

基于 SHA-256 消息认证的四次握手协议研究

蒋 华, 阮玲玲, 王 鑫

(桂林电子科技大学 计算机科学与工程学院 广西 桂林 541004)

摘 要: 分析了无线局域网安全标准 IEEE 802.11i 中的四次握手协议, 针对消息 1 未受保护而易遭受伪造消息 DoS 攻击的问题, 提出一种基于 SHA-256 的消息 1 认证改进方案. 该方案利用 PMK 对消息 1 进行认证, 并引入高安全性的 SHA-256 算法对 PMK 进行散列, 而后用其散列值来进行消息认证, 从而能够在消息 1 阶段辨别并剔除伪造的消息, 确保消息 3 验证成功, 提高握手成功率. 实验结果表明, 在同等攻击强度下, 改进方案使得 AP 的网络负载率降低, 网络接入的 STA 数量增加, 提高了网络性能.

关键词: 802.11i; 四次握手; DoS 攻击; 消息认证; SHA-256

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2014)08-0155-04

An Improving Scheme of 4-way Handshake Protocol Based on Message Authentication

JIANG Hua, RUAN Ling-ling; WANG Xin

(College of Computer Science and Engineering, Guilin University of Electronic and Technology, Guilin 541004, China)

Abstract: This paper analyzes the four-way handshake protocol of WLAN's new generation security standard IEEE 802.11i. In order to solve the problem of DoS attack of forging unprotected message, an improved scheme is proposed based on message authentication with an algorithm SHA-256. The proposed scheme uses PMK to authenticate the first message of four-way handshake protocol. It introduces the high-security hash function SHA-256 to handle PMK and then uses the hash value of PMK to make an authentication of the first message. So it can distinguish and reject the forging message and ensure successful validation of the third message. Experiments show that under the same strength attack improved scheme reduces the AP's network load rate and increases the number of STA which successfully access to WLAN, so it can improve network performance.

Key words: 802.11i; 4-way handshake; DoS attack; message authentication; SHA-256

1 引言

无线局域网(WLAN)以其组网灵活、使用方便、易于扩展、移动性好等优点得到广泛应用. 由于传输媒介的开放, 使其存在比有线网络更多的安全问题. 为此, 802.11 组织制定了安全标准 IEEE 802.11i 来保障 WLAN 安全. 标准中提供了动态密钥管理机制, 其中的四次握手协议用于动态生成会话密钥(Pairwise Transient Key, PTK)来保障 STA 与 AP 间的会话安全. 然而四次握手协议中消息 1

明文传输未得到有效保护, 所以该过程易受伪造消息 DoS 攻击.

文献[1]中对四次握手的安全性进行了分析, 指出攻击者可能通过伪造大量消息 1 发送给申请者, 从而引起握手过程阻塞或 CPU 和内存耗尽等问题. 在文献[2]中, 提出重用 Nonce 方法, 能确保 AP 身份合法而非攻击者假冒. 文献[3]中提出一种加强三次握手来代替四次握手过程, 协议中仅交换三条消息且消息均被加密, 交换消息的数量减少使得通信的花费减小. 本文设计出一种基于 SHA-256 的消

收稿日期: 2013-10-13; 修回日期: 2013-12-27

基金项目: 国家自然科学基金重点项目(61262074)

息认证方法,引入一种安全的散列算法 SHA-256 来处理 PMK,而后利用 PMK 散列值进行消息 1 认证,不仅保护了消息 1,同时提高网络性能。

2 四次握手协议及其安全性分析

2.1 四次握手过程

四次握手协议动态产生并管理 STA 与 AP 间的会话密钥 PTK,并且在握手成功之后 STA 加载加密/完整性校验机制。由文献[4]知,四次握手过程如图 1 所示。

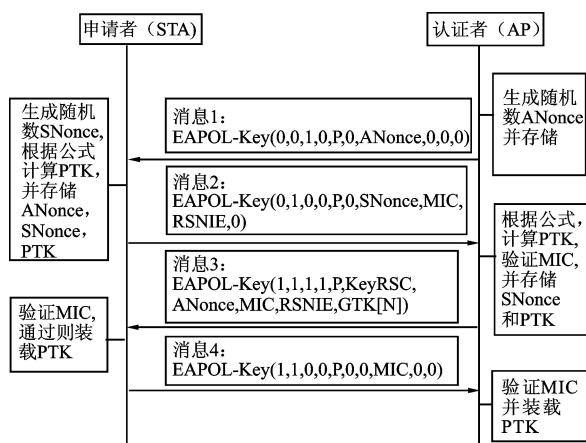


图 1 四次握手过程

协议中四次信息交换详细过程如下:

(1)消息 1 阶段:认证者生成随机数 ANonce,并构造 EAPOL-Key 帧发送给申请者,包括帧密钥信息,APA 等。EAPOL-Key 帧^[4]包含内容: EAPOL-Key(S, M, A, I, K, KeyRSC, ANonce /SNonce, MIC, RSN IE, GTK[N])。

其中 APA,SA 分别为 AP 和 STA 的 MAC 地址,S,M, A, I, K 为帧密钥信息中的标志位,RSN IE 健壮安全网络信息元素,MIC 为消息完整性校验和,GTK 为封装的组密钥。

(2)消息 2 阶段:申请者在接收到消息 1 之后,生成随机数 SNonce 并利用公式计算出 PTK,随后构造消息 2 发送给认证者,其中包括 RSN IE,出现在消息 2、3 中,用于协商密钥套件中其它材料;以及 MIC,出现在消息 2、3、4 中,防止消息被伪造篡改。PTK 的计算公式^[4]为

$$PTK = PRF-512(PMK, "Pairwise key expansion", \text{Min}(APA, SA) || \text{Max}(APA, SA) || SNonce || ANonce)$$

(3)消息 3 阶段:认证者在接收到消息 2 之后,根据公式计算出 PTK 并且验证 RSN IE 和 MIC,若通过,则构造消息 3 发送给申请者,其中包括 GTK

[N]带密钥标识的封装的 GTK,以及 Key RSC 当前将被安装的 GTK 的接收序列计数器,用于确保 802.11i 的重播同步。同时将 Key Info 中的 Install 位置为 1,表示允许装载加密/完整性校验机制。

(4)消息 4 阶段:申请者在接收到消息 3 之后,验证 RSN IE 以及 MIC,若通过则加载安装 PTK,并且构造消息 4 发送给认证者,通知其已成功安装 PTK,而认证者在收到消息 4 且验证后也会安装 PTK,以此完成四次握手过程。

2.2 安全性分析

四次握手协议动态生成与管理密钥的方式使得 WLAN 的安全性有了很大的提高。在四次握手过程中,PTK 是利用 STA 和 AP 握手过程传递的参数产生,而并非直接传递。同时,每个 PTK 只在一次会话中使用,若要建立新的会话,则需产生新的 PTK。

然而,在协议设计中却存在消息 1 未受保护易遭受攻击的问题。握手过程中,AP 为每个 STA 只保持一个握手实例,并且遵循错误丢弃,超时重发的机制^[5],而 STA 必须允许同时运行多个握手实例,在任何状态下都允许接收消息 1 且消息 1 明文传输。因此,攻击者很容易的伪造消息 1,从而发起攻击,如图 2 所示。

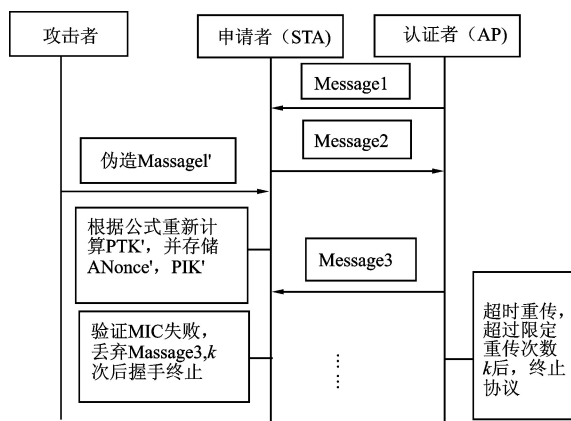


图 2 四次握手协议 DoS 攻击过程

从图 2 可知:攻击者仅通过发送一条伪造的 Message1'就可使得四次握手过程失败;若攻击者不间断地发送 Message1'给 STA,STA 必然会计算大量的 PTK',并存储这些 PTK'和 ANonce',这将会占用 STA 大量的存储资源和 CPU 计算资源,很可能导致 STA 系统瘫痪,从而引起存储 DoS 攻击和 CPU DoS 攻击。同时消息 3 的验证失败必然会带来 AP 大量重传消息 3 的问题,直接影响了网络的性能。

3 基于 SHA-256 的消息 1 认证方案

对于四次握手协议的 DoS 攻击,最根本的原因在于消息 1 缺少消息认证,攻击者容易伪造消息 1. 基于此,本文设计出一种基于 SHA-256 的消息认证^[6]方案,在消息 1 阶段加入消息认证过程,确保消息 1 是由合法 AP 正确发送,而不是由其他人伪造. 该方案可以有效防御 DoS 攻击,并且对原协议改动较小,易于实现.

本文利用 PMK 对消息 1 进行认证,将 PMK 作为消息认证的密钥,同时引入一种散列算法 SHA-256^[4,7],该算法是联邦信息处理标准 FIPS 所认证的五种安全散列算法之一. SHA-256 算法接收一段任意长度明文,然后以一种不可逆的方式将它转换成一段 256 位密文. 算法的不可逆性决定了攻击者不能由密文推导出明文及密钥,同时任何输入信息的变化都会导致散列结果的明显变化.

该方案在原始协议基础上对消息 1 构造过程及格式进行改动,认证者和申请者操作过程见图 3、4.

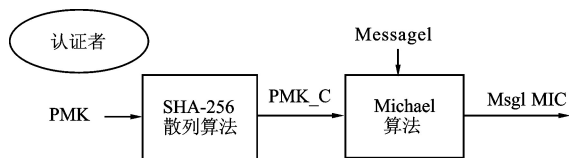


图 3 认证者消息 1 MIC 产生过程

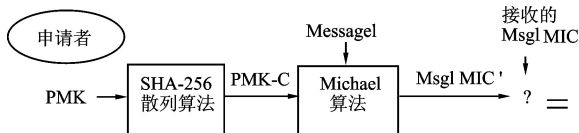


图 4 申请者消息 1 MIC 验证过程

在认证成功之后,STA 与 AP 共同协商出双方共有的 256 位 PMK. 认证者在消息 1 构造过程中,首先将 256 位 PMK 通过 SHA-256 散列算法得到同样 256 位的散列值,称为 PMK_C,然后再利用 PMK_C(后 128 位,作用等同于 PTK 的 KCK)作为 Michael 算法的消息认证密钥,得到消息 1 的 MIC,从而构造出如同消息 2、3、4 一样的具有消息认证功能的消息 1 发送给 AP. 在申请者收到消息 1 之后,首先将自己的 PMK 通过 SHA-256 算法得到 PMK_C,然后将消息 1 利用 PMK_C(后 128 位)通过 Michael 算法得到 MIC',最后比较 MIC' 与收到的 MIC,若相同,则说明通信双方拥有的 PMK 相同,即消息 1 由合法的 AP 发送,反之,说明该消息被篡改或伪

造,应直接丢弃,达到在消息 1 阶段分辨并剔除伪造消息的目的.

该方案除了对消息 1 进行认证,还利用 PMK_C 对消息进行加密. 在原协议中,512 位 PTK 被分解成不同用途的密钥,包括 128 位 EAPOL-Key 完整性密钥 KCK、128 位 EAPOL-Key 加密密钥 KEK、256 位会话密钥 TK. 在本文方案中,利用 PMK_C(前 128 位,与 KEK 作用相同)对消息 1 的 EAPOL-Key 帧进行加密,确保消息机密性;利用 PMK_C(后 128 位,与 KCK 作用相同)对消息 1 的 EAPOL-Key 帧进行消息认证,确保消息完整性.

该方案进行了 AP 身份认证,消息完整性认证,消息机密性保护,从多角度保证消息 1 的安全性.

4 仿真与分析

4.1 安全分析

基于 SHA-256 消息认证 4 次握手协议改进方案利用 PMK 实现消息 1 认证,SHA-256 算法的引入也保护了 PMK 的安全. 该方案特点如下:(1)使用 PMK 作为认证密钥实现消息 1 的认证,有效剔除伪造消息.(2)利用高安全性 SHA-256 算法对 PMK 散列后再作为认证密钥,提高了 PMK 的安全性.(3)在消息 1 阶段辨别并剔除伪造消息,提高消息 3 验证成功率,大大减小了由于伪造消息而带来的系统计算资源和存储资源的消耗,AP 重传消息 3 的数量也大幅减少,提高了网络性能.

其他方案与本文方案进行分析比较,见表 1.

4.2 仿真实验

为了验证该方案的可行性和有效性,首先需要建立一个 802.11i 网络仿真平台,并在其上实现伪造消息 1 的 DoS 攻击. 本文基于 OMNet++ 网络仿真器采用 C++ 语言设计实现仿真. 网络模型如下:50 个工作站平均分布在 200×200 的区域内,同时拥有一个接入点 AP 和一个认证服务器 Radius,以及一个恶意攻击工作站.

在该平台上对本文提出方案进行仿真,并且将其与文献[1]中的 TPTK 方案、文献[2]中的重用 Nonce 方案以及原协议进行对比. 实验中我们以攻击者攻击次数作为自变量,考虑成功接入网络的 STA 数量以及 AP 网络负载.

图 5 所示为攻击次数逐步增加时成功接入的 STA 数量,由图 5 可以看出,本文提出的方案中接入的 STA 数量明显提高,高出原协议近 3 倍(攻击

表 1 几种解决方案分析比较

改进方案	解决问题	优点	缺点
TPTK ^[1]	防止握手过程阻塞,阻止 DoS 攻击	PTK 不会因攻击者的伪造消息而更新,握手成功完成	TPTK 的大量存储,造成内存耗尽,引起二次 DoS 攻击
重用 SNonce ^[3]	消除内存 DoS 攻击	不用缓存 Nonce 和 PTK,消除内存 DoS 攻击	由于不缓存 PTK,所以需要重复计算 PTK,可能因 CPU 耗尽引起 DoS 攻击
基于 PMK 的消息 1 身份认证 ^[3]	验证消息 1 的发送者身份	利用原有参数,对协议改动小	暴力破解,PMK 泄露
加强三次握手 ^[4-5]	因消息 1 未保护而引起的 DoS 攻击	消息均被加密,且通信和计算花费减小	对协议改动比较大
本文方案	因消息 1 未保护而引起的 DoS 攻击	不会引起二次 DoS 攻击,PMK 几乎不可能被猜出,提高 AP 的网络性能	消息 1 阶段增加了少量计算量

次数达 100 时),且数量下降速度平缓,然而 TPTK 方案和重用 Nonce 方案虽然在数量上也有提高,但当攻击达到一定次数时由于引起二次攻击使得 STA 数量下降骤然加快。

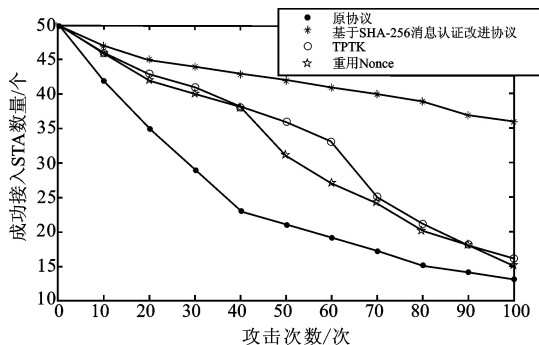


图 5 成功接入网络的 STA 数量随攻击次数变化情况

图 6 所示为 AP 网络负载随攻击次数的变化情况,当攻击次数逐渐增加时 AP 的网络负载率增加,改进方案中 AP 网络负载率普遍降低,比原协议平均降低约 15.6%,且数值随攻击次数的增加平缓增长,而 TPTK 方案和重用 Nonce 方案中则出现当攻击达到一定次数时网络负载率增长速度加快的情况,而出现这种情况的原因是消息 3 的大量重传。

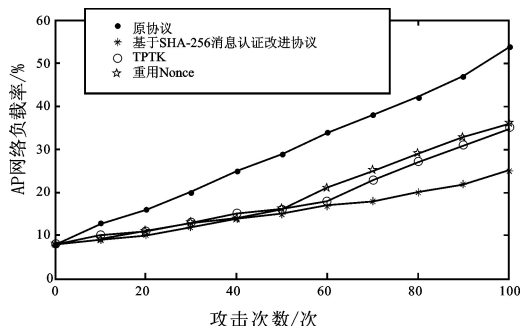


图 6 AP 网络负载率随攻击次数变化情况

5 结束语

针对四次握手协议由于消息 1 未受保护而易受

伪造消息的 DoS 攻击的缺陷,提出了基于 SHA-256 的消息认证改进方案.实验结果表明,在同等攻击强度下,改进方案使得 AP 的网络负载率降低,网络接入的 STA 数量增加,提高了网络性能。

参考文献:

- [1] Li C, Huang H B. Attack analysis of 4-way handshake protocol based on 802.11i[J]. Computer Engineering, 2009, 35(10): 145-149.
- [2] 赵伟艇. 基于 802.11i 的 WLAN 动态密钥管理机制分析及改进[J]. 微电子学与计算机, 2010, 27(4): 193-197.
- [3] Li W, Srinivasan B. Analysis and Improvements over DoS attacks against IEEE 802.11i standard[C]// 2010 Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC). Beijing, China: IEEE Computer Society Press, 2010: 109-113.
- [4] IEEE. IEEE 802.11i-2004; Amendment 6: Medium Access Control (MAC) Security Enhancements[S]. Piscataway, USA: IEEE, 2004.
- [5] 李根. IEEE 802.11 标准四次握手协议安全性分析与改进[D]. 天津: 天津大学, 2010.
- [6] 王红霞, 路赛群. 基于 HMAC-SHA1 算法的消息认证机制[J]. 山西师范大学学报: 自然科学版, 2005(1): 30-33.
- [7] Gueron S, Johnson S, Walker J. SHA-512/256[C]// Proceedings of the 2011 Eighth International Conference on Information Technology: New Generations (ITNG). Las Vegas, NV: IEEE, 2011: 354-358.

作者简介:

蒋华男, (1963-), 博士, 教授, 硕士生导师. 研究方向为网络安全、无线传感网。

阮玲玲女, (1988-), 硕士研究生. 研究方向为网络安全。

王鑫男, (1976-), 副教授, 硕士生导师. 研究方向为网络与信息安全、数据挖掘。