MIDP 2.0的平台安全性及其安全通信模型

傅鹤岗　屈洪春　周云强
（重庆大学计算机学院　重庆400044）

摘　要　本文介绍了移动计算环境所面临的诸多安全威胁和MIDP2.0新的安全机制及网络模型，分析了MIDP 2.0的平台安全性，并提出了在纯Java环境下构建从J2ME到J2EE的、适用于资源有限MIDP 2.0平台的应用层端到端的安全通信模型，为移动电子商务提出了集移动设备MIDP应用安全环境和客户服务器安全通信于一体的完整解决方案。

关键词　MIDP 2.0，移动电子商务，安全，端对端通信，AES

Security of MIDP 2.0 &Secure Model of End-to-End Communication

FU He-Gang　QU Hong-Chun　ZHOU Yun-Qiang
(College of Computer Science, Chongqing University, Chongqing 400044)

Abstract　In this paper, we give introduction to the threats in mobile computing environment, new security mechanisms and network model in MIDP 2.0, analyse security of MIDP 2.0 platform, and give an integrated solution uses pure Java components to provide end-to-end client authentication and data confidentiality between wireless J2ME based clients and J2EE based servers. This solution can be implemented with the available limited resources of a Java MIDP device, without any modification to the underlying protocols or wireless network infrastructure.

Keywords　MIDP 2.0, M-commerce, Security, End-to-end communication, AES

1　引言

近年来由于移动网络基础设施建设的飞速发展，适用于移动信息设备的软件平台不断完善，为电子商务向移动领域扩展提供了非常有利的条件。移动电子商务[1]主要是通过无线信息设备来进行与货币有关的交易和活动，如移动银行(M-Bank)、移动支付[2](M-Payments)等，在这个过程中涉及到在线支付、内容提供、加密解密、安全认证等问题。移动电子商务融合了当今信息科学发展的前沿技术：一是移动通信技术，二是对称和非对称加密技术。

移动计算最大的优点就是体现了“普及计算”[3](Ubiquitous Computing)的本质，即计算无处不在，易访问性和灵活性，使用移动信息设备，用户可以在任何地点、任何时间对企业计算资源进行实时访问。移动计算也是一个异常广阔和生机勃勃的领域，其设备极度多样化并且共存于移动计算环境中，而J2ME[4] MIDP(Mobile Information Device Profile)[5] 2.0秉承Java技术的跨平台特性、对网络访问和安全的强大支持使其成为这个新兴领域计算平台的首选。

J2ME MIDP在为移动计算带来众多便利的同时由于Java语言本身缺陷和无线环境的诸多威胁而存在许多安全问题，本文将主要讨论移动计算环境所面临的安全威胁和MIDP2.0新的安全机制及网络模型，分析MIDP 2.0的平台安全性，提出在纯Java环境下构建从J2ME到J2EE的、适用于资源有限的MIDP 2.0平台的应用层端到端的安全通信模型。

2　MIDP 2.0的平台安全性

2.1　J2ME及MIDP简介

J2ME是SUN为消费电子产品如移动电话、PDA、机顶盒、汽车导航系统等提供的高度优化的Java运行环境。由于移动设备等嵌入式系统本身的资源局限性，Java虚拟机采用KVM，Configuration的分类是根据计算能力的不同划分为CDC[6]和CLDC[7]。Configuration是一个规范，定义了这类设备的共同Java平台，定义与设备无关的Java虚拟机和核心库，是平台相容性的基础。Profile的分类是根据设备功能划分的，同类功能的设备，其各种硬件条件和需求也相近。Profile是一组API，在某一Configuration的基础上扩展了针对设备特定功能的API，使得标准能够完全适应特殊的设备，彻底发挥设备的功能，MIDP便是J2ME平台最主要的Profile。

J2ME体系可以概括为：由Configuration定义的Java虚拟机运行于设备的宿主操作系统之上，构成整个平台的基础。Configuration提供了基本的语言特性，Profile提供针对设备的特殊功能API和扩展类库。应用程序的运行环境需要一个Configuration和至少一个Profile，多个Profile可以共存，也可以叠加。

2.2　移动计算环境面临的安全威胁

现代的移动信息设备通常运行在特定的移动操作系统之上，如Symbian、Windows CE、Palm OS，而这些设备通常具有在GSM或者GPRS网络基础设施之上的网络连接并连接到Internet，所以移动计算环境面临各种各样的威胁，如Internet和wireless协议漏洞和缺陷导致的安全威胁、移动网络的威胁、Java语言本身缺陷导致的攻击，而且移动服务器必须防止恶意移动客户端的攻击，移动客户端也必须防止恶意服务器的攻击。

来自Internet的威胁可以分为几类：对隐私和秘密数据的攻击，如监听移动网络通信，或者利用通信设备在工作过程中产生的电磁泄露截获有用信息，窃取机密数据；对数据完整性的攻击，如修改用户数据，Trojan木马程序，内存修改等；DoS(Denial of Service)攻击，如阻塞服务器和网络端口，杀死用户进程；对安全认证的攻击，如IP欺骗、伪造认证数据、重

傅鹤岗　副教授，主要研究领域：软件工程，电子商务。屈洪春　硕士研究生，主要研究领域：软件工程理论及应用。周云强　硕士研究生，主要研究领域：网络安全与电子商务。

定向用户网页到其他 URL 等等。

尽管安全问题是 Java 语言考虑的重点，但是仍然有相当的威胁针对 J2ME 应用。从 Internet 中下载的 Midlets 应用可能被恶意程序或者个人篡改，他们可能拦截 TCP/HTTP 连接重定向下载地址，所以不能保证所下载的应用就是你想要的。虽然 MIDP 1.0有沙盒模型的保护，使得 Midlets 可以安全地运行在 SandBox[8]中，但是这要损失很多系统功能和一些 Java 语言的优势，如类安全检查、字节代码检查等。

2.3 MIDP 2.0的安全模型[9]

MIDP 2.0 引入了信任 MIDlets 的新概念，在 MIDP 1.0 中，所有的 MIDlets 都是不可信任的，它们都运行在 Java SandBox 中，MIDlets 无法访问特定的 API 和大部分的系统资源。在 MIDP 2.0中，MIDlets 包可以进行数字签名和验证。通过认证的 MIDlets 被认为是可以信任的，可以访问的系统资源包括电话拨打、网络访问、消息收发和 PIM(个人信息管理)等。

MIDlet 的数字签名和验证是建立在 X.509公钥基础设施 PKI[10]之上的，数字签名的加密算法使用公钥体系的椭圆曲线算法 ECC[11]。通过64位的加密过程后将其放入 MIDlet 的应用说明文档(JAD)中。当 MIDlets 包被下载到移动设备中时设备启动本地验证程序进行认证路径检查、签名检查和过期校验等来确认该 MIDlet 包是否被篡改过。

MIDP 2.0 中的安全策略是将对系统保护 API 的访问划分成细小的权限，每一个 MIDlet 要访问系统资源必须具有该资源的访问权限。应用要访问系统资源的权限必须在其 JAD 文件中预先定义，否则将不能正确地安装。权限的授予有两种方式：自动授权和用户授权，即隐式和显式。权限的作用时间范围有三种：覆盖、会话和快照，一个应用一旦具有某权限的覆盖授权则在从安装到卸载的整个生命周期都有效，会话只存在于一次连接中，快照则只能使用该权限一次，以后需要再使用时则必须重新申请。

MIDP 2.0安全模型的中心环节是保护域，类似 Oracle 数据库权限管理中的角色概念。当一个 MIDlet 包经过校验后确认是可信任的安全包后将被绑定到特定的保护域，每一个保护域包含一组特定的对本地资源访问的权限，这些权限可以授权应用程序访问非信任 MIDlet 不能访问的关键系统 API。MIDP 2.0规范规定 MIDP 2.0兼容的 GSM 和 UMTS[12]设备必须具有以下几个保护域：制造商域(Manufacture Domain)；操作域(Operator Domain)；第三方域(Third-Party Domain)；不信任域(Untrusted Domain)。每一个域都包含有不同程度的访问权限，其中制造商域是权限最大的一个域，它是为制造厂商的预装程序分配的保护域，绑定到该域的应用可以不受限制地访问系统资源。而不信任域则包括了所有的不能通过数字签名验证的 MIDlet 和所有的 MIDP 1.0应用。

MIDP 2.0 规范还引入了新的安全网络协议，根据规范要求，每个 MIDP2.0 兼容的移动设备都必须实现安全 HTTP 协议即 HTTPS 和安全套接字层协议 SSL[13]，使得网络通信得到更多的安全保障。

3 建立应用层的安全端对端通信

3.1 MIDP 2.0的网络模型

J2ME 提供了适合无线企业应用的网络环境－通用网络架构 GCF[14](Generic Connection Framework)，GCF 建立在 J2ME 体系的 CLDC 层，而在 CLDC 之上的 MIDP 提供的 HttpConnection 接口封装了 HTTP 连接所需要的方法。然而 Sun 的规范不要求移动设备厂商支持 TCP 或者 UDP 等传输层协议，仅仅要求 MIDP2.0兼容设备必须实现 HTTP 协议，使用 TCP 流传输或者 UDP 数据报传输的厂商必须自己实现 TCP/UDP 协议。庆幸的是 HTTP 可以在 TCP/IP 上实现，也可以在非 TCP/IP 如 WAP[15]协议栈上实现，这必须要求在无线网络和 Intenet 之间增加一个协议转换层－WAP 网关，MIDP 设备到 WAP 网关的通信由建立在 WAP 协议栈之上的 HTTP 实现，WAP 网关到有线网络之间的通信由 TCP/IP 和 HTTP 实现，所有支持 WAP 的 GSM 移动设备和支持蓝牙技术的无线设备都可以运用到这个通用网络计算环境中。

3.2 在传输层实现安全通信的限制

在传输层中，安全协议分成两个部分，一部分是在移动设备到 WAP 网关之间，包括无线传输层安全协议 WTLS[16]，WTLS 是传输层安全协议 TLS 在无线环境的优化和扩展。SSL 则负责 WAP 网关到 Internet 服务器端的安全数据通信。这样的通信模式具有的优点是能适应无线环境计算能力、存储能力限制的要求，但必须要增加 WAP 网关作为协议转换，这将是整个端到端通信中的薄弱环节，存在很多安全隐患，因为在传输层进行协议交换时的数据没有任何保护，非常容易受到恶意软件和个人的攻击，而且所有的无线设备都必须通过 WAP 网关访问 Internet 服务器，这将是通信性能的瓶颈，这就是通常所说的“WAP 缺口”。

WAP2.0提出了解决“WAP 缺口”的方案，是在无线设备和 WAP 网关之间增加 Internet 标准协议如 TCP/IP 及其上层协议，这样就无须在传输层进行协议转换，用户数据就可以不暴露出来。但是增加 TCP/IP 会大大增加无线设备的处理负担，而且 WAP2.0将用 XHTML 代替 WAP1.x 中的 WML，也要更进一步增加无线网络传输的数据量，增加应用程序的响应时间。

可见要在传输层实现端对端的通信有诸多限制，一是“WAP 缺口”，二是 WAP2.0的解决方案会大量增加移动设备的 CPU 处理负担、内存开销和应用程序的响应时间，这对本身资源有限的移动设备的市场推广应用来说无疑是很大的限制，而且 WAP 的市场份额在逐年减少。在传输层建立安全通信必须依赖现存的网络硬件平台及协议，这些底层的改动将影响上层应用。为了解决以上存在的问题，建立稳定的端到端安全通信必须在应用层实现。

3.3 在应用层实现安全通信

移动电子商务如移动银行、在线支付等交易过程要求很高的数据安全性，在通信的过程中必须进行符合特定规范要求的加密。现代密码系统的安全性都是基于密钥的安全性，而不是基于算法的安全性，根据密钥的不同分为两种体系，一种是私钥体系，这个系统中用于加密的密钥和用于解密的密钥是相同的，我们将其称之为对称密码算法，如 DES、RC4和 AES[17]算法；另一种是公钥体系，加密和解密的密钥不同，称之为公开密钥算法，如 RSA 算法和椭圆曲线密码算法 ECC 等。公钥体系算法一般用于数字签名、密码交换和密钥管理等领域，它们都是基于公认的 NP 难问题，计算时通常长时间占据 CPU 和消耗大量系统资源，这对于 CPU、内存等关键资源非常宝贵的移动平台来说是非常难以实现的，而且应用程序会由于加密解密产生用户难以忍受的延迟，因而公钥体系算法并不适合移动平台。而私钥算法虽然没有公钥体系那样难以攻破，但是它的算法相对简单，运算时间短，占用系统资源较小，应用于移动平台是非常合适的。AES 是美国国家标准技术研究所 NIST 旨在取代 DES 的21世纪的加密标准，该算法设计的特点是由一个密码学上的弱函数 f 与 r 个子密钥迭代 r 次组成，混乱和密钥扩散，抵御已知明文的差分和线性攻击，采用可变长密钥和分组。综合上述分析，我们选择 AES 作为安全通信的加密标准，加密算法采用 Rijndael[18]算法，明文采用128位分组，所以密钥长度为128位。

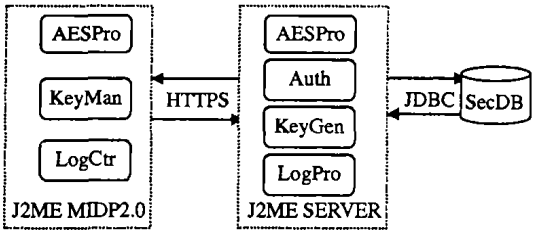


图1 移动设备和J2EE服务器组件结构

整个应用层的通信模型分为客户端(MIDP)和服务器端(J2EE[19]Web Server)两部分,组成一个纯Java计算环境,如图1所示,客户端由以下几个模块组成:一是AES算法处理模块(AESPro),负责用Rijndael算法对数据进行加密和解密处理;二是会话密钥管理模块(KeyMan),负责对数据通信加密的密钥进行管理;三是业务逻辑控制模块(LogCtr),负责整个交易的逻辑控制。服务器端由以下几个模块组成:一是服务器安全认证模块(Auth),负责对客户端进行身份认证;二是密钥初始化模块(KeyGen),负责随机产生共享密码段和数据传输密码;三是业务逻辑处理模块(LogPro),负责相应客户端的业务请求,还有和客户端一样的AES算法处理模块(AESPro);后端安全数据库服务器(SecDB),负责存储用户信息和对应密钥,字段如表1所示。

表1 安全数据库关键字段结构

PINCode	PassWord	ShareID1	ShareID2	AESCipherA	AESCipherB
移动用户身份唯一标识(64位)	移动用户访问服务器密码	上一次共享密码段(64位)	下一次共享密码段(64位)	数据传输密钥A(128位)	数据传输密钥B(128位)

系统采用两种密钥,一种是128位数据传输密钥,用来对客户端和服务器端的数据交换进行加密和解密,采用密钥对方式进行双向加密解密,数据传输密钥A用于客户端数据加密和在服务器端解密,数据传输密钥B用于服务器端数据加密和客户端解密;另一种是128位会话密钥,用于对数据传输密钥进行加密和解密。

移动用户用其64位身份标识(PINCode)到交易机构注册取得密码和初始共享密码段(ShareID),服务器端将该用户信息包括PINCode、PassWord、ShareID等存储在安全数据库中,将ShareID用两个PINCode共128位作为密钥对其进行AES加密,将加密结果和其他客户端应用程序一起打包到JAR文件中供该用户下载。用户用自己的移动设备以PINCode和PassWord作为参数向服务器发出下载请求,服务器响应请求验证用户身份后将客户端MIDP应用发给用户,客户端收到该JAR文件后用两个PINCode共128位作为密钥对ShareID解密,并将解密后的ShareID和PINCode结合成128位会话密钥并存储在本地,如图2所示。

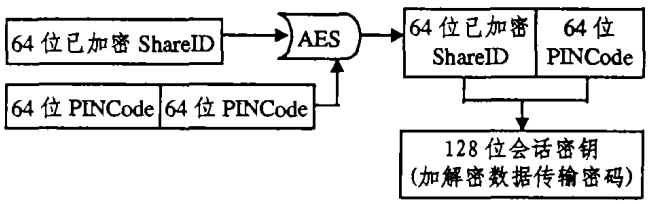
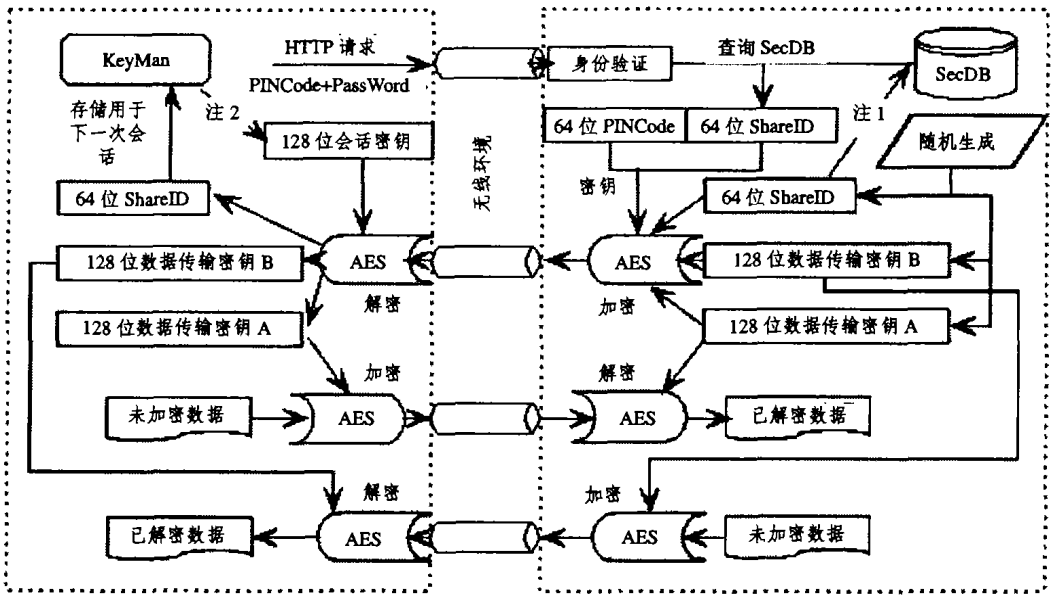


图2 会话密钥计算过程

由于HTTP是无状态的协议,它的每一次请求都是独立的,HTTP协议规范不要求其实现将属于特定用户的所有请求看成一次会话,因此在本模型中用cookie来记录特定用户的会话信息,会话过程如图3所示。



注1: 产生新的ShareID在数据传输密钥传输成功后覆盖旧的ShareID
注2: 下一次会话开始时获取新的ShareID来产生128位会话密钥

图3 J2ME MIDP和J2EE Web Server的会话过程

会话开始时,客户端MIDlet以PINCode和PassWord为参数连接服务器,服务器先进行身份认证,如果不能通过认证就返回拒绝服务信息并且结束会话,如果用户通过身份认证则启动密钥初始化模块,产生64位随机数作为下一次的共享密码段ShareID和128位数据传输密钥对存储在安全数据库中。服务器用ShareID和PINCode结合成的128位会话密钥

对数据传输密钥和新的共享密码段进行加密后传输到客户端，客户端用会话密钥对数据传输密钥和新共享密码段解密后放置在KeyMan模块中返回存储成功，服务器则用新的共享密码段替代安全数据库中的旧共享密码段，成功后发给客户端初始化成功信息并在客户端显示其所提供的服务，然后开始业务动作。以后的数据传输都由会话开始产生的数据传输密钥加密和解密，直至会话结束。新一轮的会话便会重新对客户端进行身份认证，启用上一次随机产生的共享密码段，进行服务器端初始化产生新的数据传输密钥，因而每一次连接的会话密钥和数据传输密钥对都不相同，这样大大提高了数据交换的安全性。

应用层的端对端安全通信模型对数据的加密和解密不依赖下层协议和硬件，只采用MIDP2.0规定的HTTPS协议，受底层变化影响很小，有很强的可移植性。采用的对称加密算法标准AES Rijndael，速度快、低延迟、消耗系统资源少，不在传输层进行协议转换，所以不存在由"WAP缺口"所带来的安全威胁，可见是一个比较理想的安全通信解决方案。

结束语 本文介绍了移动计算环境所面临的诸多安全威胁和MIDP2.0新的安全机制及网络模型，分析了MIDP 2.0的平台安全性，并提出了在纯Java环境下构建从J2ME到J2EE的、适用于资源有限的MIDP 2.0平台的应用层端到端的安全通信模型，为移动电子商务提出了集移动设备MIDP应用安全环境和客户服务器通信安全于一体的完整解决方案。

参考文献

1 Schwiderski-Grosche S, Knospe H. Secure mobile commerce. Electronics & Communication Engineering Journal, Oct. 2002
2 Antovski L, Gusev M. M-Payments. In: 25th Int. Conf. Information Technology Interfaces ITI, Cavtat, Croatia, June 2003
3 Boddupalli P, Al-Bin-Ali F, Davies N, Friday A, Storz O, Wu M. Payment Support in Ubiquitous Computing Environments. In: Proc. of the Fifth IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2003)
4 Ericsson. Mobile Applications with J2ME, a White Paper. July 2001
5 http://java.sun.com/products/midp/index.jsp, [Online], 2004 Available, JSR37, JSR118
6 http://java.sun.com/products/cdc/index.jsp, [Online], 2004 Available, JSR36, JSR218
7 http://java.sun.com/products/cldc/index.jsp, [Online], 2004 Available, JSR30, JSR139
8 Schmid M, Hill F. Protecting Data from Malicious Software. In: Proc. of the 18th Annual Computer Security Applications Conf. ACSAC, 2002
9 Kolsi O, Virtanen T. MIDP2.0 Security Enhancements. IEEE, 2004
10 Dankers J, Garefalakis T, Schaffelhofer R, Wright T. Public key infrastructure in mobile systems. Electronics & Communication Engineering Journal, Oct. 2002
11 Raju G V S, Akbani R. Elliptic Curve Cryptosystem and its Applications. IEEE, 2003
12 Richardson K W. UMTS overview. Electronics & Communication Engineering Journal, June 2000
13 Kambourakis G, Rouskas A, Gritzalis S. Using SSL/TLS in Authentication and Key Agreement Procedures of Future Mobile Networks. IEEE, 2002
14 Enrique Ortiz C. The Generic Connection Framework. Aug. 2003. http://developers.sun.com/techtopics/mobility/midp/articles/genericframework.html.
15 Forum WAP. WAP 2.0 Technical White Paper. Jan. 2002
16 Levi A, Savas E. Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol. In: Proc. of the Eighth IEEE Intl. Symposium on Computers and Communication, ISCC 2003
17 The Advanced Encryption Standard (Rijndael). [Online], 2004. Available at: http://home.ecn.ab.ca/~jsavard/crypto/co0401.htm
18 Daemen J, Rijmen V. The Design of Rijndael. published bySpringer-Verlag, 2002
19 Sun Microsystems. Java 2 Platform Enterprise Edition Specification, v1.4. Final Release 11/24/2003

（上接第148页）

的生命周期会超过两个节点的生命周期。但在一些情况下（如恶意攻击、密钥被破解等），密钥将失效或过期，因而共享密钥需要随着时间进行更新。密钥更新可以看作是节点密钥的自我撤销过程，需要基站重新分配给该节点一个规模为 k 的密钥环，并重新启动单跳密钥发现和多跳密钥建立过程。

4 性能分析

4.1 安全性分析

在单跳密钥发现过程中，节点 A 广播的是密钥标识符集而不是密钥本身，从而提高了通信双方建立共享密钥的安全性，攻击者无法从标识符集中获取任何与密钥有关的信息，由于它不知道 K_{AC}，因而无法伪造节点 C 对 A 的响应信息；在多跳密钥建立过程中，节点 A 在发送信息给节点 C 之前进行了身份认证，确信节点 C 不是恶意节点，且发送的消息都使用会话密钥进行了加密，因而攻击者无法破解消息的内容；在密钥撤消过程中，密钥撤消指令是由基站使用与每个传感器节点共享的密钥加密后进行单播通信的，从而有效地防止了攻击者冒充基站发布虚假的密钥撤消指令。当某节点受到攻击后，邻近节点可以向基站报告该节点行动可疑，并进行概率否决投票，当票数达到某个门限值时，基站考虑对该节点拥有的密钥集进行撤消，从而最小化部分节点受攻击后对整个网络安全的影响范围。

4.2 效率分析

在构建传感器网络密钥管理方案时，我们充分考虑到节点计算速度、电源能量、通信能力和存储空间非常有限的特点，密钥建立、更新和撤消等协议和算法都设计得比较简单，并避开了代价昂贵的公钥运算，完全使用对称加密算法来实现，计算、存储和通信开销都较小，从而使得方案的执行效率大大提高。

结论 本文提出了一种传感器网络中的密钥管理方案，它支持密钥建立、更新和撤消等过程。同时，考虑到传感器节点计算速度、电源能量、通信能力和存储空间非常有限的实际情况，方案中有关的协议和算法设计得都比较简单，并使用对称加密算法来代替了代价昂贵的公钥算法，从而使得方案的各种开销都比较小，执行效率大大提高。

参考文献

1 Akyildiz I F, Su W, Sankarasubramaniam Y, et al. A survey on sensor networks. IEEE Communications, 2002, 40(8): 102～114
2 Chan H, Perrig A. Security and Privacy in Sensor Networks. IEEE Computer, 2003, 36(10): 103～105
3 Perrig A, Stankovic J, Wagner D. Security in Wireless Sensor Networks. Communications of the ACM, 2004, 47(6): 53～57
4 Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proc. of IEEE 2003 Symposium on Research in Security and Privacy, Berkeley, CA: IEEE Computer Society, 2003. 197～213
5 Jolly G, Kuscu M C, Kokate P, et al. A Low-Energy Key Management Protocol for Wireless Sensor Network. In: Proc. of the Eighth IEEE Intl. Symposium on Computers and Communication (ISCC'03). Turkey: July 2003, 1: 335～340
6 Du W, Deng J, Han Y S, Varshney P. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security (CCS), Washington: ACM Press, Oct. 2003. 1～10
7 Wadaa A, Olariu S, Wilson L, et al. Scalable Cryptographic Key Management in Wireless Sensor Networks. In: Proc. of the 24th Intl. Conf. on Distributed Computing Systems Workshops (ICDCSW'04). Tokyo: IEEE Computer Society, March, 2004. 796～802
8 Du W, Deng J, Han Y S, et al. A Key Management Scheme for Wireless Sensor Networks Using Deploying Knowledge. In: Proc. of INFOCOM2004. Hong Kong: IEEE Computer Society, March 2004. 172～183