基于身份的无线传感器网络密钥系统*)

程宏兵[1,2] 费国臻[1,3]

(南京邮电大学计算机学院 南京 210003)[1] (江苏广播电视大学信息工程系 南京 210036)[2]

(江苏移动有限公司网络部 南京 210006)[3]

摘 要 无线传感器网络(WSN)是一类由众多微型传感器节点通过自组织的方式构成的网络。随着在军事、环境监测等方面的应用逐渐成为现实,其有效和安全通信问题由于自身的特性(如能量、计算能力和节点存储资源等的局限性)而显得更加突出。本文首先比较详细地介绍了无线传感器网络安全结构及其面临的问题;其次重点讨论了无线传感器网络密钥系统相关的研究现状;然后给出了一种有效的基于身份的无线传感器网络密钥系统方案及与其它方案的仿真比较实验。仿真实验结果表明,我们方案较其它密钥系统方案在处理时间和节点存储需求方面具有优势。

关键词 无线传感器网络,网络安全,密钥系统

Research of Identity-based Key System Scheme for Wireless Sensor Network

CHENG Hong-Bing[1,2] FEI Guo-Zhen[1,3]

(College of Computer, Nanjing University of Post Telecommunications, Nanjing 210003)[1]

(School of Information Engineering, Jiangsu Radio&TV University, Nanjing 210017)[2]

(Limited Company of Jiangsu Mobile, Nanjing 210006)[3]

Abstract Wireless sensor network is a kind of Ad hoc network consisted of hundreds or thousands or more of micro sensor nodes, which has been deployed for many practical applications, including military sensing and tracking, environment and security monitoring, equipment and human monitoring and tracking, etc. Due to limitations of power, computation capability and storage resources, security of wireless sensor networks has received considerable attention. In order to construct a secure network, it is an important challenge to find out suitable key establishment, distribution and encryption schemes for wireless sensor networks. The paper argues about the security concerns firstly and then surveys the research of key system in wireless sensor network. Finally it presents an efficient key system scheme which is based on identity encryption algorithm for wireless sensor network . Simulation results among our scheme and other traditional key system schemes suggest that our scheme is feasible in wireless sensor network.

Keywords Wireless sensor network, Network security, Key system

1 引言

集成了传感器技术、微机电系统(MEMS)技术、无线通信技术和分布式信息处理技术的无线传感器网络(WSN)是当前信息技术的前沿之一,是当今的研究热点,受到了广泛的关注[1]。它是由成百上千甚至更多具有无线通信与计算能力的微型传感器节点构成的自组织分布式网络系统,在整个网络系统中,大量的传感器节点收集、处理并且交换来自于外界环境的数据,最终传输到外部基站进行相应处理。

目前,WSN已经在很多方面得到了应用,如环境监测、森林防火、灾难急救、候鸟迁徙跟踪、军事情报收集、无线定位等,而自组织网络(Ad hoc)理论与技术的发展有力地推动了WSN的研究。与固定网络一样,WSN从理论到应用必须解决相关的安全问题,否则将极大地限制WSN的发展,特别在一些领域,如军事上对敌方的情报监测、商业上的一些利益相关的应用等,安全问题就显得尤为重要。通过分析,我们可以把WSN面临的众多安全问题归纳如下:

1) 网络密钥系统问题

网络密钥系统提供数据在存储和传输过程中的机密性和完整性保证,如数据的加密、身份认证和密钥的管理等等。加密使任何人在截获物理通信信号的时候不能直接获得消息内容,而鉴别是指网络中的节点在接收到一个数据包的时候,能有相应的机制确认这个数据包是由相应的发送者发出,同时没有被中间节点篡改或在传输中出现错误。此时需要解决密钥系统协议的相关问题,包括密钥的建立、分配、管理、认证、加密和解密算法等具体问题。

2) DoS[2]攻击问题

由于WSN采用射频传输技术,使得无线传感器网络比固定网络更容易受DoS攻击。如物理层的电磁波干扰、网络层的恶意路由、传输层的泛洪攻击等,都可以使节点甚至网络瘫痪。因此必须建立一套安全容错的路由协议,建立一个在单节点被攻击或俘获后网络仍然能全安运转的机制。采取多种措施,包括密钥系统中的认证和加密等,可以有效地防范网络的DoS攻击。

3) 应用层安全问题

高层的安全主要有安全的组管理机制、入侵检测系统(IDS)和安全的数据汇聚方法等。因此,必须建立一个安全的组管理协议,以保证组成员间的通信安全。入侵检测系统可以发现异常的入侵者,但由于WSN网络节点的计算能力和存储资源有限,如何设计有效的IDS将是一个巨大的挑战。

*)江苏省自然科学基金资助项目(编号:BK2004218)、江苏省"2006年青蓝工程青年骨干教师"资金资助计划。**程宏兵** 博士研究生,主要研究方向为信息安全、计算机网络;**费国臻** 博士研究生,主要研究方向为信息安全、网格计算、计算机网络。

数据汇聚(聚集)是 WSN 网络的主要目的之一,必须建立处理大量数据,并提炼出有效数据的方法,才能有效发挥 WSN 的作用。

另一方面,由于 WSN 的特殊性,主要表现在无线传感器网络在计算能力、存储空间、节点能量以及网络带宽上的局限性,使得 WSN 的安全更具特殊性和挑战性。我们除了要考虑一般网络需要考虑的网络数据的机密性、完整性、可用性等特征外,还要考虑这些局限性对网络安全带来的影响。显然,这种影响有些地方是巨大的,它使得我们不能完全照搬一般固定网络的安全理论与技术,如基于 PKI 的认证机制、计算量较大的非对称加密算法等。由于节点能量的有限性,在 WSN 中很难建立一个 PKI 中的认证中心节点,使得所有节点都处于对等地位。同时考虑到传感器节点有限的计算能力,在网络中实现非对称密钥系统对数据的处理过程将使网络代价太大。因此研究 WSN 的安全问题,特别在固定网络安全技术基础上结合无线网络技术及 WSN 的自身特点研究出一套适合 WSN 的密钥系统,将对其安全应用起到至关重要的作用。

随着无线传感器网络研究的深入,研究人员提出了多个传感器节点上的协议栈[3]。图 1 给出了一种目前处于主导地位的无线传感器网络协议栈。

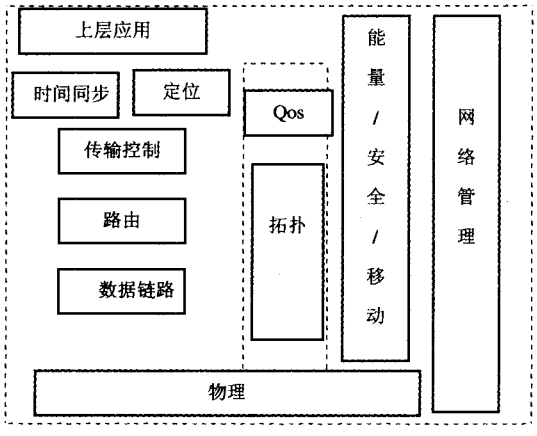

图 1 WSN 协议栈

图 1 中协议栈包括物理层、数据链路层、网络层、传输层和应用层,与互联网协议栈的五层协议相对应,且功能基本一致。定位和时间同步子层在协议栈中的位置比较特殊,它们既要依赖于数据传输通道进行协作定位和时间同步协商,同时又要为网络协议各层提供信息支持,如基于时分复用的 MAC 协议、基于地理位置的路由协议等很多传感器网络协议都需要定位和同步信息。另外,由于无线传感器网络本身的特殊性,在协议栈中充分考虑了 QoS、拓扑以及传感器的能量、移动及安全方面的因素。

针对无线传感器网络的特点,对于 WSN 协议栈各层的攻击、防御手段的解决思路和方法与传统网络安全问题不同,主要是由 WSN 自身的特点决定的:有限的存储空间和计算能力、缺乏后期节点布置的先验知识、布置区域的物理安全无法保证、有限的带宽和通信能力、不仅是点到点的安全更是整个网络的安全、应用的相关性。在构造无线传感器网络时,密钥系统的设计主要针对网络层的如汇聚节点攻击(homing)、方向误导攻击(misdirection)和黑洞攻击(blackholes)以及传输层的失步攻击(desynchronization)等。

综上所述,为了构造一个安全的无线传感器网络,首先必须建立合适密钥系统,以保证系统管理、数据传输和处理等方面的安全,这个密钥系统包括一整套适合无线传感器网络的密钥协议以及密钥建立、分配、认证、加密和解密等问题。

本文将在第 2 部分对 WSN 密钥系统研究的现状及其存在的问题进行深入的讨论;第 3 部分给出了一种有效的基于身份的密钥系统方案及相关实验结果;最后对文章进行了总结。

2 WSN 的密钥系统研究概述

对于无线传感器网络密钥系统问题,目前基本上还是研究如何有效使用传统的网络密钥系统于无线传感器网络中。由于无线传感器网络在计算能力、存储空间、节点能量以及网络带宽上的有限性,传统的网络密钥系统方案由于某些方面不适合无线传感器网络而不能得到真正的应用。下面从无线传感器网络密钥系统的密钥协议以及加、解密方案两个方面分别进行讨论。

2.1 密钥协议的相关研究

密钥协议系统方面,目前在国内外相关研究中,存在 3 种关于无线传感器网络的密钥协议、建立和分配方案,即信任服务器方案、公开密钥方案和密钥预分配方案[4]。在信任服务器方案中,节点之间密钥协议依赖信任服务器,此方案中的信任服务器即无线传感器网络中所谓的基站,本身也是由一些特殊的传感器节点组成。由于传感器节点有限的能量和计算能力无法处理为数众多的传感器节点的申请密钥、认证密钥和管理密钥的问题,因此这种方案不适合作为传感器网络的密钥协议、建立和分配方案。对于公开密钥方案,由于其依赖于非对称的密码学方法,加、解密阶段所使用规则不相同,因此需要的计算能力和存储空间以及能量的消耗都很大,与前一种方案相似,此种方案也不适合传感器网络。第三种方案是通过预分配方案来分配密钥,密钥的分配是在节点部署之前就已完成。在相关的研究中,基于密钥池的随机预分配方案是目前比较成功的成果,该方案比较适合无线传感器网络的部署特点。文[5~7]对这种方案在传感网络中的应用进行了深入的研究。

众所周知,传感器网络中的节点部署一般都是随机的,节点相互之间的信息和网络拓扑结构在部署之前通常都是未知的。鉴于此,在传感器网络中,一种简单的密钥分配方法是所有的节点都存储共同的密钥,任何节点对之间可以使用主密钥产生新的安全密钥对。然而这种方案会使网络变得不安全,假如网络中的一个节点被俘获,则整个网络的安全就会受到威胁。即使可以使用具有防止篡改功能的硬件来存储主密钥,以降低网络所受到的安全威胁,但由于这样会增加网络的能量消耗等代价而使之变得不现实。再者,文[8]表明防止篡改功能的硬件有时也会不安全。另一种简单的密钥分配方法是密钥预分配方案。在该方案中,每一个传感器节点都存储 $N-1$ 个密钥(N 是网络中的节点数目,往往非常大)。在网络中若有节点被俘获,由于解密如此多的密钥是非常困难的,因此该方案具有很好的安全性。但是由于在实际应用中 N 往往会非常大而需要很大的传感器节点存储空间,因此该方案在实际应用中很难实现。

国外关于 WSN 密钥协议及密钥建立、分配方案的代表性相关研究成果有:Eschenauer 和 Gligor 在文[5]中提出了一种适合于 WSN 的概率密钥共享方式;Pietro 等在文[9]中讨论了随机预分配密钥方法,该方法的操作方法简单描述如

下:从密钥空间选择一随机密钥池,每个传感器节点在部署之前都从该密钥池获得一些密钥,于是任意两个节点就有可能从各自所获得的密钥中找出相同的密钥来进行通信,但这种方法存在的一个问题是,任何两个节点之间存在相同的通信密钥的概率是 $p(p\in[0,1])$。基于随机预分配密钥方法研究方面,Chan 等在文[10]中研究了 q-composite 的预分配密钥和随机密钥对的方案。该方案是使得两个传感器节点在部署前至少共享 q 个密钥,然后在节点之间寻找相同密钥对进行通信。该方案由于攻击者需要俘获很多网络节点才能破坏网络,因此比较安全,是目前一种比较优越的 WSN 密钥分配方案。目前这种基于密钥预分配的研究方案受到了很大的关注,也产生了一些成果。如 Zhen Yu 等在文[11]中提出了一种基于节点分布知识的密钥分配方案,该方案利用某些先验性知识,获取传感器节点的部署情况,然后根据节点的部署情况进行合适的随机密钥分配。由于在该方案中,如何正确地获取节点的部署情况是一大难题,因此在该难题获解决之前此方案难以真正得到应用。Chorzempa 和 Par 在文[12]中研究了一种可幸免的有效群密钥预分配方案,该方案基于节点的自组织性,使用密钥群对节点进行密钥分配。Chuang 和 Chao 等在文[13]中也提出了一种随机的群密钥预分配方案,该方案是在对传感网络中的传感节点进行分组的基础上,对各组进行密钥分配,然后在各组进行通信,最后扩展到整个网络。该方案在节点分组处理中具有相当的复杂性,因此离实际应用还有一定距离。

国内对 WSN 网络已进行了大量的研究工作,但在对 WSN 安全研究,特别是密钥协议及密钥建立、分配方案相关研究目前还处在起步阶段,基本是对传感器网络的密钥系统某些方面的研究。根据发表的文献,陈克非等在文[14]中研究了无线传感器网络中对密钥管理的评估指标问题,对目前比较流行的基于 KDC 和基于预先配置这两种密钥管理方案进行了分析。王佳昊等在文[15]中讨论了随机预分配密钥在无线传感器网络跟踪算法中的应用问题。陈贵海等在文[16]中提出了一种复合式的安全模型。杨少春等在文[17]中提出了一种基于密钥预分配的无线传感器网络加密方案,该方案基于不同的密码方法,其性能会有所差异,并在具体应用时还需要考虑的诸多问题也没有得到很好的解决。因此,国内的相关研究还处于一种 WSN 密钥系统某些方面的理论探讨阶段,有待更深层次的研究。

2.2 加、解密方案的相关研究

加密、解密方案研究方面,目前国外还处在一种探讨阶段,基本上都在研究如何利用传统的网络密码方法于无线传感器网络中。例如,在常用的密钥技术中,对称密钥技术经常在认证和加密中得到应用。与非对称密钥技术相比,对称密钥技术的优点是需要较少的计算;缺点是需要有预分配密钥的过程并在网络互连和通信方面表现不佳(如在随机密钥分配中,相邻节点是以某一概率共享密钥的)。最近,在传感器网络中出现了一些使用公开密钥密码技术的成果[18~20],研究重点主要是对公开密钥密码技术进行优化。在文[20]中,基于公开密钥密码技术的椭圆曲线加密方法(ECC)由于在存储需求、计算成本以及通信带宽需求等方面有很大的优势而适合传感器网络,具有很好的应用前景。

对于无线传感器网络的安全和密钥系统我们也进行了相关的研究,尤其是对无线传感器网络 SPINS 安全框架协议(包括 SNEP 和 μTESLA)、密钥分配和加密、解密方法等方面进行了一些研究。在文[21]中我们深入研究了无线传感器网络的安全问题,并对基于基站的 SPINS 安全框架协议进行了讨论,且给出了该协议的一些改进措施。文[22]中我们给出了一种认证的无线传感器网络密钥建立和加密方案。

3 基于身份的 WSN 密钥系统方案

我们在提出一种有效的基于身份的无线传感器网络密钥系统之前,先给出以下一些定义。

3.1 定义

在我们的方案中,记 Z_q 为素数阶 q 的加法群,$Z_q=\{0,\cdots,q-1\}$,Z^+ 为正整数,G_1 为循环加法群,G_2 为循环乘法群,G_1、G_2 具有相同的素数阶 q 有如下定义。

定义 2.1 如果对所有的 $x,y\in G_1$,$a,b\in Z$,都有 $\hat{e}(x^a,y^b)=\hat{e}(x,y)^{ab}$,则映射 $\hat{e}:G_1\times G_1\to G_2$ 称为一个双线性对。

定义 2.2 对于一个双线性映射 $\hat{e}:G_1\times G_1\to G_2$ 使得 $|G_1|=|G_2|=q$ 是一个素数的 Bilinear-Diffie-Hellman 问题(BDH)定义如下:给定 $g,g^a,g^b,g^c\in G_1$,计算 $\hat{e}(g,g)^{abc}$,其中 g 是一个生成器,$a,b,c\in Z$。如果 $\Pr\lfloor A(g,g^a,g^b,g^c)=\hat{e}(g,g)^{abc}\rfloor\geqslant\varepsilon$ 的概率超过了 a,b,c,g 随机选择的概率和 A 随机比特的概率,称算法 A 是以 ε 为增益来解决 BDH 问题的。

定义 2.3 使用一个安全参数 $k\in Z^+$ 作为输入的随机算法 G 是一个 BDH 参数生成器,如果它的时间为 k 的多项式,并且输出组 G_1,G_2 的描述以及使得某些素数 q 满足 $|G_1|=|G_2|=q$ 的一个双线性函数 $\hat{e}:G_1\times G_1\to G_2$。将算法的输出表示为 $G(1^k)=\langle G_1,G_2,\hat{e},q\rangle$。

定义 2.4 如果不存在可能的多项式算法 A 能够以不可忽略的优势来解决 BDH,我们就说 G 满足 BDH 假设。

基于上述定义,下面给出基于身份的椭圆曲线上的双线性对无线传感器网络密钥系统方案。

3.2 基于身份的 WSN 密钥系统方案

1) 设置系统参数:在无线传感器网络部署之后,给定保密参数 $k\in Z$,算法为:

Step 1:输入参数 k,PKG 生成素数 q、两个 q 阶的群 G_1,G_2 和双线性映射 $\hat{e}$:$G_1\times G_1\to G_2$。随机取 $\alpha\in G_1$。

Step 2:随机取 $s\in Z_q^*$,计算 $\beta=\alpha^s$。

Step 3:选择散列函数 H_1:$\{0,1\}\to G_1^*$,H_2:$G_2\to\{0,1\}^n$。明文空间为 $M=\{0,1\}^n$,密文空间为 $C=G_1^*(\{0,1\}^n$,输出的系统公共参数为 $\pi=\{q,G_1,G_2,\hat{e},n,\alpha,\beta,H_1,H_2\}$,$s\in Z_q^*$ 为主密钥(Master key)。

2) 计算获取传感器节点密钥:对无线传感器网络中的每个节点,对其给定的身份标识 $Id\in\{0,1\}^*$(注:Id 是随机的串,可以是姓名、角色、邮件地址等等)生成密钥。

Step 4:计算 $Q_{Id}=H_1(Id)\in G_1^*$。

Step 5:取密钥为 $K_{Id}=(Q_{Id})^s$。

3) 节点广播 Id 号:

Step 6:节点向相邻节点显式广播自己的身份标识 Id,所有相邻节点获取节点 A 的标识 Id。

4) 消息加密:对无线传感器网络中的传送消息 $m\in M$ 和公钥 Id,消息加密步骤如下。

Step 7:计算 $Q_{Id}=H_1(Id)\in G_1^*$。

Step 8:随机取 $r\in Z_q^*$。

Step 9:加密的密文为:$c=\langle r\alpha,m\oplus H_2(g_{Id}^r)\rangle$,

其中 $g_{Id}=\hat{e}(Q_{Id},\beta)\in G_2$

5) 消息解密:设 $c=\langle U,V\rangle$ 为消息密文,则消息接收节

点对密文 c 解密步骤如下。

Step 10：应用密钥 $K_{id} \in G_1^*$，计算原文 $m = V \oplus H_2(\hat{e}(K_{id}, U))$。

3.3 仿真实验

针对以上研究，对我们提出的密钥系统方案和其它方案进行仿真实验。我们在广泛使用的仿真器 ns-2 的环境下进行了仿真实验，实验设备是一台运行 Redhat Linux 9.0，具有 P4 2.4G 处理器，512M DDR 内存的 PC。实验时，假设 250 个节点随机均匀地部署在一块 $200 \times 200m^2$ 的区域内，每个节点的传输半径为 30m。假设基站位于网络的左上角，源节点（加密选定的 hello 包并发送到目的节点）位于网络的 $25 \times 25m^2$ 的区域内，目的节点在部署区域的其它地方随机选取。我们选择一个简化了的定向扩散协议[23]作为网络层的协议。仿真实验方案如下：Ⅰ. 我们的方案（记为 IBE-BASED）；Ⅱ. 采用信任服务器的公共密钥系统方案进行密钥的协议、建立与分配并用 RSA 进行消息加、解密的 RSA 方案[18]；Ⅲ. 采用密钥预分配方案进行密钥的协议、建立与分配并用 DES 进行消息加、解密的 DES 方案[10]。用 C++和 TCL 实现了上述三个方案。我们在实验中考虑以下实验比较指标，密钥长度：不同方案所能提供的目前可接受安全水准的密钥字节长度，三种方案中的密钥大小选择目前可接受的同等安全程度水准，其中 IBE-BASED 方案密钥大小为 160bit，RSA 方案密钥大小为 1024 bit，DES 方案密钥大小为 64bit。实验次数：每个方案的实验次数，均为 20 次。平均初始化时间：每个方案 20 次实验密钥的协议、建立和分配所用时间平均值，在仿真实验中，设定为对网内所有节点都进行了相关处理的时间。平均加密时间：每个方案 20 次加密时间的平均值。平均解密时间：每个方案 20 次解密时间的平均值。

表 1 仿真实验结果

方案	密钥长度 (bit)	实验次数	平均初始化时间(s)	平均加密时间(s)	平均解密时间(s)
RSA	1024	20	2.8234	26.6532	45.5523
DES	64	20	30.7710	0.0025	0.0025
IBE-BASED	160	20	18.1209	6.5800	5.0820

实验数据显示，我们方案的计算复杂性是最优的。存储空间方面由于目前 64 位的 DES 方案在安全性方面受到了质疑，文[24]已经表明 64 位的 DES 比较容易被破译（最短几个小时），且如果仅靠增加密钥长度的方法来增加 DES 的安全性，将会导致计算量极大增加的同时使得占用更多传感器节点存储空间。因此在可靠的安全程度下，考虑到在实际的无线传感器网络应用中节点数目往往巨大，我们的方案在存储空间上也有较大优势。

结束语 无线传感器网络的安全问题随着其应用逐渐成为现实而备受关注，由于其自身诸多的局限性如能量有限、计算能力有限以及节点存储空间等的局限性等使得寻找一种合适的密钥系统方案变得很重要。本文就无线传感器网络的安全问题进行了讨论，并对目前无线传感器网络密钥系统的相关研究状况进行了详细的介绍，最后提出了一种有效的基于身份的无线传感器网络密钥系统方案，与目前比较流行的基于 RSA 加密方法的公共密钥系统方案和基于对称加密方法 DES 的密钥预分配方案进行了一些仿真实验比较，结果表明了我们方案在无线传感器网络中的可行性。

参 考 文 献

1 Pottie G J, Kaiser W J. Embedding the internet: wireless integrated network sensors [C]. Communications of the ACM, 2000, 43(5): 51～58

2 Wood A D, Stankovic J A. Denial of service in sensor networks [A]. IEEE Computer, 2002, 35(10): 54～62

3 Pister K, Hohlt B, Jeong J, et al. A sensor network infrastructure [R]. 2003. http://www-bsac.eecs.Berkeley.edu/projects/ivy

4 Du W, Deng J, Han Y S, et al. A pairwise key predistribution scheme for wireless sensor networks [C]. ACM Transactions on information and System Security, 2005(1): 41～77

5 Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks [C]. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002. 41～47

6 Liu D, Ning P. Multi-level μTESLA: Broadcast authentication for distributed sensor networks. ACM Transactions in Embedded Computing Systems (TECS), 2004, 3(4): 800～836

7 Liu D, Ning P. Location-based pairwise key establishments for static sensor networks [C]. In: 2003ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), 2003. 72～82

8 Anderson R, Kuhn M. Tamper resistance-A cautionary note [A]. In: Proceedings of the 2nd Usenix Workshop on Electronic Commerce, 1996. 1～11

9 Pietro R D, Mancini L V, Andmei A. Random key assignment for secure wireless sensor networks [C]. In: Ad Hoc and Sensor Networks (SASN'03), 2003. 62～71

10 Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks [C]. In: IEEE Symposium on Research in Security and Privacy, 2003. 197～213

11 Yu Zhen, Guan Yong. A Key Pre-Distribution Scheme Using Deployment Knowledge for Wireless Sensor Networks [C]. In: 05' IEEE INFOCOM

12 Chorzempa M, Par Jung-Min, et al. SECK: Survivable and Efficient Clustered Keying for Wireless Sensor Networks [C]. In: 05' IEEE INFOCOM

13 Chuang Po-Jen, Chao Tun-Hao, et al. A Scalable Grouping Random Key Predistribution Scheme for Large Scale Distributed Sensor Network [C]. In: IEEE ICITA'05

14 陈菲，宋志高，陈克非. 无线传感器网络中对密钥管理评估指标研究[J]. 计算机仿真，2005，22(5)：137～140

15 王佳昊，王胜坤，秦志光，等. 随机预分配密钥在 WSN 跟踪算法中的应用[J]. 四川大学学报，2005，27(11)：113～119

16 曹晓梅，李成法，叶懋，等. WSAN 网络密钥管理模型的研究. 计算机应用与软件，2005，20(4)：41～44

17 杨少春，郎为民，谭珂科. 基于密钥预分配的传感器网络加密方案. 信息工程大学学报，2005，6(4)：11～14

18 Gaubatz G, Kaps J, Sunar B. Public keys cryptography in sensor networks-revisited [C]. In: The Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS), 2004

19 Malan D J, Welsh M, Smith M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography [C]. In: The First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, October 2004. 71～79

20 Gura N, Patel A, Wander A, et al. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs [C]. In: Proceedings of the Workshop on Cryptography Hardware and Embedded Systems (CHES 2004), Boston, August 2004

21 程宏兵，杨庚，王江涛. APINS 安全框架协议研究[J]. 计算机科学，2006，33(8)：106～108

22 Cheng H B, Yang G, Wang J T, et al. An authenticated identity-based key establishment and encryption scheme for wireless sensor networks [J]. The Journal of China University of Posts and Telecommunications, 2006, 13(2): 31～38

23 Intanagonwiwat C, Govindan R, Estrin D, et al. Directed diffusion for wireless sensor networking. IEEE/ACM Trans on Networking, 2003, 11(1): 2～16

24 范明钰，靳蕃，李正邦. DES 的破译探讨[J]. 信息安全与通信保密，1996，66(2)：19～23