

# 无线传感器网络中密钥管理机制约束因素研究

郑彦<sup>1</sup>,王汝传<sup>1,2</sup>,高冉<sup>1</sup>,孙力娟<sup>1</sup>

(1. 南京邮电大学 计算机学院, 江苏 南京 210003;

2. 南京大学 计算机软件新技术国家重点实验室, 江苏 南京 210093)

**摘要:**无线传感器网络综合了传感器技术、嵌入式技术、分布式信息处理技术和无线通信技术,广泛应用于军事、工业、医疗、交通等诸多方面。安全问题是重要的问题,在无线传感器网络中,安全管理最核心的问题就是密钥的管理。在介绍无线传感器网络基本概念、特征基础上,结合密钥管理技术,阐述了网络影响密钥管理机制执行的约束因素,并给出研究适用于传感器网络密钥管理机制的研究思路。

**关键词:**无线传感器网络;传感器节点;安全;密钥管理

**中图分类号:**TP393.08

**文献标识码:**A

**文章编号:**1673-629X(2006)10-0118-04

## Constrains of Key Management in Wireless Sensor Network

ZHENG Yan<sup>1</sup>, WANG Ru-chuan<sup>1,2</sup>, GAO Ran<sup>1</sup>, SUN Li-juan<sup>1</sup>

(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)

**Abstract:** Wireless sensor network (WSN) integrates sensor, embedded computing system, distributed information processing and wireless communication technologies. WSN applications include military affairs, industry, medical treatment, traffic and family. Security is important, key management is the core of security. The basic concepts and characters are introduced, combining with key management technology. Constraints of key management protocol in WSN are discussed in detail and several future research directions are put forward.

**Key words:** wireless sensor network; sensor node; security; key management

## 0 引言

随着无线通信技术和嵌入计算技术的飞速发展,无线传感器网络除了环境监视功能,还广泛应用到军事、工业、医疗、交通和家庭等诸多方面,具有潜在的巨大价值<sup>[1,2]</sup>。无线传感器网络(WSN)由成千上百的传感器节点组成。传感器节点最重要的特点是资源有限,如何最大化地延长节点的生命周期是一个重要的挑战。另外,如何保证节点间的安全通信也是个重要的问题。但是目前许多的研究都关注于节能、网络协议和分布式数据库<sup>[3]</sup>,并没有太多的注意力放在安全问题上。但是在许多应用中,安全问题和其他问题相比同样重要。在 WSN 中,安全管理最核心

的问题就是密钥的管理过程,虽然不同的应用,其安全要求不同,但是对密钥管理机制的要求是相同的。文中分析 WSN 的特点,分析其限制对密钥管理机制的约束。

## 1 传感器网络的体系结构

### 1.1 传感器节点的结构

传感器节点通常是一个微型的嵌入式系统,节点由传感器模块、处理器模块、无线通信模块、能量供应模块 4 部分组成。如图 1 所示。

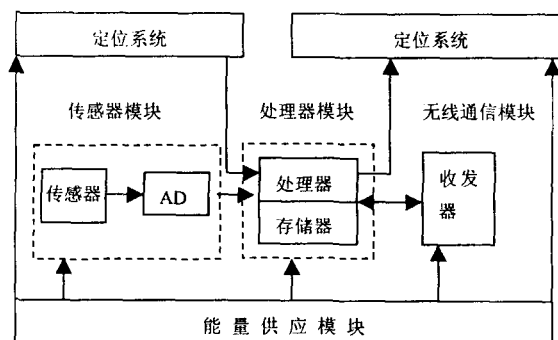


图1 传感器节点结构

传感器模块负责监测信息的采集和数据转换;处理器模块负责处理整个传感器节点的操作,存储和处理本身采

收稿日期:2006-02-05

基金项目:国家自然科学基金(60573141,70271050);江苏省自然科学基金(BK2005146);江苏省高技术研究计划(BG2004004, BG2005038);国家高科技“八六三”项目(2005AA775050);江苏省计算机信息处理技术重点实验室基金(kjs050001,kjs06);江苏省高校自然科学研究计划(04KJB520095)

作者简介:郑彦(1957-),男,江苏南京人,副教授,博士,研究方向为数据挖掘、信息安全以及移动代理等;王汝传,教授,博士生导师,研究方向是计算机软件、计算机网络和网络、信息安全、无线传感器网络、移动代理和虚拟现实技术等。

集的数据以及其他节点发来的数据;无线通信模块负责与其它传感器节点进行无线通信,交换控制信息和收发采集数据;能量供应模块为传感器节点提供运行所需的能量,通常采用微型电池。

## 1.2 传感器网络结构

WSN 系统通常包括传感器节点(sensor node)、网关节点(sink node)和管理节点。如图 2 所示。大量传感器节点通过人工、机械、空投等方式随机部署在被测区域,通过自组织的方式构成网络。

传感器节点把监测到的数据沿着其他传感器节点逐跳地进行传输,在传输过程中,监测到的数据可能被多个节点进行处理(数据融合等),经过多跳后路由到网关节点,最后经过互联网或卫星达到任务管理节点。用户通过管理节点对 WSN 进行配置和管理,发布监测任务以及收集监测数据。传感器节点的处理能力、储存能力和通信能力相对较弱,从网络功能看,每个传感器节点兼顾传统网络节点的终端和路由器双重功能,除了对本地信息收集和处

理外,还要对其他节点转发来的数据进行存储、管理和融合等处理,同时与其他节点协同完成一些任务。网关节点的处理能力、储存能力和通信能力相对较强,它连接 WSN 与 Internet 等外部网络,实现两种协议栈之间的通信协议转换,同时发布管理节点的监测任务,并把收集的数据转发到外部网络。网关节点既可以是一个具有增强功能的传感器节点,有足够的能量供给和更多的内存与计算资源,也可以是一个没有监测功能仅带有无线通信接口的特殊网关设备。

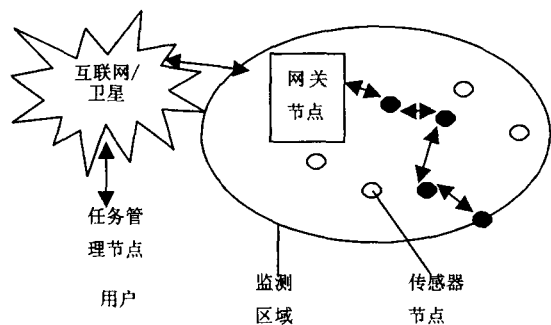


图 2 传感器网络结构

## 1.3 无线传感器网络和无线网络的差别

传统无线网络由几十至上百个节点组成,采用无线通信方式的、动态组网的、多跳的移动性对等网络。其目的:通过动态路由和移动管理技术传输具有服务质量要求的多媒体信息流。通常节点具有持续的能量供给。

WSN 由成千上万的节点组成,节点数目庞大,分布密集,采用无线通信方式,多跳的自组织网络,节点大多是固定不变的。其目的:协作的感知、采集和处理网络覆盖区域内感知对象的信息,并传送给观察者。节点的能量、处理能力、存储能力和通信能力都十分有限。

传统无线网络的设计目标是提高服务质量和高效带宽利用,其次才考虑节省能源;而 WSN 的设计目标是能

源的高效使用。这是传统无线网络和 WSN 最重要的区别之一。

## 2 无线传感器网络的安全要求

WSN 中的安全隐患在于网络部署区域的开放特性和无线电网络的广播特性。网络部署特性是指 WSN 一般部署在应用者无法监控的区域内,所以存在受到无关人员或者敌方人员破坏的可能性。无线电网络的广播特性是指通信信号在物理空间上是暴露的,任何设备,只要调制方式、频率、振幅、相位都和发送信号匹配,那么就能够获得完整的通信信号。在研究 WSN 安全支持中,不同的应有需要满足的安全要求不同,但是所有基于密钥加密的安全解决方案(如数字签名)都要求密钥管理服务,以负责跟踪密钥和节点之间绑定,以及帮助建立节点之间的共同信任和安全通信。对于所有的 WSN 而言,密钥的建立和认证的要求是相同的,下面详细介绍 WSN 中密钥管理的要求<sup>[4]</sup>。

### (1) 机密性。

密钥管理协议中通过在两个或者更多的节点之间建立共享密钥(shared key)来保证消息的机密性,在 WSN 中,所有单跳的邻居节点之间需要建立共享密钥。同样,公共的节点信息,例如节点的标识和公共密钥应该被加密以抵抗流量分析攻击。节点间配置的共享密钥对于未经授权的访问应该具有机密性。节点间的所有通信都应该使用加密机制来阻止窃听攻击带来安全威胁。密钥的建立应该达到任何节点带来的危害都是最小的,从安全的角度来看,在每对通信的传感器节点之间建立惟一的密钥比使用一个全网范围的密钥的安全性更高。

### (2) 真实性。

当保证了密钥的机密性,使用认证确保只有可识别的节点集合可以获得一个特定的密钥。许多密钥管理协议,确保了坚强级别的真实性,但是在分布的 WSN 中并不需要额外的保证,它们可以使用系统/应用协议查证密钥的分发。

### (3) 完整性。

共享的密钥连同其他的机密信息应该能抵制未被授权者发动修改操作,对外部对象进行修改。

### (4) 可扩展性。

WSN 中一般分布 10 至 10 000 个节点,其中能量充足的超级节点或者网关节点的数量小于 10 个。网络中使用的密钥管理协议应该具有可扩展性、节能高效的特性。许多的组密钥机制的相关参数如加密的次数、接收字节数随着组成员数目的增加迅速增加。在传输信息的能耗远大于计算能耗时,应该把网络化分为较小规模的分组,在组内处理信息然后重新加密发送到其他的组中会节省网络的能量消耗。

### (5) 可用性。

对于授权的参与者,密钥管理服务要保证机密性和组

层次的认证,阻止攻击者试图终止网络服务。为了达到消息保护的可用性,必须保证一个安全系统的使用并没有影响传感器节点的正常功能及节点的可用性。如应该保护节点不进行不必要的密钥管理信息的处理,尽可能地减少节点的能量消耗来延长整个网络的生命周期。另外密钥管理功能不应该限制网络的可用性并且不会创造单一的故障点,如创建一个认证管理节点来维护整个网络安全。WSN 中采用的安全机制不应该限制传感器节点数据的可用性或者阻碍 WSN 执行它的任务,并且尽量减少转发数据的延迟和提供数据保护服务。

### 3 影响密钥管理机制的约束

上文介绍了 WSN 中密钥管理的安全要求,下面主要介绍 WSN 影响密钥管理机制执行的约束。可以分别从传感器节点和整个网络的角度来分析这些约束。

#### 3.1 传感器节点的限制

##### (1) 电源能量有限。

传感器节点携带的电池的能量十分有限,且分布区域广、环境复杂,有些地方是人员无法到达的,所以传感器节点通过更换电池的方法补充能源是不可行的,因此应该尽量保存电池的能量,尽可能地延长单个节点和网络的生命周期。所以安全功能要尽可能地减少能量消耗来延长网络的生命周期。当在节点上执行加密算法时,对节点能量的影响必须考虑在内,考虑由于安全功能的处理(如:加密、解密、签名、验证)和安全相关数据的传送(如加密/解密所需的初始化向量)及安全参数的存储(如:密钥的保存)带来额外的能量消耗。在安全领域,保护每条消息所带来的额外能量消耗的量相对较小,主要的能量消耗来自密钥的建立。

##### (2) 计算能量消耗。

传感器节点的主要的计算能量消耗由处理器的能量消耗、处理器的时钟频率和处理器计算安全函数所需的时钟的数目决定。密码学算法和软件执行的效率决定了所需的时钟数目。能量的消耗并不会通过减少时钟频率大幅度地减少,因此可以通过减少电压伏数来降低处理器处理能力来减少能量消耗。

##### (3) 通信能量消耗。

除了计算过程的能量消耗以外,传感器节点之间的信息通讯也消耗能量。传输 1bit 的耗电量远大于计算 1bit 的耗电量<sup>[5]</sup>,节点的无线通信模块是主要的消耗能量模块。无线通信模块存在发送、接收、空闲和睡眠 4 种状态。从图 3 中可以比较出各个模块能量消耗的大小。应该减少不必要的转发和接收,在不需要通信时进入睡眠状态。

实现安全功能所消耗的能量包括密钥管理信息的交换、加密密钥、证书、临时交换号和信息凭证(per-message),如:初始化向量、加密填充、认证标签、签名。所交换的密钥管理信息取决于选择的密钥管理的算法、协议和参与的节点的数目。基于对称的或者椭圆曲线密码学

(elliptic curve cryptography,ECC)的密钥管理算法比 RSA 交换的字节数小,相应的消耗的能量也小。组密钥协议可以利用多点传送节省能量的优点节省能量消耗。信息凭证所消耗的通讯能量取决于交换的信息的数目。

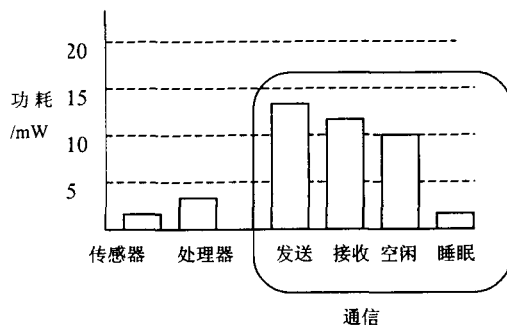


图 3 能量消耗

##### (4) 存储能力。

传感器节点的处理器根据执行的不同功能需要不同类型的存储器类型,对于嵌入式操作系统、安全模块和基本网络必须使用只读存储器(ROM)或者可擦可编程只读存储器(EPROM)。对于应用程序、节点数据和中介计算需要使用随机存储器(RAM)。对于下载的应用程序代码和睡眠期间的数据则需要使用可编程的存储器,如 EEPROM 和 FLASH。

##### (5) 位置定位。

在 WSN 中,位置信息对于 WSN 的监测活动至关重要,因此确定事件的发生位置或获取消息的节点位置是 WSN 中最基本的功能之一。随机布放的传感器节点无法事先知道自己的位置,必须能够在布放后实时地进行定位,但是由于在 WSN 中,传感器节点的能量有限、可靠性差、节点规模大,随机布防且无线模块的通信距离有限,通信易受环境干扰甚至节点失效,WSN 的定位机制必须满足自组织性、健壮性、能量高效和分布式计算等要求。全球定位系统(global position system,GPS)适用无遮挡的室外环境,传感器节点有时会部署在大楼内、密集的植物中,这就不适合采用 GPS 定位。并且 GPS 需要固定的基础设施,能耗高,成本也高,不适合低成本自组织的 WSN。其他的定位技术如 AEther 提出的 Localizer 方法,可以计算出节点间的相对位置。假设节点的位置是惟一的(没有两个节点可以使用相同的位置),可以用节点的位置信息作为消息认证。另外,位置信息还可以用来路由目标到目标的地理位置<sup>[6]</sup>。地理的路由选择可以发送安全相关的命令(如清零, rekey)到被怀疑危及安全的区域。

##### (6) 时钟同步。

时间同步机制是分布式系统基础框架的关键机制,在 WSN 中需要时间同步机制。为了维护时间同步机制,同步信息必须可以抵抗修改攻击。例如,节点发送数据时可能是时间临界的,时间戳的选择会改变数据的意义。

GPS、无线测距等技术用来提供全局时间同步。但是由于 WSN 的特点,以及能量、体积和价格等方面的约束,

使得 GPS, NTP(Network Time Protocol)等现有的时间同步机制不适合于 WSN, 需要修改和重新设计新的时间同步机制来满足 WSN 的要求。

#### (7) 无人照顾。

根据 WSN 任务, 节点在很长时间内都是没人照顾的。例如在敌方环境下的远程勘测任务, 节点在配置后虽然会被远程控制, 但是有可能和己方不再有任何的物理接触。所以物理检测篡改(通过篡改封条)和物理替换(电池替换)都是不可能的。其它的维护, 如软件、密钥更新都必须是远程的。节点无人照顾期间增加了敌方危及密钥资源安全的可能性。

### 3.2 网络的限制

WSN 与有线网络相比, 具有许多在有线环境下不可能遇到的限制。

#### (1) 有限的预配置。

由于 Ad-Hoc 网络的特性, 所预先配置的信息必须是有限的, 以支持一个可灵活的、简易配置的网络。这样在传感器网络中就限制了配置的密码学资料的数量和类型, 而这些资料对于配置一个安全的网络来说是必需的。

#### (2) 数据率/信息包的大小。

数据率和信息包的大小影响了传感器节点的能量消耗。在传感器网络中, 所传送的信息包的尺寸相对较小, 包括头在内大约 30bytes<sup>[7]</sup>。数据率低于 1000bits/s。信息包的大小决定了给定消息的能量消耗的百分比, 如果消息划分为消息包, 消息头占消息开销的很大比例。密码服务也应该遵循包大小限制以降低因传送额外的字节而带来的通信能量的开销。而且在应用密码服务时必须考虑到 WSN 是低数据速率的无线网络, 要减少信息通过网络的延迟时间。

#### (3) 信道误块率。

底层的通信协议提供了差错检测和更正服务。在应用机密性、完整性或认证服务的层上出现的差错将影响它们的验证和认证的处理过程以阻止应用数据的交换。实际上, 在不同的密码学加密和解密的方式, 差错的影响的变化取决于反馈加密和链式加密的使用, 如密码反馈模式(CFB)。

#### (4) 不可靠的通信。

WSN 中包传输是无连接的, 因此是不可靠的。由于信道错误或者阻塞有可能会损害数据包造成丢失数据包。网络协议需要引入更高层的网络协议来增加网络的可靠性。可以引入面向连接的协议如 TCP 来增加网络的可靠性。在分布密钥资源和主要的安全命令时, 必须保证传感器网络的可靠性。

信道衰弱或者节点处于睡眠模式都会引起传感器网络的间歇性连接。信道的衰落与时间、风雨雷电等自然环境和被测区域地势地貌等其他条件有关。节点根据可用的能量、周围事件的检测调至睡眠状态。在发送重要的安全相关的信息(如密钥信息)时, 必须保证可靠地分发这些

信息。可靠性机制必须可以克服间歇性的连接的限制, 否则可能引起密钥同步问题和从网络中隔离一些节点。

#### (5) 延迟。

传感器网络的多跳路由协议会引起网络的延迟。阻塞和节点处理数据也会引起延迟。虽然延迟可能非常小, 但是在安全服务(如认证)中时间是非常重要的因素, 延迟就会带来同步问题。在一些重要的事件报告和密钥分发中, 应该尽可能地减少时间延迟以保证数据的及时性。如果用户收到一些过时数据就会作出错误的判断, 而如果节点使用过去的密钥就会带来密钥同步问题, 就会把这些节点和网络中其他节点的安全通信分离。

#### (6) 单向通信。

在一些情况下, 传感器网络中存在单向通信, 就是一个节点不能兼顾发送、接收数据。例如, 节点处在活动状态, 目标已经被检测到, 节点开始收集和处理数据, 但是并不发送数据以避免被发现。在这种情况下, 降低了节点被检测到的威胁。环境和敌方干扰也会引起通信连接单向性。单向通信会影响高效的密钥分配协议的设计, 通常在协议中, 由参与者共同承担需要消耗大量能量的处理, 相反会出现一方承担大部分的计算, 损耗大量能量的情况。

#### (7) 孤立的组。

由于传感器网络的间歇性的连接和单向通信等情况会造成网络中的分组。这些被隔离的分组有可能不能接收到数据, 如重要的密钥信息。这些分组有可能只是暂时地从网络中隔离, 当它们的路由发生变化时它们就可以重新加入网络。

#### (8) 频繁的路由变化。

随着网络中关键节点的能量减少, 需要改变网络的拓扑结构来平衡网络中节点的能量消耗。频繁的路由变化意味着处理端到端会话的中间节点发生变化。另外, 由于许多的安全服务都是基于 hop-by-hop(逐个跳段)的, 需要和邻居节点建立密钥。如果拓扑结构发生改变, 节点的邻居节点的集合也发生改变, 因此, 密钥建立过程需要重新执行。

#### (9) 未知的收件人。

当数据包在传感器网络中传送时, 如果数据包经过多跳到达最终目标, 数据的发送方并不知道数据包的路径。因此, 节点可以认为在数据传送时, 中间节点是未知的且不可信任的。由此可知, 在端到端或者逐跳之间根据数据的类型和敏感程度采用安全服务。

↑

### 4 结束语

无线传感器网络是一种新的信息获取和处理技术, 其在军事和民用领域都有广泛的应用前景。近年许多的研究关注其安全问题, 密钥管理和安全组播技术被应用于 WSN。但是由于 WSN 的特点, 传统的安全管理方案不能直接被应用。文中从传感器网络和传感器节点的角度分

(下转第 170 页)

流媒体服务器的自适应功能主要利用了 MPEG-4 的可分级编码技术,给不同带宽的用户传输不同质量的数据。

### 2.3.1 Darwin 服务器的总体结构

从应用角度,Darwin 服务器可以抽象为两大系统:文件处理系统和服务器核心<sup>[5]</sup>。

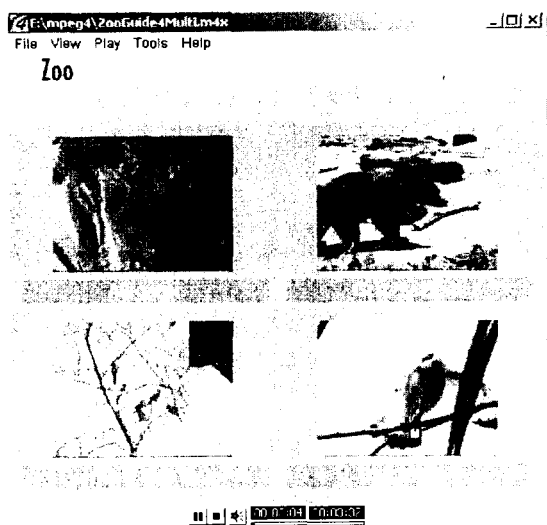


图 6 MPEG-4 播放器

\* 文件处理系统:文件处理系统负责将线索化过的 QuickTime 文件或 MPEG-4 文件通过 RTSP 和 RTP 协议流化出去。所有分析这些文件的代码都被提取出来并且封装在 QTFile 库中。目前 QTFile 可以处理的文件有 QuickTime 文件和 MPEG-4 文件。如果希望让 DSS 支持其他媒体格式,则需要针对相关格式开发文件流化工具。

\* 服务器核心:处理网络 and 协议。主要有 3 个子系统:RTSP 子系统,RTP 子系统和公共服务子系统。

### 2.3.2 自适应 QoS 的实现

文中实现的自适应 QoS 是在 Darwin 流媒体服务器的基础上进行的二次开发。在文件处理系统里面添加了一个 QoS 管理子系统。该系统负责监听客户端的收包情况,判断客户端的带宽适合接收的音频和视频效果,然后发送相应质量的数据包。

(上接第 121 页)

析了影响密钥管理机制执行的约束因素。在下一步的研究中将根据提出的约束因素,分析研究目前比较流行的几种密钥管理协议,指出其不足,提出改进的密钥管理机制。

### 参考文献:

- [1] Abelson H. Amorphous Computing[J]. Communication of ACM,2000,43:74-82.
- [2] Borriello G,Want R. Embedding the Internet:Embedded computation Meets the World Wide Web[J]. Communication of ACM,2000,43:59-66.

QoS 管理主要由 RTP 打包子系统和 QoS 管理子系统协作完成。RTP 打包子系统按一定的规则将 MPEG-4 文件打包,然后 QoS 管理子系统根据客户端的接入带宽自适应地调整发送的数据包,使客户端接受到的媒体质量达到最佳。

### 3 前景展望

文中的流媒体系统包括 3 个部分,编码部分、流媒体服务器部分和播放器部分。

编码部分和播放器部分采用了 IBM 的 ToolkitForMPEG-4SDK.jar 开发包。编码部分包括两个工具,实时的 MPEG-4 制作工具和非实时的 MPEG-4 制作工具。实时的制作工具利用 Mp4live 将实时的音频和视频编码,生成压缩媒体流直接传输,或者生成 MPEG-4 文件,再交给 Darwin 流媒体服务器流化传输。非实时的制作工具利用了 XMT-O 的工作原理,用纯 Java 语言开发。

流媒体服务器部分是在 Darwin 流媒体服务器的基础上,加入了 QoS 管理模块,与客户端的 QoS 模块一起实现质量管理。对 Darwin 流媒体服务器的 RTP 打包模块进行了修改,将 MPEG-4 文件进行特殊形式的打包,并采用“漏桶算法”实现 RTP 的调度,以适应客户端带宽的需要,最终实现自适应的传输。

### 参考文献:

- [1] 石东新,林正豹. MPEG-4 系统分析[J]. 北京广播学院学报(自然科学版),2002,9(1):10-17.
- [2] 江涛,张兆扬. 基于因特网的 MPEG-4 视频流技术[J]. 数字电视与数字视频,2002(8):23-27.
- [3] 周俊茂,李明慧,宋建新. MPEG-4 终端的系统组成及特点[J]. 通信技术,2001(8):33-35.
- [4] 王丽仪. 利用 Linux 实现 MPEG4 流媒体技术[J]. 电脑开发与应用,2003,16(10):32-34.
- [5] 鲁书喜,王川. MPEG-4 流媒体服务的机制与实现[J]. 河南师范大学学报(自然科学版),2004(3):109-111.
- [6] Hemy M,Psteenkiste U. MPEG-4 system streams in best-effort networks[A]. In:Proc IEEE Packet Video 99[C]. New York:[s. n.],1999.45-48.

- [3] Rabaey J,Ammer J,da Silva J L. PicoRadio:Ad-hoc Wireless Networking of Ubiquitous Low-Energy Sensor/Monitor Noder[A]. IEEE Computer Society Workshop on VLSI[C]. Orlando, FL, USA:[s. n.],2000.
- [4] Carman D W, Kruus P S, Matt B J. Constraints and Approaches For Distributed Sensor Network Security[R]. New York, USA: The Security Research Division NAI Inc,2000.
- [5] Kaiser W,Pottier G. The Balance Between Local Computation and Communications in Widely Distributed Wireless Embedded Systems[M]. San Diego, California, USA: Sensoria Corporation,2000.