doi:10.3969/j.issn.1000-436x.2014.07.012

可信计算环境下的 WLAN Mesh 安全关联方案

肖跃雷[1]，王育民[2]，庞辽军[3]，谭示崇[2]

（1. 西安邮电大学 物联网与两化融合研究院，陕西 西安 710061；
2. 西安电子科技大学 综合业务网理论与关键技术国家重点实验室，陕西 西安 710071；
3.西安电子科技大学 生命科学技术学院，陕西 西安 710071）

摘 要：针对第 3 版 WLAN 鉴别基础设施（WAI）协议用于建立 WLAN Mesh 安全关联时所存在的问题，提出了一种基于改进 WAI 协议的 WLAN Mesh 安全关联方案。通过性能对比分析，该方案提高了 WLAN Mesh 安全关联的性能，特别是降低了认证服务器（AS）的负载。为了适用于可信计算环境，继而在该方案的基础上提出了一种可信计算环境下的 WLAN Mesh 安全关联方案。此外，利用串空间模型（SSM）证明了这 2 个 WLAN Mesh 安全关联方案是安全的。

关键词：WLAN Mesh；可信计算；平台认证；串空间模型；安全关联
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2014)07-0094-10

WLAN Mesh security association scheme in trusted computing environment

XIAO Yue-lei[1], WANG Yu-min[2], PANG Liao-jun[3], TAN Shi-chong[2]

(1. Institute of IOT and IT-based Industrialization, Xi'an University of Posts & Telecommunications, Xi'an 710061, China;
2. State Key Lab. of Integrated Service Networks, Xidian University, Xi'an 710071, China;
3. School of Life Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: To solve the existing problems caused by that the third version of WLAN authentication infrastructure (WAI) protocol was used to establish WLAN Mesh security association, a WLAN Mesh security association scheme based on an improved WAI protocol was proposed. The results of performance analysis of the scheme show that the scheme improves the performance of WLAN Mesh security association, especially decreases the overhead of the authentication server (AS). Then, on basis of this scheme, a WLAN Mesh security association scheme in trusted computing environment was put forward to meet the demand of trusted computing environment. Moreover, the two WLAN Mesh security association schemes were proved secure in the strand space model (SSM).

Key words: WLAN Mesh; trusted computing; platform-authentication; strand space model; security association

1 引言

WLAN Mesh 网络作为一种新型的网络结构，成为近年来国内外研究的热点问题之一。在 802.11i[1]的基础上，802.11s[2]提出了 EMSA(efficient mesh security association)来建立 WLAN Mesh 安全关联，包括建立新加入的 Mesh 节点(MP, mesh point)和 Mesh 认证器(MA, mesh authenticator)之间的安全关联、新加入的 MP 和 Mesh 密钥分发器(MKD, mesh key distributor)之间的安全关联、新加入的 MP 和各个邻居 MP 之间的安全关联。WLAN Mesh 安全关联主要包括 4 个步骤：第 1 个步骤是执行一个

收稿日期：2013-03-23；**修回日期**：2014-05-20
基金项目：西安邮电大学青年教师科研基金资助项目（401-1201）；国家自然科学基金资助项目（60473072，60803151）；国家自然科学基金委员会——广东联合基金资助项目（U0835004）
Foundation Items: The Scientific Research Foundation for the Junior Teachers of Xi`an University of Posts & Telecommunications(401-1201); The National Natural Science Foundation of China (60473072, 60803151); The National Natural Science Foundation of China-Guangdong Provincial People's Government of the Joint Natural Science Fund Projects (U0632004)

认证过程，实现对新加入的 MP 的认证并导出密钥，第 2～3 个步骤是基于第 1 个步骤导出的密钥建立新加入的 MP 和 MA 之间的安全关联、新加入的 MP 和 MKD 之间的安全关联、新加入的 MP 和各个邻居 MP 之间的安全关联。近年来，随着可信计算技术的产生和发展，使得可信计算技术不仅可以建立终端的可信计算环境，而且可以将终端的可信计算环境扩展至网络，使网络成为一个可信计算环境，从而从源头上遏制住恶意攻击，有效解决日渐突出和复杂的网络安全问题。可信接入认证的目标就是将终端的可信计算环境扩展至网络，它包括用户认证和平台认证，其中平台认证包括平台身份认证和平台完整性验证[3]，平台身份认证可以基于可信第三方(私有 CA)或直接匿名证明 (DAA, direct anonymous attestation)机制来实现。因此， EMSA 在可信计算环境下不再适用，因为它不能实现 WLAN Mesh 可信接入认证。也就是说，EMSA 没有实现对新加入的 MP 的平台认证，从而不能构建可信计算环境 WLAN Mesh 网络。可信计算环境 WLAN Mesh 网络是指每一个新加入的 MP 在接入 WLAN Mesh 网络之前都必须对它进行平台认证，以保证每一个新加入的 MP 处于可信计算环境下的安全状态，从而将每一个新加入的 MP 的可信计算环境扩展至整个 WLAN Mesh 网络。于是，马卓等提出了一些 WLAN Mesh 可信接入认证协议[4~6]来增强 EMSA，并证明了它们是通用可组合安全的。

类似于 802.11i，我国也推出了 WLAN 鉴别和保密基础设施(WAPI, WLAN authentication privacy infrastructure)[7~9]来解决 IEEE 802.11 标准[10]中存在的安全问题，它包括 WLAN 鉴别基础设施(WAI, WLAN authentication infrastructure)和 WLAN 保密基础设施(WPI, WLAN privacy infrastructure)2 个部分，其中，WAI 由证书鉴别过程、单播密钥协商过程和组播密钥协商过程组成。虽然最新的 WAI 协议(即第 3 版 WAI 协议) 被证明是安全的[11,12]，但是它用于建立 WLAN Mesh 安全关联时存在以下问题：新加入的 MP 首先需要与 MA、认证服务器(AS, authentication server)执行一次 WAI 证书鉴别过程和一次单播密钥协商过程来接入 WLAN Mesh 网络并建立新加入的 MP 和 MA 之间的安全关联，然后还需要与 WLAN Mesh 网络中的 n 个邻居 MP 和 AS 执行 n 次 WAI 证书鉴别过程和 n 次单播密钥协商过程来建立新加入的 MP 和 n 个邻居 MP 之间的安全关联，这使得 WLAN Mesh 安全关联的性能较差，特别是使 AS 的负载太重。此外，由于第 3 版 WAI 协议没有考虑平台认证，所以它不适用于建立可信计算环境下的 WLAN Mesh 安全关联，也就是说它不能实现 WLAN Mesh 可信接入认证。

为了解决上述问题，本文通过对第 3 版 WAI 协议的改进，提出了一种基于改进 WAI 协议的 WLAN Mesh 安全关联方案，它提高了 WLAN Mesh 安全关联的性能，特别是降低了 AS 的负载。然后，通过对第 3 版 WAI 协议的进一步改进，在该方案的基础上提出了一种可信计算环境下的 WLAN Mesh 安全关联方案，它能实现 WLAN Mesh 可信接入认证，从而增强了 WLAN Mesh 的安全性。此外，本文利用串空间模型(SSM, strand space model)[13~15]证明了这 2 个 WLAN Mesh 安全关联方案是安全的。

2　基于改进 WAI 协议的 WLAN Mesh 安全关联方案

基于改进 WAI 协议的 WLAN Mesh 安全关联方案如图 1 所示。

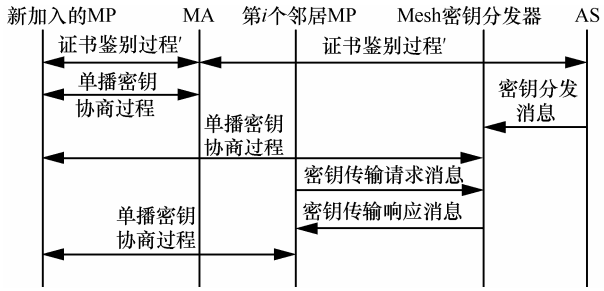


图 1　基于改进 WAI 协议的 WLAN Mesh 安全关联方案

在图 1 中，对第 3 版 WAI 协议的改进主要体现于证书鉴别过程′，它是对第 3 版 WAI 协议中的证书鉴别过程的改进。基于改进 WAI 协议的 WLAN Mesh 安全关联方案主要包括以下 3 个部分。

1) 新加入的 MP、MA 和 AS 执行证书鉴别过程′来实现新加入的 MP 与 MA 之间的双向认证，新加入的 MP 与 AS 之间的双向认证，并建立新加入的 MP 与 MA 之间的基密钥 BK，以及新加入的 MP 与 AS 之间的主密钥 MK。然后，新加入的 MP 和 MA 利用 BK 执行单播密钥协商过程建立它们之间的单播密钥，用于保护它们之间的链路层数据通信。

2) AS 通过密钥分发消息将 MK 分发给 MKD，其中密钥分发消息是利用 AS 与 MKD 之间预置的安全通道进行安全保护的。然后，MKD 和新加入

的 MP 将 MK 扩展为 2 个一级主密钥：FMK_1 和 FMK_2。最后，MKD 和新加入的 MP 利用 FMK_1 执行单播密钥协商过程建立它们之间的单播密钥，用于保护后来它们之间交互的密钥传输请求消息和密钥传输响应消息。

3) 当新加入的 MP 在接入 WLAN Mesh 网络后要与第 i 个邻居 MP 建立安全关联时，新加入的 MP 将 FMK_2 扩展为一个用于它和该邻居 MP 的二级主密钥 SMK_i，第 i 个邻居 MP 向 MKD 发送密钥传输请求消息，MKD 收到密钥传输请求消息后将 FMK_2 扩展为一个用于新加入的 MP 和该邻居 MP 的二级主密钥 SMK_i，并通过密钥传输响应消息发送给该邻居 MP，其中密钥传输请求消息和密钥传输响应消息中是利用该邻居 MP 与 MKD 之间已建立的单播密钥进行安全保护的。然后，新加入的 MP 和第 i 个邻居 MP 利用 SMK_i 执行单播密钥协商过程建立它们之间的单播密钥，用于保护它们之间的链路层数据通信。

2.1 证书鉴别过程′

证书鉴别过程′的具体步骤如下。

1) $AP \rightarrow AS$：$\underline{ECDH_{\text{params}}}$。

2) $AS \rightarrow AP$：$\underline{ECDH_{\text{params}} \| N_{AS} \| z \cdot P \| \sigma_{AS,2}}$。

3) $AP \rightarrow STA$：$N_{AP} \| ID_{AS} \| Cert_{AP} \| ECDH_{\text{params}} \underline{\| N_{AS} \| z \cdot P \| \sigma_{AS,2}}$。

4) $STA \rightarrow AP$：$N_{AP} \| N_{STA} \| x \cdot P \| ID_{AP} \| Cert_{STA} \| ECDH_{\text{params}} \| ID_{AS} \underline{\| \sigma_{STA,2} \| MAC_{STA}} \underline{\| \sigma_{STA}}$。

5) $AP \rightarrow AS$：$N_{AP,2} \| N_{STA} \| Cert_{STA} \| Cert_{AP} \underline{\| x \cdot P \| \sigma_{STA,2} \| MAC_{STA} \| N_{AP} \| y \cdot P}$。

6) $AS \rightarrow AP$：$Res_{AS} \| \sigma_{AS} \underline{\| MAC_{AS}}$。

7) $AP \rightarrow STA$：$N_{STA} \| N_{AP,2} \| Re_{\text{access}} \| x \cdot P \| y \cdot P \| ID_{AP} \| ID_{STA} \| Res_{AS} \| \sigma_{AS} \underline{\| MAC_{AS}} \underline{\| \sigma_{AP}}$。

其中，STA、AP 和 AS 分别表示站(STA，station)、接入点(AP，access point)和 AS，

$ECDH_{\text{params}}$ 为 AP 选择的 ECDH 参数，N_{STA} 和 N_{AS} 分别为 STA 和 AS 产生的随机数，N_{AP} 和 $N_{AP,2}$ 为 AP 产生的 2 个随机数，$x \cdot P$、$y \cdot P$ 和 $z \cdot P$ 分别为 STA、AP 和 AS 产生的密钥数据，ID_{STA}、ID_{AP} 和 ID_{AS} 分别为 STA、AP 和 AS 的身份标识，$Cert_{STA}$ 和 $Cert_{AP}$ 分别为 STA 和 AP 的证书，$\sigma_{AS,2}$ 为 AS 的签名且 $\sigma_{AS,2} = [z \cdot P]_{sk_{AS}}$，$sk_{AS}$ 为 AS 的私钥，$\sigma_{STA,2}$ 为 STA 的签名且 $\sigma_{STA,2} = [x \cdot P]_{sk_{STA}}$，$sk_{STA}$ 为 STA 的私钥，σ_{AS} 为 AS 的签名且 $\sigma_{AS} = [Res_{AS}]_{sk_{AS}}$，$Res_{AS} = N_{AP,2} \| N_{STA} \| Cert_{STA} \| Cert_{AP} \| Re_{STA} \| Re_{AP}$，$Re_{STA}$ 和 Re_{AP} 分别为 $Cert_{STA}$ 和 $Cert_{AP}$ 的证书验证结果，MAC_{STA} 为 STA 的消息鉴别码且 $MAC_{STA} = H_{MAC}(MK, N_{AS} \| z \cdot P \| \sigma_{AS,2} \| N_{STA} \| Cert_{STA} \| x \cdot P \| \sigma_{STA,2})$，$H_{MAC}()$ 为用于生成消息鉴别码的 Hash 函数，$MK = H_{\text{KD}}(x \cdot z \cdot P, N_{STA} \| N_{AS})$，$H_{\text{KD}}()$ 为用于扩展密钥的 Hash 函数，MAC_{AS} 为 AS 的消息鉴别码且 $MAC_{AS} = H_{MAC}(MK, N_{AS} \| z \cdot P \| \sigma_{AS,2} \| N_{STA} \| Cert_{STA} \| x \cdot P \| \sigma_{STA,2} \| MAC_{STA} \| N_{AP} \| y \cdot P \| Res_{AS} \| \sigma_{AS})$，$\sigma_{STA}$ 为 STA 的签名且 $\sigma_{STA} = [N_{AP} \| N_{STA} \| x \cdot P \| ID_{AP} \| Cert_{STA} \| ECDH_{\text{params}} \| ID_{AS} \| \sigma_{STA,2} \| MAC_{STA}]_{sk_{STA}}$，$\sigma_{AP}$ 为 AP 的签名且 $\sigma_{AP} = [N_{STA} \| N_{AP,2} \| Re_{\text{access}} \| x \cdot P \| y \cdot P \| ID_{AP} \| ID_{STA} \| Res_{AS} \| \sigma_{AS} \| MAC_{AS}]_{sk_{AP}}$，$sk_{AP}$ 为 AP 的私钥，Re_{access} 为 AP 产生的接入结果。

相对于第 3 版 WAI 协议中的证书鉴别过程，证书鉴别过程′中带单下划线的消息和字段是新增加的，而带双下划线的字段做了相应的扩展，目的是实现 STA 和 AS 之间的双向认证，并建立它们之间的 MK。由于证书鉴别过程′只是新增加了一些消息和字段，以及扩展了一些字段，所以它与第 3 版 WAI 协议中的证书鉴别过程向后兼容。

2.2 性能对比分析

假设：新加入的 MP 通过 MA 接入 WLAN Mesh 网络并建立与 MA 之间的安全关联后，还需要与 n 个邻居 MP 建立安全关联。表 1 给出了本文引言中所述的基于 WAI 协议的 WLAN Mesh 安全关联方案和基于改进 WAI 协议的安全关联方案的性能对比，其中，E 为模指数运算，F 为计算签名，M 为消息认证码。

表 1 基于 WAI 协议的 WLAN Mesh 安全关联方案和基于改进 WAI 协议的安全关联方案的性能对比

交互消息数	新加入 MP 的计算量	MA 的计算量	n 个邻居 MP 的计算量	MKD 的计算量	AS 的计算量
8+8n	(n+1)(1E+1F+1M)	1E+1F+1M	n(1E+1F+1M)	0	(n+1)F
10+(4+5n)	(2E+2F+2M)+(n+1)M	1E+1F+1M	nM	1M	1E+2F+1M

在表 1 中，第 1 行性能参数是基于 WAI 协议的 WLAN Mesh 安全关联方案的交互消息数及相关计算量，第 2 行性能参数是基于改进 WAI 协议的 WLAN Mesh 安全关联方案的交互消息数及相关计算量。从表 1 可以看出，基于改进 WAI 协议的 WLAN Mesh 安全关联方案比本文引言中所述的基于 WAI 协议的 WLAN Mesh 安全关联方案在通信效率和计算量上都具有明显的优势，具体分析如下。

方案通信效率：当 n=2 时，2 个方案中交互的消息数相同，但是，随着 n 的值增大，与本文引言中所述的基于 WAI 协议的 WLAN Mesh 安全关联方案的交互消息数相比，基于改进 WAI 协议的 WLAN Mesh 安全关联方案的交互消息数越来越少。

方案计算量：2 个方案中 MA 的计算量相同，而基于改进 WAI 协议的 WLAN Mesh 安全关联方案中 MKD 的计算量比本文引言中所述的基于 WAI 协议的 WLAN Mesh 安全关联方案中 MKD 的计算量增加了 1M，但是，随着 n 的值增大，与本文引言中所述的基于 WAI 协议的 WLAN Mesh 安全关联方案中新加入的 MP 的计算量、n 个邻居 MP 的计算量和 AS 的计算量相比，基于改进 WAI 协议的 WLAN Mesh 安全关联方案中新加入的 MP 的计算量、n 个邻居 MP 的计算量和 AS 的计算量越来越小。

3　可信计算环境下的 WLAN Mesh 安全关联方案

可信计算环境下的 WLAN Mesh 安全关联方案如图 2 所示。

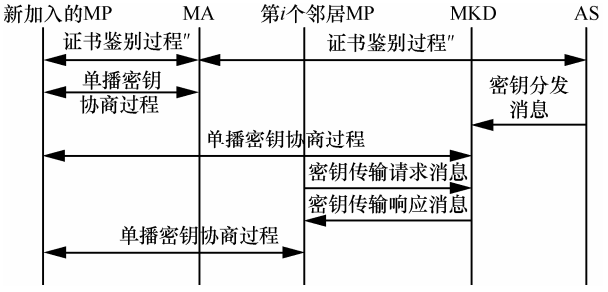


图 2　可信计算环境下的 WLAN Mesh 安全关联方案

图 2 所示的可信环境下的 WLAN Mesh 安全关联方案与图 1 所示的基于改进 WAI 协议的 WLAN Mesh 安全关联方案的区别主要体现于证书鉴别过程″，它是对图 1 中的证书鉴别过程′的改进。由于证书鉴别过程″引入了平台认证，所以证书鉴别过程″中的认证包含用户认证和平台认证，从而对证书鉴别过程″的形式化描述与上述证书鉴别过程′有所区别。

证书鉴别过程″的具体步骤如下(由于 σ_α 中绑定 BK，所以步骤 3)中需要传输 $y\cdot P$ 且 $N_{AP}=N_{AP,2}$)：

1) $AP\rightarrow AS$：$ECDH_{\text{params}}$。

2) $AS\rightarrow AP$：$ECDH_{\text{params}}\|N_{AS}\|z\cdot P\|\sigma_{AS,2}$。

3) $AP\rightarrow STA$：$N_{AP}\|ID_{AS}\|Cert_b\|ECDH_{\text{params}}\|N_{AS}\|z\cdot P\|\sigma_{AS,2}\|\underline{y\cdot P}$。

4) $STA\rightarrow AP$：$N_{AP}\|N_{STA}\|x\cdot P\|ID_b\|Cert_a\|ECDH_{\text{params}}\|ID_{AS}\|\sigma_{a,2}\|MAC_{a,2}\|\underline{y\cdot P}\|\underline{PCR_\alpha}\|\underline{\{SML_\alpha\}_{k_{STA,AS}}}\|\underline{Cert(AIK_{\text{pk},\alpha})}\|\underline{\sigma_\alpha}\|\underline{\sigma_{\alpha,2}}\|\underline{\underline{\sigma_a}}\|\underline{MAC_a}$。

5) $AP\rightarrow AS$：$N_{AP,2}\|N_{STA}\|Cert_a\|Cert_b\|x\cdot P\|\sigma_{a,2}\|MAC_{a,2}\|N_{AP}\|y\cdot P\|\underline{PCR_\alpha}\|\underline{\{SML_\alpha\}_{k_{STA,AS}}}\|\underline{Cert(AIK_{\text{pk},\alpha})}\|\underline{\sigma_{\alpha,2}}\|\underline{PCR_\beta}\|\underline{\{SML_\beta\}_{k_{AP,AS}}}\|\underline{Cert(AIK_{\text{pk},\beta})}$。

6) $AS\rightarrow AP$：$\underline{\underline{Res_{AS}}}\|\sigma_{AS}\|MAC_{AS}$。

7) $AP\rightarrow STA$：$N_{STA}\|N_{AP,2}\|Re_{\text{access}}\|x\cdot P\|y\cdot P\|ID_b\|ID_a\|\underline{\underline{Res_{AS}}}\|\sigma_{AS}\|MAC_{AS}\|\underline{PCR_\beta}\|\underline{Cert(AIK_{\text{pk},\beta})}\|\underline{\sigma_\beta}\|\underline{\underline{\sigma_b}}\|\underline{MAC_b}$。

其中，a 为 STA 的用户，α 为 STA 的平台，b 为 AP 的用户，β 为 AP 的平台，ID_a 和 ID_b 分别为 a 和 b 的身份标识，$Cert_a$ 和 $Cert_b$ 分别为 a 和 b 的证书，PCR_α 和 PCR_β 分别为 α 和 β 的平台配置寄存器(PCR，platform configuration register)值，SML_α 和 SML_β 分别为 α 和 β 的存储度量日志(SML，stored measurement log)[3]，$Cert(AIK_{\text{pk},\alpha})$ 和 $Cert(AIK_{\text{pk},\beta})$ 分别为 α 和 β 的平台身份证明密钥(AIK，attestation identity key)证书[3]，$AIK_{\text{pk},\alpha}$ 和 $AIK_{\text{pk},\beta}$ 分别为 α 和 β 的 AIK 公钥，$k_{STA,AS}$ 为 STA 和 AS 之间建立的平台配置保护密钥，$k_{AP,AS}$ 为 AP 和 AS 之间建立的平台配置保护密钥，$\sigma_{a,2}$ 为 a 的签名且 $\sigma_{a,2}=[x\cdot P]_{sk_a}$，$sk_a$ 为 a 的私钥，$Res_{AS}=N_{AP,2}\|N_{STA}\|Cert_a\|Cert_b\|Re_a\|Re_b\|PCR_\alpha\|Cert(AIK_{\text{pk},\alpha})\|Re_{AIK,\alpha}\|Re_{INT,\alpha}\|PCR_\beta$

$\|Cert(AIK_{\mathrm{pk},\beta})\|Re_{AIK,\beta}\|Re_{INT,\beta}$，$Re_a$ 和 Re_b 分别为 $Cert_a$ 和 $Cert_b$ 的证书验证结果，$Re_{AIK,\alpha}$ 和 $Re_{AIK,\beta}$ 分别为 $Cert(AIK_{\mathrm{pk},\alpha})$ 和 $Cert(AIK_{\mathrm{pk},\beta})$ 的 AIK 证书验证结果，SML_α 和 SML_β 的正确性分别为 PCR_α 和 PCR_β 所验证，$Re_{INT,\alpha}$ 和 $Re_{INT,\beta}$ 分别为 SML_α 和 SML_β 的平台完整性评估结果，σ_α 为 α 的 AIK 签名且 $\sigma_\alpha=[H_{\mathrm{MAC}}(BK,N_{AP}),PCR_\alpha]_{AIK_{\mathrm{sk},\alpha}}$，$\sigma_\beta$ 为 β 的 AIK 签名且 $\sigma_\beta=[H_{MAC}(BK,N_{STA}),PCR_\beta]_{AIK_{\mathrm{sk},\beta}}$，$\sigma_{\alpha,2}$ 为 α 的 AIK 签名且 $\sigma_{\alpha,2}=[H_{MAC}(MK,N_{AS}),PCR_\alpha]_{AIK_{\mathrm{sk},\alpha}}$，$BK$ 为 STA 和 AP 之间建立的基密钥且 $BK=H_{KD}(xyP,\ N_{STA}\|N_{AP,2})$，$MK\|k_{STA,AS}=H_{KD}(xzP,AIK_{\mathrm{sk},\alpha}$ 和 $AIK_{\mathrm{sk},\beta}$ 分别为 α 和 β 的 AIK 私钥，$MAC_{a,2}$ 为 a 的消息鉴别码且 $MAC_{a,2}=H_{MAC}(MK,N_{AS}\|z\cdot P\|\sigma_{AS,2}\|N_{STA}\|Cert_a\|x\cdot P\|\sigma_{a,2})$，$MAC_{AS}$ 为 AS 的消息鉴别码且 $MAC_{AS}=H_{MAC}(MK,N_{AS}\|z\cdot P\|\sigma_{AS,2}\|N_{STA}\|Cert_a\|x\cdot P\|\sigma_{a,2}\|MAC_{a,2}\|N_{AP}\|y\cdot P\|Res_{AS}\|\sigma_{AS})$，$\sigma_a$ 为 a 的签名且 $\sigma_a=[N_{AP}\|N_{STA}\|x\cdot P\|ID_{AP}\|Cert_a\|ECDH_{\mathrm{params}}\|ID_{AS}\|\sigma_{a,2}\|MAC_{a,2}\|y\cdot P\|PCR_\alpha\|\{SML_\alpha\}_{k_{STA,AS}}\|Cert(AIK_{\mathrm{pk},\alpha})\|\sigma_\alpha\|\sigma_{\alpha,2}]_{sk_a}$，$\sigma_b$ 为 b 的签名且 $\sigma_b=[N_{STA}\|N_{AP,2}\|Re_{\mathrm{access}}\|x\cdot P\|y\cdot P\|ID_b\|ID_a\|Res_{AS}\|\sigma_{AS}\|MAC_{AS}\|PCR_\beta\|Cert(AIK_{\mathrm{pk},\beta})\|\sigma_\beta]_{sk_b}$，$sk_b$ 为 b 的私钥。MAC_a 为 a 的消息鉴别码且 $MAC_a=H_{MAC}(BK,N_{AP}\|N_{STA}\|x\cdot P\|ID_{AP}\|Cert_a\|ECDH_{\mathrm{params}}\|ID_{AS}\|\sigma_{a,2}\|MAC_{a,2}\|y\cdot P\|PCR_\alpha\|\{SML_\alpha\}_{k_{STA,AS}}\|Cert(AIK_{\mathrm{pk},\alpha})\|\sigma_\alpha\|\sigma_{\alpha,2}\|\sigma_a)$。$MAC_b$ 为 b 的消息鉴别码且 $MAC_b=H_{MAC}(BK,N_{STA}\|N_{AP,2}\|Re_{\mathrm{access}}\|x\cdot P\|y\cdot P\|ID_b\|ID_a\|Res_{AS}\|\sigma_{AS}\|MAC_{AS}\|PCR_\beta\|Cert(AIK_{pk,\beta})\|\sigma_\beta\|\sigma_b)$。

相对于上述证书鉴别过程′和证书鉴别过程″中带单下划线的消息和字段是新增加的，而带双下划线的字段做了相应的扩展，目的是在 BK 的建立过程中引入了 STA 和 AP 之间的双向平台认证，以及在 MK 的建立过程中引入了 AS 对 STA 的平台认证，从而确保 BK 和 MK 的建立过程没有受到各个平台的恶意攻击。此外，对 STA 的平台认证，可以有效地防止病毒、木马等通过 STA 的平台带入 WLAN Mesh 网络。值得注意的是：STA 和 AS 在导出 MK 时还导出了它们之间的平台配置保护密钥 $k_{STA,AS}$，用于保护平台认证过程中的 SML。由于证书鉴别过程″只是新增加了一些消息和字段，以及扩展了一些字段，所以它与证书鉴别过程′向后兼容，从而也与第 3 版 WAI 协议中的证书鉴别过程向后兼容。

4 安全性分析

由于第 3 版 WAI 协议已经被证明是安全的[11,12]，所以对基于改进 WAI 协议的 WLAN Mesh 安全关联方案和可信计算环境下的 WLAN Mesh 安全关联方案的安全性分析主要是对 2 个方案中的证书鉴别过程′和证书鉴别过程″进行安全性分析。下面利用利用串空间模型[13~15]来分析这 2 个方案中的证书鉴别过程′和证书鉴别过程″的安全性。

4.1 证书鉴别过程′的安全性分析

定义 1 证书鉴别过程′的串空间是以下 4 类串的并集：1)发起者串 $s\in\mathrm{Init}[STA,AP,AS,\ N_{STA},\ N_{AP},\ N_{AP,2},\ N_{AS},x\cdot P,y\cdot P,z\cdot P,Cert_{STA},Cert_{AP},\ Re_{STA},\ Re_{AP},\ ECDH_{\mathrm{params}},Re_{\mathrm{access}}]$，迹为 $<+m_1,-m_2,+m_3,-m_4,\ +m_5,\ -m_6,+m_7>$，与这类串相关联的主体为 AP；2) 响应者串 $s\in\mathrm{Resp}[STA,AP,AS,N_{STA},N_{AP},N_{AP,2},\ N_{AS},\ x\cdot P,y\cdot P,z\cdot P,Cert_{STA},Cert_{AP},Re_{STA},Re_{AP},\ ECDH_{\mathrm{params}},\ Re_{\mathrm{access}}]$，迹为 $<-m_3,+m_4,-m_7>$，与类串相关联的主体为 STA；3) 服务者串 $s\in\mathrm{Serv}[STA,\ AP,AS,\ N_{STA},N_{AP},N_{AP,2},N_{AS},x\cdot P,y\cdot P,z\cdot P,Cert_{STA},\ Cert_{AP},\ Re_{STA},Re_{AP},ECDH_{\mathrm{params}}]$；4) 入侵者串 $s\in P$。m_1，m_2，m_3，m_4，m_5，m_6 和 m_7 分别为证书鉴别过程′中 7 个步骤中所发送的消息。

定理 1 假设如下。1) $\sum$ 为证书鉴别过程′的串空间，C 为 $\sum$ 中含有一个发起者串 s 的丛，发起者串 s 的迹为：$s\in\mathrm{Init}[STA,AP,AS,N_{STA},N_{AP},N_{AP,2},\ N_{AS},\ x\cdot P,\ y\cdot P,z\cdot P,Cert_{STA},Cert_{AP},Re_{STA},Re_{AP},\ ECDH_{\mathrm{params}},\ Re_{\mathrm{access}}]$。2) $sk_{STA},\ sk_{AP},sk_{AS}\notin K_P$。3) $x\cdot P$、$y\cdot P$ 和 $z\cdot P$ 唯一产生于 $\sum$ 中，且 $x\cdot P\neq y\cdot P\neq z\cdot P$。那么 C 中存在一个响应者串 $t\in\mathrm{Resp}[STA,AP,\ AS,\ N_{STA},N_{AP},N_{AP,2},\ N_{AS},x\cdot P,y\cdot P,z\cdot P,Cert_{STA},\ Cert_{AP},\ Re_{STA},Re_{AP},\ ECDH_{\mathrm{params}},Re_{\mathrm{access}}]$ 和一个服务者串 $r\in\mathrm{Serv}[STA,\ AP,AS,N_{STA},N_{AP},N_{AP,2},N_{AS},x\cdot P,\ y\cdot P,\ z\cdot P,Cert_{STA},\ Cert_{AP},Re_{STA},Re_{AP},ECDH_{\mathrm{params}}]$。

证明 由定义 1、假设 2）和假设 3）可知，$\sigma_{STA}\subset\mathrm{term}(<s,4>)$ 唯一源发于一个响应者串 $t\in\mathrm{Resp}[STA,AP,AS,N_{STA},N_{AP},N_{AP,2}',N_{AS},x\cdot P,y'\cdot P,z\cdot P,Cert_{STA},Cert_{AP},Re_{STA}',Re_{AP}',ECDH_{\mathrm{params}},Re_{\mathrm{access}}']$。

由定义 1、假设 2）和假设 3）可知，$\sigma_{AP} \subset \text{term}(<t,3>)$ 唯一源发于一个发起者串 $s' \in \text{Init}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}', N_{AS}, x \cdot P, y' \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}', Re_{AP}', ECDH_{\text{params}}, Re_{\text{access}}']$。由假设 3）可知，$s' = s$，所以 $N_{AP,2}' = N_{AP,2}$，$y' = y$，$Re_{STA}' = Re_{STA}$，$Re_{AP}' = Re_{AP}$ 和 $Re_{\text{access}}' = Re_{\text{access}}$。

由定义 1、假设 2）和假设 3）可知，$\sigma_{AS,2} \subset \text{term}(<t,1>)$ 唯一源发于一个服务者串 r，从而根据假设 3）可知，$z \cdot P$ 唯一产生于 $<r,2>$。由定义 1 和假设 3）可知，$x \cdot P$ 唯一产生于 $<t,2>$。因为定义 1 所述的证书鉴别过程′满足沉默性(silent)和保守性(conservative)，所以 $x \cdot z \cdot P$ 不源发于 C 中(文献[14]中的定理 9)，从而 $MK \notin K_P$，使得 $MAC_{AS} \subset \text{term}(<t,3>)$ 唯一源发于服务者串 $r \in \text{Serv}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}]$。

定理 2　假设如下。1) $\sum$ 为证书鉴别过程′的串空间，C 为 $\sum$ 中含有一个响应者串 s 的丛，响应者串 s 的迹为 $s \in \text{Resp}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}, Re_{\text{access}}]$。2) $sk_{AP}, sk_{AS} \notin K_P$。3) $x \cdot P$、$y \cdot P$ 和 $z \cdot P$ 唯一产生于 $\sum$ 中，且 $x \cdot P \neq y \cdot P \neq z \cdot P$。那么 C 中存在一个发起者串 $t \in \text{Init}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}, Re_{\text{access}}]$ 和一个服务者串 $r \in \text{Serv}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}]$。

证明　由定义 1、假设 2）和假设 3）可知，$\sigma_{AP} \subset \text{term}(<s,3>)$ 唯一源发于一个发起者串 $t \in \text{Init}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}, Re_{\text{access}}]$。由于 C 中包含一个发起者串 t，所以 C 中包含一个服务者串 $r \in \text{Serv}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}]$，与定理 1 的证明同理。

定理 3　假设如下。1)$\sum$ 为证书鉴别过程′的串空间，C 为 $\sum$ 中含有一个服务者串 s 的丛，服务者串 s 的迹为 $s \in \text{Serv}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}]$。2) $sk_{STA}, sk_{AP}, sk_{AS} \notin K_P$。3) $x \cdot P$、$y \cdot P$ 和 $z \cdot P$ 唯一产生于 $\sum$ 中，且 $x \cdot P \neq y \cdot P \neq z \cdot P$。那么 C 中存在一个发起者串 $r \in \text{Init}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}, Re_{\text{access}}]$ 和一个响应者串 $t \in \text{Resp}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}, Re_{\text{access}}]$。

证明　由定义 1、假设 2）和假设 3）可知，$\sigma_{STA,2} \subset \text{term}(<s,3>)$ 唯一源发于一个响应者串 t，从而由假设 3）可知，$x \cdot P$ 唯一产生于 $<t,2>$。由假设 1）和假设 3）可知，$z \cdot P$ 唯一产生于 $<s,2>$。因为定义 1 所述的证书鉴别过程′满足沉默性和保守性，所以 $x \cdot z \cdot P$ 不源发于 C 中(文献[14]中的定理 9)，从而 $MK \notin K_P$，使得 $MAC_{STA} \subset \text{term}(<s,3>)$ 唯一源发于响应者 $t \in \text{Resp}[STA, AP, AS, N_{STA}, N'_{AP}, N'_{AP,2}, N_{AS}, x \cdot P, y' \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re'_{STA}, Re'_{AP}, ECDH_{\text{params}}, Re'_{\text{access}}]$。同理，$MAC_{AS} \subset \text{term}(<t,3>)$ 唯一源发于一个服务者串 $s' \in \text{Serv}[STA, AP, AS, N_{STA}, N_{AP}', N_{AP,2}', N_{AS}, x \cdot P, y' \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}', Re_{AP}', ECDH_{\text{params}}]$。由假设 3）可知，$s' = s$，所以 $N_{AP}' = N_{AP}$，$N_{AP,2}' = N_{AP,2}$，$y' = y$，$Re_{STA}' = Re_{STA}$ 和 $Re_{AP}' = Re_{AP}$，进而由定义 1 可知，$Re_{\text{access}}' = Re_{\text{access}}$。由于 C 中包含一个响应者串 t，所以 C 中包含一个发起者串 $r \in \text{Init}[STA, AP, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x \cdot P, y \cdot P, z \cdot P, Cert_{STA}, Cert_{AP}, Re_{STA}, Re_{AP}, ECDH_{\text{params}}, Re_{\text{access}}]$，与定理 2 的证明同理。

由定理 1、假设 2）和假设 3）可知，证书鉴别过程′是安全的，使得：1) *STA* 和 *AP* 实现了它们之间的双向认证，并建立了它们之间的基密钥 *BK*，其中它们实现了对 *AS* 的认证并从 *AS* 获得了对对方的证书验证结果；2) *STA* 和 *AS* 实现了它们之间的双向认证，并建立了它们之间的主密钥 *MK*。

4.2　证书鉴别过程″的安全性分析

由于证书鉴别过程″引入了平台认证，所以需要利用文献[15]中所述的针对于可信网络接入协议的串空间模型来分析证书鉴别过程″的安全性。为了分析可信网络接入协议的安全性，文献[15]引入了双身份协议主体、内部攻击者和外部攻击者的定义，并给出了针对于平台认证的定理。双身份协议主体是指具有 2 个可认证身份的协议主体。内部攻

击者是指在一轮协议中进行内部攻击的合法协议主体，它是因双身份协议主体而存在的，其密钥集用 K_{ip} 表示。外部攻击者是指除内部攻击者以外的攻击者，其密钥集用 K_{ep} 表示。针对于平台认证的定理是指：对于一个平台的完整性报告[16]，如果该完整性报告显示该平台是可信赖的，那么该完整性报告必然源发于一个常规者串。下面利用这些定义和定理对证书鉴别过程″进行安全性分析。

定义 2 证书鉴别过程″的串空间是以下 4 类串的并集：1) 发起者串 $s\in \mathrm{Init}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\mathrm{params}}, Re_{\mathrm{access}}, Cert(AIK_{\mathrm{pk},\alpha}), Cert(AIK_{\mathrm{pk},\beta}), Re_{\mathrm{AIK},\alpha}, Re_{\mathrm{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\mathrm{INT},\alpha}, Re_{\mathrm{INT},\beta}]$，迹为 $<+m_1,-m_2,+m_3,-m_4,+m_5,-m_6,+m_7>$，与这类串相关联的主体为 AP，它是一个双身份协议主体，用 $b\cdot\beta$ 表示，前者表示 AP 的用户，后者表示 AP 的平台；2) 响应者串 $s\in \mathrm{Resp}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\mathrm{params}}, Re_{\mathrm{access}}, Cert(AIK_{\mathrm{pk},\alpha}), Cert(AIK_{\mathrm{pk},\beta}), Re_{\mathrm{AIK},\alpha}, Re_{\mathrm{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\mathrm{INT},\alpha}, Re_{\mathrm{INT},\beta}]$，迹为 $<-m_3,+m_4,-m_7>$，与类串相关联的主体为 STA，它是一个双身份协议主体，用 $a\cdot\alpha$ 表示，前者表示 STA 的用户，后者表示 STA 的平台；3) 服务者串 $s\in \mathrm{Serv}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\mathrm{params}}, Cert(AIK_{\mathrm{pk},\alpha}), Cert(AIK_{\mathrm{pk},\beta}), Re_{\mathrm{AIK},\alpha}, Re_{\mathrm{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\mathrm{INT},\alpha}, Re_{\mathrm{INT},\beta}]$；4) 入侵者串 $s\in P$。m_1，m_2，m_3，m_4，m_5，m_6 和 m_7 分别为证书鉴别过程″中 7 个步骤中所发送的消息。SML_α 显示 α 是可信赖的，而 SML_β 显示 β 是可信赖的。

定理 4 假设如下。1) $\sum$ 为证书鉴别过程″的串空间，C 为 $\sum$ 中含有一个发起者串 s 的丛，发起者串 s 的迹为 $s\in \mathrm{Init}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\mathrm{params}}, Re_{\mathrm{access}}, Cert(AIK_{\mathrm{pk},\alpha}), Cert(AIK_{\mathrm{pk},\beta}), Re_{\mathrm{AIK},\alpha}, Re_{\mathrm{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\mathrm{INT},\alpha}, Re_{\mathrm{INT},\beta}]$。2) $sk_a\notin K_{ep}$ 且 $sk_{AS}\notin K_P$。3) $x\cdot P$、$y\cdot P$ 和 $z\cdot P$ 唯一产生于 $\sum$ 中，且 $x\cdot P\neq y\cdot P\neq z\cdot P$。那么 C 中存在一个响应者串 $t\in \mathrm{Resp}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\mathrm{params}}, Re_{\mathrm{access}}, Cert(AIK_{\mathrm{pk},\alpha}), Cert(AIK_{\mathrm{pk},\beta}), Re_{\mathrm{AIK},\alpha}, Re_{\mathrm{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\mathrm{INT},\alpha}, Re_{\mathrm{INT},\beta}]$ 和一个服务者串 $r\in \mathrm{Serv}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\mathrm{params}}, Cert(AIK_{\mathrm{pk},\alpha}), Cert(AIK_{\mathrm{pk},\beta}), Re_{\mathrm{AIK},\alpha}, Re_{\mathrm{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\mathrm{INT},\alpha}, Re_{\mathrm{INT},\beta}]$。

证明 1) 如果 $sk_a\notin K_{ip}$，那么由假设 2）可知，$sk_a\notin K_P$。由定义 2 和假设 3）可知，$\sigma_a\subset \mathrm{term}(<s, 4>)$ 唯一源发于一个响应者串 t，从而根据假设 3）可知：$x\cdot P$ 唯一产生于 $<t,2>$。由假设 1）和假设 3）可知，$y\cdot P$ 唯一产生于 $<s,3>$。因为定义 2 所述证书鉴别过程″满足沉默性和保守性，所以 $x\cdot y\cdot P$ 不源发于 C 中(文献[14]中的定理 9)，从而 $BK\notin K_P$，使得 $MAC_a\subset \mathrm{term}(<s,3>)$ 源发于响应者串 $t\in \mathrm{Resp}[a\cdot\alpha, b\cdot\beta', AS, N_{STA}, N_{AP}, N_{AP,2}', N_{AS}, x\cdot P, y'\cdot P, z\cdot P, Cert_a, Cert_b, Re_a', Re_b', ECDH_{\mathrm{params}}, Re_{\mathrm{access}}', Cert(AIK_{\mathrm{pk},\alpha}), Cert(AIK_{\mathrm{pk},\beta})', Re_{\mathrm{AIK},\alpha}', Re_{\mathrm{AIK},\beta}', PCR_\alpha, PCR_\beta', SML_\alpha, SML_\beta', Re_{\mathrm{INT},\alpha}', Re_{\mathrm{INT},\beta}']$。同理，$MAC_b\subset \mathrm{term}(<t,3>)$ 唯一源发于一个发起者串 $s'\in \mathrm{Init}[a\cdot\alpha, b\cdot\beta', AS, N_{STA}, N_{AP}, N_{AP,2}', N_{AS}, x\cdot P, y'\cdot P, z\cdot P, Cert_a, Cert_b, Re_a', Re_b', ECDH_{\mathrm{params}}, Re_{\mathrm{access}}', Cert(AIK_{\mathrm{pk},\alpha}), Cert(AIK_{\mathrm{pk},\beta})', Re_{\mathrm{AIK},\alpha}', Re_{\mathrm{AIK},\beta}', PCR_\alpha, PCR_\beta', SML_\alpha, SML_\beta', Re_{\mathrm{INT},\alpha}', Re_{\mathrm{INT},\beta}']$。由假设 3）可知，$s'=s$，所以 $\beta'=\beta$，$N_{AP,2}'=N_{AP,2}$，$y'=y$，$Re_{STA}'=Re_{STA}$，$Re_{AP}'=Re_{AP}$，$Re_{\mathrm{access}}'=Re_{\mathrm{access}}$，$Cert(AIK_{\mathrm{pk},\beta})'=Cert(AIK_{\mathrm{pk},\beta})$，$Re_{\mathrm{AIK},\alpha}'=Re_{\mathrm{AIK},\alpha}$，$Re_{\mathrm{AIK},\beta}'=Re_{\mathrm{AIK},\beta}$，$PCR_\beta'=PCR_\beta$，$SML_\beta'=SML_\beta$，$Re_{\mathrm{INT},\alpha}'=Re_{\mathrm{INT},\alpha}$ 和 $Re_{\mathrm{INT},\beta}'=Re_{\mathrm{INT},\beta}$。2) 如果 $sk_a\in K_{ip}$，那么由定义 2 和假设 3）可知，$\sigma_\alpha\subset term(<s,4>)$ 唯一源发于一个响应者串 t'（文献[15]中的定理 1)，从而 $x\cdot P$ 唯一产生于 $<t',2>$。由假设 1）和假设 3）可知，$y\cdot P$ 唯一产生于 $<s,3>$。因为定义 2 所述的证书鉴别过程″满足沉默性和保守性，所以 $x\cdot y\cdot P$ 不源发于 C 中(文献[14]中的定理 9)，从而 $BK\notin K_P$。因此，由 1)的证明可知，$t'=t$。

由定义 2、假设 2）和假设 3）可知，$\sigma_{AS,2}\subset \mathrm{term}(<t,1>)$ 唯一源发于一个服务者串 r，从而根据假设 3）可知，$z\cdot P$ 唯一产生于 $<r,2>$。因为定义 2 所述的证书鉴别过程″满足沉默性和保守性，所以 $x\cdot z\cdot P$ 不源发于 C 中(文献[14]中的定理 9)，从而

$MK \notin K_P$，使得 $MAC_{AS} \subset \text{term}(<t,3>)$ 唯一源发于服务者串 $r \in \text{Serv}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$。

定理 5　假设如下。1)$\sum$ 为证书鉴别过程″的串空间，C 为 $\sum$ 中含有一个响应者串 s 的丛，响应者串 s 的迹为 $s \in \text{Resp}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Re_{\text{access}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$。2) $sk_b \notin K_{ep}$ 且 $sk_{AS} \notin K_P$。3) $x\cdot P$、$y\cdot P$ 和 $z\cdot P$ 唯一产生于 $\sum$ 中，且 $x\cdot P \neq y\cdot P \neq z\cdot P$。那么 C 中存在一个发起者串 $t \in \text{Init}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Re_{\text{access}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$ 和一个服务者串 $r \in \text{Serv}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$。

证明　1) 如果 $sk_b \notin K_{ip}$，那么由假设 2）可知，$sk_b \notin K_P$。由定义 2 和假设 3）可知，$\sigma_{AP} \subset \text{term}(<s, 3>)$ 源发于一个发起者串 $t \in \text{Init}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Re_{\text{access}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$。2)如果 $sk_b \in K_{ip}$，那么由定义 2 和假设 3）可知，$\sigma_\beta \subset \text{term}(<s,3>)$ 唯一源发于一个发起串 t'（文献[15]中的定理 1），从而 $y\cdot P$ 唯一产生于 $<t',3>$。由假设 1）和假设 3）可知，$x\cdot P$ 唯一产生于 $<s,2>$。因为定义 2 所述的证书鉴别过程″满足沉默性和保守性，所以 $x\cdot y\cdot P$ 不源发于 C 中(文献[14]中的定理 9)，从而 $BK \notin K_P$，使得 $MAC_b \subset \text{term}(<s, 3>)$ 源发于发起者串 $t' = t \in \text{Init}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Re_{\text{access}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$。

由于 C 中包含一个发起者串 t，所以 C 中包含一个服务者串 $r \in \text{Serv}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$，与定理 4 的证明同理。

定理 6　假设如下。1) $\sum$ 为证书鉴别过程″的串空间，C 为 $\sum$ 中含有一个服务者串 s 的丛，服务者串 s 的迹为：$s \in \text{Serv}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Cert(AIK_{\text{pk},\alpha}), Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$。2) $sk_a \notin K_{ep}$ 且 $sk_b \notin K_{ep}$。3) $x\cdot P$、$y\cdot P$ 和 $z\cdot P$ 唯一产生于 $\sum$ 中，且 $x\cdot P \neq y\cdot P \neq z\cdot P$。那么 C 中存在一个发起者串 $t \in \text{Init}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Re_{\text{access}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$ 和一个响应者串 $r \in \text{Resp}[a\cdot\alpha, b\cdot\beta, AS, N_{STA}, N_{AP}, N_{AP,2}, N_{AS}, x\cdot P, y\cdot P, z\cdot P, Cert_a, Cert_b, Re_a, Re_b, ECDH_{\text{params}}, Re_{\text{access}}, Cert(AIK_{\text{pk},\alpha}), Cert(AIK_{\text{pk},\beta}), Re_{\text{AIK},\alpha}, Re_{\text{AIK},\beta}, PCR_\alpha, PCR_\beta, SML_\alpha, SML_\beta, Re_{\text{INT},\alpha}, Re_{\text{INT},\beta}]$。

证明　1) 如果 $sk_a \notin K_{ip}$，那么由假设 2）可知，$sk_a \notin K_P$。由定义 2 和假设 3）可知，$\sigma_{a,2} \subset \text{term}(<s, 3>)$ 唯一源发于一个响应者串 r，从而根据假设 3）可知，$x\cdot P$ 唯一产生于 $<r,2>$。由假设 1）和假设 3）可知，$z\cdot P$ 唯一产生于 $<s,2>$。因为定义 2 所述的证书鉴别过程″满足沉默性和保守性，所以 $x\cdot z\cdot P$ 不源发于 C 中(文献[14]中的定理 9)，从而 $MK \notin K_P$，使得 $MAC_{a,2} \subset \text{term}(<s,3>)$ 源发于响应者串 $r \in \text{Resp}[a\cdot\alpha', b\cdot\beta', AS, N_{STA}, N_{AP}', N_{AP,2}', N_{AS}, x\cdot P, y'\cdot P, z\cdot P, Cert_a, Cert_b, Re_a', Re_b', ECDH_{\text{params}}, Re_{\text{access}}', Cert(AIK_{\text{pk},\alpha})', Cert(AIK_{\text{pk},\beta})', Re_{\text{AIK},\alpha}', Re_{\text{AIK},\beta}', PCR_\alpha', PCR_\beta', SML_\alpha', SML_\beta', Re_{\text{INT},\alpha}', Re_{\text{INT},\beta}']$。同理，$MAC_{AS} \subset term(<r,3>)$ 唯一源发于一个服务者串 $s' \in \text{Serv}[a\cdot\alpha', b\cdot\beta', AS, N_{STA}, N_{AP}', N_{AP,2}', N_{AS}, x\cdot P, y'\cdot P, z\cdot P, Cert_a, Cert_b, Re_a', Re_b', ECDH_{\text{params}}, Cert(AIK_{\text{pk},\alpha})', Cert(AIK_{\text{pk},\beta})', Re_{\text{AIK},\alpha}', Re_{\text{AIK},\beta}', PCR_\alpha', PCR_\beta', SML_\alpha', SML_\beta', Re_{\text{INT},\alpha}', Re_{\text{INT},\beta}']$。由假设 3）可知，$s' = s$，所以 $N_{AP}' = N_{AP}$，$N_{AP,2}' = N_{AP,2}$，$y' = y$，$Re_a' = Re_a$，$Re_b' = Re_b$，$\alpha' = \alpha$，$\beta' = \beta$，

$Cert(AIK_{\mathrm{pk},\alpha})'=Cert(AIK_{\mathrm{pk},\alpha})$，$Re_{\mathrm{AIK},\alpha}'=Re_{\mathrm{AIK},\alpha}$，$Cert(AIK_{\mathrm{pk},\beta})'=Cert(AIK_{\mathrm{pk},\beta})$，$Re_{\mathrm{AIK},\beta}'=Re_{\mathrm{AIK},\beta}$，$PCR_\alpha'=PCR_\alpha$，$PCR_\beta'=PCR_\beta$，$SML_\alpha'=SML_\alpha$，$SML_\beta'=SML_\beta$，$Re_{\mathrm{INT},\alpha}'=Re_{\mathrm{INT},\alpha}$ 和 $Re_{\mathrm{INT},\beta}'=Re_{\mathrm{INT},\beta}$，进而由定义 2 可知，$Re_{\mathrm{access}}'=Re_{\mathrm{access}}$。2) 如果 $sk_a\in K_{ip}$，那么由定义 2 和假设 3）可知，$\sigma_{\alpha,2}\subset \mathrm{term}(<s,4>)$ 唯一源发于一个响应者串 r' (文献[15]中的定理 1)，从而 $x\cdot P$ 唯一产生于 $<r',2>$。由假设 1）和假设 3）可知，$z\cdot P$ 唯一产生于 $<s,2>$。因为定义 2 所述的证书鉴别过程″满足沉默性和保守性，所以 $x\cdot z\cdot P$ 不源发于 C 中(文献[14]中的定理 9)，从而 $MK\notin K_P$。因此，由 1) 的证明可知，$r'=r$。

由于 C 中包含一个响应者串 r，所以 C 中包含一个发起者串 $t\in \mathrm{Init}[a\cdot\alpha,b\cdot\beta,AS,N_{STA},N_{AP},N_{AP,2},N_{AS},x\cdot P,y\cdot P,z\cdot P,Cert_a,Cert_b,Re_a,Re_b,ECDH_{\mathrm{params}},Re_{\mathrm{access}},Cert(AIK_{\mathrm{pk},\alpha}),Cert(AIK_{\mathrm{pk},\beta}),Re_{\mathrm{AIK},\alpha},Re_{\mathrm{AIK},\beta},PCR_\alpha,PCR_\beta,SML_\alpha,SML_\beta,Re_{\mathrm{INT},\alpha},Re_{\mathrm{INT},\beta}]$，与定理 5 的证明同理。

由定理 4~定理 6 可知，证书鉴别过程″可以抵抗内部攻击者和外部攻击者的攻击，它是安全的，使得 1) *STA* 和 *AP* 实现了它们之间的双向用户认证和平台认证，并建立了它们之间的基密钥 *BK*，其中它们实现了对 *AS* 的认证并从 *AS* 获得了对对方的用户证书验证结果、AIK 证书验证结果和平台完整性评估结果；2) *STA* 和 *AS* 实现了它们之间的双向用户认证，以及 *AS* 对 *STA* 的平台认证，并建立了它们之间的主密钥 *MK* 和平台配置保护密钥 $k_{STA,AS}$。

5 结束语

通过对第 3 版 WAI 协议的改进，本文提出了一种基于改进 WAI 协议的 WLAN Mesh 安全关联方案。然后，在该方案的基础上，通过对第 3 版 WAI 协议的进一步改进，本文提出了一种可信计算环境下的 WLAN Mesh 安全关联方案，它能实现 WLAN Mesh 可信接入认证，从而增强了 WLAN Mesh 的安全性。通过性能对比分析，基于改进 WAI 协议的 WLAN Mesh 安全关联方案在通信效率和计算量上都具有明显的优势，从而提高了 WLAN Mesh 安全关联的性能，特别是降低了 AS 的负载，有效地解决了第 3 版 WAI 协议用于建立 WLAN Mesh 安全关联时所存在的问题。最后，利用串空间模型证明了这 2 个 WLAN Mesh 安全关联方案是安全的。

参考文献：

[1] IEEE Supplement to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security[S]. IEEE 802.11i, 2004.

[2] IEEE Draft Amendment to Standard for Information Technology –Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment to ESS Mesh Networking[S]. IEEE P802.11s/D1.0, 2007.

[3] Trusted computing group. TCG trusted network connect architecture for interoperability specification version 1.4[EB/OL]. http://www.trustedcomputinggroup.org/.

[4] 马卓，马建峰，曾勇等. 通用可组合安全的 WLAN Mesh 网络可信接入认证协议[J]. 通信学报，2008，29(10):126-134.
MA Z, MA J F, ZHENG Y, *et al*. Universally composable secure trusted access protocol for WLAN Mesh networks[J]. Journal on Communications, 2008, 29(10):126-134.

[5] MA Z, MA J F, SHEN Y L. Provably secure trusted access protocol for WLAN Mesh networks[A]. 2008 IEEE 5th International Conference on Embedded and Ubiquitous Computing[C]. Shanghai, China, 2008.43-48.

[6] MA Z, MA J F, SHEN Y L. An efficient authentication protocol for WLAN Mesh networks in trusted environment[J]. IEICE Transactions on Information and Systems, 2010, E93-D(3): 430-437.

[7] 中华人民共和国国家标准. GB 15629.11-2003（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）[S]. 北京：中国标准出版社，2003.
National Standard of the People's Republic of China. GB 15629.11-2003(Information Technology - Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications)[S]. Beijing: Chinese Standard Publishing House, 2003.

[8] 中国宽带无线 IP 标准工作组. GB 15629.11-2003（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）和 GB 15629.1102-2003（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：2.4 GHz 频段较高速物理层扩展规范）实施指南[EB/OL]. http://www. chinabwips.org/.
China broadband wireless ip standard group. Guide for GB 15629.11-2003(information technology-telecommunications and information exchange between systems - LAN/MAN specific requirements - part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications) and GB 15629.1102-2003 (information technology - telecommunications and information exchange between systems - LAN/MAN specific requirements - part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher-speed physical layer extension in the 2.4 GHz band) [EB/OL]. http://www.chinabwips.org/.

[9] 中华人民共和国国家标准. GB 15629.11-2003/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）[S]. 北京：中国标准出版社，2006.
National Standard of the People's Republic of China. GB 15629.11-2003/XG1-2006(Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 1)[S]. Beijing: Chinese Standard Publishing House, 2006.

[10] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications[S]. IEEE 802.11, 1999.

[11] TANG Q. On the security of three versions of the WAI protocol in Chinese WLAN implementation plan[A]. CHINACOM'07 Proceedings of the Second International Conference on Communications and Networking in China, 2007 Conference[C]. Shanghai, China, 2007.333-339.

[12] 铁满霞, 李建东, 王育民. WAPI 密钥管理协议的 PCL 证明[J]. 电子与信息学报, 2009, 31(2):444-447.
TIE M X, LI J D, WANG Y M. A correctness proof of WAPI key management protocol based on PCL[J]. Journal of Electronics & Information Technology, 2009, 31(2):444-447.

[13] FABREGA F J T, HERZOG J C, GUTTMAN J D. Strand spaces: proving security protocols correct[J]. Journal of Computer Security, 1999, 7(2/3):191-230.

[14] HERZOG J C. The Diffie-Hellman key-agreement scheme in the strand space model[A]. 2003 IEEE 16th IEEE Computer Security Foundations Workshop[C]. Pacific Grove, USA, 2003.234-247.

[15] XIAO Y L, WANG Y M, PANG L J. Verification of trusted network access protocols in the strand space model[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A(3): 665-668.

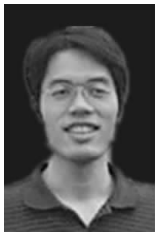
[16] SAILER R, ZHANG X L, JAEGER T, *et al*. Design and implementation of a TCG-based integrity measurement architecture[A]. 2004 ACM 13th USENIX Security Symposium[C]. California, USA, 2004.223-238.

作者简介：

肖跃雷（1979-），男，江西吉安人，博士，西安邮电大学讲师，主要研究方向为可信计算、安全协议分析与设计、无线网络安全等。

王育民（1936-），男，北京人，博士，西安电子科技大学教授，主要研究方向为信息论、编码学、密码学等。

庞辽军（1978-），男，陕西渭南人，博士，西安电子科技大学教授，主要研究方向为密码学、生物特征加密、网络与信息安全等。



谭示崇（1979-），男，广西贵港人，博士，西安电子科技大学副教授，主要研究方向为安全协议分析与设计等。