包软件捕获登录南开大学无线WIFI——**NKU\_WLAN**的过程，根据抓包结果对所涉及的身份认证密码协议及其安全性进行分析。

抓包工具不限，可以使用Wireshark/Microsoft Network Monitor等。

实验环境不限，可基于Linux/Windows等。

## 2.2 实验原理

本节以捕获到密钥信息报文EAPoL-Key为例，即分析WiFi身份认证中四次握手的过程。

### 2.2.1 协议描述

**1) 名词解释**

Authenticator：认证者，指AP，即无线接入点

Supplicant：请求者，指Station，即任何企图接入AP服务集的设备

ANonce：由AP生成的随机数

SNonce：由Station生成的随机数

Mac(AA)：AP的Mac 地址

Mac(SA)：Station的Mac地址

PRF：Pseudo-Random Function，表示伪随机函数

MSK：Master Session Key，主会话密钥

PMK：Pairwise Master Key，成对主密钥，由MSK生成，用于生成PTK

GMK：Group Master Key，组主密钥，同样由MSK生成，用于生成 GTK

PTK：Pairwise Transit Key，成对临时密钥，用来加密 AP 和 Station 通讯的单播数据包，AP与每个Station 通讯用的PTK都是唯一的。PTK的生成函数如下：

GTK：Group Temporal Key，组临时密钥，用来加密 AP 和 Station 通讯的多播/广播数据包，连接该 AP 的所有 Station 共享一个 GTK。GTK的生成函数如下：

MIC：Message Integrity Check，消息完整性校验码，针对一组需要保护的数据计算出的散列值，用来防止数据遭篡改

**2) 协议描述**

四次握手是 AP（Authenticator）和Station（Supplicant）为了生成一个用于加密无线数据的密钥而进行四次消息交换的过程。协议流程可以参考图7。

（1）第一次握手：AP—>Station：ANonce

AP产生随机数Anonce，用EAPOL-KEY帧发送给Station，Station在收到消息后用它生成 PTK，前面已经提到PTK的生成函数：。其中，PTK的前128位是KCK（EAPOL-Key Confirmation Key），用来校验EAPOL-Key帧的完整性。

（2）第二次握手：Station—>AP：SNonce，MIC

Station 创建了自己的PTK后，会立即响应一条包含SNonce和MIC的 EAPoL 消息给 AP，AP将进行同样的计算得到PTK， 然后用得到的前128位对EAPoL

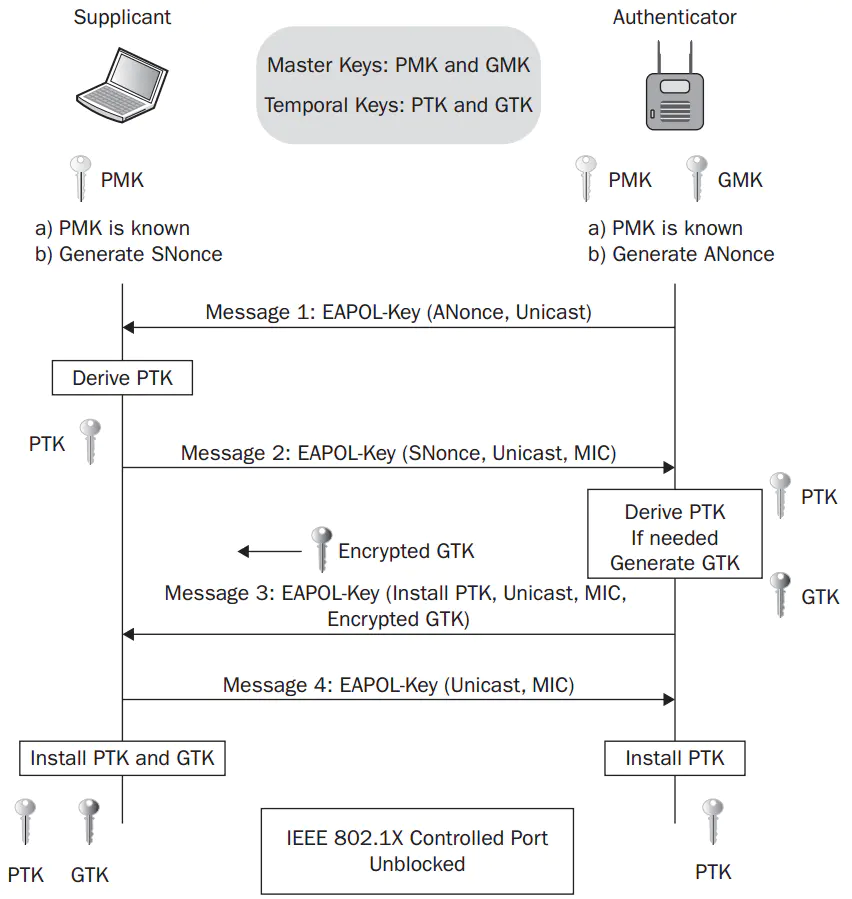


图7 四次握手流程图

报文进行完整性校验：比较所得到的值是否和收到报文中的WPA Key MIC的值一致，如果一致，则验证成功，说明Client端（即Station）拥有正确的PMK，否则判定Client端拥有的PMK错误，整个握手就此停止。

（3）第三次握手：AP—>Station：MIC，Encryted GTK

验证成功后，AP将 MIC和用PTK加密后的GTK 发送给 Station，并且告知 Station 安装 PTK 和 GTK。Station收到消息后检查MIC，同第二次握手的检查流程一样，如果不一致，将默默丢弃第三个报文，握手就此停止。验证成功后，Station可以使用掌握的PTK进行解密，恢复GTK的值，并安装PTK和GTK。

（4）第四次握手：Station—>AP：MIC

Station向AP发送EAPOL-Key消息，确认密钥已经安装，AP 收到该消息后再次检查MIC，验证成功后也安装PTK。安装的意思是指使用PTK 和GTK来对数据进行加密。

### 2.2.2 安全性分析

1. 数据安全性

协议使用的成对临时密钥PTK包含3个部分，KCK（Key Confirmation Key），KEK（Key Encryption Key），TK（Temporal Key）。其中，KEK和KCK在四次握手中用于数据加密和完整性验证。协议还使用MIC来防止数据遭篡改，保证数据完整性。

1. 拒绝服务攻击（DoS）

消息1并没有使用任何加密或完整性校验措施，而且如果AP在规定时间内没有收到客户端发回的应答消息2，就会启动超时装置，重传刚才发送的消息1。因此，客户端会对收到的每一个消息1计算SNonce和PTK。攻击者可以根据这一点伪造消息1，使客户端重新计算PTK，由于前后的Nonce值不一样，因此很容易造成PTK生成的混乱。若攻击者重复这样的攻击过程，那么客户端永远无法与AP完成四次握手过程，更不可能通过AP访问其他合法资源，从而实施DoS攻击。

## 2.3 实验内容和步骤

使用抓包工具捕获报文，例如：

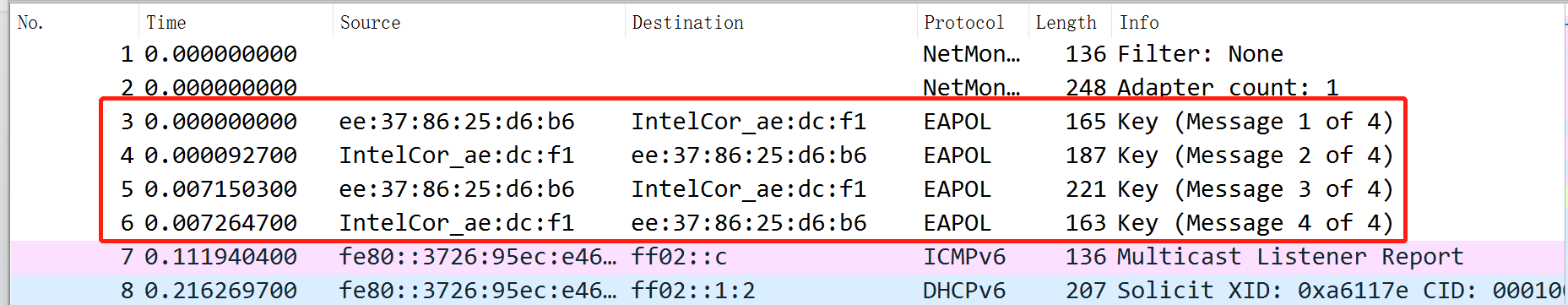


图8 抓包结果示例

根据协议内容，针对每一条报文进行具体分析：

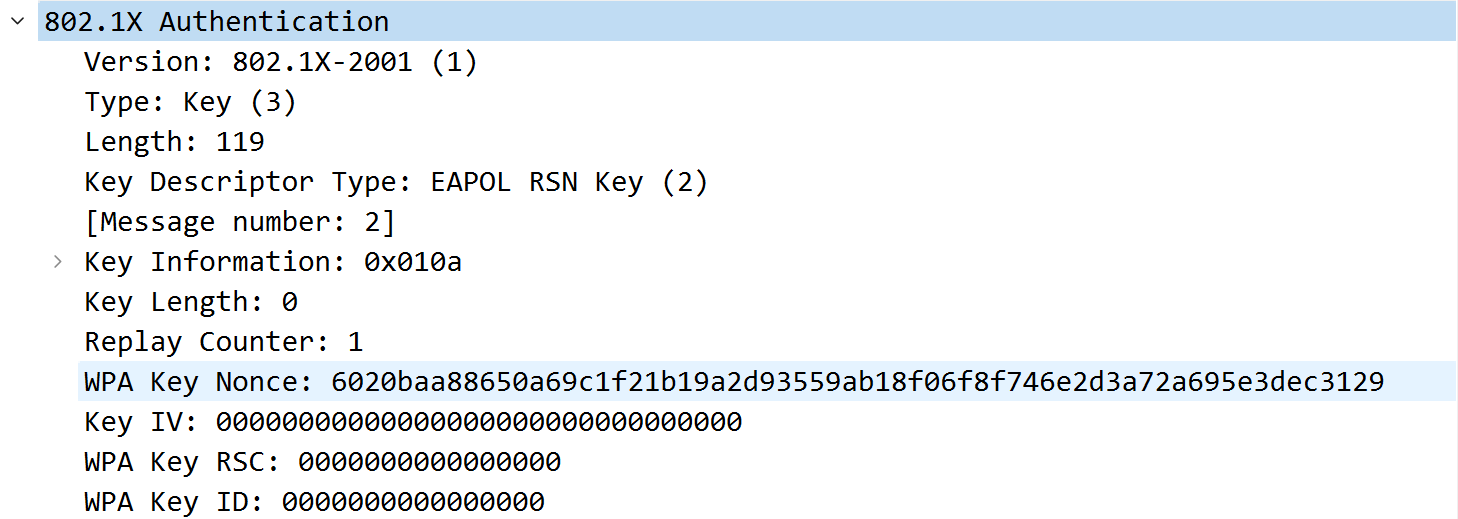


图9 第一次握手报文内容

## 2.4 实验报告和要求

使用抓包软件捕获登录南开大学无线WIFI——NKU\_WLAN的过程，分析协议并撰写实验报告（2.5课时），模板如下：

|  |
| --- |
| **密码学课程第 次实验报告**  **实验名称：**  学号： 姓名： 班级：   1. 实验目的 2. 实验内容说明   （概述本次实验要做什么）   1. 实验原理   （画出所分析的协议流程图并简要说明）   1. 实验步骤   （抓包并根据协议流程具体分析报文内容）   1. 实验结果分析   （对抓包获得的协议进行安全性分析，例如节2.2.2）   1. 总结感想   （说说本次实验的总结感想） |

# 

# 第三章 拓展部分

解决以下任意一个问题，额外增加10~20分。

1. 针对所分析协议的安全漏洞，对协议提出改进方案。
2. 通过抓包对南开大学SSO（Single Sign On单点登录）协议进行分析。
3. 在安全协议设计中，常使用时间戳和随机数，分析这两种机制的作用和优缺点。

# 参考文献

1. 刘晓龙,董琰.802.1x在学生公寓网络中的应用.中国教育信息化2008(02):47-50．
2. 杨岿,刘尧辉.校园网PPPoE和802.1x认证方式的对比分析[J].微计算机信息,2012,28(09):359-361.
3. 唐学岭,姚跃飞,张力军,郭升良.高校校园网认证方式选择分析[J].计算机与网络,2005(16):45-47.
4. 汤小康.多校区校园网接入认证技术分析[J].软件导刊,2014,13(05):138-139.
5. 于承斌,尚年基.802.Ix协议的认证系统的研究与改进.计算机工程.2008(17):117-119.
6. 韩荣珍.深入剖析802.1x协议.计算机安全.2008(11):61-64.
7. IEEE 802.1x Standard For Local and Metroplitian Area Networks Port-based Network Access Control.
8. IEEE 802.1x Overview Port Based Network Access Contrls. Hewlett Packard, March 2000.
9. 陈群,周健.局域网安全认证的EAP策略.计算机技术与发展.2008(9):123-126.
10. 王斐,陈玲.基于802.1x的无线园区网AAA系统的设计与实现.计算机技术与发展.2008(10):143-147.
11. 雷怀玉,任新华.基于EAP/TLS的无线局域网安全认证系统的研究与实现.太原理工大学学报.2005(5):525-528.
12. 冯雯,郑炳伦.基于802.1x的校园网身份认证系统的设计与实施.四川大学学报(自然科学版).2006(4):1237-1241.
13. M. Vanhoef and E. Ronen. Dragonblood: Attacking the Dragonfly handshake of WPA3. In Black Hat US Briefings,2019.
14. 汪定,马春光,翁臣,贾春福.强健安全网络中的中间人攻击研究[J]. 计算机应用, 2012, 32(01):42-44, 65.
15. M. Vanhoef and F. Piessens. Key reinstallation attacks: Forcing nonce reuse in wpa2. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications (ACM CCS 2017), pp.1313-1328.
16. Ding Wang, Debiao He, Ping Wang, Chao-Hsien Chu. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Transactions on Dependable and Secure Computing 2015, 12(4): 228-442.
17. Qingxuan Wang, Ding Wang. Understanding Failures in Security Proofs of Multi-factorAuthentication for Mobile Devices, IEEE Transactions on Information Forensics and Security (TIFS), 2023, 18: 597-612.
18. Neal Koblitz and Alfred J. Menezes. Another look at "provable security". Journal of Cryptology, vol. 20, no. 1, pp. 3–37, 2007.