实验研究

文章编号:1671－251X(2011)10－0026－06　　DOI:CNKI:32－1627/TP.20110922.1310.008

无线传感器网络移动汇聚节点密钥管理方案

张绛丽[1]，　柳亚男[2]，　李永忠[1]

(1.江苏科技大学计算机科学与工程学院，江苏 镇江　212003；
2.南京航空航天大学计算机科学与技术学院，江苏 南京　210016)

摘要:针对传统的移动汇聚节点密钥管理方案即能耗最低方案、概率型方案、多项式方案等存在抗俘获能力低的问题,提出了一种改进的移动汇聚节点密钥管理方案。该方案实现原理:全体节点共享一个多项式池 F,传感器节点的多项式环大小为 1,移动汇聚节点的多项式环大小为 $|F|$;利用移动汇聚节点存储资源丰富的优势保证移动汇聚节点与附近的任一传感器节点都存在一个共享多项式,进而通过该共享多项式计算出共享密钥;若规定每个多项式被分配的次数不大于多项式的阶数时,可保证多项式的绝对安全,从而实现节点抗俘获能力最优的目标。实验结果表明,与概率型方案相比,该方案有效地提高了节点的抗俘获能力,并降低了节点能耗。

关键词:无线传感器网络;移动汇聚节点;传感器节点;共享密钥;密钥管理

中图分类号:TD655.3　　文献标识码:A　　网络出版时间:2011－09－22 13:10

网络出版地址:http://www.cnki.net/kcms/detail/32.1627.TP.20110922.1310.008.html

Key Management Scheme of Mobile Sink in Wireless Sensor Networks

ZHANG Jiang-li[1],　LIU Ya-nan[2],　LI Yong-zhong[1]

(1.School of Computer Science and Engineering of Jiangsu University of Science and Technology, Zhenjiang 212003, China. 2.College of Computer Science and Technology of Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: In view of problem of low anti-capture ability of traditional key management scheme of mobile sink, namely minimum energy consumption scheme, probabilistic scheme and polynomial scheme, the paper proposed an improved key management scheme of mobile sink. The implementing principle of the scheme is as follows: all nodes share a polynomial pool F, size of polynomial loop of sensor is 1 and size of polynomial loop of mobile sink is $|F|$; using advantage of abundant storage resources of mobile sink to ensure exist a shared polynomial in mobile sink and any sensor nearby, then to calculate shared key through the polynomial. If regulating distributed times of each polynomial are less than orders of the polynomial, it can ensure absolute security of polynomial, so as to realize the best anti-capture ability of

收稿日期:2011－05－06

基金项目:江苏省高校自然科学基金资助项目(05KJD52006),江苏科技大学科研资助项目(2005DX006J)

作者简介:张绛丽(1975－),女,湖南邵阳人,讲师,工学硕士,研究方向为网络信息安全、无线通信协议分析及安全协议研究。
E-mail:jiangli@just.edu.cn

nodes. The experiment result showed that the scheme improves anti-capture ability and reduces energy consumption effectively of nodes comparing with probabilistic scheme.

Key words: wireless sensor networks, mobile sink, sensor node, shared key, key management

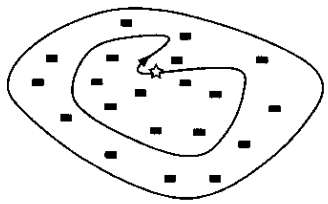
0　引言

无线传感器网络(Wireless Sensor Networks, WSNs)中，汇聚节点(Sink)是数据融合和数据处理的中心。随着传感器网络研究的不断深入，移动汇聚节点(Mobile Sink, MS)代替了 WSNs 中传统的静止汇聚节点。资源丰富的移动汇聚节点能够在整个网络范围内移动，减少了数据在传感器节点(Sensor)间的存储转发，能够极大地降低传感器节点的通信负载、网络能耗，并有效地避免了孤立节点的产生[1-2]。

近年来，WSNs 的密钥管理问题一直是研究的热点与难点，如以参考文献[3]～[5]为代表的“概率型方案”，以及以参考文献[6]～[8]为代表的“计算型方案”等。为了满足移动汇聚节点的应用需求[1-2]，本文将对移动型无线传感器网络的密钥管理问题开展研究，探讨现有的经典方案直接应用于移动型无线传感器网络后容易出现的问题，并提出一个改进方案，专门解决移动汇聚节点与传感器节点间的共享密钥建立问题。实验结果表明，改进方案兼顾了无线传感器网络在高安全与低能耗方面的需求，并且可保证移动汇聚节点能够与任一传感器节点建立唯一的共享密钥。

1　移动型无线传感器网络结构

移动型无线传感器网络结构是基于 Chakrabarti 等人提出的无线传感器网络模型[9]改进而来的，如图 1 所示。



■ —传感器节点；☆ —移动汇聚节点；➡ —运动方向

图 1　移动型无线传感器网络结构

该模型有 2 种网络节点：大量的传感器节点和 1 个移动汇聚节点，其中传感器节点的资源和能源受限，节点部署后保持静止；而移动汇聚节点是功能较强的无线通信设备，除了在存储、通信、计算和供电等方面具备较高的能力外，还可以在整个网络中按照一定的移动模型进行运动。这种网络的最大优点就是把复杂的数据处理、接入处理、数据转发传输、路由维护等工作交由移动汇聚节点完成，减轻了无线传感器网络的能量负担，而且移动汇聚节点可以给传感器节点补充能量。

2　传统的移动汇聚节点密钥管理方案

(1) 能耗最低方案

能耗最低方案原理：从密钥池中为每个传感器节点随机选取一个密钥，该密钥分别存储在该传感器节点与移动汇聚节点中。由此汇聚节点能够与网络中任意一个传感器节点建立独一无二的共享密钥。该方案对于传感器节点来说存储、计算和通信是最优的，因此，能耗是最低的，而且敌方无法获得被俘获传感器节点以外的任何密钥信息，即该方案能够完全抵抗传感器节点的物理俘获攻击。但是，该方案要求移动汇聚节点必须具备硬件保护设施，否则，一旦汇聚节点被俘获将会泄露整个网络的密钥信息。

(2) 概率型方案

2002 年由 Eschenauer 和 Gligor 提出的随机密钥预分配方案(E－G 方案)[3]是经典的概率型方案[4-5]，它要求每个传感器节点都持有一定数目的密钥(密钥环)，邻居节点根据各自密钥环中存在的共享密钥来建立密钥对。将 E－G 方案应用于移动型无线传感器网络时，由于移动汇聚节点的存储力更大，因此，可分别设置移动汇聚节点密钥环大小 R 和传感器节点密钥环大小 $r(R>>r)$。概率型方案中节点的通信量和计算量非常小，但邻居节点间存在共享密钥的概率为

$$F_r = 1 - \frac{C_{P-r}^{R}}{C_P^R} \leqslant 1 \qquad (1)$$

式中：P 为密钥池的大小。

传感器节点和移动汇聚节点必须通过提高密钥存储量来提高连通概率，然而这不但会增加节点的存储负载，同时也会降低节点的抗俘获能力。

(3) 多项式方案

1992 年，由 Blundo 等人提出了基于对称多项式的组密钥管理方案[10]，定义了有限域 $GF(\lambda)$ 上的 t 阶多项式为

$$f(x,y)=\sum_{i=0,j=0}^{t}a_{ij}x^iy^j \tag{2}$$

式(2)具备对称性,为网络中的每个节点预分配多项式算子 $f(ID,y)$。对于任意 2 个相邻节点 u 和 v,节点 u 将 ID_v 代入自己的多项式算子后得到 $f(ID_u,ID_v)$,同样节点 v 也可得到 $f(ID_v,ID_u)$:$key_{(u-v)}=f(ID_u,ID_v)=f(ID_v,ID_u)$。2005 年,Liu 等人将多项式应用到无线传感器网络的密钥管理中[6-7],研究表明,多项式方案在少量增加节点通信量和计算量的情况下,有效地提高了节点抗俘获能力。移动汇聚节点可以与附近的任一传感器节点建立密钥:$key_{(sensor-MS)}=f(ID_{MS},ID_{sensor})=f(ID_{sensor},ID_{MS})$。相比之下,多项式方案有着安全连通概率为 100%、节点抗俘获性好、节点的存储负载小等优势。但是,所有节点共享一个主多项式时,多项式 f 并不是绝对安全的:一旦收集到 $(t+1)$ 个多项式算子,敌方便可解出多项式 f,由此可计算网络中任意 2 个节点的密钥对。参数 t 是一个安全门陷,当被俘节点数$\leqslant t$ 时,节点抗俘获性最优;当被俘节点数$>t$ 时,节点抗俘获性最差。但是传感器节点有限的存储空间决定了 t 不可能很大,因此,敌方很容易通过破解多项式 f 来获取节点的密钥信息。

3 改进的移动汇聚节点密钥管理方案

基于 Chakrabarti 网络模型,笔者提出的改进的移动汇聚节点密钥管理方案用于解决移动汇聚节点与普通传感器节点的密钥建立问题。主要思路:全体节点共享一个多项式池 F,传感器节点的多项式环大小 $m=1$,移动汇聚节点的多项式环大小 $M=|F|$。利用移动汇聚节点存储资源丰富的优势,可保证移动汇聚节点与附近的任一传感器节点都存在一个共享多项式,进而通过该共享多项式计算出共享密钥。若规定每个多项式被分配的次数$\frac{n}{M}\leqslant t$ 时(n 为传感器节点个数),可保证多项式的绝对安全,从而实现节点抗俘获性最优的目标。

3.1 密钥预分配

节点投放前,密钥预分配包括以下 4 步:

(1) 生成多项式池 F,其中包括 M 个 t 阶二元多项式:

$$f_{k=1,2,\cdots,M}(x,y)=\sum_{i=0,j=0}^{t}a_{ij}x^iy^j \tag{3}$$

多项式满足对称性,即 $f(x,y)=f(y,x)$。

(2) 从 F 中随机选取一个多项式 f_k 分配给传感器节点 S_i,将传感器节点 S_i 的 ID 代入 f_k 后得到多项式算子 $f_k(S_i)$ 存入传感器节点 S_i 中。每个多项式最多被选取 q 次。

$$f_k(S_i)=f_k(ID_{S_i},y) \tag{4}$$

(3) 将移动汇聚节点 MS 的 ID 分别代入 F 中的每个多项式 $f_{k=1,2,\cdots,M}$,将 M 个多项式算子 $f_{k=1,2,\cdots,M}(MS)$ 存入 MS 中。

$$f_{k=1,2,\cdots,M}(MS)=f_{k=1,2,\cdots M}(ID_{MS},y) \tag{5}$$

(4) 选取 Hash 函数 H 存入移动汇聚节点 MS 及每个传感器节点 S_i 中。

3.2 共享密钥建立

传感器节点 S_i 将 ID_{MS} 代入多项式算子 $f_k(S_i)$ 得到密钥:$k_{S_i}=f_k(ID_{S_i},ID_{MS})$。传感器节点 S_i 生成随机数 R_1 并用 k_{S_i} 加密后发送给移动汇聚节点 MS,同时传感器节点 S_i 向移动汇聚节点 MS 发送 R_1 的 Hash 值 $H(R_1)$;移动汇聚节点 MS 将 ID_{S_i} 分别代入 M 个多项式算子得到密钥:$k_{j=1,2,\cdots,M}=f_{j=1,2,\cdots,M}(ID_{MS},ID_{S_i})$。移动汇聚节点 MS 用 $k_{j=1,2,\cdots,M}$ 解密 $E(k_{S_i},R_1)$ 后得到 M 个不同的值 $R_{1j=1,2,\cdots,M}$。检查 $H(R_{1j=1,2,\cdots,M})=H(R_1)$ 是否成立。

$$S_i\rightarrow MS:E(k_{S_i},R_1)\,||\,H(R_1) \tag{6}$$

因为移动汇聚节点 MS 中存储了 F 中全部多项式的因子,且多项式具备对称性,如果传感器节点 S_i 是合法的,则移动汇聚节点 MS 一定能够找到一个 R_{1k} 满足 $H(R_{1k})=H(R_1)$,进而确定密钥:

$$k_k=f_k(ID_{MS},ID_{S_i})=f_k(ID_{S_i},ID_{MS})=k_{S_i} \tag{7}$$

作为移动汇聚节点 MS 与传感器节点 S_i 的共享密钥。移动汇聚节点 MS 保留密钥 k_k 并删除其余的 $(M-1)$ 个密钥。

3.3 认证

移动汇聚节点 MS 向传感器节点 S_i 发送认证消息 $E(k_k,R_{1k}||H(R_{1k}))$。传感器节点 S_i 解密后检查 $R_1=R_{1k}$ 是否成立,成立则意味着移动汇聚节点 MS 身份合法且已找到正确的密钥 k_{S_i}。

$$MS\rightarrow S_i:E(k_k,R_{1k}\,||\,H(R_{1k})) \tag{8}$$

4 方案分析

4.1 安全性分析

在敌对区域中,敌方物理俘获节点以获得其秘密信息是主要的攻击手段之一。节点抗俘获性,即敌方根据被俘获节点泄漏的信息能够直接得到或者间接计算出未俘获节点密钥的概率,是衡量一个密

钥管理方案安全性的重要参数。用未俘获节点的密钥泄漏概率 F_r 来描述节点抗俘获性：

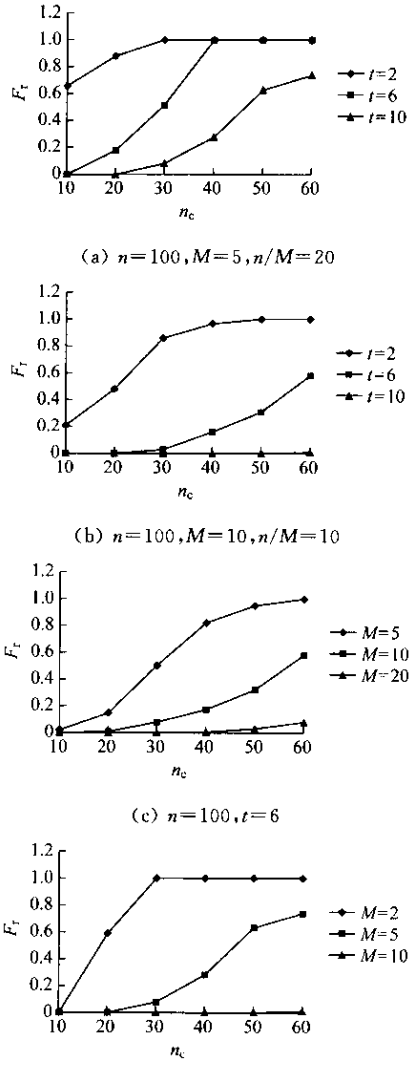
$$F_r = \frac{\text{未俘获节点中被泄漏的密钥数}}{\text{未俘获节点中的密钥总数}} \quad (9)$$

F_r 越大说明节点抗俘获性越差，即安全性越弱；反之，F_r 越小说明节点抗俘获性越好，即安全性越强；当 $F_r=0$ 时，网络对物理捕获节点具备完全抵抗能力，安全性最优。

改进方案中，所有节点存储的是多项式算子而非密钥本身，当敌方物理俘获 1 个或少量节点时无法得到未俘获节点的任何密钥信息，即使敌方俘获了移动汇聚节点也只能得到 M 个不同多项式的算子；但是，当敌方同时捕获了大量节点时，根据收集到的多项式算子可能将 1 个或多个多项式解出，进而计算出密钥本身。

为验证改进方案的安全性能，通过仿真实验来模拟密钥预分配、共享密钥建立和物理俘获节点的过程。图 2 为未俘获节点的密钥泄漏概率 F_r 与被俘获节点数 n_c 的关系。

从图 2 可看出，未俘获节点的密钥泄露概率 F_r 与多项式环大小 M 和多项式阶数 t 直接相关：对于确定的 M 和 t，F_r 随着 n_c 的增大而增大；对于确定的 n_c，F_r 随着 $\left|\frac{n}{M}-t\right|$ 的减小而减小，这说明当 t 与 $\frac{n}{M}$ 越接近，节点的抗俘获性越好，网络越安全。当 $\left(\frac{n}{M}-t\right)\leqslant 0$ 时，$F_r=0$，节点能够完全抵抗敌方的物理俘获。通过调节 t、n 和 M 的取值，可以满足任何节点的抗俘获性需求。



(a) $n=100, M=5, n/M=20$

(b) $n=100, M=10, n/M=10$

(c) $n=100, t=6$

(d) $n=100, t=10$

图 2　未俘获节点的密钥泄漏概率 F_r 与被俘获节点数 n_c 的关系

4.2　安全连通度

网络的安全连通度定义为通信双方能够建立共享密钥的概率 P_c。与概率型密钥管理方案不同，改进方案保证任一传感器节点都能够与移动汇聚节点成功建立共享密钥，即该方案确定连通且 $P_c=1$。

4.3　节点能耗分析

(1) 存储开销：在改进方案中，每个传感器节点只需要保存 1 个多项式算子和 1 个单向 Hash 函数，存储量较小且与网络规模无关；移动汇聚节点需要存储 M 个多项式算子和 1 个 Hash 函数。其中，单向 Hash 函数都是公开的，需要保密的只有多项式算子，则传感器节点的存储量为 $(t+1)\log\lambda$，移动汇聚节点的存储量为 $M(t+1)\log\lambda$。

(2) 通信开销：传感器节点与移动汇聚节点建立共享密钥的过程中，传感器节点只需发送 1 次消息，移动汇聚节点只需发送 1 次认证消息，通信量非常低。

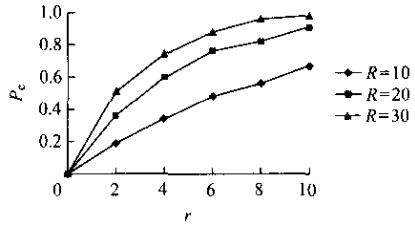
(3) 计算开销：每个节点需要调用 1 次多项式 f 来产生共享密钥，调用 1 次 Hash 函数用于认证，调用 1 次对称加密算法用于加密，计算量也是较低的、可接受的。移动汇聚节点的计算量约是普通传感器节点的 M 倍，但这对于资源丰富的移动汇聚节点来说也是可接受的。

4.4　密钥管理方案比较

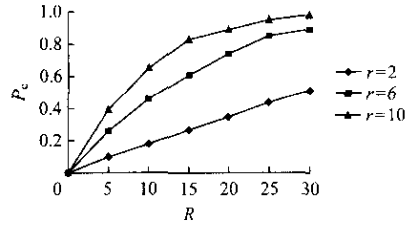
将随机密钥预分配方案改良后（概率型方案）应用于带移动汇聚节点的无线传感器网络：由于移动汇聚节点的存储力比普通传感器节点更强，因此，分别设置移动汇聚节点的密钥环大小 R 和传感器节点的密钥环大小 $r(R>>r)$，移动汇聚节点与传感器节点根据各自密钥环中存在的共同密钥来建立密钥对。通过仿真实验模拟该概率型方案的密钥预分

配、共享密钥建立和物理俘获节点等过程，并将实验结果与改进方案进行比较。

图 3 为概率型方案中传感器节点与移动汇聚节点的密钥环大小与安全连通度 P_c 的关系。



(a) $n=100$，|密钥池|=100



(b) $n=100$，|密钥池|=100

图 3 概率型方案中节点的密钥环大小与安全连通度的关系

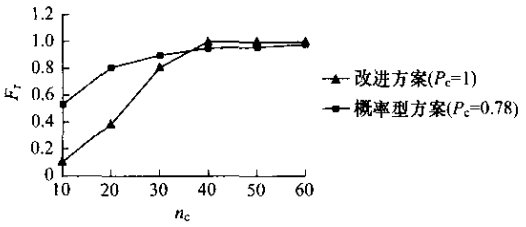
在相同的存储负载下，比较改进方案与概率型方案的节点抗俘获性，实验结果如图 4 所示(其中传感器节点数 $n=100$、概率型方案中密钥池大小为 100)。在有限域 $GF(\lambda)$ 上，一个密钥的长度为 $\log\lambda$，一个 t 阶多项式算子的长度为 $(t+1)\log\lambda$，因此，$(t+1)$ 个密钥与一个 t 阶多项式算子的存储负载相同。

从图 4 可看出，概率型方案中，节点必须通过增加密钥环大小来提高安全连通度 P_c，这不但会提高节点的存储负载，同时也会降低节点的抗俘获性；而改进方案在保证网络确定连通($P_c=1$)的前提下，传感器节点的存储负载更小、节点抗俘获性更强。

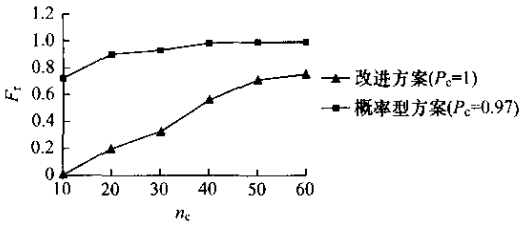
5 结语

利用对称多项式提出了一种改进的密钥管理方案，有效地解决了传感器节点与移动汇聚节点间密钥协商的问题。该方案利用移动汇聚节点资源较丰富的特点，通过少量增加移动汇聚节点的存储和计算开销，降低了传感器节点的能耗。实验结果表明，与传统的概率型方案相比，改进方案在保证网络全连通的前提下显著提高了节点的抗俘获能力。

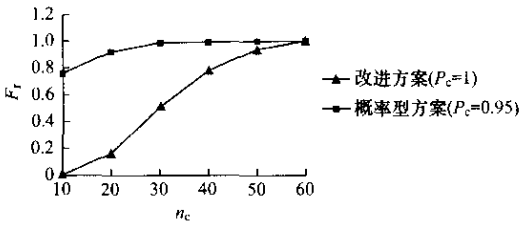
移动型无线传感器网络是无线传感器网络的发展方向，而引入移动汇聚节点是建立移动型无线传感器网络的第一步。目前，国内外的研究者已经提出很多适用于静止传感器网络的密钥管理方案，但



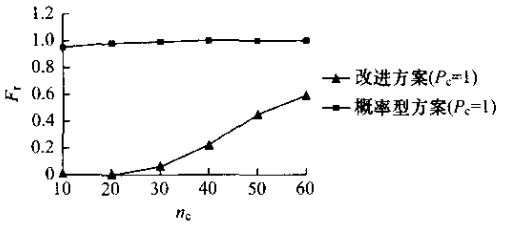
(a) $t=4, M=5; r=5, R=25$



(b) $t=4, M=10; r=5, R=50$



(c) $t=6, M=5; r=7, R=35$



(d) $t=6, M=10; r=7, R=70$

图 4 改进方案与概率型方案的节点抗俘获性比较

专门针对移动网络的研究还非常少。该改进方案的提出填补了这一研究空白，为移动型无线传感器网络密钥管理的进一步发展提供了新思路。

参考文献：

[1] CHAKRABARTI A, SABHARWAL A, AAZHANG B. Communication Power Optimization in a Sensor Network with a Path-Constrained Mobile Observer [J]. ACM Transactions Sensor Networks, 2006, 2(3): 297-324.

[2] JAIN S, SHAH R C, BRUNETTE W, et al. Exploiting Mobility for Energy Efficient Data Collection in Wireless Sensor Networks [J]. Mobile Networks and Applications, 2006, 11(3): 327-339.

[3] ESCHENAUER L, GLIGOR V D. A Key Management Scheme for Distributed Sensor Networks [C]//The 9th ACM Conference on Computer and Communication, 2002, Washington: 41-47.

文章编号:1671-251X(2011)10-0031-03 DOI:CNKI:32-1627/TP.20110922.1311.009

智能声发射仪的研究

袁臣, 童敏明, 贺新民, 唐守锋, 童夏敏, 邓世建

(中国矿业大学信电学院, 江苏 徐州 221008)

摘要:针对现有的声发射仪仅具有声发射数据采集功能,而无数据分析处理功能的问题,提出了一种智能声发射仪的设计方案。该声发射仪在数字式声发射仪的基础上,通过建立已知缺陷模式库,采用模糊识别模式对活动缺陷进行类型判定并作出等级评估。下一步工作重点是建立一个比较完善的标准声发射源数据库,为仪器的智能化实现打下基础。

关键词:声发射仪;数据分析;数据处理;缺陷模式库;模糊识别;活动缺陷;声发射源数据库

中图分类号:TD67 文献标识码:A 网络出版时间:2011-09-22 13:11

网络出版地址:http://www.cnki.net/kcms/detail/32.1627.TP.20110922.1311.009.html

Research of Intelligent Acoustic Emission Instrument

YUAN Chen, TONG Min-ming, HE Xin-min, TANG Shou-feng,
TONG Xia-min, DENG Shi-jian

(School of Information and Electrical Engineering of CUMT., Xuzhou 221008, China)

Abstract: In view of problems that current acoustic emission instruments have only collection function of acoustic emission data, but no function of data processing and analysis, the paper proposed a design scheme of an intelligent acoustic emission instrument. The instrument is built on digital acoustic emission instrument and known defects pattern base, and uses fuzzy recognition model to make type identification

收稿日期:2011-05-16

基金项目:国家重点基础研究发展计划("973"计划)资助项目(2007CB209407)

作者简介:袁臣(1988-),男,江苏镇江人,硕士研究生,主要从事声发射方面的研究工作。E-mail:yc13813484845@163.com

[4] CHAN H W, PERRIG A, SONG D. Random Key Predistribution Schemes for Sensor Networks[C]// 2003 IEEE Symposium on Security and Privacy, 2003, Berkeley: 197-213.

[5] JAWORSKI J, REN M, RYBARCZYK K. Random Key Predistribution for Wireless Sensor Networks Using Deployment Knowledge[J]. Computing, 2009, 85(1-2): 57-76.

[6] WANG J, XIA Z Y, HARN L, et al. Storage-Optimal Key Sharing with Authentication in Sensor Networks [C]//Parallel and Distributed Processing and Applications, 2005: 466-474.

[7] LIU D G, NING P, LI R F. Establishing Pairwise Keys in Distributed Sensor Networks [J]. ACM Transactions on Information and System Security, 2005, 8(1): 41-77.

[8] WEN M, ZHENG Y F, YE W J, et al. A Key Management Protocol with Robust Continuity for Sensor Networks[J]. Computer Standards and Interfaces, 2009, 31(4): 642-647.

[9] CHAKRABARTI A, SABHARWAL A, AAZHANG B. Using Predictable Observer Mobility for Power Efficient Design of Sensor Networks[C]//Proceeding Second Int'l Workshop Information Processing in Sensor Networks, 2003.

[10] BLUNDO C, SANTIS A D, HERZBERG A, et al. Perfectly-secure Key Distribution for Dynamic Conferences [C]//Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag Press, 1992: 471-486.