通用可组合安全的 Mesh 网络认证协议

杨 超，曹春杰，马建峰
(西安电子科技大学 计算机学院，陕西 西安 710071)

摘要：无线 Mesh 网络的现有认证协议不支持双向 802.1X 的认证端口开放. 基于密钥交换协议交换，利用“通用可组合”安全模型的组合特性与信任传递技术，在应答消息中安全结合反向认证信息，实现了满足 Mesh 网络双向认证需求的认证协议，不仅具有可证明的安全性，且通信开销较原协议降低 60%以上.

关键词：Mesh 网络；通用可组合；认证协议；可证明安全
中图分类号：TP309 **文献标识码**：A **文章编号**：1001-2400(2007)05-0814-04

Universally composable secure authentication protocol for wireless mesh networks

YANG Chao, *CAO Chun-jie*, *MA Jian-feng*
(School of Computer, Xidian Univ., Xi'an 710071, China)

Abstract: The authentication protocol of Wireless Mesh Networks does not support 802.1X-based mutual authentication. Based on Diffie-Hellman (DH) exchange and making use of the combination characteristic of the Universally Composable (UC) security model and trust transfer, a new authentication protocol is proposed. Piggybacking opposite direction authentication messages in response, this protocol not only provides two-way authentication for Wireless Mesh Networks but also affords provably UC-security. Furthermore, compared with the original scheme, the communication cost decresses by 60%.

Key Words: mesh networks; UC-security; authentication protocol; provable security

无线网状网[1]通过 802.1X 和四步握手实现认证者(A) 和认证服务器(AS)对申请者(S)的单向认证，但 Mesh 点接入时需要进行两次 802.1X 认证和四步握手密钥协商，极大的降低了协议运行效率. 笔者提出了一种新的 Mesh 网接入点(MP)接入认证协议，只需要 4 轮交互便可实现 S，A 和 AS 3 者之间的相互认证；该协议还可作为一种扩展认证协议(EAP)协议[2]扩展到 802.11i 的 EAP 协议族中，因而不存在兼容性问题. 最后，基于目前一种流行的认证及密钥交换协议的形式化分析方法——“通用可组合安全模型”[3]，对笔者所设计的认证协议进行分析并给出了安全性证明.

1 新的 Mesh 网密钥交换协议

新的 Mesh 网密钥交换协议(MKE)的运算定义在一乘法群 Z_p^* 的子群 G 上，G 的阶为素数 q，g 为 G 的生成元. 假定 A 与 AS 间运行 Radius 协议存在安全信道，S 预存储 AS 的证书，协议进行 4 轮交互完成认证的密钥建立，执行过程如图 1 所示.

(1) Sid 为当前会话标识符，SK_S，SK_{AS} 分别为 S 和 AS 的长期私钥，D_S，D_A，D_{AS} 分别为 S，A 和 AS 的 MAC 地址，g^x，g^y，g^z 分别为 S，A 和 AS 随机选择的临时公钥用于 DH 交换；

(2) SIG_S，SIG_{AS} 别为 S 和 AS 产生的消息签名：SIG_S 为 $\{Sid|D_A|D_{AS}|g^x|g^z\}_{SK_S}$，$SIG_{AS}$ 为 $\{Sid|D_A|D_S|$

收稿日期：2006-12-30
基金项目：国家自然科学基金重大研究计划资助(60633020)；国家自然科学基金资助(60573036)
作者简介：杨 超(1979-)，男，西安电子科技大学博士研究生.

$g^z \mid g^x \mid g^y\}_{SK_{AS}}$;

(3) MIC_S,MIC_{AS} 分别为 S 和 AS 产生的消息认证码:$MIC_{S,1}$ 为 $\{D_S \mid SIG_S\}_{K_{S,AS}}$,$MIC_{S,2}$ 为 $\{D_S \mid D_{AS}\}_{K_{S,A}}$,$MIC_A$ 为 $\{D_A \mid MIC_{AS}\}_{K_{S,A}}$,$MIC_{AS}$ 为 $\{D_{AS} \mid SIG_{AS}\}_{K_{S,AS}}$;

(4) $K_{S,AS}K_{S,A}$ 分别为 S 与 AS,S 与 A 之间产生的共享密钥,其值采用密钥推导函数 prf(·),$K_{S,AS}$ 为 prf(g^{xz},D_S,D_{AS}),$K_{S,A}$ 为 prf(g^{xy},D_S,D_A).

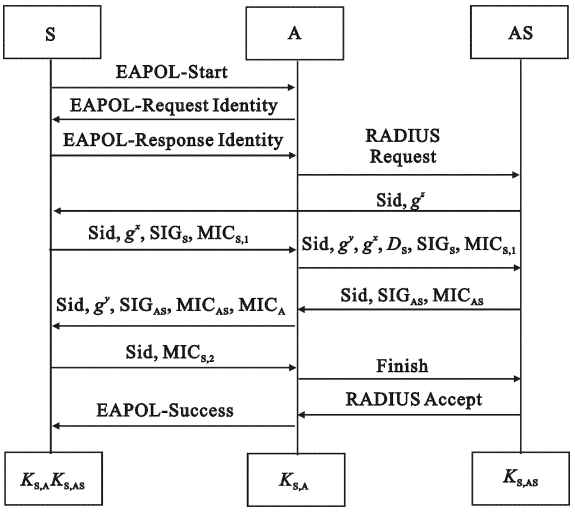

图 1　协议 MKE

2　新协议的安全性证明

Bellare 等人[4]在 1998 年引入了可证明安全理论模块化的设计思想,后来由 Canetti 等人[3,5]进一步扩展,称之为通用可组合安全(UC)模型. 该模型最优秀的性质就是模块组合思想:可以单独设计子协议,只要协议满足 UC 安全,则可以进行组合构造新的 UC 安全协议,并保证协议安全性. 这里采用该安全模型来分析、证明所设计的新协议.

2.1　安全假设

定义 1　判定 DH 问题(DDH)假设　设 p 和 q 为大素数,k 为系统的安全参数. q 的长度为 k 比特且 $q/(p-1)$,g 是群 Z_p^* 上阶为 q 的生成元,x,y 和 z 是从 Z_p 中均匀选择的,则对于任何多项式时间算法 $\mathcal{D}$,$Q_0 = \{\langle p,q,g,g^x,g^y,g^{xy}\rangle : x,y \xleftarrow{R} Z_q\}$ 和 $Q_1 = \{\langle p,q,g,g^x,g^y,g^z\rangle : x,y,z \xleftarrow{R} Z_q\}$ 的概率分布是计算不可区分的.

2.2　协议的安全性证明

把新协议 π 拆分成两个子协议 π_1 与 π_2,主要证明 π_1 的安全性,π_2 的证明同理;最后说明 π_1 结合 π_2 与 π 等价.

首先构造实现理想函数 F_{sig} 的协议 ρ_s:

协议参与者 P_i 与 P_j,运行基于签名算法 S 为(gen,sig,ver)的协议 ρ_s,进行交互.

(1) P_i 收到输入(signer,sid)后执行算法 gen,保留的签名密钥 s,将验证密钥 v 发送给 P_j.

(2) 当 P_j 需要对某消息 m 进行签名,则将(sign,sid,m) 发送给 P_i:P_i 令 $\sigma = \mathrm{sig}(s,m)$. 并将(signature,sid,$m$,$\sigma$) 发送给 P_j.

(3) 当 P_j 需要对某消息 m 签名进行验证,则将(verify,sid,m,σ) 发送给 P_i:P_i 则输出(verified,sid,m,ver(v,m,σ)) 给 P_j.

引理 1　令 S 为(gen,sig,ver)是文献[6]描述的签名,那么协议 ρ_s 对于静态的攻击者,在真实环境下,可以安全实现 F_{sig},当且仅当 S 是抗击选择消息存在性伪造[3].

其次,构造实现密钥交换理想函数 F_{KE} 的协议 π_1':

(1) 令 p 和 q 为大素数,k 为安全参数,q 长为 k 比特且 $q/(p-1)$,g 是群 Z_p^* 上阶为 q 的生成元,协议参与者 P_i 与 P_j,在混合模型 F_{sig}-hybrid 中运行协议 π_1',进行交互.

(2) 当协议发起者 P_i 得到输入(P_i,P_j,sid),则发送初始化消息(signer,0,sid) 给 F_{sig};同样,当协议响应者 P_j 得到输入(P_j,P_i,sid),则发送(signer,1,sid) 给 F_{sig}.

(3) P_i 选择一个 $z \xleftarrow{R} Z_q$,并发送(P_i,sid,$\alpha = g^z$) 给 P_j.

(4) 当 P_j 收到(P_i,sid,α),选择一个 $x \xleftarrow{R} Z_q$,令 $\beta = g^x$,并发送(sign,1,sid,(sid,β,α)) 给 F_{sig};F_{sig} 返回签名 σ_j 后,P_j 计算 $k_1 = \mathrm{prf}(\alpha^x,\cdot)$ 及 $\gamma = \mathrm{MIC}_{k1}(\sigma_j)$,并删除 x,同时发送(sid,β,σ_j,γ) 给 P_i.

(5) 当 P_i 收到(sid,β,σ_j,γ),发送(verify,1,sid,P_j,(sid,β,α),σ_j) 给 F_{sig},如果验证通过,则 P_i 计算 $k_1' = \mathrm{prf}(\beta^z,\cdot)$ 进一步验证 $\mathrm{MIC}_{k1}(\sigma_j)$,如果验证也通过,则 P_i 发送(sign,0,sid,(sid,α,β)) 给 F_{sig},F_{sig} 返回

签名 σ_i 后，P_j 计算$\gamma' = \mathrm{MIC}_{k_1'}(\sigma_i)$，发送$(\mathrm{sid},\sigma_i,\gamma')$ 给 P_j. 最后删除 z，本地输出$(\mathrm{sid},P_i,P_j,k_1')$.

(6) 当 P_j 收到$(\mathrm{sid},\sigma_i,\gamma')$，发送$(\mathrm{verify},0,\mathrm{sid},P_j,(\mathrm{sid},\alpha,\beta),\sigma_i)$ 给 F_{sig}，如果验证通过，且 $\mathrm{MIC}_{k_1'}(\sigma_i)$ 的验证也通过，则本地输出$(\mathrm{sid},P_j,P_i,k_1)$.

其中 $\mathrm{prf}(\cdot)$ 为密钥推导函数，$\mathrm{MIC}_k(\cdot)$ 为用密钥 k 产生的消息认证码，其他符号含义同协议 ρ_s.

引理 2 如果 DDH 假设成立，消息认证码 $\mathrm{MIC}_k(\cdot)$ 的认证算法是安全的，则协议 π_1' 在混合模型 F_{sig}-hybrid 下安全实现了 F_{KE}.

证明 构造一个理想环境下的攻击者 S(仿真器)，使得任何环境机 Z 都不能辨别它是与 H 及 π_1' 在 F_{sig}-hybrid 下进行的交互，还是与 S 及 F_{KE} 在 Ideal-life 下进行的交互. 即，对任何环境机 Z，等式 $\mathrm{HYB}^{F_{\mathrm{sig}}}_{\pi_1',H,Z} \approx \mathrm{IDEAL}_{F_{\mathrm{KE}},S,Z}$ 均成立.

(1) 仿真器 S 的构造：S 运行一个模拟的攻击者 H，并按下面的规则进行操作：

① 任何从 Z 的输入均传递给 H，任何 H 的输出将作为 S 的输出使 Z 可以读取；

② 当 S 从 F_{KE} 处收到$(\mathrm{sid},P_i,P_j,\mathrm{role})$，则表明 P_i 发起了密钥交换，那么让 S 仿真出 F_{sig} 及 F_{sig}-hybrid 下与 H 交互的协议 π_1'，并给定同样的输入. 并且，S 让 H 和 P_i 按照 π_1' 的执行规则与 Z 交互；

③ 为了仿真 π_1' 的执行，S 可以激活 F_{sig} 得到相应的签名值 σ；S 也能计算 $k'' = \mathrm{prf}(r'',\cdot)$ 及 $\gamma'' = \mathrm{MAC}_{k''}(\sigma)$，其中 r'' 是 F_{KE} 给 P_i 和 P_j 的密钥输出；

④ 当 π_1' 中的某个 P_i 需要产生本地输出，如果对端 P_j 没有被攻陷，则 S 将 F_{KE} 的输出发送给 P_i；如果 P_j 已被攻陷，F_{KE} 会让 S 决定密钥，而 S 则使用 P_i 前面的输出来确定仿真的 P_i 与 P_j 的本地输出；

⑤ 当 H 执行攻陷 P_i 的操作，S 同样攻陷理想环境下对应的 P_i. 如果 F_{KE} 已经给 P_i 发送了密钥，则 S 将得到该密钥；如果 P_i 和 P_j 均没有产生本地输出，则 S 将其内部状态传递给 H，包括它们的秘密选值；如果 P_i 或 P_j 其中一方已经产生了本地输出，则它们的秘密选值均被擦除，所以 S 直接将本地的输出的密钥传递给 H.

(2) 仿真器 S 的有效性： 假设在仿真器 S 的执行下，存在一个环境机 Z'，成功辨别与 H 及 π_1' 在 F_{sig}-hybrid 下进行交互及与 S 及 F_{KE} 在 Ideal-life 下进行交互的概率不可忽略，即，使$\mathrm{HYB}^{F_{\mathrm{sig}}}_{\pi_1',H,Z} \neq \mathrm{IDEAL}_{F_{\mathrm{KE}},S,Z}$ 成立的概率为$1/2+\varepsilon$，且该值远远大于$1/2$，其中 ε 表示 Z' 的辨别优势. 那么构造一个区分器 D，利用环境机 Z' 的辨别优势，来破解 DDH 假设难题，进而规约到矛盾. 构造的区分器 D 步骤为：

① 选择 $Q \xleftarrow{R} \{Q_0,Q_1\}$ 作为区分器 D 的输入，记为$(p,g,\alpha^*,\beta^*,\gamma^*)$；

② 选择 $\tau \xleftarrow{R} \{1,2,\cdots,l\}$，$l$ 为攻击者所能发起的会话数的上届. 然后，区分器 D 仿真 F_{sig}-hybrid 中协议 π_1 与 H 和 Z 进行交互；

③ 当 H 激活一个参与方建立一个新的会话 $t(t \neq \tau)$ 或者接收一条消息时，D 代表该参与方按照协议 π_1' 在 F_{sig}-hybrid 中进行正常交互；如果 $t=\tau$，则 D 代表 P_i 向 P_j 发送消息$(P_i,\mathrm{sid},\alpha^*)$；当 P_j 收到$(P_i,\mathrm{sid},\alpha^*)$，$D$ 调用 F_{sig} 进行相应计算，发送$(\mathrm{sid},\beta^*,\sigma_j)$ 给 P_i；最终，D 让 P_i 与 P_j 本地输出$(\mathrm{sid},P_i,P_j,\gamma^*)$；

④ 如果 H 攻陷一个参与方，则 D 把该参与方的内部状态返回给 H：如未被攻陷的参与方是会话 t 的参与方之一，则 D 输出$b' \xleftarrow{R} \{0,1\}$，并终止；

⑤ 如果 F_{sig}-hybrid 中的协议 π_1' 运行完后 Z 输出 b，则 D 输出 $b'(b'=b)$ 并终止.

分析区分器 D 的执行，如果其输入$(p,g,\alpha^*,\beta^*,\gamma^*)$ 是从 Q_0 选出的，则 γ^* 是 π_1' 运行后 P_i 与 P_j 输出的真实密钥，这种情况下，环境机 Z' 看到了本地输出，其视角等同于 F_{sig}-hybrid 下 π_1' 与 H 所进行的交互；如果$(p,g,\alpha^*,\beta^*,\gamma^*)$ 是从 Q_1 选出的，则 γ^* 是个随机值，这种情况下环境机 Z' 的视角则等同于理想模型下 S 与 F_{KE} 所进行的交互(理想环境下，F_{KE} 发送给 P_i 与 P_j 的密钥恰好是它自己选出的随机值). 根据区分器的构造原理，D 成功区分 Q_0 与 Q_1 的概率等于环境机 Z' 成功辨别理想和混合两种环境的概率，即，D 能以不可忽略的优势成功区分 Q_0 与 Q_1，而这与 DDH 假设矛盾，所以得证.

引理 3 令 π_1' 为 F_{sig}-hybrid 下的协议，ρ_s 为安全实现 F_{sig} 的协议，那么对于任何攻击者 A 都存在一个攻击者 H，使得对任何环境机 Z 来说，等式$\mathrm{REAL}_{\pi_1'^{\rho_s},A,Z} \approx \mathrm{HYB}^{F_{\mathrm{sig}}}_{\pi_1',H,Z}$ 均成立，即，组合协议 $\pi_1'^{\rho_s}$ 安全仿真了 F_{sig}-hybrid 下的 π_1'[3].

命题 1　真实环境下,组合协议 $\pi_1^{\prime\rho_s}$ 与协议 π_1 等价.

证明　将混合模型 F_{sig}-hybrid 下协议 π_1' 对所有理想函数 $F_{\text{sig(id)}}$ 的访问均替换为对协议 $\rho_{s(\text{id})}$ 的访问,可以得出协议 $\pi_1^{\prime\rho_s}$ 与协议 π_1 等价,得证.

定理 1　真实模型下的协议 π_1 安全实现了理想函数 F_{KE},即,对任何环境机 Z,等式 $\text{REAL}_{\pi_1,A,Z} \approx \text{IDEAL}_{F_{\text{KE}},S,Z}$ 均成立.

证明　由引理 1～3 及命题 1 得证.

命题 2　协议 π 与协议 π_1 与 π_2 的结合等价.

证明　在协议 π_1 的第 2,3 条消息中稍带发送协议 π_2 的第 1,2 条消息,可以得出协议 π_1 与 π_2 的组合与新协议 π 等价,得证.

由定理 1 得知,协议 π_1 是"UC 安全"的(π_2 的证明同理),而"UC 安全"理论中一个特点就是能够确保许多的协议实例在并发执行,以及同任意的协议组合时的安全[3],所以由命题 2 可知协议 π 达到了同样的"UC 安全".

3　新协议 MKE 的分析

表 1 给出了一个新节点接入时需要进行的计算和通信开销. 其中发送和接收一次消息称为一轮交互,E 表示模指数运算,S 表示计算签名,M 表示计算消息认证码 MIC.

表 1　协议性能对比

协议名称	交互轮数	S 的计算量	A 的计算量	AS 的计算量
EAP-TLS+四步握手	14	2E+1S+4M	2E+1S+4M	4E+2S+2M
新的协议 MKE	4	2E+1S+2M	2E+2M	2E+1S+1M

协议计算量　新协议 MKE 中 S 和 A 的计算量都要略少于 EAP-TLS,且 AS 的运算量相对于 EAP-TLS 来说则减少了一半,这对于系统控制者 AS 来说无疑是一个非常大的改善.

协议通信效率　新的 MP 接入时要执行两次"EAP-TLS+四步握手",总共需要 14 轮的协议交互;而新协议只需要 4 轮的交互便可完成相应的功能,这相对于前者具有较大的优势.

4　结 束 语

无线 Mesh 网络的现有认证协议不支持双向 802.1X 的认证端口开放. 笔者基于"通用可组合"的安全模型与 DH 交换,利用组合与信任传递技术设计了一种新的接入认证协议,不仅满足 Mesh 网络对双向认证的特殊需求,而且具有可证明的安全性和必要的安全性质,并且在通信效率和计算开销上优于原协议.

参考文献:

[1] 段宁, 马建峰. 基于 IEEE802.11b 网卡的 WPA 与 WAPI 集成接入方法[J]. 西安电子科技大学学报,2006, 33 (5): 804-808.

[2] Aboba B, Simon D. On the Security of Public Key Protocols[J]. IEEE Trans on Information Theory, 1983, 29(2): 198-208.

[3] Canetti R. Universally Composable Security: a New Paradigm for Cryptographic Protocols[C]//Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science (FOCS). New York: IEEE Press, 2001: 136-145.

[4] Bellare M, Canetti R, Krawczyk H. A Modular Approach to the Design and Analysis of Authentication and Key-exchange Protocols[C]//Proc of the 30th Annual Symp. on the Theory of Computing. New York: ACM Press, 1998: 419-428.

[5] Canetti R, Krawczyk H. Security Analysis of IKE's Signature-based Key-exchange Protocol[C]//LNCS2442. Berlin: Springer-Verlag, 2002: 143-161.

[6] Goldwasser S, Micali S, Rivest R. A Digital Signature Scheme Secure Against Adaptive Chosen-message Attacks[J]. SIAM Journal on Computing, 1998, 17(2): 281-308.

(编辑: 齐淑娟)