面向无人装置协同操作的安全认证协议

牛文生 李亚晖 郭 鹏

(中航工业西安航空计算技术研究所 西安 710075) (机载弹载计算机航空科技重点实验室 西安 710075)

摘 要 无人装置协同操作动态组网需要安全的群组通信。依据无线环境中的不同安全域,提出了一种具有身份保护的安全组网协议。该协议采用基于身份的匿名签名算法设计了安全组网机制,实现了传感器节点、作动器节点、密钥分发中心和控制台的四方安全认证和密钥交换,并为安全域内的无人操作装置建立了安全传输通道;采用匿名身份认证与可追溯机制相结合的方式,构建了无人操作装置间动态组网和数据安全传输,以为协同操作提供实时、安全的数据通道,实现无人操作装置在传感器和作动器级的协同。

关键词 无人装置,动态组网,群组通信,多级安全,密钥管理

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.1.040

Authentication Protocol for Cooperation of Unmanned Vehicles

NIU Wen-sheng LI Ya-hui GUO Peng

(AVIC Xi'an Aeronautics Computing Technique Research Institute, Xi'an 710075, China)

(Aviation Key Laboratory of Science and Technology on Airborne and Missile-borne Computer, Xi'an 710075, China)

Abstract The cooperation of unmanned vehicles needs dynamic networking for the secure group communication. Based on the different security domain of wireless environments, an authentication protocol with identity protection for cooperation of unmanned vehicles was proposed, which consists of a four-party security information exchange protocol for the data transmission between nodes in the dynamic network and an ID-based anonymous authentication scheme for the secure session keys of a node, which supports the combination of the decryption process and the identity protection. Finally, it is shown that the session key has the security characters of unforgeability, confidentiality and non-repudiation, and the new protocol has a secure, flexible and efficient method of key management for dynamic networking.

Keywords Unmanned vehicles, Dynamical networking, Group communication, Multilevel secure, Key management

1 引言

随着无人设备在各领域的迅速发展,如无人机、排险机器人、深海无人艇等,在各种人类无法生存的危险领域,无人设备已经进入了一个全面应用的时期。在未来的复杂任务场景中,多台无人设备协同操作是应对越来越复杂环境的必然趋势。无人设备的系统操作对控制精度和准确性的要求逐渐提高,仅仅通过远程的人为操作已经难以满足未来操作场景的需求。美军在有人机空中加油和无人机的编队飞行都采用了无线局域网技术来实现有人和无人设备的协同操作,并进行了试验飞行[1-5]。随着信息物理融合系统技术的发展,通过计算、控制和通信技术的紧密融合,在无人设备端的操作装置间实现互操作是有效的技术途径。无人操作装置间的动态组网,提供安全、实时的数据通道是面临的一种技术挑战。

无人操作装置的协同操作需要在传感器级实现实时通信,时间同步精度需要达到微秒级,因而基于无线动态组网的高速通信机制是一种有效的技术途径。自组织网络是无线网络的一种典型拓扑结构,具有无基础设施、组网灵活、多跳路由、抗毁性强等特点,因此得到了人们越来越多的关注。在自组织网络发展过程中出现了无线网状网,它是一种能够具有自组织网络灵活特性的全连通网络,更加适合无人设备的动态组网,因而在无人装置协同操作的通信中引入动态自组织网络是一个理想的选择[6-8]。

无人设备的工作场景往往是人类无法生存的危险环境。当无人设备需要处理一些敏感任务时,其通信数据的安全性成为关注的问题。例如,战场环境的无人设备布雷、排爆,无人机群空中协同攻击,以及核工业中的无人设备远程操作等等。无人操作装置的协同操作的通信数据安全保护需要在其协同组网时构建安全通信通道并提供身份信息保护。

本文提出的方案采用基于身份标识的公钥技术,利用安全域内的匿名认证机制,结合四方安全组网协议,实现了动态的身份保护密钥管理方案,能够为动态群组的通信提供实时安全的信息保护隔离,可有效应用于无人操作装置协同操作的多种场景。

到稿日期:2014-11-24 返修日期:2015-04-27 本文受航空科学基金项目(2013ZC31005)资助。

牛文生(1967-),男,研究员,博士生导师,CCF会员,主要研究方向为嵌入式计算机、网络安全,E-mail:nwsheng@avic.com;李亚晖(1976-),男,博士,高级工程师,主要研究方向为嵌入式系统安全、网络安全协议,E-mail:ml_0902@163.com;郭 鹏(1987-),男,硕士,助理工程师,主要研究方向为嵌入式系统建模与仿真,E-mail:nwpu062475@163.com(通信作者)。

2 预备知识

在描述匿名广播认证机制之前，先给出一些定义和术语。如果 S 是一个有限集，$x \xleftarrow{R} S$ 或 $x \in_R S$ 表示 x 是从集合 S 中随机选择的[7-9]。一个函数 $v(k)$ 是可忽略的，如果对于每个正多项式 $p(\cdot)$ 和足够大的 k，有 $v(k)<1/p(k)$。一个算法 Setup 的输入是 1^k，其输出是 $(p,G_1,G_2,G,g_1,g_2,e) \leftarrow Setup(1^k)$。一种对消息 m 具体的知识证明签名算法，对于 u_1 和 u_2，则有 $y_1=g_1^{u_1} \cdot h_1^{u_2}$ 和 $y_2=g_2^{u_2}$，其中 g_1,h_1,g_2 是有限循环群的生成元 $G_1=\langle g_1\rangle=\langle h_1\rangle$ 和 $G_2=\langle g_2\rangle$，那么对消息 m 的签名可以表示为 $SKP\{(x_1,x_2):y_1=g_1^{x_1} \cdot h_1^{x_2} \wedge y_2=g_2^{x_2}\}(m)$。

q-SDH 假设[9]：假设 $G_1=\langle g_1\rangle$ 和 $G_2=\langle g_2\rangle$ 是 Setup 算法建立的群，那么对于所有的概率多项式时间(PPT)攻击者 A，可忽略函数 $v(k)$ 可以定义如下：

$$(p,G_1,G_2,G,g_1,g_2,e) \leftarrow Setup(1^k); a \xleftarrow{R} Z_p; \Pr[(x,y) \leftarrow A(g_2^a, g_2^{a^2}, \cdots, g_2^{a^q}): x \in Z_q \wedge y=g_1^{1/(a+x)}]=v(k)$$

定理 1[9] 假设在由算法 Setup 选择的群 $G_1=\langle g_1\rangle$ 和 $G_2=\langle g_2\rangle$ 中，q-SDH 假设是成立的。设 $(h_1=g_1,h_2,\cdots,h_k) \in G_1^k$，$A=g_2^a \in G_2$。$O_A(\cdot)$ 是一个预言机，输入是 $x \in Z_p$，输出是一个二元集合 (t_j,x)，$j=1,2,\cdots,k$，则 $e(t_j,A \cdot g_2^x)=e(h_j,g_2)$。那么对于所有 PPT 攻击者 A，可忽略函数 $v(k)$ 可以定义如下：

$$(p,G_1,G_2,G,g_1,g_2,e) \leftarrow Setup(1^k); h_1=g_1; (h_2,h_3,\cdots,h_k) \xleftarrow{R} G_1^{k-1}; a \xleftarrow{R} Z_p; A=g_2^a; Q \leftarrow A^{O_A}(p,G_1,G_2,G,g_2,e,h_1,h_2,\cdots,h_k); \Pr[(t,x) \leftarrow A(Q,p,G_1,G_2,G,g_2,e,h_1,h_2,\cdots,h_k,A): x \notin Q \wedge t^{a+x}=\prod_{j=1}^{k} h_j]=v(k)$$

3 身份保护的安全组网

当前无人设备动态组网可以采用无线自组网络，并利用自组网的动态灵活性，构建适合作业环境的实时网络拓扑，形成一个基于云端中转实现远程控制的无线网络[13]，如图 1 所示。无人操作装置协同操作的组网模式是一种无线自组网网络模型，成员通信属于一个广播通信管理模式，因而需要一种身份保护的密钥管理机制[14]。由于一些敏感任务的需求，各种无人设备的身份信息需要在通信过程中进行保护，为了防止恶意攻击者获知有效身份信息，对认证协议中的身份信息采取匿名方式，结合事后有条件的可追踪机制，能够满足无人操作装置协同操作的安全需求。

针对无人装置协同操作场景，本文提出了一种具有身份保护的安全组网协议，采用匿名认证的方法，通过云端的安全中心(即密钥分发中心，作为系统的管理平台可以认为是可信的第三方)可以实现无人操作装置的前端动态组网以及与后端操作人员的远程控制通信，不仅能提供设备身份信息保护，而且能够保证消息的不可伪造性、不可否认性和机密性。

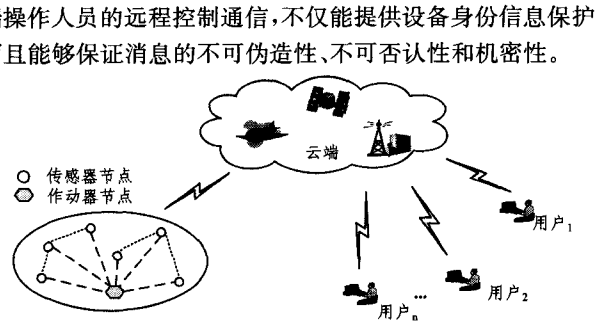

图 1 无人装置协同操作场景

4 匿名广播认证

4.1 根证书

在系统初始化的阶段，密钥分发中心(Key Distributed Center，KDC)需要确定所需要的安全强度，产生它的私钥，并发布相应的公钥信息。以下步骤描述了 KDC 的构建过程。

(1)KDC 定义安全参数，并调用 Setup 算法；

(2)KDC 选择一个安全的单项哈希函数 $Hash(\cdot):\{0,1\}^* \rightarrow \{0,1\}^p$；

(3)KDC 选择一个整数 $a \in_R Z_p$ 作为私钥，并计算 $A=g_2^a \in G_2$。

KDC 选择 $(h_1,h) \in_R G_1^2$，KDC 发布其公钥 $(p,G_1,G_2,G,g_1,g_2,e,h_1,h,A)$ 和 $Hash(\cdot)$ 函数。

4.2 根证书签发

给定 KDC 公钥 $(p,G_1,G_2,G,g_1,g_2,e,h_1,h,A)$，身份为 ID 的用户为了在 KDC 注册，需要有私钥 $x \in_R Z_p$ 和根公钥 $(h,y=h^x) \in G_1^2$，然后与 KDC 执行下面的注册步骤：

(1)用户计算 $y'=g_2^x \in G_2$，并且发送 ID,y,y' 给 KDC；

(2)用户与 KDC 交互，生成 s_{id}，用于证明用户拥有身份 ID 与根公钥 $(h,y=h^x) \in G_1^2$ 之间的绑定关系；

(3)KDC 验证 $e(y,g_2)=e(h,y')$ 成立；

(4)KDC 选择 $\xi \in_R Z_p$，并计算 $z=Hash(ID|y|s_{id}|\xi) \in Z_p$，其中 | 标识字符连接，然后计算 $(t_g=g_1^{1/(a+z)}, t_h=(h_1 \cdot h^x)^{1/(a+z)}) \in G_1^2$；

(5)KDC 将 (ID,y,s_{id},y',ξ) 保存在其数据库中，然后将 (t_g,t_h,z) 发送给用户作为根证书；

(6)用户收到根证书后，验证 $e(t_g,A \cdot g_2^z)=e(g_1,g_2)$ 和 $e(t_h,A \cdot g_2^z)=e(h_1 \cdot h^x,g_2)$ 成立，然后保存 KDC 的公钥 $(p,G_1,G_2,G,g_1,g_2,e,h_1,h,A)$；

(7)用户计算 $(v_1=e(g_1 \cdot h_1,g_2), v_2=e(t_g \cdot t_h,g_2^{-1}), v_3=e(h,g_2)) \in G^3$，并将 (t_g,t_h,z) 保存。

4.3 广播消息

用户计算产生了 $APK(t,t_y)$ 后，当要发送广播消息 M 时，进行如下步骤：

(1)对于 $APK(t,t_y)$，设 $m=(TS|M)$，其中 TS 标识时间戳，M 表示要发送的广播消息；

(2)用户计算关于 m 的消息签名 $s_m=SKP\{(x_1):t_y=t^{x_1}\}(m) \in Z_p^2$；

(3)用户将 $APK(t,t_y)$，m 和 s_m 作为广播消息发送出去。

4.4 验证消息

如果一个用户拥有 KDC 的公钥 $(p,G_1,G_2,G,g_1,g_2,e,h_1,h,A)$，当接收到一个广播消息 $APK(t,t_y)$，m 和 s_m 后，用户验证 s_m 对消息 m 签名的正确性。其中，当 r,z,x 没有公开时，s 和 s_m 的验证计算如下：

$$e(t,A)=e(g_1 \cdot h_1,g_2)^r \cdot e(t,g_2^{-1})^z \cdot e(h,g_2)^{rx}$$

$$e(t^a,g_2)=e((g_1 \cdot h_1 \cdot h^x)^r \cdot t^{-z},g_2)$$

$$t_y=t^x, t^a=(g_1 \cdot h_1 \cdot h^x)^r \cdot t^{-z}$$

$$t^{a+z}=(g_1 \cdot h_1 \cdot h^x)^r$$

$$(t^{1/r})^{a+z}=g_1 \cdot h_1 \cdot h^x$$

4.5 匿名用户追踪

给定一个有效的集合 $APK(t,t_y)$，m 和 s_m，在合法的条件下 KDC 可以恢复出发送消息的用户的身份 ID。对于所有

保存在 KDC 中的 y_i'，KDC 可以计算 $e(t,y_i')\overset{?}{=}e(t_y,g_2)$，从而能够得出 y'，最终找到用户保存在 KDC 中的信息（ID,y,s_{id},y',ξ）。

5 安全组网协议

5.1 安全组网模型

在无人操作平台协同操作的场景中，一个用户需要控制多个传感设备和作动装置来实现实时性要求较高的远程操作，其中需要传感设备和作动装置通过局部组网来实现现场信息的实时共享，如图 2 所示。协议假设，在这些成员组成安全网络之前，每个成员都已和安全中心 KDC 各自建立了安全通道。

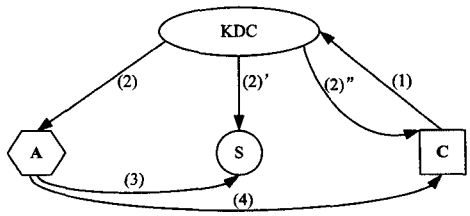

图 2 安全组网模型

每个成员在安全组网模型中执行以下步骤：

(1)控制者 C 利用其私有的安全通道发送一个消息给 KDC，请求组建一个由(A,S,C)构建的安全网络域来实现实时信息的共享；

(2)KDC 收到请求消息后，将发送消息给作动装置 A、传感设备 S 和控制者 C，通知它们加入到一个安全域来共同完成任务；

(3)作动装置 A 收到来自安全通道的 KDC 指令消息后，将通过无线广播方式发送请求安全链接的消息给传感设备 S；

(4)同时，作动装置 A 还将通过无线广播方式发送安全组网的响应消息给控制者 C，告知其已完成一个安全域的动态组网。

5.2 安全组网协议流程

无人装置的协同操作需要构建一个安全域，来实现前端协同操作数据的安全传输，因而每个无人装置都需要在 KDC 中注册并申请一个匿名公钥证书，用于动态安全组网时的相互认证。图 3 中给出了一个典型的安全组网协议流程。

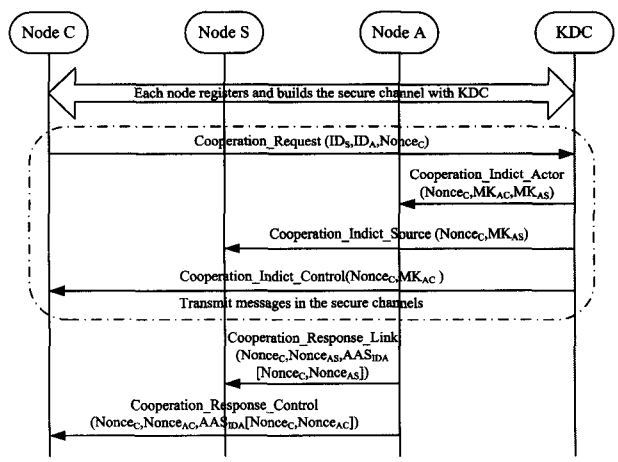

图 3 安全组网协议流程

每个参与到安全组网协议的无人装置都需要符合下述协议流程：

(1)控制台 C 首先发送 Cooperation_request 消息给 KDC，用于发起一个安全组网流程，其中包含了需要协同操作的无人装置身份信息(IDS,IDA)和一个随机数 $Nonce_C$，该随机数用于标识这个组网协议流程。请求消息需要通过 C 和 KDC 之间在注册过程中建立的安全通道进行传输，防止身份信息(IDS,IDA)被 KDC 之外的实体获知。

(2)KDC 收到请求消息后，将检查身份信息(IDS,IDA)的合法性，即该无人装置是否已经注册；KDC 生成两个随机数(MK_{AS},MK_{AC})作为无人装置的主密钥，用于计算生成会话密钥。KDC 发送消息 Cooperation_indict_Actor 给节点 A，其中包含了 MK_{AS}，MK_{AC} 和 $Nonce_C$；并且发送 Cooperation_indict _Source消息给节点 S，其中包含了 MK_{AS} 和 $Nonce_C$；发送 Cooperation_indict_ Control 消息给节点 C，其中包含了 MK_{AC} 和 $Nonce_C$。KDC 发送的这 3 条消息都是采用在无人装置注册阶段建立的安全通道进行传输。

(3)节点 A 收到 Cooperation_indict_Actor 后，产生一个随机数 $Nonce_{AS}$，并计算节点 A 与节点 S 之间的会话密钥 $SK_{AS}=HMAC_{MK_{AS}}(Nonce_C\mid Nonce_{AS})$ 和消息签名信息 $AAS_{ID_A}[Nonce_C,Nonce_{AS}]$；然后，节点 A 保存会话密钥 SK_{AS}，并发送广播消息 Cooperation_Response_ Link 给节点 S。

节点 S 收到广播消息后，首先验证消息中的签名信息的合法性，然后计算 $SK_{AS}=HMAC_{MK_{AS}}(Nonce_C\mid Nonce_{AS})$，并将其保存作为与节点的会话密钥。

(4)节点 A 产生一个随机数 $Nonce_{AC}$，并计算 $SK_{AC}=HMAC_{MK_{AC}}(Nonce_C\mid Nonce_{AC})$，将其作为与节点 C 的会话密钥保存，并计算签名信息 $AAS_{ID_A}[Nonce_C,Nonce_{AS}]$，然后发送广播消息 Cooperation_Response_Control 给节点 C。

当节点 C 收到广播消息后，首先验证消息中签名信息的合法性，然后计算 $SK_{AC}=HMAC_{MK_{AC}}(Nonce_C\mid Nonce_{AC})$，并将其作为与节点 A 的会话密钥加以保存。

6 协议安全性分析

本文利用基于身份加密的公钥技术，构造了一种加密协议。在安全域内，每个成员都向 KDC 申请自己的匿名公钥证书 $APK(t,t_y)$。当一个成员要匿名广播一个消息给其他成员时，他利用自己的私钥对传输消息进行签名，并将自己的匿名公钥证书和签名的消息发送出去。安全域内的成员接收到该消息后，必须使用自己保存的安全参数与收到的公钥证书，才能计算验证消息的签名。

(1)身份信息的保护

由于在广播消息中携带的是无人装置的匿名证书，因此恶意监听者不能获得消息发送者的身份信息。同时，在动态组网的场景中，只用发起组网的控制台指导前端协同操作的无人装置的身份信息，前端的无人设备相互之间只是能认证相互的可信性，并不知道相互的身份信息，因而能够进一步防止身份信息扩散。

(2)签名信息的不可伪造性

广播通信的通信消息中，消息签名使用安全域内动态组网无人装置的私钥进行，只要无人装置的私钥是安全的，那么其他无人装置就无法伪造该消息。

(下转第 201 页)

姜伟,方滨兴,田志宏,等.基于攻防博弈模型的网络安全测评和最优主动防御[J].计算机学报,2009,32(4):817-827

[3] Wang Yuan-zhuo, Lin Chuang, Cheng Xue-qi, et al. Analysis for Network Attack-Defense Based on Stochastic Game Model [J]. Chinese Journal of Computers, 2010, 33(9): 1748-1762(in Chinese)
王元卓,林闯,程学旗,等.基于随机博弈模型的网络攻防量化分析方法[J].计算机学报,2010,33(9):1748-1762

[4] Jiang Wei, Fang Bin-xing, Tian Zhi-hong, et al. Research on Defense Strategies Selection Based on Attack-Defense Stochastic Game Model [J]. Journal of Computer Research and Development, 2010, 47(10): 1714-1723(in Chinese)
姜伟,方滨兴,田志宏,等.基于攻防随机博弈模型的防御策略选取研究[J].计算机研究与发展,2010,47(10):1714-1723

[5] 谢政.对策论导论[M].北京:科学出版社,2010

[6] Lin Wang-qun, Wang Hui, Liu Jia-hong, et al. Research on Active Defense Technology in Network Security Based on Non-Cooperative Dynamic Game Theory [J]. Journal of Computer Research and Development, 2011, 48(2): 306-316(in Chinese)
林旺群,王慧,刘家红,等.基于非合作动态博弈的网络安全主动防御技术研究[J].计算机研究与发展,2011,48(2):306-316

[7] Liu Yu-ling, Feng Deng-guo, Wu Li-hui, et al. Performance Evaluation of Worm Attack and Defense Strategies Based on Static Bayesian Game [J]. Journal of Software, 2012, 23(3): 712-723 (in Chinese)
刘玉玲,冯登国,吴丽辉,等.基于静态贝叶斯博弈的蠕虫攻防策略绩效评估[J].软件学报,2012,23(3):712-723

[8] Shi Le-yi, Jiang Lan-lan, Jia Chun-fu, et al. A Game Theoretic Analysis for the Honeypot Deceptive Mechanism [J]. Journal of Electronics & Information Technology, 2012, 34(6): 1420-1424 (in Chinese)
石乐义,姜蓝蓝,贾春福,等.蜜罐诱骗防御机理的博弈理论分析[J].电子与信息学报,2012,34(6):1420-1424

[9] Carin L, Cybenko G, Hughes J. Quantitative evaluation of risk for investment efficient strategies in cyber security: The queries methodology [J]. IEEE Computer System, 2013, 47(7): 235-242

[10] Gueye A, Walrand J C. Security in Networks: A Game-Theoretic Approach [C]// Proceedings of the 47th IEEE Conference on Decision and Control Cancun. Mexico: Springer, 2013: 829-834

[11] Gordon L, Loeb M, Lucyshyn W. CSI/FBI computer crime and security survey [C]// Proceedings of the Computer Security Institute. San Francisco: Springer, 2012: 12-29

[12] National vulnerability database version 2.3 [EB/OL]. http://nvd.nis.gov/2013

[13] Nash J. Non-cooperative games [J]. Annals of Mathematics, 1951, 54(2): 286-295

[14] Mckelvey T, Richard D, Mclennan K. Gambit: Software tools for game theory[EB/OL]. http://www.gambit-project.org

(上接第 180 页)

(3)签名信息的不可否认性

无人装置采用私钥对广播消息进行签名保护,具有唯一性,而且接收到消息的节点只有使用发送者的匿名公钥证书才能正确验证该消息的合法性,通信消息具有可验证性,是不可否认的。

(4)身份信息的可追溯性

由于无人装置的身份信息在 KDC 中有注册,如果在安全组网过程中采用了匿名证书进行签名,在合法条件下可以追溯签名消息对应匿名证书的真实身份。

结束语 本文分析了无人装置协同操作的安全组网的特性和需求,并针对协同操作前端动态组网的问题,提出了一种具有身份保护的认证协议。该协议采用基于匿名证书的广播认证机制,为安全域内的无人装置动态建立安全传输密钥,并为传输密钥提供机密性、不可否认性和不可伪造性等安全属性。

参 考 文 献

[1] Mark C C. A Discussion of a Modular Unmanned Demonstration Air Vehicle: A GARD CP2600[R]. 2000

[2] John A T. The Air Force is Pursuing Uninhabited Combat Air Vehicles in a Big Way[J]. Air Force Magazine, 2001, 84(8): 64

[3] Jones M C A. Unmanned Aerial Vehicles (UAVS)- an Assessment of Historical Operations and Future Possibilities: AU/ACSC/0230D/97-03[R]. 1997

[4] Siddiqui M S, Seon V C. Security Issues in Wireless Mesh Networks[C]// IEEE International Conference on Multimedia and Ubiquitous Engineering (MUEy07). 2007

[5] Zhang W, Wang Z, Das S K, et al. Security Issues in Wireless Mesh Networks[M]// Wireless Mesh Networks: Architectures and protocols. New York: Springer, 2008

[6] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems: IEEE Std 802.16-2004[S]. 2004: 1-857

[7] Shamir A. Identity-based cryptography and signature schemes [M]// Advances in Cryptology(CRYPTO'84): Lecture Notes in Computer Science 196. Berlin: Springer-Verlag, 1985: 47-53

[8] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[M]// Advances in Cryptology(CRYPTO 2001): Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2001: 213-229

[9] Ke Zeng. Pseudonymous PKI for ubiquitous computing[M]// Public Key Infrastructure: Lecture Notes in Computer Science. Springer Berlin Heideleberg, 2006: 207-222

[10] Tu Jun-yang. Research on Synthesis Data Links of Multi-UAV Cooperative Combat[C]// China Unmanned Aircraft Systems Summit 2008. Beijing, 2008: 735-739

[11] Wang Gang, Wen Tao, Guo Quan, et al. An Efficient and Secure Group Key Management Scheme in Mobile Ad Hoc Networks [J]. Journal of Computer Research and Development, 2010, 47(5): 911-920

[12] Hu Liang, Liu Zhe-li, Sun Tao, et al. Survey of Security on Identity-Based Cryptography[J]. Journal of Computer Research and Development, 2009, 46(9): 1537-1548

[13] Shi Rong-hua, Yuan Qian. A secure hierarchical key management scheme in mobile ad hoc networks[J]. Journal of Central South University (Science and Technology), 2010, 41(1): 201-206

[14] Lauter K. The advantages of elliptic curve cryptography for wireless security[J]. IEEE Wireless Communications, 2004, 11(1): 62-67