协议组合逻辑安全的 WiMAX 无线网络认证协议

冯　涛[①②③]　　张子彬[①]　　马建峰[②]
[①](兰州理工大学计算机与通信学院　兰州　730050)
[②](西安电子科技大学计算机网络与信息安全教育部重点实验室　西安　710071)
[③](福建师范大学网络安全与密码技术重点实验室　福州　350007)

摘　要：国际标准 IEEE 802.16e-2005 中 PKMv2 协议的安全性是 WiMAX 无线网络安全的重要保证。论文基于协议组合逻辑(PCL)分析了 PKMv2 协议中认证协议的安全性，发现 PKMv2 安全认证协议存在交错攻击，在此基础上基于协议演绎系统(PDS)提出了一种新的 WiMAX 无线网络安全认证协议，并使用协议组合逻辑(PCL)给出新协议的模块化正确性和安全性证明，新协议相对于 PKMv2 安全认证协议更加安全，更适应 WiMAX 无线网络复杂的网络应用环境。

关键词：无线网络；认证协议；协议演绎系统；协议组合逻辑；WiMAX
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2010)09-2106-06
DOI: 10.3724/SP.J.1146.2009.01191

Security Authentication Protocol for WiMAX Wireless Network Based on Protocol Composition Logic

Feng Tao[①②③]　　Zhang Zi-bin[①]　　Ma Jian-feng[②]
[①](*School of Computer and Communication*, *Lanzhou University of Technology*, *Lanzhou* 730050, *China*)
[②](*Key Laboratory of Computer Networks and Information Security of Ministry of Education*, *Xidian University*, *Xi'an* 710071, *China*)
[③](*Key Lab of the Network Security and Cryptology*, *Fujian Normal University*, *Fuzhou* 350007, *China*)

Abstract: IEEE 802.16e-2005 standard's PKMv2 protocol is an important secure guarantee for WiMAX (Worldwide Interoperability for Microwave Access) wireless network. In this paper, based on Protocol Composition Logic (PCL), the PKMv2 authentication protocol's security is analyzed, the interleaving attack is found, and a new authentication protocol is proposed by using the Protocol Derivation System (PDS) in WiMAX wireless network based on the vulnerability of system security, finally a formal correctness and security proof of it is presented with Protocol Composition Logic (PCL). This new protocol is more secure than the PKMv2 security authentication protocol, and more suitable for complicated wireless network application environment used in WiMAX.

Key words: Wireless network; Authentication protocol; Protocol Derivation System (PDS); Protocol Composition Logic (PCL); WiMAX

1　引言

宽带无线接入技术是指以无线传输方式向用户提供接入宽带固定网络的接入技术。2005年IEEE 802.16工作组推出了WiMAX无线网络的国际新标准IEEE 802.16e-2005[1−3]，WiMAX(全球微波接入互操作性)无线网络基于IEEE 802.16空中接口，是一项新兴的无线城域网[4] (WMAN)宽带技术。IEEE 802.16e-2005 标准将以前版本中使用的PKM (Privacy and Key Management)安全接入协议升级为PKMv2[5]安全协议。PKMv2安全协议包括安全认证协议和密钥管理协议两个子协议，其中PKMv2安全认证协议是整个协议的基础与核心。

国内外学者针对 PKMv2 安全认证协议可能存在的安全隐患做了分析与研究，例如， Liu 与 Lu[6] 针对 IEEE 802.16e 标准中 PKMv2 安全认证协议在高速移动过程中缺乏保证完整性和不可抵赖性的机

2009-09-08 收到，2010-02-09 改回
国家高技术研究发展计划(863)(2007AA01Z429)，国家自然科学基金(60702059，60972078)，甘肃省自然科学基金(2007GS04823)，网络安全与密码技术福建省高校重点实验室开放课题(09A006)和兰州理工大学博士基金(BS14200901)资助课题
通信作者：张子彬　zzb020511@hotmail.com

制，存在移交攻击(handover vulnerability)，终端能力限制等问题，提出了使用无线公钥基础设施(wireless public key infrastructure)来保证其安全性，并通过仿真证明新方案加解密延迟短，性能更加优越。Sun 等[7]基于重认证的需要，提出了一种更加安全快速的重认证机制。Shon 与 Choi [8]针对 IEEE 802.16e 标准中 PKMv2 安全认证协议在其认证初始阶段会产生安全内容泄露等问题，提出了使用 DH 密钥协商产生会话加密密钥，并使用该会话加密密钥来保证认证初始阶段的安全性。Xu 与 Huang [9]针对 IEEE 802.16e 标准中 PKMv2 安全认证协议所受到的交错攻击，对 PKMv2 安全认证协议提出了修改意见(这里称该修改过的协议为 SC-PKMv2)，并使用 BAN 逻辑证明其方案安全性。

本文使用了 DDMP 组合理论[10−13]对 PKMv2 安全认证协议进行形式化分析，发现 PKMv2 安全认证协议存在交错攻击。DDMP 组合理论包括协议演绎系统(PDS)和协议组合逻辑(PCL)。其理论的核心是协议可组合的安全性证明，该理论以简单协议模块的相加性组合与非破坏性组合作为演绎操作的前提，将复杂的组合协议看成是由简单协议模块经过一系列演绎操作得到的，这样复杂协议的模块化正确性证明就可以通过对简单协议模块证明的组合得到。该理论不仅提供了一种全新的分析复杂组合协议的形式化方法，也可以作为协议设计的新方法。本文运用该理论，基于协议组合逻辑(PCL)证明了 PKMv2 安全认证协议具有密钥机密性、不具有会话认证性，发现 PKMv2 安全认证协议存在交错攻击，并且在此基础上运用协议演绎系统(PDS)提出了一种新的 WiMAX 无线网络安全认证协议，并使用协议组合逻辑(PCL)给出新协议的模块化正确性和安全性证明，新协议具有密钥机密性和会话认证性，相对于 PKMv2 安全认证协议更加安全。

2　预备知识

2.1 PKMv2 安全认证协议

PKMv2 安全认证协议的定义如下：

$X \to Y$：　N_X , ID_X

$Y \to X$：　$\mathrm{SIG}_Y(N_X$, N_Y , ID_Y , $E_{K_x}(\mathrm{PAK}$, $\mathrm{ID}_X))$

$X \to Y$：　N_Y ,　XAddr ,　$\mathrm{MAC}_{\mathrm{AK}}(N_Y$, XAddr)

X 代表客户端，Y 代表基站

其中 K_x 表示客户端 X 的公钥，认证密钥(AK)则是客户端得到预认证密钥(PAK)以后，通过计算式 $\mathrm{AK} = \mathrm{MAC}_{\mathrm{PAK}}(N_X, N_Y, \mathrm{XAddr}, \mathrm{YAddr}, 160)$ [14] 计算得出。

2.2 协议演绎系统

协议演绎系统(PDS)由构件集合和操作集合组成。构件是简单协议的一步或者几步，基本的构件可用于构造更复杂的协议。操作集合包含 3 类不同的演绎操作：组合、求精和转换。本文中主要应用到的演绎操作[10]包括串行组合操作、转换操作 T1 以及求精操作 R3，R4 和 R6 (本文将以前相关文献之 HASH_K 修改为 MAC_K)。

R 3：　$\mathrm{SIG}_X(m) \to \mathrm{SIG}_X(m)$, $\mathrm{MAC}_K(m$, $\mathrm{ID}_X)$

R 4：　$\mathrm{SIG}_X(m) \to \mathrm{SIG}_X(m$, $\mathrm{ID}_Y)$

R 6：　$\mathrm{SIG}_X(m) \to \mathrm{SIG}_X(m)$, ID_X

2.3 协议组合逻辑

协议组合逻辑(PCL)是用于证明网络安全协议安全属性的证明逻辑，具有精确，易部署，提供信息量丰富等特性。本文中主要应用到的公理与规则[10−13]，具体有协议行为公理 AA1，AA4，AN3 和 ARP，原子谓词公理 REC，时间排序公理 FS1 和 FS2，消息认证码公理 MAC1，MAC3 和 MAC4 (本文将以前相关文献之 HASH_K 修改为 MAC_K)。

AA 1：　$\theta[a]_X a$

AA 4：　$\theta[a_1; a_2; \cdots; a_k]_X a_1 < a_2 < \cdots < a_{k-1} < a_k$

AN 3：　$\theta[\mathrm{New}\, x]_X \mathrm{Fresh}(X, x)$

ARP：　$\mathrm{Receive}(X, p(x))[\mathrm{match}\, q(x) / q(t)]_X$ $\mathrm{Receive}(X, p(t))$

REC：　$\mathrm{Receive}(X, x) \supset \mathrm{Has}(X, x)$

FS1：　$\mathrm{Fresh}(X, t)[\mathrm{send}\, t']_X \mathrm{Firstsend}(X, t, t') \forall t \subseteq t$

FS 2：　$\mathrm{Firstsend}(X, t, t') \wedge \alpha(Y, t'') \supset \mathrm{Send}(X, t') < \alpha(Y, t''), \mathrm{where}\, X \neq Y \wedge t \subseteq t''$

MAC 1：　$\mathrm{Computes}(X, \mathrm{MAC}_K(x)) \supset \mathrm{Has}(X, x) \wedge \mathrm{Has}(X, K)$

MAC 3：　$\mathrm{Receive}(X, \mathrm{MAC}_K(x)) \supset \exists Y.\mathrm{Computes}(Y, \mathrm{MAC}_K(x)) \wedge \mathrm{Send}(Y, \mathrm{MAC}_K(x))$

MAC 4：　$\mathrm{Has}(X, \mathrm{MAC}_K(x)) \supset \mathrm{Computes}(X, \mathrm{MAC}_K(x)) \vee \exists Y, m.\mathrm{Computes}(Y, \mathrm{MAC}_K(x)) \wedge \mathrm{Send}(Y, m) \wedge \mathrm{Contains}(m, \mathrm{MAC}_K(x))$

$$\mathrm{HON}_Q: \frac{\mathrm{Start}(X)[\,]_X \phi (\forall \rho \in Q. \forall P \in \mathrm{BS}(\rho). \phi[P]_X \phi)}{\mathrm{Honest}(\widehat{X}) \supset \phi}$$

3　PKMv2 安全认证协议的形式化分析

3.1 基于 PCL 的协议模型

PKMv2 安全认证协议的参与实体有客户端(Client)和基站(Server)两个，用 $\widehat{X}$ ， $\widehat{Y}$ 表示，各自

相应的实例用 X，Y 表示，该协议的客户端认证程序 WiMAX : Client 和基站认证程序 WiMAX : Server 描述如下，其中"client"，"server"分别表示客户端和基站的身份信息，XAddr, YAddr 分别表示客户端和基站的 MAC 地址，且根据文献[5]中所述协议第 3 条消息中的客户端 MAC 地址 XAddr 包含 X 的证书，则将 XAddr 形式化描述为：$\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X}, K_x)$。

$$\begin{aligned}\mathrm{WiMAX:Client}=(X,\widehat{Y})[&\mathrm{new}\,N_X;\mathrm{send}\,\widehat{X},\widehat{Y},N_X,\\&\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{Y},K_x);\mathrm{receive}\,\widehat{Y},\widehat{X},z;\\&\mathrm{verify}\,z,(N_X,N_Y,\mathrm{cert},\mathrm{encsec}),\\&\widehat{Y};\mathrm{match\,cert}/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{Y},K_y);\\&\mathrm{match\,encsec}/\mathrm{ENC}_{K_x}(\mathrm{PAK},\\&\text{"client"});\mathrm{match}\,\mathrm{MAC}_{\mathrm{PAK}}(N_X,\\&N_Y,\mathrm{XAddr},\mathrm{YAddr},160)/\mathrm{AK};\\&\mathrm{send}\,\widehat{X},\widehat{Y},N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x),\\&\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x))]_X\end{aligned}$$

$$\begin{aligned}\mathrm{WiMAX:Server}=(Y)[&\mathrm{receive}\,\widehat{X},\widehat{Y}z;\mathrm{match}\,z/N_X,\\&\mathrm{cert}_1;\mathrm{match\,cert}_1/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x);\\&\mathrm{new}\,N_Y;\mathrm{send}\,\widehat{Y},\widehat{X},\mathrm{SIG}_{V_y}(N_X,N_Y,)\\&\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{Y},K_y),\mathrm{ENC}_{K_x}(\mathrm{PAK},\\&\text{"client"}));\mathrm{receive}\,\widehat{X},\widehat{Y},w;\mathrm{match}\\&w/N_X,\mathrm{cert}_2,\mathrm{mac};\mathrm{match\,cert}_2/\\&\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x);\mathrm{match}\,\mathrm{MAC}_{\mathrm{PAK}}(N_X,\\&N_Y,\mathrm{XAddr},\mathrm{YAddr},160)/\mathrm{AK};\\&\mathrm{match\,mac}/\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{cert}_3);\\&\mathrm{match\,cert}_3/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x)]_Y\end{aligned}$$

3.2 前提与恒定量

前提[11,15]是实例执行动作的初始状态，是协议组合逻辑(PCL)的语法的重要组成部分。恒定量[11,15]则相当于协议运行的操作环境，是协议安全运行的基本保证。PKMv2 安全认证协议的前提与恒定量如下所示：

前提 θ_{WiMAX} 描述 Client 和 Server 两个实体共享预认证密钥(PAK)且不被第 3 方知晓(只有客户端才能解开协议第 2 条消息中用客户端公钥加密的预认证密钥[9])。

$$\begin{aligned}\theta_{\mathrm{WiMAX}}\coloneqq&\mathrm{Honest}(\widehat{X})\wedge\mathrm{Honest}(\widehat{Y})\supset\mathrm{Has}(\widehat{Z},\mathrm{PAK})\\&\supset\widehat{Z}=\widehat{X}\vee\widehat{Y}\end{aligned}$$

恒定量 $\tau_{\mathrm{WiMAX,1}}$ 描述 Client 和 Server 在计算认证密钥(AK)时，不会泄露给第三方。

$$\begin{aligned}\tau_{\mathrm{WiMAX,1}}\coloneqq&\mathrm{Computes}(\widehat{Y},\mathrm{MAC}_{\mathrm{PAK}}(N_X,N_Y,\mathrm{XAddr},\\&\mathrm{YAddr},160))\supset\neg(\mathrm{Send}(\widehat{Y},m)\wedge\mathrm{Contains}\\&(m,\mathrm{MAC}_{\mathrm{PAK}}(N_X,N_Y,\mathrm{XAddr},\mathrm{YAddr},160)))\end{aligned}$$

恒定量 $\tau_{\mathrm{WiMAX,2}}$ 描述同一网元不能同时即作为 Client 又作为 Server，同时兼任两个角色会引起反射攻击[16]。

$$\begin{aligned}\tau_{\mathrm{WiMAX,2}}\coloneqq&\mathrm{Honest}(\widehat{Y})\wedge\mathrm{Send}(Y,N_X,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x))\supset\\&\neg\mathrm{Receive}(Y,N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x),\ \mathrm{MAC}_{\mathrm{AK}}\\&(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x)))\wedge(\mathrm{Honest}(\widehat{Y})\wedge\\&\mathrm{Receive}(Y,N_X,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x))\supset\\&\neg\,\mathrm{Receive}(Y,\mathrm{SIG}_{V_y}(N_X,N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{Y},\\&K_y),\mathrm{ENC}_{K_x}(\mathrm{PAK},\text{"client"}))))\end{aligned}$$

3.3 安全属性及证明

将 PKMv2 安全认证协议的安全目标形式化描述为两个安全属性[11,15]：密钥机密性($\phi_{\mathrm{WiMAX,sec}}$)和会话认证性($\phi_{\mathrm{WiMAX,auth}}$)，且只有保障密钥机密性，才能确保具有会话认证性。这里仅给出 Server 端的情况，Client 端的情况类似，略去。

定理 1 (PKMv2 安全认证协议具有密钥机密性) 该协议为 Server 提供密钥机密性是指：$\tau_{\mathrm{WiMAX,1}}\wedge\tau_{\mathrm{WiMAX,2}}\mapsto\theta_{\mathrm{WiMAX}}[\mathrm{WiMAX:Server}]_Y\cdot\phi_{\mathrm{WiMAX,sec}}$，其中 $\phi_{\mathrm{WiMAX,sec}}$ ::=$\mathrm{Honest}(\widehat{X})\wedge\mathrm{Honest}(\widehat{Y})\supset(\mathrm{Has}(\widehat{Z},\mathrm{AK})\supset\widehat{Z}=\widehat{X}\vee\widehat{Z}=\widehat{Y})\wedge\mathrm{Has}(\widehat{X},\mathrm{AK})\wedge\mathrm{Has}(\widehat{Y},\mathrm{AK})$。

证明

(1) $\mathrm{ARP,MAC3}:\theta_{\mathrm{WiMAX}}[\mathrm{receive}\,\widehat{X},\widehat{Y},w;\mathrm{match}\,w/N_Y,\mathrm{cert}_2,\mathrm{mac};\mathrm{match\,cert}_2/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x);\ \mathrm{match}\ \mathrm{MAC}_{\mathrm{PAK}}(N_X,N_Y,\mathrm{XAddr},\mathrm{YAddr},160)/\mathrm{AK};\mathrm{match\,mac}/\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{cert}_3);\mathrm{match\,cert}_3/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x)]_Y\,\mathrm{Receive}(Y,\widehat{X},\widehat{Y},N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x),\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x)))\supset\exists Z.\mathrm{Computes}(Z,\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x)))\wedge\mathrm{Send}(Z,\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x)))\wedge(\mathrm{Send}(Z,\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x)))<\mathrm{Receive}(Y,\widehat{X},\widehat{Y},N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x),\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x))))$

(2) $\mathrm{MAC1}:\mathrm{Computes}(Z,\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x)))\equiv\mathrm{Has}(\widehat{Z},\mathrm{AK})\wedge\mathrm{Has}(\widehat{Z},N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\widehat{X},K_x))$

(3) $\mathrm{MAC4}:\mathrm{Has}(\widehat{Z},\mathrm{AK})\equiv\mathrm{Has}(\widehat{Z},\mathrm{MAC}_{\mathrm{PAK}}(N_X,N_Y,\mathrm{XAddr},\mathrm{YAddr},160))\supset\mathrm{Computes}(Z,\mathrm{MAC}_{\mathrm{PAK}}$

$(N_X, N_Y, \text{XAddr}, \text{YAddr}, 160)) \vee (\exists K, m.$
$\text{Computes}(K, \text{MAC}_{\text{PAK}}(N_X, N_Y, \text{XAddr}, \text{YAddr},$
$160)) \wedge \text{Send}(K, m) \wedge \text{Contain}(m, \text{MAC}_{\text{PAK}}(N_X,$
$N_Y, \text{XAddr}, \text{YAddr}, 160)))$
$(4)\ (3), \tau_{\text{WiMAX},1} : \theta_{\text{WiMAX}}[\text{receive}\,\widehat{X}, \widehat{Y}, w; \text{match}\,w /$
$N_Y, \text{cert}_2, \text{mac}; \text{match}\,\text{cert}_2 / \text{SIG}_{\widehat{\text{CA}}}(\widehat{X}, K_x); \text{match}$
$\text{MAC}_{\text{PAK}}(N_X, N_Y, \text{XAddr}, \text{YAddr}, 160) / \text{AK};$
$\text{match}\,\text{mac} / \text{MAC}_{\text{AK}}(N_Y, \text{cert}_3); \text{match}\,\text{cert}_3 /$
$\text{SIG}_{\widehat{\text{CA}}}(\widehat{X}, K_x)]_Y$
$\text{Has}(\widehat{Z}, \text{AK}) \equiv \text{Has}(Z, \text{MAC}_{\text{PAK}}$
$(N_X, N_Y, \text{XAddr}, \text{YAddr}, 160)) \supset \text{Computes}(Z,$
$\text{MAC}_{\text{PAK}}(N_X, N_Y, \text{XAddr}, \text{YAddr}, 160))$
$(5)\ (4), \text{MAC1} : \theta_{\text{WiMAX}}[\text{receive}\,\widehat{X}, \widehat{Y}, w; \text{match}\,w / N_Y,$
$\text{cert}_2, \text{mac}; \text{match}\,\text{cert}_2 / \text{SIG}_{\widehat{\text{CA}}}(\widehat{X}, K_x); \text{match}$
$\text{MAC}_{\text{PAK}}(N_X, N_Y, \text{XAddr}, \text{YAddr}, 160) / \text{AK};$
$\text{match}\,\text{mac} / \text{MAC}_{\text{AK}}(N_Y, \text{cert}_3); \text{match}\,\text{cert}_3 /$
$\text{SIG}_{\widehat{\text{CA}}}(\widehat{X}, K_x)]_Y$
$\text{Honest}(\widehat{X}) \wedge \text{Honest}(\widehat{Y}) \supset$
$\text{Computes}(Z, \text{MAC}_{\text{PAK}}(N_X, N_Y, \text{XAddr}, \text{YAddr},$
$160)) \supset \text{Has}(\widehat{Z}, \text{AK}) \supset \text{Has}(\widehat{Z}, \text{PAK})$
$\supset \widehat{Z} = \widehat{X} \vee \widehat{Z} = \widehat{Y}$

即可得出 $\tau_{\text{WiMAX},1} \wedge \tau_{\text{WiMAX},2} \mapsto \theta_{\text{WiMAX}}[\text{WiMAX} : \text{Server}]_Y \phi_{\text{WiMAX,sec}}$ 成立。

定理 2　(PKMv2 安全认证协议不具有会话认证性) 该协议为 Server 提供会话认证性是指：$\tau_{\text{WiMAX},1} \wedge \tau_{\text{WiMAX},2} \mapsto \theta_{\text{WiMAX}}[\text{WiMAX} : \text{Server}]_Y$ $\phi_{\text{WiMAX,auth}}$，其中 $\phi_{\text{WiMAX,auth}} ::= \text{Honest}(\widehat{X}) \wedge \text{Honest}(\widehat{Y}) \supset \exists\ Y.\text{ActionsinOrder}(\text{Send}(X,\ \widehat{X},\ \widehat{Y},$ $\text{Message 1}), \text{Receive}(Y, \widehat{X}, \widehat{Y}, \text{Message 1}), \text{Send}(Y, \widehat{Y}, \widehat{X},$ $\text{Message 2}), \text{Receive}(X, \widehat{Y}, \widehat{X}, \text{Message 2}), \text{Send}(X, \widehat{X}, \widehat{Y},$ $\text{Message 3}), \text{Receive}(Y, \widehat{X}, \widehat{Y}, \text{Message 3}))$。因篇幅原因证明过程略去，经证明 $\tau_{\text{WiMAX},1} \wedge \tau_{\text{WiMAX},2} \mapsto \theta_{\text{WiMAX}}[\text{WiMAX} : \text{Server}]_Y \phi_{\text{WiMAX,auth}}$ 不成立，并且根据文献[17]可知存在交错攻击。

4　演绎新的认证协议

本文首先选取两个单方认证协议，一个是基于签名的挑战应答协议 P_1，一个是基于消息认证码的挑战应答协议 P_2 (消息认证码的密钥 AK 由用 X 公钥 K_x 加密的预认证密钥 PAK 计算得出，原理同 PKMv2 安全认证协议)。

$$P_1 : X \to Y:\ N_X$$
$$Y \to X:\ \text{SIG}_Y(N_X)$$
$$P_2 : Y \to X:\ N_Y\ , E_{K_x}(\text{PAK})$$
$$X \to Y:\ N_Y\ , \text{MAC}_{\text{AK}}(N_Y)$$

对协议 P_1 与 P_2 进行串行组合，用协议 P_1 的输出代替协议 P_2 的输入，从而得到协议 P_3。

$$P_3 : X \to Y:\ N_X$$
$$Y \to X:\ \text{SIG}_Y(N_X)$$
$$Y \to X:\ N_Y\ , E_{K_x}(\text{PAK})$$
$$X \to Y:\ N_Y\ , \text{MAC}_{\text{AK}}(N_Y)$$

对协议 P_3 应用转换 T1，将 $N_Y, E_{K_x}(\text{PAK})$ 移动到较早的消息中，从而得到协议 P_4，其主要目的是减少消息数量。

$$P_4 : X \to Y:\ N_X$$
$$Y \to X:\ \text{SIG}_Y(N_X\ , N_Y\ , E_{K_x}(\text{PAK}))$$
$$X \to Y:\ N_Y\ , \text{MAC}_{\text{AK}}(N_Y)$$

由于应用转换操作 T1 后协议第 2 步使用了客户端 X 的公钥，但是协议第 1 步并未向基站 Y 发送 X 的公钥证书，根据转换操作的定义，这里可以应用转换操作在协议第 1 步加入 ID_X，从而得到协议 P_5。ID_X 表示客户端 X 的公钥证书，以防止基站 Y 未持有 X 的公钥。

$$P_5 : X \to Y:\ N_X\ , \text{ID}_X$$
$$Y \to X:\ \text{SIG}_Y(N_X\ , N_Y\ , E_{K_x}(\text{PAK}))$$
$$X \to Y:\ N_Y\ , \text{MAC}_{\text{AK}}(N_Y)$$

对协议 P_5 应用求精 R6 得到协议 P_6，其中 ID_Y 表示基站 Y 的公钥证书，从而防止客户端 X 未持有基站 Y 的签名-证明密钥。

$$P_6 : X \to Y:\ N_X\ , \text{ID}_X$$
$$Y \to X:\ \text{SIG}_Y(N_X\ , N_Y\ , E_{K_x}(\text{PAK}))\ , \text{ID}_Y$$
$$X \to Y:\ N_Y\ , \text{MAC}_{\text{AK}}(N_Y)$$

为了防止客户端 X 的 MAC 地址被修改，根据转换操作的定义，运用转换操作在第三条消息中加入包含 X 证书的 MAC 地址 XAddr (根据文献[11]所述，加入 XAddr 也是保护认证密钥 AK 的一种加盐操作)，从而得到协议 P_7。

$$P_7 : X \to Y:\ N_X\ , \text{ID}_X$$
$$Y \to X:\ \text{SIG}_Y(N_X\ , N_Y\ , E_{K_x}(\text{PAK}))\ , \text{ID}_Y$$
$$X \to Y:\ N_Y\ , \text{XAddr}\ , \text{MAC}_{\text{AK}}(N_Y\ , \text{XAddr})$$

对协议 P_7 应用求精 R4 得到协议 P_8，协议 P_8 拥有协议 P_7 的一切安全属性，并能有效抵御 Lowe's 攻击[18]。此时，协议已经具备了一定的安全性，但还与 PKMv2 安全认证协议一样会受到交错攻击。

$$P_8 : X \to Y:\ N_X\ , \text{ID}_X$$
$$Y \to X:\ \text{SIG}_Y(N_X\ , N_Y\ , E_{K_x}(\text{PAK})\ , \text{ID}_X)\ , \text{ID}_Y$$
$$X \to Y:\ N_Y\ , \text{XAddr}\ , \text{MAC}_{\text{AK}}(N_Y\ , \text{XAddr})$$

对协议 P_8 应用求精 R3 得到协议 P_9，协议 P_9 拥有协议 P_8 的一切安全属性，加入求精 R2 后证明第二条消息是基站 Y 产生发送的，从而有效的防御交错攻击。

$P_9: X \to Y:\ N_X, \mathrm{ID}_X$

$Y \to X:\ \mathrm{SIG}_Y(N_X, N_Y, E_{K_x}(\mathrm{PAK}), \mathrm{ID}_X),$

$\mathrm{MAC}_{\mathrm{PAK}}(N_X, N_Y, \mathrm{ID}_X, \mathrm{ID}_Y, E_{K_x}(\mathrm{PAK})), \mathrm{ID}_Y$

$X \to Y:\ N_Y, \mathrm{XAddr}, \mathrm{MAC}_{\mathrm{AK}}(N_Y, \mathrm{XAddr})$

到此为止，我们就通过协议演绎系统(PDS)演绎得到了一个新的安全认证协议，命名其为 FZM-PKMv2 安全认证协议，其现实流程图如下图 1 所示。

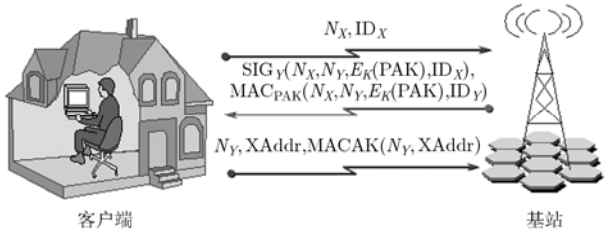

图 1 FZM-PKMv2 安全认证协议现实流程图

5 FZM-PKMv2 协议模块化正确性和安全性证明

5.1 基于 PCL 的协议模型

FZM-PKMv2 安全认证协议的参与实体也是客户端(Client)和基站(Server)两个，同样也分别用 $\hat{X}$，$\hat{Y}$ 表示，各自相应的实例用 X，Y 表示，其它信息描述与 PKMv2 安全认证协议一致。该协议的客户端认证程序 WiMAX′: Client 和基站认证程序 WiMAX′: Server 描述如下：

$$\begin{aligned}\mathrm{WiMAX}'\text{: Client} = (X,\hat{Y})[&\mathrm{new}\,N_X;\mathrm{send}\,\hat{X},\hat{Y},N_X,\\ &\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{Y},K_x);\mathrm{receive}\,\hat{Y},\hat{X},z;\\ &\mathrm{match}\,z/\mathrm{cert},w,\mathrm{mac};\mathrm{match}\\ &\mathrm{cert}/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{Y},K_y);\mathrm{verify}\,w,(N_X,\\ &N_Y,\text{"client"},\mathrm{encsec}_1),\hat{Y};\mathrm{match}\\ &\mathrm{encsec}_1/\mathrm{ENC}_{K_x}(\mathrm{PAK});\mathrm{match}\\ &\mathrm{mac}/\mathrm{MAC}_{\mathrm{PAK}}(N_X,N_Y,\text{"client"},\\ &\text{"server"},\mathrm{encsec}_2);\mathrm{match}\,\mathrm{encsec}_2\\ &/\mathrm{ENC}_{K_x}(\mathrm{PAK});\mathrm{match}\,\mathrm{MAC}_{\mathrm{PAK}}\\ &(N_X,N_Y,\mathrm{XAddr},\mathrm{YAddr},160)/\mathrm{AK};\\ &\mathrm{send}\,\hat{X},\hat{Y},N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{X},K_x),\\ &\mathrm{MAC}_{\mathrm{AK}}(N_Y,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{X},K_x))]_X\end{aligned}$$

$$\begin{aligned}\mathrm{WiMAX}'\text{: Server} = (Y)[&\mathrm{receive}\,\hat{X},\hat{Y},z;\mathrm{match}\,z/N_X,\\ &\mathrm{cert}_1;\mathrm{match}\,\mathrm{cert}_1/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{X},K_x);\\ &\mathrm{new}\,N_Y;\mathrm{send}\,\hat{Y},\hat{X},\mathrm{SIG}_{V_y}(N_X,N_Y,\\ &\text{"client"},\mathrm{ENC}_{K_x}(\mathrm{PAK})),\mathrm{MAC}_{\mathrm{PAK}}\\ &(N_X,N_Y,\text{"client"},\text{"server"},\mathrm{ENC}_{K_x}\\ &(\mathrm{PAK})),\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{Y},K_y);\mathrm{receive}\,\hat{X},\\ &\hat{Y},w;\mathrm{match}\,w/N_X,\mathrm{cert}_2,\mathrm{mac};\\ &\mathrm{match}\,\mathrm{cert}_2/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{X},K_x);\mathrm{match}\\ &\mathrm{MAC}_{\mathrm{PAK}}(N_X,N_Y,\mathrm{XAddr},\mathrm{YAddr},\\ &160)/\mathrm{AK};\mathrm{match}\,\mathrm{mac}/\mathrm{MAC}_{\mathrm{AK}}\\ &(N_Y,\mathrm{cert}_3);\mathrm{match}\,\mathrm{cert}_3/\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{X},\\ &K_x)]_Y\end{aligned}$$

5.2 前提与恒定量

FZM-PKMv2 安全认证协议的前提与恒定量如下所示(同理 3.2 节)：

$$\begin{aligned}\theta'_{\mathrm{WiMAX}} :=\ &\mathrm{Honest}(\hat{X})\wedge\mathrm{Honest}(\hat{Y})\supset\mathrm{Has}(\hat{Z},\mathrm{PAK})\\ &\supset\hat{Z}=\hat{X}\vee\hat{Y}\end{aligned}$$

$$\begin{aligned}\tau'_{\mathrm{WiMAX},1} :=\ &\mathrm{Computes}(\hat{Y},\mathrm{MAC}_{\mathrm{PAK}}(N_X,N_Y,\mathrm{XAddr},\\ &\mathrm{YAddr},160))\supset\neg(\mathrm{Send}(\hat{Y},m)\wedge\mathrm{Contains}\\ &(m,\mathrm{MAC}_{\mathrm{PAK}}(N_X,N_Y,\mathrm{XAddr},\mathrm{YAddr},\\ &160)))\end{aligned}$$

$$\begin{aligned}\tau'_{\mathrm{WiMAX},2} :=\ &\mathrm{Honest}(\hat{Y})\wedge\mathrm{Send}(Y,N_X,\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{Y},K_x))\\ &\supset\neg\,\mathrm{Receive}(Y,N_Y,\mathrm{XAddr},\mathrm{MAC}_{\mathrm{AK}}(N_Y,\\ &\mathrm{XAddr}))\wedge(\mathrm{Honest}(\hat{Y})\wedge\mathrm{Receive}(Y,N_X,\\ &\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{Y},K_x))\supset\neg\,\mathrm{Receive}(Y,\mathrm{SIG}_{V_y}(N_X,\\ &N_Y,\text{"client"},\mathrm{ENC}_{K_x}(\mathrm{PAK})),\mathrm{MAC}_{\mathrm{PAK}}(N_X,\\ &N_Y,\text{"client"},\text{"s erver"},\mathrm{ENC}_{K_x}(\mathrm{PAK})),\\ &\mathrm{SIG}_{\widehat{\mathrm{CA}}}(\hat{Y},K_y))\end{aligned}$$

5.3 安全属性及证明

将 FZM-PKMv2 安全认证协议的安全目标同样形式化为两个安全属性：密钥机密性($\phi'_{\mathrm{WiMAX,sec}}$)和会话认证性($\phi'_{\mathrm{WiMAX,auth}}$)，这里同样仅给出 Server 端的情况，Client 端的情况类似，略去。

定理 3 (FZM-PKMv2 安全认证协议具有密钥机密性) 该协议为 Server 提供密钥机密性是指：$\tau'_{\mathrm{WiMAX},1}\wedge\tau'_{\mathrm{WiMAX},2}\mapsto\theta'_{\mathrm{WiMAX}}[\mathrm{WiMAX}'\text{: Server}]_Y$ $\phi'_{\mathrm{WiMAX,sec}}$，其中 $\phi'_{\mathrm{WiMAX,sec}} ::= \mathrm{Honest}(\hat{X})\wedge\mathrm{Honest}(\hat{Y})\supset(\mathrm{Has}(\hat{Z},\mathrm{AK})\supset\hat{Z}{=}\hat{X}\vee\hat{Z}{=}\hat{Y})\wedge\mathrm{Has}(\hat{X},\mathrm{AK})\wedge\mathrm{Has}(\hat{Y},\mathrm{AK})$。因证明方法同 PKMv2 安全认证协议的密钥机密性证明，故在此略去。

定理 4 (FZM-PKMv2 安全认证协议具有会话

认证性)该协议为 Server 提供会话认证性是指：$\tau'_{\mathrm{WiMAX},1} \wedge \tau'_{\mathrm{WiMAX},2} \mapsto \theta'_{\mathrm{WiMAX}}[\mathrm{WiMAX}' : \mathrm{Server}]_Y \phi'_{\mathrm{WiMAX,auth}}$，其中 $\phi'_{\mathrm{WiMAX,auth}} ::= \mathrm{Honest}(\widehat{X}) \wedge \mathrm{Honest}(\widehat{Y}) \supset \exists Y.\mathrm{ActionsinOrder}(\mathrm{Send}(X,\widehat{X},\widehat{Y},\mathrm{Message1}), \mathrm{Receive}(Y,\widehat{X},\widehat{Y},\mathrm{Message1}),\mathrm{Send}(Y,\widehat{Y},\widehat{X},\mathrm{Message2}), \mathrm{Receive}(X,\widehat{Y},\widehat{X},\mathrm{Message2}),\mathrm{Send}(X,\widehat{X},\widehat{Y},\mathrm{Message3}), \mathrm{Receive}(Y,\widehat{X},\widehat{Y},\mathrm{Message\ 3}))$，因篇幅原因证明过程略去。

FZM- PKMv2 与其他 PKMv2 安全认证协议的安全性比较如下表 1 所示。

表 1 几类 PKMv2 安全认证协议的安全性比较

	PKMv2 认证协议	SC- PKMv2 认证协议	FZM-PKMv2 认证协议
密钥机密性	良好	良好	良好
Lowe's 攻击	有效防御	有效防御	有效防御
交错攻击	未能有效防御	有效防御	有效防御交错攻击，且比 SC-PKMv2 认证协议发现攻击更早
协议安全性	不安全	基于 BAN 逻辑安全	基于 PCL 安全

6 结束语

基于协议演绎系统(PDS)本文提出了一种新的 WiMAX 无线网络安全认证协议 —— FZM-PKMv2，与 PKMv2 安全认证协议不同的是，它有效地防御了交错攻击，并且运用协议组合逻辑(PCL)给出了新协议的模块化正确性和安全性证明。

本文主要讨论了 WiMAX 无线网络接入认证的安全问题，以后将用类似方法讨论其它类型的网络安全认证协议。再者，将通过网络仿真对 FZM-PKMv2 安全认证协议的效率进行分析与优化。

参 考 文 献

[1] Yarali A and Rahman S. WiMAX broadband wireless access technology: Services, architecture and deployment models [C]. Electrical and Computer Engineering, 2008. CCECE 2008, Canada, 2008: 77–82.

[2] IEEE 802.16e-2005. Air interface for fixed broadband wireless access systems, Amendment 2: Physical and medium access control layers for combined fixed and mobile operation in licensed bands[S], NJ, USA, IEEE Press, 2006.

[3] Kim Dongmyoung, Cai Hua, and Na Minsoo, *et al*.. Performance measurement over Mobile WiMAX/IEEE 802.16e network[C], 2008 IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, Newport Beach, CA, United states, 2008: 1–8.

[4] Agrawal Dharma P, Gossain Hrishikesh, and Cavalcanti Dave, *et al*.. Recent advances and evolution of WLAN and WMAN standards[C]. IEEE Wireless Communications, USA, 2008: 54–55.

[5] Johnston D and Walker J. Mutual authentication for PKMv2, IEEE C802.16e-04_229rl. 2004.

[6] Liu Fu-qiang and Lu Lei. A WPKI-Based security mechanism for IEEE 802.16e[C]. WiCOM International Conference, Wuhan, 2006: 1–4.

[7] Sun Hung-min, Lin Yue-hsun, and Chen Shuai-min, *et al*.. Secure and fast handover scheme based on pre-authentication method for 802.16/WiMAX infrastructure networks[C]. 2007 IEEE Region 10 Conference, Taipei, 2007: 1–4.

[8] Shon Taeshik and Choi Wook. An analysis of mobile WiMAX security: vulnerabilities and solutions [J]. *Lecture Notes in Computer Science*, 2007, 4658: 88–97.

[9] Xu Sen and Huang Chin-tser. Attacks on PKM protocols of IEEE 802.16 and its later versions[C]. Proceedings of 3rd International Symposium on Wireless Communication System (ISWCS 2006), Valencia, 2006: 185–189.

[10] Datta A. Security analysis of network protocols: compositional reasoning and complexity-theoretic Foundations[D]. [Ph.D. dissertation], Computer Science Department, Stanford University, 2005.

[11] Datta A, Derek A, and Mitchell J C, *et al*.. Protocol Composition Logic (PCL)[J]. *Electronic Notes in Theoretical Computer Science*, 2007, 172: 311–358.

[12] Cremers C. On the protocol composition logic PCL[C]. Proceedings of the 2008 ACM symposium on Information, computer and communications security, Tokyo, Japan, 2008: 66–76.

[13] Doug K, Ryan M, and Tony B, *et al*.. A correctness proof of a mesh security architecture[C]. Proceedings of the 2008 21st IEEE Computer Security Foundations Symposium, 2008: 315–330.

[14] Johnston D and Walker J. Overview of IEEE 802.16 security[J]. *IEEE Security & Privacy*, 2004, 2: 40–48.

[15] He Chang-hua, Sundararajan M, and Datta A, *et al*.. A modular correctness proof of IEEE 802.11i and TLS[C], Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05), Alexandria, VA, USA, 2005: 2–15.

[16] 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 Man-xia, Li Jian-dong, and Wang Yu-min. A correctness proof of WAPI key management protocol based on PCL[J]. *Journal of Electronics & Information Technology*, 2009, 31(2): 444–447.

[17] Meadows C and Pavlovic D. Deriving, attacking and defending the GDOI protocol[C]. Proceedings of 9th European Symposium On Research in Computer Security, France, 2004: 53–72.

[18] Lowe G. Some new attacks upon security protocols[C]. Computer Security Foundations Workshop, 1996, Proceedings, 9th IEEE, Kenmare, Ireland, 1996: 10–12.

冯　涛：男，1970 年生，博士，研究员，研究方向为可证明安全协议理论、安全协议自动化验证技术、无线和移动网络安全.

张子彬：男，1984 年生，硕士，研究方向为网络与信息安全.

马建峰：男，1963 年生，博士，教授，博士生导师，研究方向为计算机安全、密码学、移动与无线网络安全.