A Study on the Application of Symmetric Ciphers and Asymmetric Ciphers in Wireless Sensor Networks*

JIN Ning, ZHANG Daoyuan, GAO Jianqiao, WANG Zhaofeng*
(*College of Information Engineering, China Jiliang University, Hangzhou* 310018, *China*)

Abstract: Security issues are badly needed in the data acquiring and transmission in wireless sensor networks which can be widely used in many areas. The traditional complex encryption algorithms could not be directly used in the fields of wireless sensor networks. This is due to the constraints of limited capability of CPU computing, storage space, narrow bandwidth and battery support energy. After analyzing a typical symmetric cipher (e. g. Data Encryption Standard, DES) and an asymmetric cipher (e. g. elliptic curve cryptography), the CPU executing time, RAM/ROM space and energy consumption of these two cipher algorithms are compared and studied on the platform of MICAz. Experiment result shows that the DES has advantages of its algorithm efficiency, RAM/ROM space and energy consumption, but it is hard to do key management, and is less security compared with elliptic curve cryptography. Either DES or elliptic curve cryptography is application-specific.

Key words: wireless sensor networks; security; DES; elliptic curve cryptography
EEACC: 6150P **doi**: 10.3969/j.issn.1004-1699.2011.06.019

对称密码和非对称密码算法在无线传感器网络中应用研究*

金 宁*, 张道远, 高建桥, 王赵峰
(中国计量学院信息工程学院, 杭州 310018)

摘 要: 无线传感器网络许多应用领域需要保证数据获取和传输过程中的安全性。传感器网络节点的计算、存储、通信以及能量等资源十分有限, 传统加密算法因计算复杂并占用大量资源而无法直接应用于无线传感器网络。在阐述和分析典型对称加密体制的 DES 和非对称加密体制中的椭圆曲线密码 ECC 基础上, 基于 MICAz 无线传感器网络节点平台, 对上述两种密码体制在算法时间、空间、能耗和安全性等方面进行了分析和比较。实验结果表明, 在算法用时、RAM/ROM 占用以及能耗上 DES 算法占优, 而在密钥数量及密钥管理复杂性上 ECC 占优, 两种加密算法适合不同需求的 WSNs 应用场景。

关键词: 无线传感器网络; 安全; DES; 椭圆曲线密码体制
中图分类号: TP393.08 **文献标识码**: A **文章编号**: 1004-1699(2011)06-0874-05

无线传感器网络(Wireless Sensor Networks, WSNs)通常部署在无人值守的区域, 传感器节点之间使用无线通信链路进行数据传输, 节点的计算、存储、通信以及能量等资源都十分有限。同时, WSNs 节点具有分布性、移动性和独立性等特点, 使得无线传感器网络很容易受到各种入侵和恶意攻击的威胁。在军事、智能安全防盗、医疗卫生健康远程监护等领域, 无线传感器网络数据采集和传输的安全性显得尤为重要[1-7]。

数据加密/解密的安全体系常取决于对动态数据流的保护。由于传感器节点资源受限的特点, 一些应用于传统网络中的复杂数据加密解密算法移植到 WSNs 中会产生一些新的矛盾。因此, WSNs 中应用安全机制要考虑轻量化问题, 同时也带来了挑战。

作为比较, 本文采用了典型对称密码体制中的数据加密标准(Data Encryption Standard, DES)和非对称密码体制的椭圆曲线密码(Elliptic Curve Cryptography, ECC)算法[13,16-18], 对二种加密算法在无线传感器网络平台上的相关应用特性进行了分析和实验。对两种算法各自在算法时间、空间、能耗和安全性等方面进行了对比分析, 得出了一些有用的结果。

项目来源: 浙江省科技计划项目(2008C23022)
收稿日期: 2011-03-29 **修改日期**: 2011-04-22

1　对称加密方案和非对称加密方案

对称密码体制和非对称密码体制在现代密码技术中使用非常广泛。对称密码系统中对数据进行加密的密钥和对数据进行解密的密钥是相同的,即使两者不同,也可以通过一定的关系知道其中一个可推导得到另一个,加密方和解密方公用一套密钥,比较典型的如数据加密标准 DES 和高级加密标准 AES 等。非对称密码体制中加密数据的密钥和用来解密数据的密钥是不相同的,并且无法从其中一个密钥推导出另一个密钥,这样对密钥的保护力度就比较大,典型的非对称密码系统有椭圆曲线密码 ECC 和 RSA 算法等[13]。作为比较,我们分别研究了 DES 和 ECC 算法,并对二种算法做了相关对比实验。

1.1　数据加密标准 DES 介绍

DES 是使用最广的分组加密算法之一,是一种典型的对称密码体制[13-14],其加密的主要思想是:

(1)给定 64 位明文首先经过初始置换 IP 变换,按 IP 置换后将明文重新排列,前 32 位作为 L0,后 32 位作为 R0。

(2)再将 56 位密钥经过 DES 固有的密钥算法,得到 16 个 48 位子密钥,用 k1,k2,k3,…,k16 表示,分别供 16 次迭代算法使用。

(3)通过 16 轮完全相同的算法变换后,得到两个 32 位的 L16 和 R16。

(4)最后将 R16 和 L16 进行 IP^{-1} 置换(IP 变换的逆变换)得到 64 位密文,即密文结果为 $IP^{-1}R16L16$。

DES 解密过程是加密的相反过程。密钥的使用顺序和加密时相反,即用 k16,k15,…,k1 表示,解密和加密算法程序通用(即加密和解密的算法空间占用是一样的,此项数据可以在下面的图 1 相关实验中得到体现)。

有 n 个节点的 WSNs 网络,采用 DES 算法整个网络密钥数量为 $O(n^2)$,若 n 较大,则密钥数量大,因而密钥管理较复杂。

1.2　椭圆曲线集成密码体制 ECIES(Elliptic Curve Integrated Encryption Scheme)介绍

椭圆曲线定义:令素数 $p \geqslant 3$,F_p 是模 p 的有限域,$a,b \in F_p$,使得有限域 F_p 上的椭圆曲线 $E: y^2 = x^3+ax+b$ 是满足同余方程的全部解 $(x,y) \in F_p$ 和一个无穷远点 O 组成,这里参数应满足以下条件:

$$4a^3+27b^2 \neq 0 (\mathrm{mod}p) \qquad (1)$$

G 为椭圆曲线 $E\mathrm{p}(a,b)$ 上的一个基点,n 为基点 G 的阶,即有 $nG=O$ 的关系。

设 $K=kG$(其中 K 和 G 为椭圆曲线 $E\mathrm{p}(a,b)$ 上的点),k 为小于 n 的整数。如果给定 k 和 G,则计算 $K=kG$ 比较容易,但是给定 K 和 G,求 k 则是非常困难的。我们把 $k(k<n)$ 称为椭圆曲线加密算法的私钥,由 WSNs 节点秘密保存,而 K 作为该节点相对应的公钥,可以向 WSNs 网络内所有节点公开,可广播传输给所有节点,或节点在网络初始化时设定。

WSNs 中两个节点 A 和 B 利用椭圆曲线加密 ECC 进行保密通信的实现过程为:

(1)某一节点 A 选定一条椭圆曲线 $E\mathrm{p}(a,b)$,其中 a,b 满足式(1),并取椭圆曲线上任意一点作为基点 G。

(2)A 随机选择一个私钥 k,秘密保存在节点 A 中,并根据 $K=kG$ 生成与之对应的公钥 K。

(3)A 将 $E\mathrm{p}(a,b)$ 和椭圆曲线上的点 K 和 G 传给节点 B。

(4)B 接到 $(E\mathrm{p},K,G)$ 信息后,将待传输的明文 m 编码到椭圆曲线 $E\mathrm{p}(a,b)$ 上一点 M,并产生一个随机整数 $r(r<n)$,r 作为 B 的私钥秘密保存。

(5)B 计算点 $C_1=M+rK$,$C_2=rG$。

(6)B 将 C_1、C_2 传给节点 A。

(7)A 接到 (C_1,C_2) 信息后,计算 C_1-kC_2,其计算结果就是椭圆曲线上点 M,再对 M 进行解码就可以得到原始明文 m。因为我们有:

$$C_1-kC_2=M+rK-krG=M+rkG-krG=M$$

在这个加密通信过程中,如果有一个偷窥者 D,他只能看到 $E\mathrm{p}(a,b)$、K、G、C_1、C_2 等公开信息,而通过 K、G 求私钥 k 或通过 C_2、G 求随机数 r 都是非常困难的(这些困难性由求解椭圆曲线上的离散对数问题加以保证[13])。因此,D 无法得到 A、B 间传送的加密信息,也就无法破解相关明文,达到了保密通信的目的。

由于每个节点有一对私钥和公钥,有 n 个节点的 WSNs 网络,采用椭圆曲线加密算法的整个网络密钥数量为 $O(n)$,密钥数量相比 DES 而言要少,非对称密码体制的密钥传递和更新不需要安全信息通道,所以该方案的密钥管理较简单。

2　WSNs 数据传输能耗模型

在 WSNs 中,其核心问题是低能耗问题[1-2,11]。为了使得 WSNs 全网能耗降低,必须考虑每个节点的能耗情况。我们采用和文献[10,12]类似的一种传输能量模型,这种模型比较全面地考虑了节点发射模块消耗能量,节点功率放大器消耗能量,还有节点接收模块接收数据包消耗能量。发送和接收能量的损耗与发送方和接收方的通信路径长度和数据包数量有

关,设 d 为 WSNs 网内两节点间的通信距离,如果两个节点的距离较短,传播损耗指数为 d^2,如果两个节点距离较长,传播损耗指数为 d^4。d_{co} 为判断两种模式的距离常数,一般取 86.4 m。由此可见,为了节省全网络能量消耗,WSNs 节点应尽量减少长距离的单跳传输,改为短距离多跳传输以节省能量。

由上述能量消耗和距离关系可知,节点发送 k bit 数据包到距离为 d 的另一个节点,其能量消耗为:

$$E_{Tx}(d)=E_{Tx-elec}(k)+E_{Tx-amp}(d) \tag{2}$$

$$E_{Tx}(d)=\begin{cases} kE_{elec}+k\varepsilon_{fs}d^2 & d<d_{co} \\ kE_{elec}+k\varepsilon_{mp}d^4 & d\geqslant d_{co} \end{cases} \tag{3}$$

节点接收 k bit 数据包能量消耗为:

$$E_{Rx}(k)=kE_{Rx-elec}(k)=kE_{elec} \tag{4}$$

其中 E_{elec} 为发送或者接收每比特数据节点所消耗的能量,k 为数据包的长度,ε_{fs} 和 ε_{mp} 为不同放大模型下的常数,具体取值可参考文献[10,12]。

3 相关实验数据分析

3.1 硬件和软件平台

上述两个算法的对比实验在同一平台上进行,无线传感器节点采用美国 Crossbow 公司的 MICAz 节点[9],MICAz 是 2.4 GHz、IEEE 802.15.4 协议的 Mote 模块,用于低功耗无线传感器网络。此节点采用的 CPU 为 ATMega128L 主频 8 MHz 的 8 位微处理器,带有 128 kB 的内部存储器,512 kB 的外部存储器,4 kB RAM,节点的理论收发数据速率为 250 kbit/s,可见该传感器网络平台的资源比较有限。软件平台采用开源的 NesC 语言编写,操作系统为 TinyOS 系统,支持 Version 1.1.7 或更高版本。路由协议采用 Crossbow 的 Xmesh 协议与基站进行多跳通信。我们采用非对称密码体制中素数域上的椭圆曲线密码体制,TinyECC[8] 是无线传感器网络中运用极其广泛的椭圆曲线密码系统软件包,它有多种优化方式可供选择和配置,其加密算法运行效率、占用空间和算法执行时间等都是可变化的。

在实验中,传输数据包中用于组网控制和数据包信息的包头部分为 16 byte,传感器节点电压部分为 2 个字节,另外 2 个字节用于 CRC 校验,剩下字节为实际传输的数据部分。

3.2 实验数据分析

3.2.1 算法时间消耗分析

对称密码体制得到广泛应用的一个主要原因是其加密和解密算法处理速度快、效率高,算法安全性也较好,结合硬件方面的实现它能适应大批量节点、实时和对安全性要求较高的应用场合。而非对称密码体制如椭圆曲线加密 ECC 算法,WSNs 需要进行相当多的数据前期预处理操作,如系统初始化、椭圆曲线相关参数选择、私钥生成和公钥生成等,其加密和解密算法实现过程较为复杂,同时还需要发送公钥、密文和消息鉴别码等内容,从而影响了算法加/解密速度。二种算法的执行时间如图 1 所示,DES 算法加密和解密的执行时间都处于毫秒级水平,而椭圆曲线在加密和解密时间消耗上都需要数秒。因为传感器网络需要采集大量信息,比如在实时医疗卫生健康远程监护领域中[5-7],采集脉搏跳动信息的传感器每秒钟需要发送多达 60 个数据包,即使采用数据融合、过滤冗余数据等手段后,每秒钟也要发送起码 4 个数据包。如果采用椭圆曲线密码体制,不仅单个数据采集节点采集到的数据不能及时传送出去,而且作为解密端的基站节点虽然比数据采集节点有着更高的计算、存储和能量等资源,但是也无法处理来自整个网络的成千上万个节点的加密数据包。这样就使得椭圆曲线密码体制在传感器网络中的使用受到一定限制。所以,在对实时性要求较高的应用场景中,一般采用 DES 算法实现。而在数据发送周期时间较长的应用中,可以采用椭圆曲线密码体制,来获得较好的安全性能,同时增加密码系统中密钥管理的便捷性。

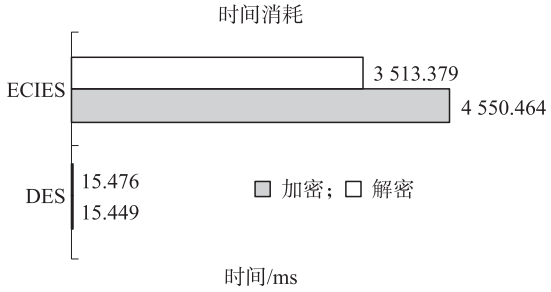

图 1 DES 和 ECIES 二种算法加/解密所用时间

3.2.2 算法空间占用分析

在 TinyOS 系统上分别实现 DES 和 ECIES 密码体制,在程序运行占用空间上,DES 比 ECIES 有着更好的性能,如图 2 所示。在 RAM 占用上,两者大致相

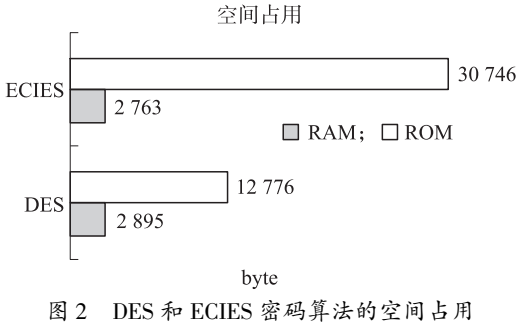

图 2 DES 和 ECIES 密码算法的空间占用

同。在 ROM 占用上,ECIES 应用程序需要初始化、选择大素数、生成公钥、加密数据、生成鉴别码和进行零点检查等操作,需要较多的存储空间。而 DES 算法只需要进行有限的置换、替代等相关代数操作,从而占用较少的代码空间。从图 2 可知,在 ROM 占用上,椭圆曲线密码 ECIES 比 DES 要多 2.5 倍。当然,在不同的应用平台,如 MICAz 和 Imote 2 平台中,前者采用 DES 密码体制会比采用 ECIES 密码体制能承载更多的应用程序。后者是性能较先进的传感器平台,采用 Intel PXA271 XScale 处理器(主频 13 ~416 MHz),配置 256 kB SRAM,32 MB FLASH,32 MB SDRAM,该平台因其高性能和节点资源丰富,可以相对较少地考虑 DES 和 ECIES 算法在代码空间占用上的多寡。

3.2.3　算法处理能耗分析

接下来,我们考察 WSNs 节点在未经过无线模块发送数据时的能耗。根据公式 $W = U * I * t$,其中 U 为节点当前时刻的电压,I 为节点关闭无线模块但是处于激活状态时的工作电流,t 为进行加密或解密操作执行所需时间。根据参考文献[9]中的相关数据,MICAz 平台的电压 U 为 3 V,在关闭无线模块而处于激活状态时的最大电流为 8 mA。图 3 为 DES 和 ECIES 算法在加/解密处理时的能耗比较。DES 因只需要进行置换、替代和相关代数等基本操作,就能完成加/解密过程,处理器存取指令和数据以及进行数据处理操作需要的指令少,程序执行时间短,执行一遍加/解密算法消耗能量约为 0.37 mJ 左右。而 ECIES 在初始化、选择椭圆曲线及参数、生成公钥和私钥、加密数据和产生鉴别码等关键操作上耗时较多,需要进行较多的存取指令和数据,从而影响处理器能耗,执行一遍加/解密算法共需约 100 mJ 左右,是 DES 算法能耗的 200 多倍,这在仅仅依靠两节电池或者纽扣电池供电的无线传感器网络应用中,能耗是个必须考虑的问题。

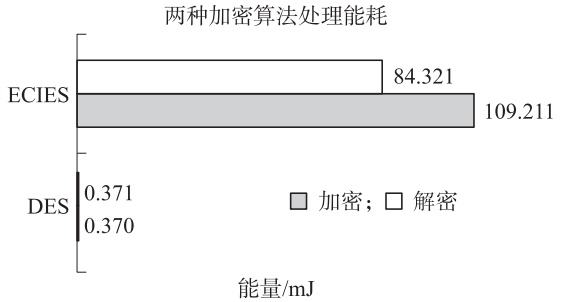

图 3　DES 和 ECIES 加/解密处理能耗

3.2.4　无线发送数据传输能耗分析

在文献[10,12]的设置中,电路消耗能量 E_{elec} 取决于信号编码、调制方式以及滤波和信号扩散等因素。放大器消耗能量 $\varepsilon_{fs}d^2$ 和 $\varepsilon_{mp}d^4$ 取决于发送方和接收方的距离和可接受的误码率。上述文献中,E_{elec} 在 1 Mbit/s 的传输率下为 50 nJ/bit,d_{co} 为 86.4 m。根据文献[13]的设定,ε_{fs} 为 3×10^{-12} J/bit/m^2,而 ε_{mp} 为4×10^{-16} J/bit/m^4。为了做比较实验,我们统一设置加密的明文数据为 8 个字节,发送方和接收方距离约为 50 m。在 DES 密码系统中,传输的数据包的有效负载部分长度为 64 bit,即为整个密文数据的长度。而 ECIES 密码系统中传输数据包的有效负载为 480 bit,包括发送方的公钥、密文数据和消息鉴别码。根据传输能量模型,发送数据包的能耗要高于接收数据包的能耗,而发送方在加密数据后发送数据包到接收方,接收方只接收数据包,然后进行解密,即发送方发送的数据包是加密的数据包,接收方接收了加密后的数据包进行解密。得到如图 4 所示的 DES 和 ECIES 加/解密传输数据包过程中的能耗。从图中可以看出,因为传输数据包的有效数据部分位数显著增加,ECIES 密码系统要比 DES 密码系统在数据包的传输能耗上高 3 倍左右。如上分析,在对能耗比较关注的应用中,选择 ECIES 这种非对称密码体制会影响网络的生存周期,而 DES 则是一种较好的选择。

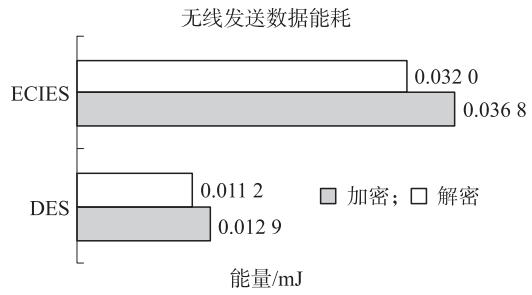

图 4　DES 和 ECIES 加/解密传输能耗

3.2.5　DES 和 ECIES 算法比较分析

从上述实验数据以及密钥管理分析我们得出表 1,对二种算法进行了全面比较。从算法用时、RAM/ROM 占用情况以及能耗方面考虑,对称密码体制的 DES 算法占优;而从密钥数量及密钥管理复杂性方面考虑,非对称密码体制的 ECIES 占优。

表 1　DES 和 ECIES 比较表

算法	算法用时	RAM 占用	ROM 占用	能耗	适用场景	密钥管理	密钥数量	安全性
DES	少	相同	少	小	实时	复杂	较多	一般
ECICS	较多	相同	较多	大	非实时	简单	少	很好

采用 160 bit ECC 密钥长度的加密数据安全强度等同于密码长度为 1024 bit RSA 加密和 80 bit 分组密码加密的安全强度[13-15]。采用 ECC 密码体制能保证 WSNs 的安全性。DES 在早期应用中,受限于当时的硬

件和软件水平,在很长的一段时间内,是十分安全的。随着计算机软硬件、通信和网络技术的发展,DES 的安全性受到挑战。但是在 WSNs 领域,由于传感器节点的计算能力、存储能力以及通信能力都十分有限,如 Crossbow 公司的高端产品 Imote 2,采用 Intel PXA271 XScale 处理器(13 MHz ~416 MHz),只配置了 256 kB SRAM,32 MB FLASH,32 MB SDRAM。这样的配置基本上无法破译节点通信时候用 DES 加密传输的数据,所以,DES 在 WSNs 中依然有着广泛的应用前景。

4 结论

无线传感器网络在物联网应用发展的带动下,已经逐渐从实验室阶段走向实际应用,并作为人类感知世界的一部分。而传感器网络中存在的一些安全因素,如数据窃取、篡改和一些入侵攻击等,严重影响着 WSNs 在需要保证数据传输安全性场合的应用。在实时性要求高的场景中,可考虑采用加密/解密处理速度快、效率高和计算复杂度低的 DES 等对称密码体制,而在其它非实时应用场景中,可以考虑密钥分配简单、系统密钥量少便于管理、系统开放性好和可以方便地实现数字签名、抗抵赖性好的 ECC 等非对称密码体制。在不同的应用平台和数据流量,以及对安全性和密钥管理难度需求不同的应用场合,可以灵活地选择两种密码体制中的一种,或者采用二种算法混合密钥管理方案,来充分利用对称密码算法高效性和公钥密码体系在密钥管理中的简捷性。

如果不考虑密钥管理的数量和复杂性,从上述的比较实验中我们可知 DES 要比 ECC 算法在时空效率及能量消耗方面都要好。但是,由于对称密码体制中密钥管理要求安全信道进行密钥传输和更新,DES 密钥管理数量大导致了密钥管理效率低。而非对称密码则不存在要求安全信道传输密钥问题,密钥管理效率相对较高。所以,DES 和 ECC 两种算法是互补的。

参考文献:

[1] Akyildiz I F, Weilian Su, Sankarasubramaniam Y, et al. A Survey on Sensor Networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.

[2] 李建中,高宏. 无线传感器网络的研究进展[J]. 计算机研究与发展,2008,45(1):1-15.

[3] Chen Xiangqian, Makki K, Yen Kang, et al. Sensor Network Security: A Survey [J]. IEEE Communications Surveys & Tutorials, 2009, 11(2): 52-73.

[4] Malan D, Fulford-Jones T R F, Welsh M, et al. CodeBlue: an Ad Hoc Sensor Network Infrastructure for Emergency Medical Care [C]//Proc of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES 2004), 2004, 12-14.

[5] 赵泽,崔莉. 一种基于无线传感器网络的远程医疗监护系统[J]. 信息与控制,2006,35(2):265-269.

[6] 吴水才,李浩敏,白燕萍,等. 生理多参数远程实时监护系统的设计[J]. 仪器仪表学报,2007,28(6):1035-1039.

[7] 潘巨龙,李善平,张道远. 一种基于无线传感器网络安全的社区卫生保健监护系统设计[J]. 传感技术学报,2009. 22(6): 838-843.

[8] Liu An, Ning Peng. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks[C]//International Conference on Information Processing in Sensor Networks. 2008, IPSN'08. 245-256.

[9] CROSSBOW Company. MICAz: Wireless Measurement System [EB/OL]. [Mar. 11, 2011], http://www. xbow. com/Products/Product_pdf_files/Wireless_pdf/MICAz_Datasheet. pdf.

[10] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An Application-Specific Protocol Architecture for Wireless Microsensor Networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670.

[11] Mao Ye, Li Chengfa, Chen Guihai, et al. EECS: an Energy Efficient Clustering Scheme in Wireless Sensor Networks[C]//Conference on Performance, Computing, and Communications. IPCCC 2005, 535-540.

[12] Hui J, Aida H. A Cooperative Game Theoretic Approach to Clustering Algorithms for Wireless Sensor Networks[C]//IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, PacRim, 2009, 140-145.

[13] Stallings W. Cryptography and Network Security: Principles and Practices[M]. Fourth Edition. Pearson Education, Inc. 2006.

[14] 刘嘉勇,任德斌,胡勇,等. 应用密码学[M]. 北京:清华大学出版社,2008.

[15] Hankerson D, Menezes A, Vanstone S. Guide to Elliptic Curve Cryptography[M]. 2004: Springer-Verlag New York, Inc.

[16] Gura N, Patel A, Wander A, et al. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs[C]//CHES, 2004, 119-132.

[17] Malan D J, Welsh M, Smith M D. A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography [C]//2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. IEEE SECON 2004, 71-80.

[18] Gaubatz G, Kaps J P, Sunar B. Public Key Cryptography in Sensor Networks-Revisited [C]//Security in Ad-hoc and Sensor Networks. Springer Vol. 3313, 2004, 2-18.

金 宁(1967-),女,中国计量学院信息工程学院副教授,硕士生导师。1991 年 3 月毕业于浙江大学信息与电子工程学系,获硕士学位。2005 年 7 月到 2006 年 1 月期间作为访问学者赴德国物理技术研究院(P. T. B)从事研究工作。主要研究领域为无线传感器网络、无线通信和通信信号处理等,jinning1117@ cjlu. edu. cn。