一种适用于 IBSS 网络的无线接入认证协议

铁满霞[①②] 李建东[①] 张变玲[①] 黄振海[①]
[①](西安电子科技大学通信工程学院 西安 710071)
[②](中国科学院研究生院信息安全国家重点实验室 北京 100039)

摘 要：针对目前无线局域网接入认证协议 WAPI 与 RSNA 在 IBSS 模式下运行复杂及密钥管理协议存在 DoS 攻击等问题，该文采用实体认证角色的自适应选择策略，对密钥管理协议进行改进，提出了一种安全性更强、执行效率更高的适用于 IBSS 网络的无线接入认证协议，并利用 CK 模型对其进行了分析。分析结果表明：在密钥加密算法是 CCA 安全及密钥导出算法是伪随机的前提下，协议在 UM 下是 SK-secure 的。最后，以 WAPI 协议为例，给出新协议与原始协议的性能对比。

关键词：无线局域网；IBSS；认证协议；Canetti-Krawczyk 模型；安全分析
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2008)01-0006-04

A Wireless Access Authentication Protocol Suitable for IBSS Networks

Tie Man-xia[①②] Li Jian-dong[①] Zhang Bian-ling[①] Huang Zhen-hai[①]
[①](*School of Telecommunication Engineering*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*State Key Laboratory of Information Security*, *Graduate University of Chinese Academy of Sciences*, *Beijing* 100039, *China*)

Abstract: It is relatively complex for the existing protocols of WAPI and RSNA of WLAN to run in IBSS networks. There are DoS attacks in their key management procedures. In order to resolve these problems, adopting adaptive selection of entity authentication role and redesigning a new key management protocol, a new wireless access authentication protocol more robust, more efficient and more suitable for IBSS networks is presented. With Canetti-Krawczyk model, this new protocol is analyzed in detail. The analysis results show that it is SK-secure in UM if key encryption algorithm is CCA-secure and the key derivation function is pseudo-random. Finally, based on WAPI, the performance comparison between the new protocol and its original one is made.

Key words: WLAN; IBSS; Authentication protocol; Canetti-Krawczyk model; Security analysis

1 引言

为了解决无线局域网 (Wireless Local Area Network，WLAN) 国际标准 ISO/IEC 8802-11 中定义的 (Wired Equivalent Privacy，WEP)安全机制存在的安全漏洞，我国颁布了无线局域网国家标准及其第 1 号修改单[1, 2]，采用无线局域网认证与保密基础结构 WAPI(WLAN Authentication and Privacy Infrastructure)替代 WEP，解决无线局域网的安全问题。几乎同期，IEEE 组织也颁布了 IEEE 802.11i 标准[3]，在后向兼容的基础上，提出了鲁棒安全网络关联(Robust Security Network Association，RSNA)技术弥补 WEP 存在的安全漏洞。

WAPI 利用证书认证及密钥管理协议，RSNA 通过基于扩展认证协议(Extended Authentication Protocol，EAP)的 IEEE 802.1x 与 4 步握手协议，分别实现认证与密钥分发功能，较好地解决了 WLAN 的安全问题，但存在如下两个缺点：(1)运行在 IBSS 网络模式下，协议执行过于复杂，而此种模式的网络中，节点资源(电源、CPU 与存储能力等)通常受限；(2)密钥协商协议的第一个消息未采取保护措施，攻击者可通过伪造消息实施协议阻塞与存储耗尽等(Denial of Service，DoS)攻击。

笔者将针对这两个问题，设计一种适用于 IBSS 网络的无线认证协议，不仅显著降低协议的执行复杂度，而且增强其安全性能。

2 问题分析

通常 WLAN 具有 BSS 和 IBSS 两种组网模式。在 BSS 模式下，无线接入点(Access Point，AP)作为认证器实体(Authenticator Entity，AE)，用户终端作为认证请求者实(Authentication Supplicant Entity，ASUE)，通过认证服务实体(Authentication Service Entity，ASE)完成认证功能后，进行 ASUE 和 AE 之间的单播密钥协商与 AE 的组播(包括多播与广播)密钥通告过程。在 IBSS 模式下，所有加入网络中的每个用户终端地位对等，除两两之间存在单播数据需要

2007-02-13 收到，2007-09-26 改回
国家自然科学基金和微软亚洲研究院联合项目(60372048)和中科院研究生院信息安全国家重点实验室开放课题资助课题

传输外，每个工作站还需发送各自的组播数据，即每个站均须担当 AE，与作为 ASUE 的其他站点分别完成组播密钥通告过程。

同一网元既作为 AE 又作为 ASUE，会引起组播通告协议的反射攻击(Reflection Attack，RA)[4]，为此，可采用同一实体担当两种认证角色时所基于的预共享密钥不相同的方法来防止此类攻击，即同一实体作为 AE 和作为 ASUE 所执行的密钥管理协议应依赖于不同的基密钥(Base Key，BK)和单播会话密钥(Unicast Session Key，USK)，因此 RSNA 与 WAPI 协议在 IBSS 模式下，每个站点均须作为 AE 与其他所有站点之间执行完整的认证与密钥管理协议。可见，对于具有 N 个节点的 IBSS 网络而言，完整的认证与密钥管理协议需执行 $N(N\text{–}1)$次，当节点经常移动或资源受限时，如此高的计算复杂度使协议难以在实际中得到应用。

RSNA 和 WAPI 协议的密钥管理协议还存在一种 DoS 攻击。密钥协商协议是两种安全机制中一个非常关键的部件，其目的就是为了验证 AE 和 ASUE 之间是否拥有认证成功协商的 BK，并导出后续数据通信使用的新鲜 USK。在两种密钥管理协议执行过程中，除消息 1 之外的其他消息均被最新协商的 BK 认证保护，但裸露的消息 1 可被攻击者利用。攻击者可通过伪造消息 1，使得 ASUE 和 AE 协商的 USK 不一致，造成协议阻塞，或攻击者大量伪造消息 1 而引入 ASUE 端的存储耗尽等 DoS 攻击。这种伪造攻击易于实施，造成的危害也比较严重，一次成功的攻击将使得先期的对认证过程的种种努力化为泡影。

文献[5]针对 RSNA 存在的这种 DoS 攻击提出如下解决方法：(1)ASUE 采用随机出队策略实现一个队列，有助于弥补这种脆弱性，但不能完全防止它；(2)由于 AE 和 ASUE 已完成了认证，共享了基密钥 BK，可以对消息 1 添加认证字段，然而这需要修改消息格式，另外，AE 需要在消息 1 中包含一个单调递增序号来避免重放攻击；(3)在单播密钥协商成功之前，ASUE 对收到的所有消息 1 采用同一 $\text{Nonce}_{\text{ASUE}}$ 进行回应；(4)ASUE 还可以采用混合方法，即将方法(3)和方法(1)结合使用提高性能。

在此分析文献[5]倾向使用的方法(4)，即 ASUE 存储自己生成的 $\text{Nonce}_{\text{ASUE}}$，一个或若干个接收到的 Nonce_{AE} 及对应的 USK，但由于方法(1)收效甚微，因此从消息伪造的概率上来讲，对于绝大多数消息 3，ASUE 还需第二次基于 $\text{Nonce}_{\text{ASUE}}$ 和消息 3 中携带的 Nonce_{AE} 计算 USK，即多数情况下 ASUE 需要对收到的消息 1 和消息 3 两次计算同一 USK，将耗去 CPU 较多的计算能力。虽然 ASUE 在存储和 CPU 消耗之间可以进行折衷，但对 DoS 攻击的防御效果并不理想。

如何增强密钥管理协议的安全性，并使两种安全机制在 IBSS 网络中运行简单实用，是笔者在本文中重点解决的问题。

3　新协议的提出

3.1 自适应的认证角色

为了降低协议执行的复杂度，笔者在此提出一种认证实体的角色配置方法，即通过网络管理手段对每个工作站担当的认证角色静态配置，或根据网络运行情况自适应动态选择；对于分别采用静态配置与自适应选择的一对实体而言，如果静态配置的一方是 AE，则采用自适应方式的认证实体将采用 ASUE 角色，若静态配置的一方是 ASUE，则自适应认证实体将自动采用 AE 角色完成认证；如果双方都采用自适应方式，则可根据优先级和物理地址(MAC 地址)来确定角色，优先级高的认证实体担当 AE，而另外一个担当 ASUE；若优先级相同，则物理地址大的将成为 AE，物理地址小的将成为 ASUE。当然也可根据别的策略确定实体的认证角色。

当认证实体采用自适应角色策略后，在一对工作站之间，完成认证与密钥管理功能时，每个工作站所扮演的认证角色相对确定，要么 ASUE，要么 AE，即一对工作站之间只需执行一次完整的协议过程，就可完成双向身份认证与所需的密钥分发。对于具有 N 个节点的网络，完成两两之间的认证功能，协议执行的次数降低了一半，为 $N(N\text{–}1)/2$ 次。

3.2 重新设计的密钥管理协议

针对密钥管理协议存在 DoS 攻击问题，本文将采用模块化和可组合化的方法进行协议的改进设计。改进后的协议由两部分构成：第 1 部分为原来的 WAPI 证书认证协议或基于 EAP 的 IEEE 802.1x 协议，完成认证实体之间的身份认证与基密钥 BK 协商；第 2 部分为新设计的密钥管理协议，替代 WAPI 中的单播密钥协商与组播密钥通告或者 RSNA 中的 4 步握手过程，完成 USK 的协商和组播主密钥(Multicast Master Key，MMK)的通告，即新提出的密钥管理协议将单播密钥协商与组播密钥通告功能集成在一个协议模块中实现。

新密钥管理协议应完成如下功能：(1)验证 ASUE 和 AE 之间具有一致的 BK；(2)协商新鲜且一致的 USK；(3)通告各自的组播密钥且保证对端获得一致的组播密钥。

协议中采用的符号说明如下：$E(K,m)$ 为采用密钥 K 对消息 m 进行加密；为 Nonce_A 为实体 A 的询问(challenge)；BKID 为基密钥 BK 标识；MMK_A 为实体 A 的组播主密钥；KNID 为密钥协商过程标识；msgID 为消息类型标识；MAC(K,m) 为消息认证码，利用密钥 K 对消息 m 进行杂凑计算所得；

密钥协商请求为

$$\text{AE} \rightarrow \text{ASUE:msgID1,BKID,KNID,Nonce}_{\text{AE}}\text{,MAC(BK},m_1) \tag{1}$$

其中 $m_1 = \text{msgID1,BKID,KNID,Nonce}_{\text{AE}}$；

密钥协商响应为

$$\text{ASUE} \rightarrow \text{AE:msgID2, BKID, KNID, Nonce}_{\text{ASUE}}\text{,}\ E(\text{USK, MMK}_{\text{ASUE}})\text{, MAC(USK},m_2) \tag{2}$$

其 中 m_2 = msgID2, BKID, KNID, $\text{Nonce}_{\text{ASUE}}$, E(USK, MMK_{ASUE})；

密钥协商确认：

$$\text{AE} \rightarrow \text{ASUE:msgID3, BKID, KNID, } E(\text{USK, MMK}_{\text{AE}}),\text{MAC}(\text{USK},m_3) \quad (3)$$

其 中 m_3 = msgID3, BKID, KNID, E(USK, MMK_{AE}), MMK_{ASUE}。

对于身份认证成功后的首次密钥协商，KNID 为 AE 实体产生的随机数，密钥协商成功后，AE 和 ASUE 在利用 BK 和 Nonce_{AE}，$\text{Nonce}_{\text{ASUE}}$ 导出单播密钥时，同时推演出下一次密钥协商过程所使用的 KNID，实现密钥协商过程的同步锁，避免或杜绝攻击者对消息 1 的伪造攻击。

4 协议分析

利用模块化的分析方法，在 CK 模型下给出新密钥管理协议的安全性证明。

4.1 Canetti-Krawczyk 模型

Canetti 和 Krawczyk 提出了一种模块化分析密钥交换(Key Exchange，KE)协议的思想，称之为 Canetti-Krawczyk 模型[6−8]，简称 CK 模型。该模型主要包含认证链路模型(Authenticated-links Model，AM)、非认证链路模型(Unauthenticated-links adversarial Model，UM)及认证器 3 个重要的组成部分。

(1)AM 模型 AM 模型可被视为理想环境。在 AM 环境下，攻击者只能通过传递由参与者产生的真实消息激活主体；攻击者可以选择不传递消息，但一旦传递，就只能传送一次，并且忠实地传送到消息的预定目的地，且不能篡改消息。

(2)UM 模型 UM 模型可被视为真实环境。UM 下的攻击者除了具备 AM 模型中的能力外，还可主动激活主体与另外一个主体的会话，并可任意篡改和重放消息。

(3)认证器

定义 1[6] 令 π 和 π' 为两个消息驱动的 n 方协议，称 π' 在 UM 下仿真 π，仅当对任意 UM 下的攻击者 U，必然存在 AM 下的攻击者 A，使得协议输出 $\text{UAUTH}_{\pi',U}$ 和 $\text{AUTH}_{\pi,A}$ 计算上是不可区分的。

定义 2[6] 编译器 C(compiler)是一种算法，其输入是一个协议，输出另一个协议。对任意 AM 下的协议 π，如果协议 $C(\pi)$在 UM 下具有和协议 π 相同的属性，则将这样的编译器 C 称为认证器。所谓认证器就是一个协议编译器，使得 AM 下安全协议可以转换为 UM 下安全程度相同的协议。

定义 3[6] 消息传输(Message Transmission，MT)协议，其唯一功能就是将一条消息由一个参与者发送给另一个参与者。

定理 1[6] 如果 λ 是一个 MT-认证器，则 C_λ 就是一个认证器。

(4)会话密钥安全 SK-secure 攻击者 U 除了通常的攻击手段外，还能够进行测试会话查询，即可在其运行的任何时刻，从那些已完成的、没过期的、未被暴露的会话中选择一个做为测试会话。设 k 是该会话的会话密钥，当 U 对测试会话查询时，掷币 b，$b \xleftarrow{R} \{0,1\}$，若 b 为 0，将 k 给 U；否则，从协议产生密钥的概率分布空间随机选择一个值 r 给 U。U 不允许对该会话和其匹配的会话发动会话状态暴露、会话密钥查询及攻陷参与者攻击。最后，U 输出一个比特 b'，作为 b 的猜测。

定义 4[6] 一个 KE 协议 π 是 SK-secure 的，当且仅当满足以下两条性质：

性质 1 协议 π 能够保证任意两个诚实的实体在完成协议后能够得到相同的密钥；

性质 2 在 UM 下的攻击者 U 正确猜出比特 b 的概率不超过 $0.5+\varepsilon$，其中 ε 为一个在安全参数下可忽略的概率，称之为“优势”。

定理 2[6] 令 π 是一个 AM 下 SK-secure 的 KE 协议，λ 是一个 MT-认证器，则 $C_\lambda(\pi)$ 是一个 UM 下 SK-secure 的 KE 协议。

4.2 密钥管理协议的 CK 模型分析

认证器 1[6,7] 基于 MAC 的 MT-认证器 λ_{MAC}

设：安全参数为 k，K_{ij} 是实体 P_i 和 P_j 的共享密钥，m 为 P_i 传送给 P_j 的消息。

(1) P_i 将消息 m 发送给 P_j；

(2)收到 m 后，P_j 选取一个随机数 r，$r \xleftarrow{R} \{0,1\}^k$，并将其发送给 P_i；

(3)收到 r 后，P_i 将 $\text{MAC}_{Kij}(P_j,r,m)$发送给 P_j。

定理 3[6,7] 假设 MAC 函数是安全的，那么，λ_{MAC} 认证器在 UM 下模拟了协议 MT。

密钥管理协议记为 π'，它使用了认证器 λ_{MAC}，可将其中的认证器去掉而得到 AM 模型下的协议 π，如下：设安全参数为 k，有

消息 1 AE 随机选取 Nonce_{AE} 和 KNID，$\text{Nonce}_{\text{AE}} \xleftarrow{R} \{0,1\}^k$，$\text{KNID} \xleftarrow{R} \{0,1\}^k$，将 {msgID1, BKID, KNID, Nonce_{AE}} 发送给 ASUE。

消息 2 ASUE 收到 $\text{Nonce}'_{\text{AE}}$ 后，随机选取 $\text{Nonce}_{\text{ASUE}}$，$\text{Nonce}_{\text{ASUE}} \xleftarrow{R} \{0,1\}^k$，并根据 BKID 计算单播会话 $\text{USK} = f_{\text{Nonce}'_{\text{AE}},\text{Nonce}_{\text{ASUE}}}(\text{BK})$，随机选取 MMK_{ASUE}，$\text{MMK}_{\text{ASUE}} \xleftarrow{R} \{0,1\}^k$，利用 USK 加密，将 {msgID2,BKID,NKID, $\text{Nonce}_{\text{ASUE}}, c_1 = E(\text{USK},\text{MMK}_{\text{ASUE}})$} 发送给 AE。

消息 3 AE 收到 $\text{Nonce}'_{\text{AUSE}}$ 后，计算单播会话 $\text{USK}' = f_{\text{Nonce}_{\text{AE}},\text{Nonce}'_{\text{ASUE}}}(\text{BK})$，对 c'_1 解密得到 $\text{MMK}'_{\text{AUSE}}$。随机选取 MMK_{AE}，$\text{MMK}_{\text{AE}} \xleftarrow{R} \{0,1\}^k$，利用 USK 加密，将 $\{\text{msgID3,BKID,NKID},c_2 = E(\text{USK},\text{MMK}_{\text{AE}})\}$ 发送给 ASUE。

ASUE 收到消息 3 后，校验认证码，解密 c'_2 得到 $\text{MMK}'_{\text{AUSE}}$。

定理 4　如果密钥加密算法是 CCA 安全的，BK 是安全的，且 f 和 Nonce_{AE}，$\text{Nonce}_{\text{ASUE}}$ 是伪随机的，则协议 π 在 AM 下是 SK-secure 的。

证明　与文献[6]中协议 ENC 的证明相类似，这里不再赘述。

根据定理 2、定理 3 和定理 4 可得，π' 协议在 UM 下是 SK-secure 的。

5　性能比较

新协议相比原始协议，实体采用灵活的认证角色，不仅减少了协议交互的轮数，而且在保障安全性的前提下，提高了协议执行的效率。以 WAPI 协议为例说明，在一个具有 N 个节点的网络中，完成两两之间的认证，原始协议需要执行 $N(N\text{–}1)$个完整过程，而当采用改进后的密钥管理协议时，只需执行 $N(N\text{–}1)/2$ 个完整过程，且公钥运算与单钥计算次数显著减少，如表 1 所示。其中 WAPI 表示原始的 WAPI 认证与密钥管理协议，WAPI*表示原始的 WAPI 证书认证与新定义的密钥管理协议的组合，且各种算法指标单位为 $N(N\text{–}1)/2$ 次。

表 1 协议性能比较

协议	交互轮数	乘法 (MN)	签名 (MN)	验证签名及证书 (MN)	单钥加密 (MN)	单钥解密 (MN)	HASH (MN)
WAPI	20	4	8	10	2	2	22
WAPI*	8	2	4	5	2	2	9

在预计算下，协议的性能比较见表 2。

表 2 预计算下协议性能比较

协议	交互轮数	乘法 (MN)	签名 (MN)	验证签名及证书 (MN)	单钥加密 (MN)	单钥解密 (MN)	HASH (MN)
WAPI	10	0	0	0	2	2	18
WAPI*	3	0	0	0	2	2	7

可见，改进后的 WAPI 协议的性能明显优于改进前协议的性能，从而更适合应用在 IBSS 网络中。

5　结束语

本文针对目前 WLAN 现有的安全接入认证协议在 IBSS 网络中运行存在的问题，提出了一种安全性能更高、实用性更强的认证与密钥分发协议，并利用 CK 模型对其进行了安全性证明，指出其具有满足应用的安全属性。基于 WAPI 协议，将改进后的协议与原始协议进行了性能比对，协议执行与计算的复杂度大大降低，可以较好地满足 IBSS 网络中资源通常受限的节点需求。

参 考 文 献

[1] 黄振海，郭宏，王育民等. GB15629.11《信息技术 系统间远程通信和信息交换 局域网和城域网特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范》，中国标准出版社，2003.

[2] 赖晓龙，曹军，铁满霞等. GB15629.11-2003/XG1-2006《信息技术 系统间远程通信和信息交换 局域网和城域网特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范 第 1 号修改单》，中国标准出版社，2006.

[3] IEEE Computer Society LAN MAN Standards Committee, Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specifications: Medium Access Control(MAC) Security Enhancements, ANSI/IEEE Std 802.11i, 2004–6–24.

[4] Mao W B. Modern Cryptography: Theory & Practice. Pearson Education, 2003–7–1.

[5] He C H and Mitchell J C. Security analysis and improvements for IEEE 802.11i. Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS'05), San Diego, 2005: 90–110.

[6] Canetti R and Krawczyk H. Analysis of key-exchange protocol and their use for building secure channels. Proceeding of Eurocrypt 2001, LNCS 2045. Berlin, Springer-Verlag, 2001: 453–474.

[7] Bellare M, Canetti R, and Krawczyk H. A modular approach to the design and analysis of authentication and key-exchange protocols, 30th STOC, ACM Press, New York, 1998: 419–428.

[8] Wilson S, Johnson D, and Menezes A. Key exchange protocols and their security analysis. Proceedings of the 6th IMA International Conference on Cryptography and Coding, Cirencester, 1997: 30–45.

铁满霞：　女，1968 年生，副教授，研究方向为宽带无线 IP 技术、移动通信、信息安全等.

李建东：　男，1962 年生，教授，研究方向为宽带无线 IP 技术、移动通信、软件无线电、Ad hoc 自组织网络等.

张变玲：　女，1975 年生，博士，研究方向为宽带无线 IP 技术、移动通信、信息安全等.

黄振海：　男，1976 年生，讲师，研究方向为宽带无线 IP 技术、移动通信、信息安全等.