IEEE802.11i 协议密钥协商机制的分析与改进

邬春学,王吉霞,张凤娜

(上海理工大学 光电信息与计算机工程学院,上海 200093)

摘 要:通过分析无线局域网的安全协议,发现密钥协商机制——四次握手协议在第一次握手时未对消息进行任何处理,导致该协议存在拒绝服务攻击的安全隐患,就此提出加密管理帧的方法来消除该安全隐患,并对该方法加以论证。

关键词:网络安全存取;四次握手;客户端加密伪随机数;管理帧

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1674-7720(2011)06-0062-04

Analysis and improvement for key agreement based on IEEE802.11i protocol

Wu Chunxue, Wang Jixia, Zhang Fengna

(College of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China)

Abstract: In this paper, it analysis the security protocol of wireless network and found that the key agreement——the 4-way handshake didn't encrypt the first message, which made the defeat of Dos attack in this protocol. It proposes the method: encrypt the management frame to avoid this defeat and proves it.

Key words: Wi-Fi protected access(WPA); 4-way handshake; EANonce; management frame

近年来,无线网络得到了飞速的发展,然而无线网络的安全未能跟上使用的步伐。目前,无线网络还无法阻止黑客监听等网络攻击,由于无线网络安全存在的缺陷,导致许多使用无线的用户在无线网络安全上耗资巨大。其中,伪造 MAC 地址是目前无线局域网仍未解决的安全威胁之一。攻击者利用多种工具截获数据包并获取已授权的 MAC 地址,例如 AirJack、WireShark 等工具。黑客伪装成一个已授权的客户端就能发起攻击[1]导致网络服务失败。

目前,IEEE802.11i 是无线网络安全的标准协议,它采用 802.1X+EAP 与 AES 结合的认证方式与数据加密方式。无线网络安全标准主要有有线等效加密协议 WEP、网络安全存取协议 WPA、WPA2 和 IEEE802.11i (WPA2 改进版的标准化,在下层的数据链路机密机制比WPA2 多一个无线强壮认证协议 WRAP)。本文对比了目前主流的无线网络安全标准,详细分析了目前广泛使用的无线网络安全标准 IEEE802.11 协议的四次握手协议,分析四次握手协议的优缺点并提出改进方案加以论证。

1 无线局域网安全机制分析

WEP 使用 RC4 算法加密,给有线局域网的双方通信提供安全保护。ICFCC2009 会议总结了 WEP 存在的问题:WEP 不能预防伪造包、不能抵制重放攻击、错误地使用 RC4、初始化向量可重复使用、黑客篡改信息、RC4 算法本身的缺陷、密钥管理更新功能较弱、容易伪造认证信息等缺陷[2]。

WPA 对 WEP 协议做了改进,提供了暂时密钥完整性协议/信息完整性检查加密算法 TKIP/MIC,避免了 WEP 中 IV(向量初始化)和 MIC 的错误,但它们仍只是临时性的安全协议,并没有形成正式的标准。WPA/WPA2 身份认证加密对比如表 1 所示。

在 2004 年 6 月由 IEEE 正式颁布的(WPA2)IEEE 802.11i 标准是真正的 WLAN 安全标准。802.11i 基于强大的高速加密标准-计数器模式和密码块链消息认证码协议加密算法 AES-CCMP/CBC-MAC,通过使用 AES-CCMP,802.11i 不仅能加密数据包的有效负载,还可以保护被选中数据包的头字段。因此,WLAN 使用802.1X+EAP 与 EAP 加密结合的方式进行身份认证与数据加密。

表 1 WPA 与 WPA2(IEEE802.11i)对比

	WPA	WPA2
企业应用模式	身份认证：IEEE 802.1X+EAP 加密：TKIP+MIC	身份认证：IEEE 802.1X+EAP 加密：AES-CCMP
SOHO/个人应用模式	身份认证：PSK(PMK=PSK) 加密：TKIP+MIC	身份认证：PSK(PMK=PSK) 加密：AES-CCMP

作为 802.11i 协议的重要组成部分，四次握手协议用来进行密钥管理，确保移动请求者和认证者之间的无线传输的安全。因此，在现有四次握手的基础上，更好地研究它的安全性、性能，提高它的可靠性、效能是非常必要的也是非常重要的[3]。

2 分析四次握手及改进方案

2.1 四次握手过程分析

四次握手协议是密钥管理机制中最主要的组成部分，在四次握手中 STA 和 AP 之间在数据链路层发送和接收 4 条消息，主要目的是确定 STA 和 AP 得到的 PMK 是相同且是最新的，它们基于双方共有的 PMK 和握手过程中的参数利用函数 PRF 分别在各自一端生成暂时对等传输密钥 PTK(Pairwise Transient Key)。PTK 包含数据加密密钥，数据完整性密钥，EAPOL-KEY 加密密钥和 EAPOL-KEY 完整性密钥。前两个密钥进行数据保护，后两个密钥在无线设备与接入点之间进行初始化握手时保护通信[4]。同时，通过第 4 次握手的结果通知 STA 是否可以加载加密/整体性校验机制。其中，PMK、PTK 计算公式如下：

PMK=pbkdf2_SHA1(passphrase, SSID, SSIDlength, 4096)(SOHO 应用模式，PMK=PSK) (1)

PTK=MIN(AP_MAC, STA_MAC)||Max(AP_MAC, STA_MAC)||(Min(ANonce, SNonce))||Max(ANonce, SNonce) (2)

其中 PTK 各个字段值如图 1 所示。

KCK 用于 4-Way Handshake 中对数据原始性进行保障，即 MIC Key；KEK 用于 4-Way Handshake 和 Group Key Handshake 中的 EAPOL-Key 帧的加解密；TEK 也就是 TK，用于数据帧的加密；TMK 是 TKIP 中的 MIC 校验 Key。

四次握手过程如图 2 所示。

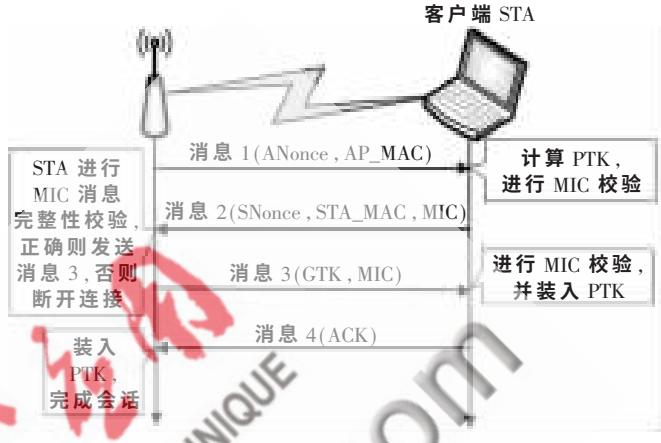

图 2 四次握手过程

(1)第 1 次握手

认证者发送消息帧 1(其中包含 AP 的随机数 ANonce 和 AP 的 MAC 地址 AP_MAC)到 STA。

(2)第 2 次握手

STA 收到消息帧 1 后提取 ANonce 和 AP_MAC，连同自己的随机数 SNonce 和 MAC 地址 STA_MAC，计算 PTK。然后发送消息帧 2，该帧中包含 SNonce，STA_MAC 及 RSN 信息元素 RSNIE，并且该帧使用了已经计算出的 PTK 中 KCK 部分对消息帧 2 进行 MIC 完整性认证，然后放入 EAPOL-Key 帧中一同发送。

(3)第 3 次握手

AP 收到信息帧 2 后，得到 SNonce 和 STA_MAC，计算出 PTK，根据该 PTK 中的 KCK 进行 MIC 验证，与消息帧 2 中的 MIC 进行比较，若不同则丢弃消息帧 2；相同

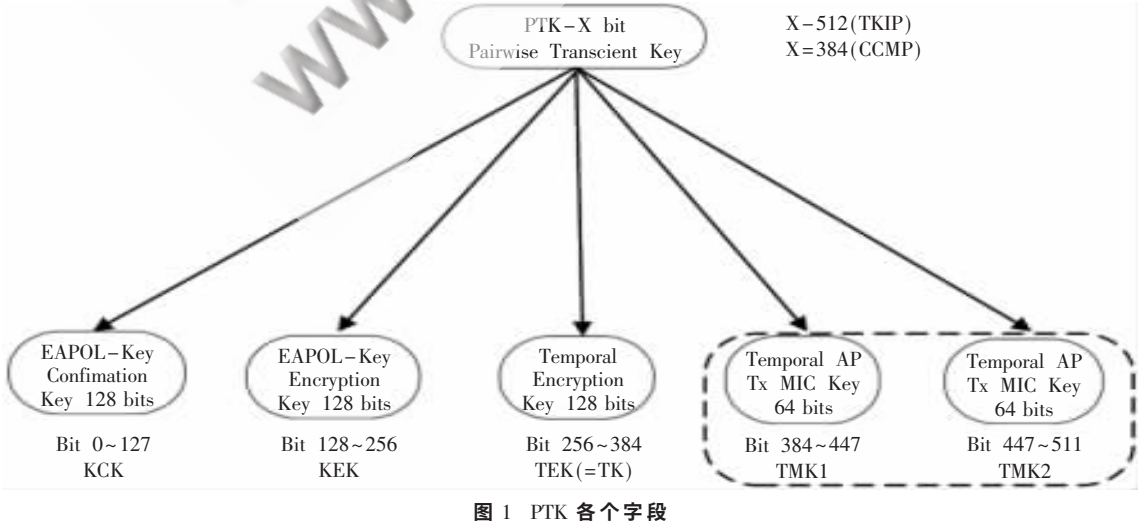

图 1 PTK 各个字段

则向 STA 发送消息帧 3。消息帧 3 中包含 AP 的 RSN 信息元素 RSNIE 和 GTK，用 KEK 加密 GTK，再用 KCK 进行 MIC 认证，最后发送。

(4)第 4 次握手

STA 收到消息帧 3 后装入 PTK，并发送空信息(EAPOL-Key 帧的 Key Data 字段无任何数据)，表示已经装入 PTK。AP 在收到消息帧 4 后就装入 PTK。四次握手完成，至此 PTK 产生并装载完成，双方的密钥协商完成。

2.2 四次握手缺陷分析

第 1 次握手时，认证者 AP 发送消息帧 1 的同时启动超时装置，如果在计时器规定的时间内，认证者 AP 没有收到客户端 STA 的消息帧 2，那么认证者 AP 重新发送消息帧 1 并启动超时装置。四次握手的这种机制，造成客户端 STA 可以多次接收消息帧 1。

应注意，在使用 WEP 或 WPA 机制时，包含 MAC 地址的管理帧并未加密[1]。因此攻击者可以通过嗅探，截获包含合法用户 MAC 地址的数据帧，将自己的 MAC 地址伪装成合法 AP 的 MAC 地址。在认证者 AP 发送消息帧 1 之后发送消息帧 3 之前，攻击者可以不断地向客户端发送伪消息帧 1，客户端在收到伪消息帧 1 后，由于不能识别该消息是伪造的，于是仍然启动计算 PTK 的值进行 MIC 校验的过程。

根据分析，得出：四次握手协议易受 Dos 攻击。攻击示意图如图 3 所示。

图 3 拒绝服务攻击

由于客户端每次收到的消息帧 1 中，由认证者产生的伪随机数 ANonce′的值不同，由式(2)可知：

$ANonce' \neq ANonce \Rightarrow$

$PTK' \neq PTK \Rightarrow$

$MIC' \neq MIC$

客户端计算所得 PTK 的值不同，当消息帧 3 到达客户端时 PTK′≠PTK，造成了 PTK 混乱，数据完整性校验失败，四次握手终止，攻击者 Dos 攻击成功。

2.3 改进方案及效果

认证者与客户端之间共享密钥 PMK，针对 Dos 攻击的问题产生的原因是未对第 1 次握手进行加密，因此在消息 1 中增加加密管理帧 EANonce，就能防止攻击者伪造消息 1。如果 PMK 是由 802.1X 认证动态生成的，那么本文提出的方案就能解决 Dos 攻击问题。然而，当使用预共享密钥方式时，由表 1 可知，PMK=PSK，由于 PSK 一般很长时间不会修改，因而当攻击者获得 PSK 后，造成了消息 1 的 MIC 失效。这种方式需要对四次握手协议进行较多修改，这里暂不予讨论。

802.11i 的建议草案提出：为了防止在请求方通过发送伪消息 1 改变 PTK 的值，现有一种称为 TPTK 暂时对称暂时密钥的机制，在消息 3 到达并验证之前只改变 TPTK 的值。这就表示，请求者在收到消息 1 后会产生两个值 PTK 和 TPTK，在收到并验证消息 3 之前只更改 TPTK 的值。直到收到并验证消息 3 之后才更改 PTK 的值。

然而在这种情况下，这种机制并不能阻当 Dos 攻击，因为这种机制只能阻挡当请求者安装并更新了 PTK 之后，又发送的伪消息 1。如果伪消息 1 是在请求者收到并验证消息 3 之后发送的，那么 TPTK 机制就可行，因为伪消息 1′通不过伪消息 3′的验证。但是在这种攻击时，伪消息 1′是在请求者收到消息 3 之前发送的，因此 TPTK 是根据收到的伪随机数 ANonce′来更新的。并且更新的 TPTK′会用来对合法的消息 3 进行验证，如果 MIC 校验失败，则会话终止。总之，这种单消息攻击会在四次握手中成功实行，并阻塞请求者与认证者的会话[5]。

针对上述分析，客户端极易遭受 Dos 攻击，是由于 IEEE802.11i 协议中四次握手协议的第 1 次握手过程未对管理帧进行加密造成的。本文提出的解决方案如下：

在第 1 次握手过程中，对管理帧进行加密操作，确认消息 1 是由 AP 发送的而不是由攻击者伪造的，将攻击者发送的伪消息 1 丢弃并断开与之的通信过程，可以避免拒绝服务攻击。其实现方法为：在消息 1 中增加字段值 EANonce(加密伪随机数)，改进后的四次握手过程如图 4 所示。

该方案中，在认证者发送的消息 1 中添加了加密随伪机数 EANnoce 字段，当 STA 收到消息 1 后，首先将 EANonce 解密与未加密的 ANonce 进行比较，如果一致则认为是合法 AP 发送的消息，STA 会用该 ANonce 计算新的 PTK，否则，客户端 STA 认为该消息 1 是由攻击者伪造的，丢弃该消息 1 断开通信。其后的过程和 80211i 标准中的四次握手协议完全相同。方案改进前后的效果对比如表 2 所示。

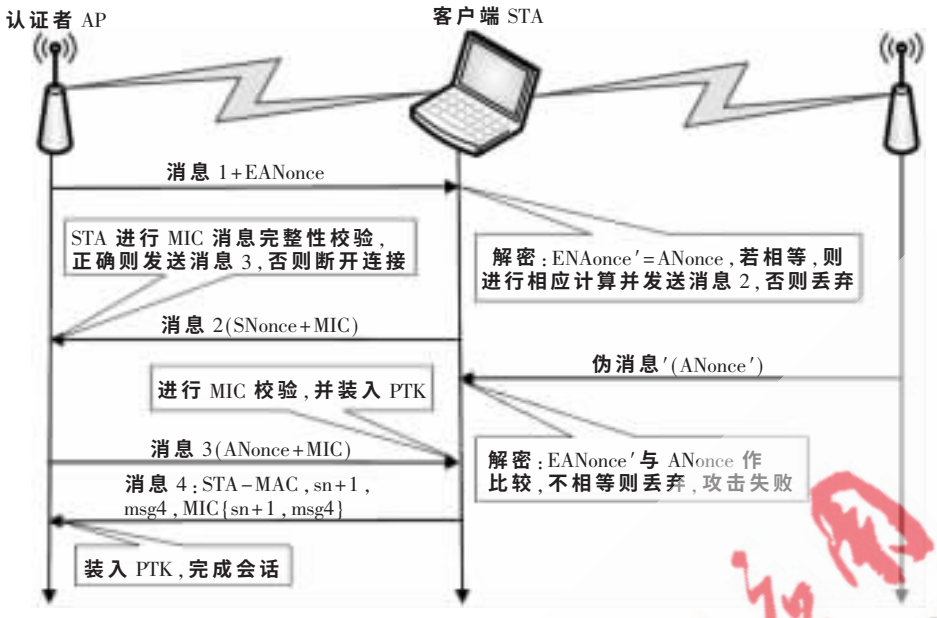

图 4 四次握手过程改进方案

表 2 802.11i 协议与改进方案对比表

对比项	802.11i 协议	改进方案
管理帧	管理帧未加密	管理帧加密
第 1 次握手	消息 1 字段信息：AP-MAC，ANonce	消息 1 字段增加 EANonce 字段
PTK	黑客频繁向 STA 发送消息 1，造成 PTK 混乱	EANonce 解密=ANonce，则断开连接，避免 PTK 重复计算防止 PTK 混乱
服务性能	存在拒绝服务 Dos 攻击隐患	消除拒绝服务攻击隐患

改进方案通过加密管理帧对消息 1 进行保护，有效避免了上文中提到的缺陷。解密后的 EANonce 与未加密的 ANonce 的比较结果用来侦别消息 1 的合法性，因此改进方案在客户端收到消息 1 后就能判断该连接的合法性，若校验失败则将非法通信切断，这可以避免之后过程 PTK 重复计算，防止客户端在收到消息 3 时发生 PTK 混乱，从而达到消除拒绝服务攻击隐患的目的。

IEEE802.11i 协议中四次握手协议为客户端 STA 和认证者 AP 之间提供暂时密钥协商机制，为每次会话提供安全保证，但是协议本身存在的缺陷未对第 1 次握手进行加密，导致客户端存在 Dos 安全威胁。本文提供的改进方案是在四次握手协议的消息 1 字段中增加加密伪随机数 EANonce 字段值，能有效避免 PTK 重复计算消除拒绝服务安全隐患，防止客户端受到 Dos 攻击，从而使无线网络安全性能大大增强。

参考文献

[1] NANGARAJAN V，ARASAN V，HUANG Di Jiang.Using power hopping to counter MAC spoof attacks in WLAN[C]：Consumer Communications and Networking Conference (CCNC)，2010.

[2] LASHKARI A H，DANESH M M S，SAMADI B.A survey on wireless security protocols(WEP，WPA and WPA2/802.11i)[C].2009 2nd IEEE International Conference on Computer Science and Information Technology，2009.

[3] Liu Jing，Ye Xingming，Zhang Jun.Security verification of 802.11i 4-way handshake protocol[C].ICC′08.IEEE International Conference on Communications，2008.

[4] Duan Qi，VIRENDRA M.Server based PMK generation with identity protection for wireless networks[C].2008 4th Workshop on Secure Network Protocols，2008.

[5] Wang Li，SRINIVASAN B.Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard[J].Networks Security Wireless Communications and Trusted Computing (NSWCTC)，2010，2(251)：109-113.

(收稿日期：2010-10-25)

作者简介：

邬春学，男，1964年生，教授，博士，主要研究方向：网络控制系统、骨干网技术。