

# 网络与终端协同选择及切换机制的研究

马飞<sup>1</sup> 杨飞霞<sup>2</sup> 徐光宪<sup>1</sup>

(辽宁工程技术大学电子与信息工程学院 葫芦岛 125105)<sup>1</sup>

(辽宁工程技术大学电气与控制工程学院 葫芦岛 125105)<sup>2</sup>

**摘要** 提出了一种智能切换机制,用于实现在异构网络中网络与终端的协同选择及切换功能。随着各种业务和应用的发展,异构网络融合是信息和通信技术的必然趋势。根据多接入、多终端等应用环境的要求,采用AHP与GRA等多属性决策理论,为用户选择最佳的目标网络和目标终端,并提出相应的智能切换信令流程,包括网络切换、终端切换、网络与终端联合切换方式,最终构建以用户为中心的多终端智能空间,实现个人移动性管理。仿真表明,该智能切换机制可以有效地实现网络和终端的协同选择,并可以保证在异构网络切换QoS性能,为现代服务业的业务及应用的发展提供可靠的理论依据。

**关键词** 异构网络,网络选择,终端切换,多属性决策

**中图分类号** TN929.5 **文献标识码** A

## Research on Collaborative Selection and Handoff Mechanism for Networks and Terminals

MA Fei<sup>1</sup> YANG Fei-xia<sup>2</sup> XU Guang-xian<sup>1</sup>

(School of Electronics and Information Engineering, Liaoning Technical University, Huludao 125105, China)<sup>1</sup>

(School of Electric and Control Engineering, Liaoning Technical University, Huludao 125105, China)<sup>2</sup>

**Abstract** This paper proposed a novel intelligent handoff mechanism to achieve cooperative selection and handoff functions of networks and terminals in heterogeneous networks. With the development of various services and applications, heterogeneous network convergence is the inevitable trend for information and communication technologies. Considering the requirements of multi-access and multi-terminal environment, this paper took AHP and GRA methods to select the best destination network and the optimal terminal. The paper also put forward terminal selection and handoff signaling flow to implement the individual mobility management for ultimate goal of user-central smart space, which comprises three types of handoff methods including network vertical handoff, terminal handoff along with joint network and terminal handoff. Simulations illustrate that the intelligent handoff can effectively achieve network/terminal selection, and guarantee QoS performance of services and applications in heterogeneous networks for modern service industry.

**Keywords** Heterogeneous networks, Network selection, Terminal handoff, Multiple attribute decision making

## 1 引言

随着新型业务与应用的不断出现,异构网络融合已成为信息与通信技术(ICT, Information and Communication Technology)发展的必然趋势,是支撑现代服务业应用与发展的前提与基础。根据多接入、多终端环境的要求,如何构建智能空间,实现最佳的网络和终端协同选择与切换,成为亟待解决的关键问题。

### 1.1 网络选择的现状

异构网络选择的研究目前已经非常广泛,并已取得了不少成果。在网络选择过程中,将RSS(接收信号强度)等指标看作代价函数而作为判决依据<sup>[1,2]</sup>,但是单一的衡量指标,通常会导致大的偏差。文献[3]提出基于Elman神经网络的自适应网络选择算法,其将用户数量、带宽成本、用户的移动速

度作为代价函数,选择最佳的接入方式访问当前的网络。文献[4]提出了基于模糊逻辑的网络选择算法,其考虑的因素包括接收信号强度、用户移动速度和网络吞吐量等,但面临网络参数全面性、模糊数据配置量大、需要较长的学习过程等问题。选最好的网络实际上是一个典型的多目标决策过程。文献[5-7]采用多属性决策理论计算网络参数的权重,然后从多个可用的网络中选择最优网络。然而每个接入网络所有属性不可能同时达到最优,一个无线网络的所有属性可以通过权重设置来达到目标的总体性能最优的状态。

### 1.2 终端选择的研究现状

终端选择的研究还相对较少,因为大部分的异构网络环境假设用户只有一个终端。现有的研究多考虑基于终端位置或电池供电的终端接口选择问题。文献[8]提出了一个终端切换的方案,即其解决的是异构网络环境中不同用户/终端的选择

到稿日期:2011-04-21 返修日期:2011-07-09 本文受辽宁工程技术大学青年基金(F010201)和博士启动基金(10-434)资助。

马飞(1978-),男,博士,讲师,主要研究方向为网络融合、智能信息处理等方向,E-mail:mafee2007@gmail.com;杨飞霞(1979-),女,硕士,讲师,主要研究方向为智能信息处理等;徐光宪(1977-),男,博士,副教授,主要研究方向为信息管理与控制、智能信息处理等。

问题,而不是单个用户的多终端管理。文献[9]提出一种基于端到端的可重构系统的动态阈值的联合负载控制方法,但方案的选择是实现小区内或网络内用户终端的选择。为了满足多终端的应用需求,本文提出基于个人用户的多终端选择算法来选择最佳的可用终端,从而实现网络/终端移动性的协同管理。

### 1.3 切换技术的研究现状

切换技术的研究主要分布在协议栈的不同层次,如网络层、传输层和应用层,其中每一层都有各自的典型协议,如MIP(移动IP)、mSCTP和SIP。文献[10,11]提出了预切换的方案,即在网络层和传输层上实现流量控制,以降低切换时延。文献[12]扩展TCP报头中的一个可选择的领域字段,并为每个不同的状态分配不同的值,以实现切换的控制。文献[13]提出基于mSCTP协议的UMTS-WLAN切换的判决算法和流程,并仿真了垂直切换的性能。文献[14]提出了一个软切换方案,即通过使用SIP技术,在切换前建立一个新的连接,以避免通信链路断开。

然而,以上不同层次的切换技术均存在一些不足之处。例如,MIP的网络层切换难以适应新的业务或应用的需求,mSCTP切换技术不能实现对用户和终端位置的有效管理,SIP切换最大的问题是切换延时太长而导致其通常无法独立应用。因此,为了解决上述短缺,通常采用跨层设计方法实现

快速平滑切换。文献[15]提出了基于mSCTP和FMIPv6相结合的切换方法,文献[16]提出一个基于SIP和mSCTP的切换方案SmSCTP。这些方法表明,跨层设计的方法能有效地实现异构网络切换的控制,当然这会增加系统开销为代价。

通过分析现代服务业的业务及应用,包括电子商务、数字物流、远程医疗等,可以获取异构网络的共性需求,这对于构建以用户为中心的支持多接入、多终端智能空间异构平台是非常重要的。因此,通过相关的分析和研究,本文提出了网络与终端的协同选择算法,并引入终端切换,以实现跨终端、跨网络移动性管理。

## 2 网络与终端协同选择算法

基于效用理论的多属性决策方法,是将每个属性的权重归一化,作为判决最优方案的评价指标。联合AHP(Analytic Hierarchy Process)和GRA(Grey Relation Analysis)算法理论可用于网络选择,考虑的因素包括网络的QoS性能、业务需求、用户偏好等信息。AHP算法是用来确定不同的网络特性参数的权重,然后利用GRA算法来计算可用的网络标准和理想的网络之间的可相似度,最后将所有可用网络按照相关度依次排序,从而选择最佳的目标网络,该算法的过程如图1所示。

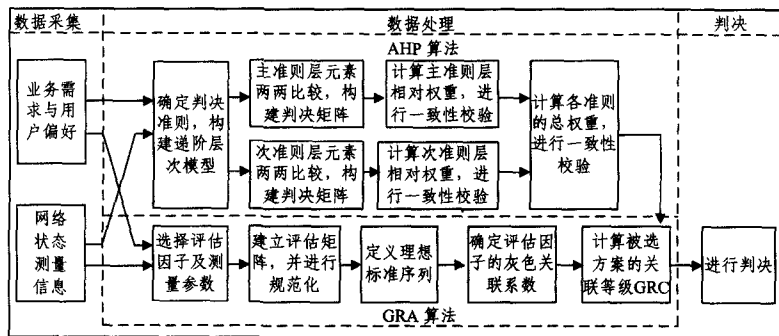


图1 联合AHP与GRA网络选择算法

网络选择的过程分为数据采集、数据处理和决策3个部分。数据采集是为了获取网络状态信息、业务需求和用户偏好等信息,具体包括带宽、吞吐量、时延、时延抖动、可靠性、安全性、成本、用户喜好等,这些信息是衡量网络性能的指标,也是数据处理的对象。网络处理具体包括AHP和GRA算法,首先采用AHP算法根据以上的指标参数建立网络分层模型,如图2所示。由于目标层包含多个子层,因此需要构建多个决策矩阵,分别计算其相对权重,并检查目标层和子层的一致性。用GRA算法建立评估矩阵时,需要指标参数与AHP信息采集保持一致,并建立理想的标准序列,确定影响因素的相关系数。这时,利用AHP算法得出的权重来计算GRC,生成可用网络的灰色等级序列,进而确定最佳的目标网络,完成网络选择过程。

根据多终端环境的需求,本文提出了基于AHP的终端选择算法,建立了以用户为中心的多终端智能空间,层次结构模型如图3所示。其考虑的影响因子包括终端电池性能、处理能力、显示能力、移动性能、用户偏好等因素。假设有 $N$ 个可用的终端和 $M$ 个决定因素,建立决策矩阵,计算权重向量并检验其一致性。最后采用SAW(Simple Additive Weight)算法获得总权重,以选择最优的终端。此外,用户可以在终端

列表中根据个人实际需要或喜好主动选择终端。如果不主动选择,系统则会自动选择默认的终端并实现切换过程。

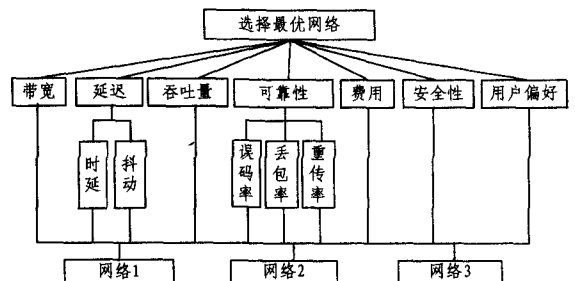


图2 网络选择AHP层次结构

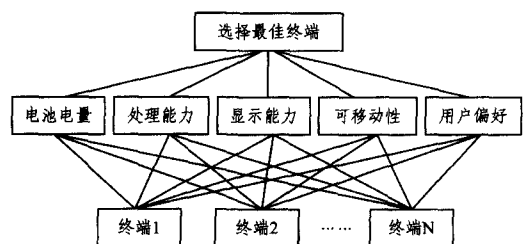


图3 终端选择算法的AHP模型

对异构网络的切换技术而言,目前的研究重点在网络的

选择上而没有考虑终端。然而,在现实的应用环境中,用户可能有多个终端,每个终端可以访问不同网络,那么如何实现多终端之间的切换,构成一个以用户为中心的多终端智能空间,是本文需要解决的重点。因此,本文提出了网络与终端的协同选择,以便为用户选择最佳的终端和接入网络。异构网络与终端的协同选择算法实现过程如下。

- Step1 周期地测量网络状态信息;
- Step2 查询当前可用网络;
- Step3 判断可用网络的数目,如果  $N \leq 1$ , 执行 Step7; 否则执行 Step4;
- Step4 分析用户与网络需求;
- Step5 执行网络选择算法,选定目标网络;
- Step6 判断目标网络是否是当前网络,如果 Yes, 执行 Step8;
- Step7 检测目标网络的可用终端数目,如果  $M \leq 1$ , 执行 Step9;
- Step8 执行终端选择算法;选择目标终端;
- Step9 执行相应的切换流程。

### 3 智能切换信令流程

为了满足个人移动性管理的要求,基于网络适配层的异构网络平台可以根据测量参数、用户喜好等信息,实现网络与终端的协同选择,在选定目标网络与终端后,需要执行相应的切换过程。因此,本文提出了跨网络、跨终端的智能切换,以保证业务的连续性和 QoS 性能。根据目标网络、目标终端与当前网络、当前终端的关系,切换机制包括网络切换、终端切换、联合网络与终端切换,在各切换过程中适配层需要周期性地检测并获取网络/终端的状态或切换请求。网络切换过程如图 4 所示,终端 A\_MT 和 B\_MT 周期性地向网络适配层发送信息 Notify\_Info、反馈网络状态及其切换服务请求等信息。当适配层检测到切换请求后,将查询可用目标网络及其地址信息,发送切换协商请求信息 Request\_Nego\_HO, 终端 B\_MT 利用 N2 接口通过接入网 AN2 与终端 A\_MT 建立链路后进行数据的传输,并断开原链接。

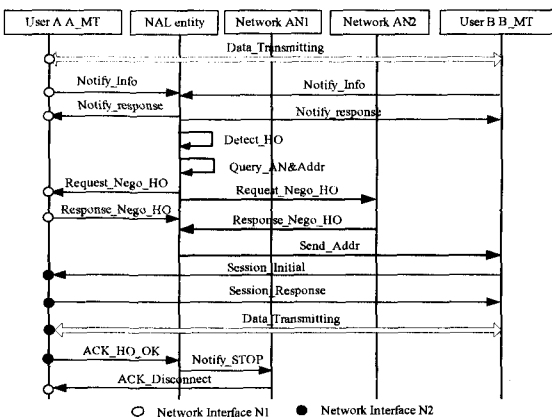


图 4 网络切换信令流程

在以用户为中心的现代服务业应用中,一个用户可能有多个终端,由于在实际应用中极为常见的是媒体流或视频服务,因此以流媒体业务环境下的终端切换的过程如图 5 所示。当适配层检测到切换请求时,查询终端 A\_MT2 的地址,并向终端 A\_MT2 与接入网 AN1 节点发送切换协商请求信息 Request\_Nego\_HO, Media\_SP\_Server 与 A\_MT 建立链接并进行数据传输,断开 A\_MT1 终端的链接。

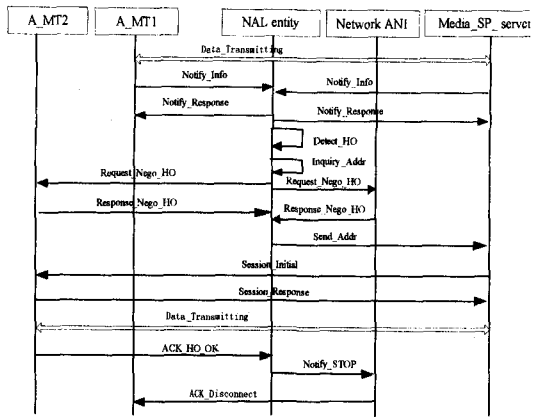


图 5 终端切换信令流程

联合网络与终端切换,即实现不同网络 and 不同终端之间的切换,联合切换过程的时序如图 6 所示。当适配层检测到切换请求时,查询可用目标网络 AN2 及其可用终端 A\_MT2 地址,并向接入网 AN2 节点和终端 A\_MT2 发送切换协商请求信息 Request\_Nego\_HO, B\_MT 与 A\_MT2 通过 Session\_Initial 和 Session\_Response 信息交互建立链接,进行数据传输,断开与 A\_MT1 终端的链接。

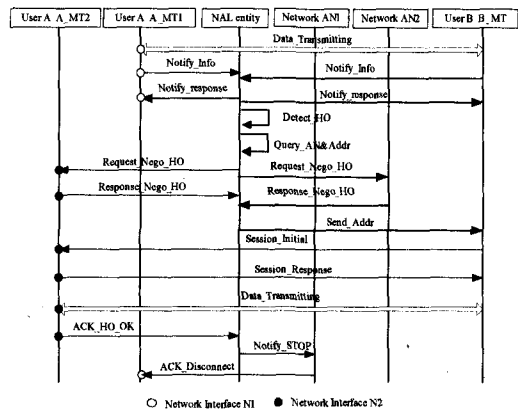


图 6 联合网络与终端切换信令流程

### 4 仿真与分析

本文的仿真内容包括两部分:一是验证网络与终端选择算法的功能,二是仿真切切换过程及性能。本文构建一个异构网络的原型系统,其备选网络包括一个半径 50m、带宽 11Mbps 的 WLAN 网络、速率为 384 kbps 的 WCDMA 网络以及速率为 85.6 kbps 的 GPRS 网络。基站和 RNC 之间的链路为 622 Mbps 的数据速率和 15ms 的延迟时间, RNC 和路由器之间的链路是 622 Mbps 和 0.4ms, 路由器和服务器之间的链路是 100Mbps 和 30ms。本文考虑的业务类型包括 Voice, Video 和 Data, 由于不同业务对于接入网络及终端的需求不同,因此采用不同的选择策略实现不同的业务。

#### 4.1 网络选择仿真

网络选择采用 AHP 与 GRA 算法实现,其候选网络依次是 WLAN, GPRS 和 UMTS, 决策的属性包括带宽、时延、安全性等性能参数。针对不同业务,其网络选择的仿真结果如图 7 所示。从图中可以看出, Video 业务网络性能的要求也相对比其他业务更高,网络的首选序列依次是 WLAN, UMTS 和 GPRS, 其中, WLAN 网络的性能明显比其他的网

络要高,这与实际环境的性能相一致。对于语音服务,网络性能的要求较低,当前网络都可以支持语音业务,其安全性和用户喜欢的程度均超过带宽。Voice业务的网络序列是 GPRS, UMTS 和 WLAN。对于 Data 业务而言,其可用网络序列为 WLAN, UMTS 和 GPRS。

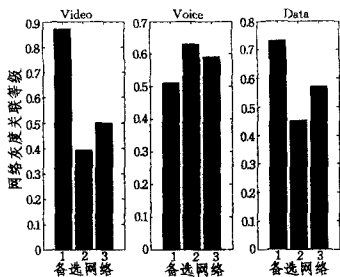


图 7 不同业务的网络选择

#### 4.2 终端选择算法

终端选择过程采用 AHP 和 SAW 算法实现,仿真结果如图 8 所示。其中可用终端依次是智能终端、笔记本终端和普通单模手机。从图中可以看出,Video 业务的可用终端序列是笔记本电脑、智能终端和普通单模手机终端,其中笔记本电脑的性能明显比其他终端好。所有终端均可以支持各种语音服务,语音业务可用终端序列是智能终端、普通单模手机终端和笔记本终端。数据业务的可用终端序列依次是笔记本电脑、智能终端、普通单模手机终端。

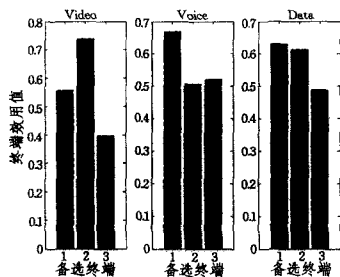


图 8 不同业务的终端选择

#### 4.3 智能切换仿真

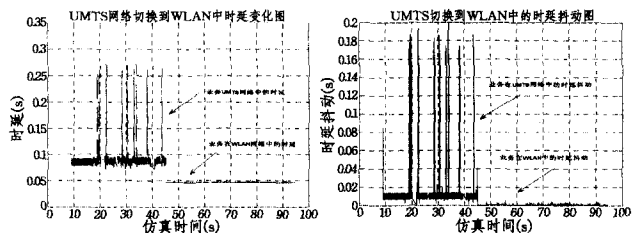


图 9 网络切换的时延

图 10 网络切换的时延抖动

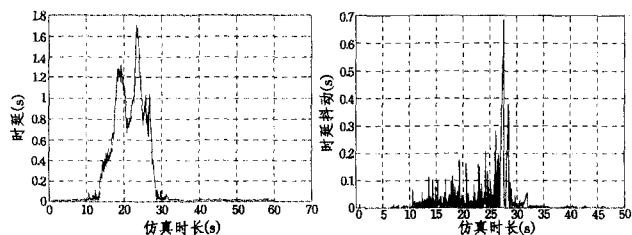


图 11 终端平滑切换的时延

图 12 终端平滑切换的时延抖动

如上所述,切换机制包括 3 种模式:网络垂直切换、终端切换、联合网络与终端切换。在实际应用中,将联合网络与终端切换作为由适配层发起的二次呼叫进行处理,因此,本文终

端研究的是网络切换和终端切换,并侧重于 Video 业务的 UMTS 和 WLAN 之间的切换。在这个场景中,当 MS 移动到重叠区域,从 UMTS 和 WLAN, UMTS 无线切换触发切换的性能如图 9 和图 10 所示。仿真结果表明,在网络切换过程中没有数据包丢失,特别是在时延和抖动性能上, WLAN 比 UMTS 更好。实际上,就其终端切换而言,包括平滑切换、非连续性业务硬切换、连续性业务硬切换,考虑到性能需求,本文重点研究了平滑切换,即原链接断开之前与目标终端建立新的链接。仿真的性能如图 11 和图 12 所示,在时间为 30s 左右、业务性能出现明显恶化时触发切换。仿真结果表明,终端平滑切换时延和抖动较小,并且没有数据包丢失。该切换机制能完成相应的切换功能,能够有效地保证服务的连续性与高性能。

**结束语** 本文基于适配层的异构网络环境,提出了网络与终端的协同选择机制。为了构建以用户为中心的多终端智能空间,本文还提出了终端切换功能,并且给出了网络切换、终端切换以及联合网络与终端切换的信令流程,最后对网络/终端的协同选择及切换机制性能进行了模拟与仿真。仿真结果表明,网络/终端的协同选择及切换机制能够有效地选择最佳目标网络及终端。

#### 参考文献

- [1] Yang K, Gondal I, Qiu B, et al. Combined SINR-based Vertical Handoff Algorithm for Next Generation Heterogeneous Wireless Networks [C]// Proc. Global Telecommunications Conference (GLOBECOM '07). 2007; 4483-4487
- [2] Chang B J, Chen J F. Cross-Layer-Based Adaptive Vertical Handoff with Predictive RSS in Heterogeneous Wireless Networks [J]. IEEE Transactions on Vehicular Technology, 2008, 57(6): 3679-3692
- [3] Wong K D, Dutta A, Burns J, et al. A multilayered mobility management scheme for auto-configured wireless IP networks [J]. Wireless Communications, 2003, 10(5): 62-69
- [4] Wang Q, Mosa A, Abu R. Mobility management architectures based on joint mobile IP and SIP protocols [J]. Wireless Communications, 2006, 13(6): 68-76
- [5] Farooq B, Victor C M, Leung. Automated network selection in a heterogeneous wireless network environment [J]. Network, 2007, 21(1): 34-40
- [6] Sehgal A, Agrawal R. QoS based network selection scheme for 4G systems [J]. IEEE Transactions on Consumer Electronics, 2010, 56(2): 560-565
- [7] Nasser N, Hasswa A, Hassanein H. Handoffs in fourth generation heterogeneous networks [J]. Communications Magazine, 2006, 44: 96-103
- [8] 于高, 陈永生, 郭玉臣. 异构网络查询终端切换整合系统的研究与设计 [J]. 计算机应用, 2009(8)
- [9] 冯志勇, 张平, 张永靖, 等. 可重配置系统中的联合负载控制及其终端选择算法 [J]. 电子与信息学报, 2009(4)
- [10] Choi H H, Song O, Cho D H. A seamless handoff scheme for UMTS-WLAN interworking [C]// Global Telecommunications Conference. Vol 3, 2004: 1559-1564
- [11] Shenoy N, Montalvo R. A framework for seamless roaming across cellular and wireless local area networks [J]. Wireless Communications, IEEE, 2005, 12(3): 50-57

[12] Lee J H, Song J S. TCP Aware Link Layer Agent for Seamless Vertical Handoff in the Cellular/WLAN Integrated Network [J]. Communications Letters, 2010, 14(11): 1017-1019

[13] Nkansah-Gyekye Y, Agbinya J I. Vertical Handoff Decision Algorithm for UMTS-WLAN [J]. Wireless Broadband and Ultra Wideband Communications, 2007: 37-37

[14] Zhang W, Wang J L. A Vertical Soft Handoff Scheme Based on SIP in the Ubiquitous Wireless Network [J]. Computer Sciences

and Convergence Information Technology, 2009: 794-799

[15] Tao M, Yu H W. A smooth handoff scheme based on mSCTP for speed-aware application in mobile IPV6 [J]. Broadband Network & Multimedia Technology, 2009: 586-591

[16] Chen Y S, Chiu K L, Hwang R H. SmSCTP; SIP-based MSCTP Scheme for Session Mobility over WLAN/3G Heterogeneous Networks [C] // Proc. Wireless Communications and Networking Conference. 2007: 3307-3312

(上接第 72 页)

复杂度分析(见 3.2 节), 不进行具体加、解密时间比对。

### 3.4 安全性分析

1. 窃听攻击: 在这种攻击中, 对手企图窃听在传感器与存储数据库间传输的元组  $(c_1, c_2)$ 。因为所有数据都经过加密, 所以对手无法获悉明文。

2. 跟踪攻击: 对手通过跟踪获取用户隐私, 如果已知元组  $(c_1, c_2)$ , 对手仅能知道来自同一传感器网络, 无法获悉更多元组间的关系, 因为每个密文中都有随机数  $n$ , 即使是由同一个公钥加密的两个元组的密文, 它们之间也无法有确定的关系。

3. 替换攻击: 如果攻击者想替换用户及传感器节点的主公钥, 这是不可行的, 因为主公钥经过 LCA 签名产生辅公钥, 通信双方通过检查 LCA 签名来判定主公钥是否合法, 且与相应辅公钥绑定。

4. 攻陷传感器: 假如对手攻陷一个或多个传感器节点, 即使它可以获取存储在传感器上的所有数据, 对手也不能获取明文。因为这些数据是经用户或传感器的主公钥加密, 除非对手可以破解椭圆曲线加密算法, 并且知道用户与 LCA 间的零知识证明, 才能破译  $(c_1, c_2)$ , 由椭圆曲线加密算法的难解性可知, 这是不可行的。

5. 欺骗攻击: 攻击者可以伪造  $(ID_{attacker}, PK_{attacker}^{(Master)}, PK_{attacker}^{(Slavery)})$ , 声称自己是合法用户, 向用户或传感器节点要求数据。但是攻击者的  $PK_{attacker}^{(Slavery)}$  没有经过 LCA 签名, 即用 LCA 的公钥解密  $PK_{attacker}^{(Slavery)}$  无法得到  $(ID_{attacker} | PK_{attacker}^{(Master)})$ , 因此很容易判定攻击者不是经 LCA 认证的合法用户。

6. 匹配攻击: 攻击者可能也会使用不同的串组合, 按照相同语义产生主公钥, 但这个公钥没有经过 LCA 签名, 因此无法拥有辅公钥; 经用户或传感器节点的主公钥加密的元组  $(c_1, c_2)$ , 因为随机数  $n$  的存在, 攻击者无法通过截获大量密文而用伪造的公钥试图用匹配法找出它们之间的关联。

**结束语** 无线传感器网络由于与固定网络和一般无线网络不同, 有其自身的特征, 因此为网络通信和信息安全提出新的挑战。本文结合基于身份的公钥机制及基于轻量级 CA 思想给出了一种应用于无线传感器网络的密钥建立、分配和加密签名一体化方法, 并对其特点、计算复杂性和安全性进行了分析。理论及实验分析表明, 方案具有产生公钥轻量化、公钥验证轻量化、密钥管理无需证书、安全性高, 可抵御无线环境下易于实施的多种攻击, 适用于资源受限的无线环境, 为该类型的网络安全提供了新的解决方案。

### 参考文献

[1] Malan D J, Welsh M, Smith M D. A public-key infrastructure for

key distribution in TinyOS based on elliptic curve cryptography [A] // Proceedings of the 1st IEEE International Conference on Sensor and Ad hoc Communications and Networks [C]. 2004: 71-80

[2] Kohnfelder L M. Towards a practical public key cryptosystem [D]. Boston, MIT Department of Electrical Engineering, 1978

[3] Shamir A. Identity-based cryptosystems and signature schemes [A] // Advances in Cryptology-CRYPTO' 84 [C]. Springer, 1985: 47-53

[4] Dang Lan-jun, Kou Wei-dong, Zhang Jun, et al. Improvement of mobile IP registration using self-certified public keys [J]. IEEE Transactions on Mobile Computing, 2007, 1(4): 167-173

[5] 杨庚, 王江涛, 程宏兵, 等. 基于身份加密的无线传感器网络密钥分配方法 [J]. 电子学报, 2007, 35(1): 180-185

[6] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [A] // Advances in Cryptology-AsiaCrypt' 03 [C]. Springer, 2003: 452-473

[7] Jiang Yi-lin, Lin Chuang, Shen Xue-min, et al. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks [J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 2569-2577

[8] Dong Xiao-lei, Wang Li-heng, Cao Zhen-fu. New public key cryptosystems with lite certification authority [EB/OL]. <http://ePrint.iacr.org/2006/154>, 2006

[9] 潘耘, 王励成, 曹珍富, 等. 基于轻量级 CA 的无线传感器网络密钥分配方案 [J]. 通信学报, 2009, 30(3): 130-134

[10] Dong Xiao-lei, Wei Li-fei, Zhu Hao-jin, et al. EP<sup>2</sup>DF: An efficient privacy-preserving data-forwarding scheme for service-oriented vehicular Ad Hoc networks [J]. IEEE Transactions on Vehicular Technology, 2011, 60(2): 580-591

[11] Tan Cu C, Wang Hao-dong, Zhong Sheng, et al. IBE-Lite: A lightweight identity-based cryptography for body sensor networks [J]. IEEE Transactions on Information Technology in Biomedicine, 2009, 13(6): 926-932

[12] Feige U, Fiat A, Shamir A. Zero knowledge proofs of identity [J]. Journal of Cryptology, 1988, 1(2): 77-94

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

[14] Watro R, Kong D, Cut I S, et al. TinyPK: securing sensor networks with public key technology [A] // Proceedings of the 2nd ACM work shop on Security of Ad hoc and Sensor Networks SASN'04 [C]. New York, ACM Press, 2004: 59-64