一种无线传感器网络预配置对密钥的改进方案 *

田 丰[1], 李 伟[1], 孙小平[1], 刘华艳[2]
(1. 沈阳航空工业学院 计算机学院, 沈阳 110136; 2. 辽宁大学 信息科学与技术学院, 沈阳 110036)

摘 要: 针对预配置对密钥管理方案存在的缺点,引入一个临时初始密钥和混沌加密算法,提出一种预配置随机对密钥的改进方案。该方案能够使加密密钥随机地改变,且可以更新密钥,提高了网络抗破译的能力,实现了对称和非对称密钥体制的结合。分析表明该方案在安全性、密钥连通性、内存需求和密钥协商的计算量等方面有一定的优势,易于在 Mica2 节点上软件实现。

关键词: 无线传感器网络; 混沌; 加密密钥; 对密钥; 密钥管理
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1856-04
doi:10.3969/j.issn.1001-3695.2010.05.071

Improved wireless sensor network key pre-configured scheme

TIAN Feng[1], LI Wei[1], SUN Xiao-ping[1], LIU Hua-yan[2]
(1. *College of Computer Science, Shenyang Institute of Aeronautical Engineering, Shenyang* 110136, *China*; 2. *College of Information Science & Technology, Liaoning University, Shenyang* 110036, *China*)

Abstract: In order to resolve the problem of pairwise key pre-configured scheme in wireless sensor network, the introduction of a temporary initial key and chaotic encryption arithmetic, this paper put forward an improved wireless sensor network key pre-configured scheme. The program enabled encryption key random change, and could update the key, effectively enhance the capacity of the network of anti-decipher, the realization of the symmetric and asymmetric key system integration. The analysis shows that the scheme has a certain advantage in terms of network security, key connectivity, memory requirements and computation of key agreement, etc. It has implemented by easy software on Mica2 node.

Key words: wireless sensor networks; chaos; encryption key; pairwise key; key management

0 引言

无线传感器网络(wireless sensor networks, WSN)集微机电技术、传感器技术、无线通信技术、计算机网络技术于一体,能够协作地实时监测、感知和采集分布区域内的各种环境或监测对象的信息,并对这些数据进行处理,从而获得详细而准确的信息,将其传送到需要这些信息的用户,可广泛应用于教育、军事、医疗、交通等诸多领域,拥有巨大的应用潜力和商业价值[1],引起了国内外广泛的关注和研究[2,3]。WSN 被部署在无人区域、恶劣环境或敌方阵地中,加之无线网络本身固有的脆弱性,因而传感器网络安全引起了人们的极大关注[4]。

全网络范围内预配置对密钥是最简单、最节约能源的一种对密钥管理方案[5]。该方案是把整个网络中的所有节点在部署之前配置一个完全相同的密钥,这个密钥可以作为认证密钥,然后使用这个密钥来协商会话密钥,整个网络具有百分之百的密钥连通性,而且加密密钥和认证密钥只需要很少的通信开销,能量消耗以及计算操作。但是这种方法最主要的缺点就是密钥单一且无法更新。因为传感器节点非常容易遭到各种攻击,一旦一个节点被攻破,那么整个网络的认证密钥就会泄露,通信中使用的会话密钥也肯定会被敌方攻破。

E-G 基本随机密钥预分配模型[6]和 q-composite 随机密钥预分配模型[7]都是基于密钥池的预分配方案。该方案的缺点是密钥池的大小难以确定,若密钥池越大,则网络的安全性就越好,但任意两个节点存储的密钥数目存在共享的概率就越小,因此网络的连通性就越差,同时也会导致节点的存储资源占用过多;相反,密钥池越小,网络的连通性越好,但共享密钥的重复概率增大,随着被攻破的节点数的增多,越来越多的密钥将会被暴露,导致网络安全性变差。

针对预配置对密钥管理方案存在的缺点,引入混沌加密算法,提出一种预配置随机对密钥的改进方案。本方案在全网预配置对密钥方案的基础上,引入一个临时初始密钥 Kinit 和混沌密钥,实现了对称与非对称密钥体制的结合。使用临时初始密钥初始化网络,然后使用混沌加密算法推导会话密钥;利用混沌的初值敏感性,可以在通信过程中动态地改变加密密钥,实现一次一密,使得任意两个相邻节点都能建立一个对密钥,并可以适时更新密钥;利用混沌的遍历性,有效地提高网络抗破译的能力;以节点标志符实现身份认证,防止伪节点加入网络;以 MAC 认证实现消息的防窜改。

收稿日期: 2009-08-20; **修回日期**: 2009-10-20 **基金项目**: 辽宁省自然科学基金资助项目(20082011); 沈阳市科学技术计划资助项目(1091185-1-00)

作者简介:田丰(1958-),男,辽宁沈阳人,教授,博士,CCF 高级会员,主要研究方向为计算机检测与控制、无线传感器网络(tianfeng5861@163.com);李伟(1982-),男,河南焦作人,硕士研究生,主要研究方向为无线传感器网络;孙小平(1963-),男,黑龙江阿城人,教授,博士,主要研究方向为计算机检测与控制;刘华艳(1957-),女,辽宁沈阳人,高级工程师,主要研究方向为多媒体教学.

1　方案设计思想

1.1　混沌系统

混沌[8]是非线性系统中存在的一种普遍现象,是连续或离散动力系统产生的无固定周期的循环行为。混沌的一个基本特征是它对初始条件的敏感性,即在一个确定性系统中,初始条件任意小的改变都会引发系统在演化过程中得到完全不同的结果,表现出明显的随机性,由此使系统的长期预测不可能。

Logistic 映射是一个典型的非线性混沌方程,其定义如下:

$$f(x_0,\lambda,n):x_{n+1}=\lambda x_n(1-x_n) \tag{1}$$

其中:$x_n\in(0,1)$ 为系统的状态变量,迭代次数 $n=0,1,2,\cdots$;$\lambda\in(0,4)$ 为系统参数。

1.2　方案描述

在本方案中,每个传感器节点分配了惟一的标志符,采用预配置对密钥模型,每个节点都可以与其他任意邻居节点形成一个对密钥,节点内置 Logistic 映射的初值 $x_0=x_1$ 和参数 $\lambda=\lambda_0$,作为传感器节点间的共享密钥;密钥动态地随机生成,实现一次一密,必要时可以修改。

假设在网络初始化时的节点都设置了一个共享的对称密钥,称为临时初始密钥 K_{init},该密钥与会话密钥没有任何联系,而网络初始化以后补充加入的节点则没有此密钥。传感器网络内所有节点都保持严格的时间同步机制。

每个节点可以随机产生一个(0,100)范围内的正整数 r。其中 r 是该节点计算混沌映射所需要的迭代次数,节点计算对密钥。

$$k_i=\phi(f(x_0,\lambda,r_i)) \tag{2}$$

ID_i 表示为网络内的一个传感器节点,k_{ia} 为节点 I 与节点 A 所共享的密钥,由混沌映射产生。将参数 (x_1,λ_0,r_i) 代入式(1),得到 $x_{r_i}\in(0,1)$,然后通过映射函数(2)得到 64 位的密钥 k_i。映射函数 $k_i=\phi(x_{r_i})$ 通过使用取小数点后第 3、4、5 位组合的方式,可以得到一个正整数。节点 i 的混沌密钥 k 与其进行通信的节点的标志符绑定、存储。

2　方案具体实现

2.1　通信密钥的建立

通信密钥的建立分为以下三步:

a)在初始配置阶段。每个节点分配一个惟一的节点标志符。不用的节点标志符在新加入的节点加入到网络中时使用,以提高网络的扩展性。

b)当节点布置到网络中之后,每个节点 i 首先广播自己的 ID_i 给其邻居节点,邻居节点在收到来自 ID_i 的广播包后,存储其节点标志符并立即回复节点 i,通过一次加密的握手来确认两个节点建立联系。已建立起联系的节点则不再广播。

$$A\rightarrow *:|\text{ID}_A|t_A|k_{\text{init}}$$

$$B\rightarrow A:|\text{ID}_B|\text{ID}_A|t_A,t_B|k_{\text{init}}$$

c)节点 i 收到邻居节点的回复后存储其节点标志符;所有的节点利用临时初始密钥建立起联系,而后网络内各节点传输数据则启用混沌密钥进行加密和认证。

2.2　数据的加密和认证

在规定时间内网络初始化完成后,网络开始工作,各节点通信联系启用混沌密钥,产生的随机迭代次数与密文一同明文发送,接收方使用这个迭代次数解密密文,即使第三方收到了这个随机迭代次数而不知道预存的 Logistic 映射的初值 x_1 和参数 λ_0,就无法解密消息。具体过程如下:

假设传感器节点 A 发送消息 D 给传感器节点 B,则在 A 处:

a)节点 A 随机生成一个正整数 r_{AB},然后将 r_{AB} 作为迭代次数代入式(1)(2)进行运算,得到混沌加密密钥 k_{AB}。

b)用混沌密钥 k_{AB} 对数据、时间 t_{AB} 及节点 A 的标志符进行绑定加密,得到密文 E。

$$E=(D|t_{AB}|\text{ID}_A)k_{AB}$$

c)节点 A 对密文 E、迭代次数 r_{AB} 进行 MAC 认证。其中 K_{mac} 为消息认证算法的密钥,C_A 为计数器值。

$$M=\text{MAC}(K_{\text{mac}},E|C_A)$$

d)将密文 E 连同迭代次数 r_{AB},MAC 一起发送给传感器节点 B。

$$A\rightarrow B:E|r_{AB},M$$

当传感器节点 B 接收到来自 A 的消息,则将执行过程如下:

a)节点收到数据包后马上对密文 E 进行认证,可以得到密文 E',若 $E'=E$,则密文在传送的过程中未被窜改,实现了消息的完整性。若发现问题直接丢弃,无须对数据包进行解密;若无问题则进入下一阶段。

b)将收到的 r_{AB} 作为迭代次数代入式(1)(2)进行逆计算,可以得到解密密钥 k_{AB}。

c)用解密密钥 k_{AB} 解密 E,可以得到消息 M'、时间 t_{AB} 和节点标志符 ID'_A。

d)若 $\text{ID}'_A=\text{ID}_A$,则是节点 A 发送的;若时间比节点 B 的时间早,保证了消息的新鲜性。

数据加密和认证模型如图 1 所示,会话密钥可以随机动态生成,理论上实现了一次一密;MAC 认证可有效地避免伪密文穷举攻击,防止消息被窜改;节点标志符防止伪节点的欺骗,进而提高了传感器网络的安全性,严格的时间同步机制使得时间 t_{AB} 可以保证消息在规定的时间内的新鲜性。

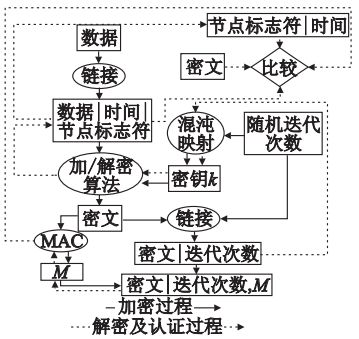


图1　数据加密和认证模型

2.3　密钥管理

1)增加传感器节点

新的传感器节点是随机部署的,不能确定其位置。

当新节点 U 加入到网络后,产生一个(0,100)间的随机正整数 r,使用混沌密钥 k_u 加密,然后向周围的邻居节点发送一个广播包告知自己是新加入和 ID_U。

$$U\rightarrow *:\text{broadcast}(|\text{NEW}_U|\text{ID}_U|k_U|r)$$

各节点收到该广播消息,判断是否在自己的一跳通信范围之内,如果在其范围内则响应节点 U;不在则不响应。

$$A\rightarrow U:\text{ack}(\text{NEW}_U|\text{ID}_U|\text{ID}_A|k_{AU}|r_{AU})$$

节点 A 存储其节点标志符并产生一个随机数 r_{AU},根据式(1)(2)计算混沌密钥 k_{AU},然后将 r_{AU} 和确认信息一起发送给

节点 U,节点 U 收到后解密、验证、存储。

2)撤除传感器节点

传感器节点内置电池监测机制,当节点电池即将耗尽时,应及时发出一个请求信息,请求网内其他节点清除自己;网内各节点收到该信息后,清除该节点,删除与之相关的所有数据。

$$A\rightarrow *:\text{broadcast}(\{\text{delete}\,|\,r_{a\text{-delete}}\,|\,\text{ID}_A\}k_{a\text{-delete}}\,|\,r_{A*})$$

当有传感器节点感知到其邻居节点被入侵时(主要是被复制节点、被俘节点),立即发出一个请求,请求控制中心更新混沌映射的初始值及参数并删除被入侵节点的数据,网内各节点也删除与之相关的所有数据。

$$A\rightarrow PC:\text{request}((\{\text{update}\,|\,\text{log},\text{istic},\text{delete},|\,\text{ID},t_A\})k_{AP}\,|\,r_{AP})$$

$$PC\rightarrow N_i:\text{broadcast}((\text{update log, istic}\{x,\lambda\},\text{delete}\,|\,\text{ID},t_{pc}\})k_{pc}\,|\,r_{pc})$$

$$N_i(i=1,2,\cdots),\text{delete}(\text{pack}\,|\,\text{ID}_A)$$

3)更新密钥

在本方案中,远程控制中心 PC 利用混沌的初值敏感性定期进行密钥更新[9]。如果远程控制中心收到网内节点请求更新混沌映射参数的消息数达到一定的阈值后,启动更新程序并删除相关数据。远程控制中心随机产生一个(0,1)内的实数,并用其更新各节点所存储的混沌初值 x_1;再随机产生一个正整数 r_{new},广播 update 消息给网内的每个传感器节点,更新消息包用原混沌映射参数得到的密钥加密传输,传感器节点收到后,仍用原混沌映射参数解密消息包,得出新的混沌参数并更新存储。

$PC\rightarrow *:\text{update}(\{x_1\,|\,r_{\text{new}}\,|\,\text{ID}_{pc}\,|\,t_{pc*}\}k_{pc}\,|\,r_{pc*})$ 更新完成以后所有节点立即启用新的混沌密钥,混沌的初值敏感性能够保证新的密钥不可能从旧的混沌映射参数推算出来,被删除的传感器节点是难以获得新混沌密钥,从而可以避免因为节点被入侵而导致的密钥泄露。

3 方案分析

3.1 混沌算法的实验验证及其资源需求分析

无线传感器网络节点的处理器运算能力较低,难以处理浮点数据、除法运算,而擅长处理单(双)字节的加法、减法、乘法以及移位运算,因此实现混沌映射产生、加解密算法需要运用低字节运算实现多字节的混沌运算,实现的混沌算法所需要的存储资源必须满足 WSN 节点现有的存储资源要求。

在 WSN 节点中存储和处理的数据是由多个字节构成的整数。在本方案混沌密钥算法中,WSN 节点需要进行整数的加法、减法、移位、乘法等运算。其中混沌多次乘法迭代运算最耗时间。混沌算法主要进行两次乘法运算,一次哈希函数运算等,加密过程和解密过程需要运用低字节运算实现多字节的混沌运算。与随机密钥预分配方案比较,其密钥发现过程中,哈希函数运算、XOR 运算和节点间的通信都是必需的,而通信对能量的消耗很大,远大于节点内部运算所消耗的能量,因此,节点的能量消耗并没有增加。同时,当新增加节点时随机密钥预分配算法必须重新执行密钥发现过程,需要消耗节点能量。而本方案密钥发现过程中只需要执行混沌密钥的一次握手和节点间的通信,且新增节点无须密钥发现过程,计算量小,能量消耗少。因此,与本方案相比,在新增节点处理上处于同一层次,但本方案的算法复杂性要优于随机密钥预分配方法。

利用 KeilC51 软件模拟验证混沌算法的可行性,以 Ateml 的通用 8 位微处理器 AT89S52 为例,具有基本的单字节运算指令:8 位加、8 位减、8 位乘、移位等,可以直接调用,其主要指标为 8 MHz 主频,8 KBFlash,256 ByteRAM,无硬件乘法器,而执行一次迭代 100 次的混沌算法约耗时 0.001s,对于 Mica2 节点的微处理器 ATmega128L 有 128 KB 的 Flash,4 KB 的 EEPROM,4 KB 的 SRAM 及只需两个时钟周期的硬件乘法器,其进行混沌迭代运算的速度更快、耗时更少。

采用基于无线传感器网络操作系统 TinyOS 的编译器来估算需要的存储单元,编译平台采用 Mica2 平台,估计需要的存储单元如表 2 所示,多跳路由协议不加密只需 RAM 为 2 190 Byte,而本方案加密增加的代码最多需要额外的 ROM 为 4 624 Byte(26 664 ~ 22 040),增加额外的 RAM 为 73 Byte(2 263 ~ 2 190)[10],美国加州大学伯克利分校电子工程与计算机系为 SPINS 协议开发的模型系统采用 RC5 计数器模式加密协议却需要 80 Byte 的内存[11]。因此在 Mica2 节点上是可以软件实现混沌加密算法的。

表 1 算法运行效率比较

算法	执行 10 次的时间	执行 100 次的时间	执行 1 000 次的时间
Rijndael 加密算法	0.001	0.099	0.996
混沌算法	0.005 9	0.06	0.621

表 2 加密算法所占存储资源(基于 TinyOS 操作系统)

加密方式	RAM	ROM
不加密多跳路由	2 190	22 040
计数器不加密,增加采用 CTR 模式加密数据的多跳路由	2 251,增加 61	26 512,增加 4 472
SPINS 协议 ——RC5 计数器模式加密协议的多跳路由协议	2 270,增加 80	24 740,增加 2 700
计数器不加密,增加采用混沌加密模式与 CTR 模式,加密数据的多跳路由	2 263,增加 73	26 664,增加 4 624

3.2 安全性分析

由式(1)产生的混沌序列的不收敛性,并且对初值的敏感性。当参数 $\lambda=4$ 时,该序列的概率分布函数 PDF(probability density function)为

$$p(x)=\begin{cases}\dfrac{1}{\pi\sqrt{x(1-x)}} & 0<x<1\\ 0 & \text{其他}\end{cases}$$

通过 $p(x)$ 从上式表示的概率密度函数可以很容易计算出 Logistic 映射产生的序列中一些很有意义的统计特性,如混沌序列轨迹点的分布均值为

$$\bar{x}\lim_{n\rightarrow\infty}\frac{1}{N}\sum_{i=0}^{N-1}x_i=\int_0^1 xp(x)\,\mathrm{d}x=0$$

独立地取两个初始值 x_0 和 y_0 产生的序列的自相关函数为

$$C(m)=\lim_{N\rightarrow\infty}\frac{1}{N}\sum_{i=0}^{N-1}(x_1-\bar{x})(y_{i+1}-\bar{y})=$$

$$\int_0^1\int_0^1 p(x,y)(x-\bar{x})(f^m(y)-\bar{y})\,\mathrm{d}x\mathrm{d}y=0$$

可以看出 Logistic 映射通过迭代所产生的序列的自相关函数(auto-correlation functions,ACF)等于 delta 函数。

通过以上分析可以看出,混沌动力系统具有确定性,其遍历统计特性等同于白噪声,所以适用于保密通信系统中信息的加密。根据混沌系统的不可逆的特点,不可能通过迭代次数 r 或密钥 k 来推算出初值 x_0 和参数 λ;又由混沌的初值敏感性如图 2 可知,初值的细微变化其表现出来的混沌图像明显不同想通过 r 或 k 用穷举法来计算初值 x_0,代价是不可承受的。

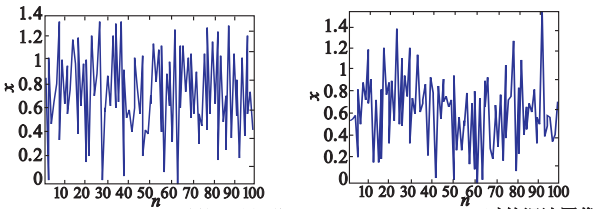
根据经典的随机图理论[12],节点的度 d 与网络节点总数

n 存在以下关系:

$$d=\frac{n-1}{n}(\ln n-\ln(-\ln p_c))$$

其中: p_c 为全网连通概率。若节点的期望邻居节点数为 n' ($n'<<n$),则两个相邻节点共享一个密钥的概率 $p'=\frac{d}{n'-1}$。在给定 p'的情况下,p 与 k 之间的关系表示如下:

$$p'=1-\frac{((p-k)!)^2}{(p-2k)!\ p!}$$



(a)λ=3.6,x=0.6,n=100时的混沌图像　(b)λ=3.6,x=0.601,n=100时的混沌图像

图2　x=3.6,λ=0.6与0.601时的混沌图像

本文采用的是预配置对密钥预分配改进方案模型,网络内所有的节点都有相同的初值 x_0 和参数 λ,使得传感器网络内每个节点都能够与其任意一个邻居节点建立起共享通信密钥,同时也支持组播通信。在不考虑诸如网络因障碍物阻隔造成的通信延迟及敌方电磁干扰的情况下,本方案的网络密钥连通概率是百分之百。在本文的算法中,生成的每对对密钥都不相同,只有进行通信的双方拥有该对密钥,混沌密钥动态改变,使得可以独立建立起点到点的安全信道,且避免了网络安全对基站的依赖。综上所述,本方案与其他几种对密钥管理方案的比较如表 3 所示。

表 3　几种方案的比较

方案名称	网络扩展性	安全性	内存开销	计算复杂度	连通概率
预配置对密钥	较好	差	小	无	1
随机密钥方案	一般	一般	一般	一般	$p'=1-\frac{(p-k)!}{(p-2k)!}$
基于密钥池方案	一般	一般	较大	一般	$p'=1-\sum_{s=0}^{q-1}(P(s)$, 与密钥池 $\|s\|$ 大小有关
本方案	较好	较好	较小	一般	1

4　结束语

在无线传感器网络安全机制中,密钥管理是系统所有安全服务的基础,它包括加密系统密钥的产生、分配、存储、使用、失效及撤除等全过程。本文提出的针对全网范围内预配置对密钥的改进方案,引入混沌算法和临时初始密钥,混沌序列的不可预测性、不可分解性等非线性特征是混沌算法具有良好安全性的理论基础,利用混沌的遍历性和初值敏感性解决了原方案在密钥安全性方面的不足,动态地改变加密密钥且密钥空间大,抗破译能力强,实现了数据传输的加密和认证,保证了传输数据的安全性、真实性和完整性;在密钥管理方面实现了密钥的更新和撤除。该方案对节点资源要求具有较好的适应性,与目前的随机密钥类型算法相比,在计算量与内存需求增加不大的情况下获得了较好的网络安全性,易于在 Mica2 节点上软件实现。

参考文献:

[1] AKYILDIZ F, SU W, SANKARASUBRAMANIAM Y, *et al*. Wireless sensor network: a survey[J]. Computer Networks, 2002,38(4):393-422.

[2] ESTRIN D, GOVINDAN R, HEIDEMANN J, *et al*. Next century challenges: Scalable coordination in sensor networks[C]// Proc of ACM/IEEE Int'l Conf on Mobile Computing and Networking. New York: ACM Press, 1999: 263-270.

[3] GENI. Global environment for network innovations [EB/OL]. (2006). http://www.geni.net.

[4] 苏忠,林闯,封富君,等.无线传感器网络密钥管理的方案和协议[J].软件学报,2007,18(5):1218-1231.

[5] 陈菲.无线传感器网络安全问题研究——对密钥管理研究[D].上海:上海交通大学,2005.

[6] ESCHENAUER L, GLIOR V D. A key management scheme for distributedsensor networks[C]// Proc of the 9th ACM Conference on Computer and Communication Security. New York: ACM Press, 2002: 41-47.

[7] CHEN H W, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]// Proc of IEEE Symposium on Security and Privacy. Berkeley, California: IEEE Computer Society, 2003: 197-205.

[8] 张化光,王智良,黄玮.混沌系统的控制理论[M].沈阳:东北大学出版社,2003.

[9] 温蜜,陈克非,郑燕飞,等.传感器网络中一种可靠的对密钥更新方案[J].软件学报,2007,18(5):1232-1245.

[10] 孙利民,李建中,陈渝,等.无线传感器网络[M].北京:清华大学出版社,2005.

[11] 陈帅.无线微传感器网络混沌加密理论及其关键技术研究[D].重庆:重庆大学,2006.

[12] BOLLOBAS B, FULTON W, KATOK A, *et al*. Rand graphs[M]. 2nd ed. Cambridge: Cambridge University Press, 2001:160-200.

[13] 张楠,张建华,陈建英,等.无线传感器网络中基于混沌的密钥预分配方案[J].计算机应用,2007,27(8):1901-1903.

[14] 马虹博,刘连浩.基于混沌的魔方置乱算法设计[J].计算机工程与应用,2006,42(12):138-140.

[15] 付争方.基于标志的无线传感器网络密钥预分配方案[J].计算机工程与设计,2008,29(13):3313-3315.

(上接第 1846 页)

[2] WOLFMANN J. Negacyclic and cyclic codes over Z_4[J]. IEEE Trans Inform Theory, 1999, 45(7):2527-2532.

[3] WOLFMANN J. Binary images of cyclic codes over Z_4[J]. IEEE Trans Inform Theory, 2001, 47(5):1773-1779.

[4] WAN Zhe-xian. Quaternay code[M]. Singapore: World Scientific, 1997.

[5] CARLET C. Z_{2k}-linear codes[J]. IEEE Trans Inform Theory, 1998,44(4):1543-1547.

[6] LIN San, BLACKFORD T T. $Z_{p^{k+1}}$-linear codes [J]. IEEE Trans Inform Theory,2002, 48(9):2592-2605.

[7] BONNECAZE A, UDAYA P. Cyclic codes and self-dual codes over F_2+uF_2[J]. IEEE Trans Inform Theory,1999,45(4): 1250-1255.

[8] TAPIA-RECILLAS H, VEGA G. A generalization of negacyclic codes [C]// AUGOT D, CARLET C. Proc of International Workshop on Coding and Cryptography. 2001:519-529.

[9] UDAYA P, BONNECAZE A. Decoding of cyclic codes over F_2+uF_2 [J]. IEEE Trans Inform Theory,1999,45(4):2148-2157.

[10] DOUGHERTY S T, GABORIT P, HARAD M, *et al*. Type II codes over F_2+uF_2[J]. IEEE Trans Inform Theory,1999,45(1):32-45.

[11] PLESS V, QIAN Z. Cyclic codes and quadratic residue codes over Z_4 [J]. IEEE Trans Inform Theory,1996,42(5):1594-1600.

[12] Mac WILLIAMS F J, SLOANE N J A. The theory of error-correcting codes[M]. Amsterdam: North-Holland,1977.