·物联网专题· 文章编号：1000—3428(2013)09—0064—05 文献标识码：A 中图分类号：TP393

基于 EBS 的分组分层 WSN 密钥管理策略

邓绍江，王 宇，田 袁，唐继强
(重庆大学计算机学院，重庆 400044)

摘 要：传统无线传感器网络(WSN)的基站通信模型安全性较差，对资源的依赖性较强。为此，提出一种基于组密钥排他基础系统的 WSN 密钥管理策略(EBS-GL)。采用网络分化思想提高系统的通信效率，利用分组分层加密算法提高系统的安全性，通过汇总消息比对方法进行信息完整性认证，使用奇异点排除策略增强系统的可恢复能力。仿真结果表明，与 JERT 策略相比，EBS-GL 可增强 WSN 基站的验错、纠错和排错能力，提高节点通信的安全性。

关键词：无线传感器网络；安全；密钥管理；排他基础系统；恰当冗余传输；分组分层

Grouping and Layered Key Management Strategy in WSN Based on EBS

DENG Shao-jiang, WANG Yu, TIAN Yuan, TANG Ji-qiang
(College of Computer Science, Chongqing University, Chongqing 400044, China)

【**Abstract**】There are many security problems in Wireless Sensor Network(WSN) on the base station model. These security problems include the low efficiency of error verification, correction and removal. Meanwhile, the information authentication has poor credibility, low communication security, and heavily depends on resource dependence. To improve the security of such network, an grouping and layered key management strategy in WSN based on Exclusion Basis System(EBS) which named EBS-GL is proposed. This model employs technologies such as network decoupling, a novel grouping and layered information encryption algorithm, the information integrity authentication mechanism, and the strategy of removing singularity. Simulation results prove that this model has stronger abilities of error verification, correction and removal of base stations than JERT strategy.

【**Key words**】Wireless Sensor Network(WSN); security; key management; Exclusion Basis System(EBS); appropriate redundancy transmission; grouping and layered

DOI: 10.3969/j.issn.1000-3428.2013.09.014

1 概述

无线传感器网络(Wireless Sensor Network, WSN)[1-2]由许多传感器节点组成，传感器节点的任务是收集数据。随着应用的普及，传感器网络的安全[3-4]日益显得重要，尤其是其中最基础和关键的密钥管理[5-6]问题。由于传感器能量[7]有限，为了能让传感器更有效地收集数据，可在网络中增加一些基站来负责传感器节点之间的数据通信。在无线传感器网络的基站通信模型[8]中，研究者已经提出了基于随机密钥预分配(Random Key Pre-distribution, RKP)[9]的网络分化方案(Random Key Pre-distribution of network Decoupling, RKP-DE)[10]和基于多路径加密[11]的恰当冗余传输方案(Just Enough Redundancy Transmission, JERT)[12]。而排他基础系统(Exclusion Basis System of dimension, EBS)[13]则是组合数学中研究的一个领域，其构建的无线传感器网络具有连通性好、易扩展、可恢复等优点。

在上述研究的基础上，本文提出一种分组分层的 EBS 密钥管理策略(EBS-GL)。改变基于 MDS[14-15]的编码方式，采用基于 EBS 的全新分组、分层加密算法，在此基础上建立信息验证机制和纠错、排错策略，以提高基站验错、纠错、排错能力和节点通信的安全性。

2 传统基站通信模型

2.1 基于 RKP-DE 的基站通信模型

随机密钥预分配不适用于低稠密度图和节点通信开销大的情况。RKP-DE 方案将 WSN 分化为逻辑图(信息加密)和物理图(信息传输)。RKP-DE 方案的分化过程如图 1 所示，包括以下步骤：(1)建立局部逻辑图和局部物理图；(2)邻居之间建立多密钥路径；(3)消除多密钥路径依赖关系(连接依赖消除和路径依赖消除)；(4)邻居之间建立对密钥路径。

基金项目：国家自然科学基金资助项目“多层次无线传感器网络结构及动态密钥管理研究”(6117317)
作者简介：邓绍江(1971－)，男，教授、博士，主研方向：无线传感器网络，信息安全；王 宇、田 袁，硕士；唐继强，博士
收稿日期：2013-03-06 **修回日期：**2013-04-16 **E-mail：**38326792@qq.com

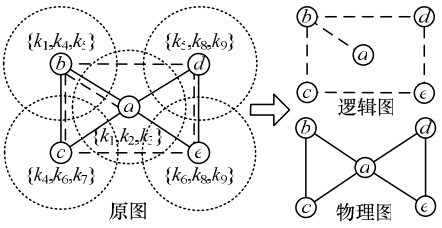

图 1　RKP-DE 网络分化过程

2.2　基于 JERT 的基站通信模型

JERT 方案基于 MDS 编码方式，具有强大的纠错能力，是以减小通信负载和增强通信安全性为目的的多路径设计方案。JERT 要求发送信息方根据通信路径的跳数数量和路径条数来决定通信信息的大小，其工作原理如图 2 所示。

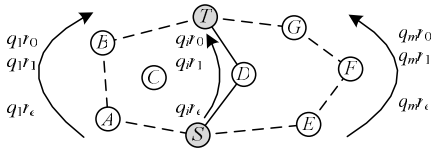

图 2　JERT 工作原理

其中，q_i 表示第 i 条路径所传输的信息占总信息的比例，$\sum_{i=1}^{i=m} q_i = 1$；$r_1, r_2, \cdots, r_e$ 表示第 i 次额外传输的信息，r_e 为 MDS 纠错的最大码字。

以节点 $S \to T$ 加密信息为例，已知 S 共有 m 条密钥路径可以到达 T，总传输信息量为 C。第 1 次第 i 条路径所传输的信息大小为 $C_i = q_i r_i$，$C = \sum_{i=1}^{i=m} C_i$，信息到达 T 后节点解密来自 m 条路径的信息将它们汇总，当有任意条路径发生问题时，通过 MDS 编码的信息就会检测出来，抛弃此路径信息，节点 S 将重新发送具有纠错功能的信息 r_i 从 m 条路径到达 T，对原来 T 中的信息进行纠错，最终实现信息的安全传输和信息验证。

2.3　基于 EBS 的密钥管理方案

EBS 是组合数学中研究的一个领域，其中与本文相关的定义如下：

定义 对正整数 m,n,k 都满足 $1 < k, m < n$ 条件下，由元素 $[1 \cdots n]$ 所构成的子集中，对于每个整数 $1 \leqslant t \leqslant n$，均满足以下条件：

(1)t 元素最多在 k 个子集中。

(2)对于子集 $A_1, A_2, \cdots, A_m$ 中，存在 $\bigcup_{i=1}^{m} A_i = [1 \cdots n] - [t]$，即存在 m 个子集元素总和为 $[1 \cdots n]$ 且不包含元素 t。

以 $EBS(8,3,2)$为例，制定密钥池 $A: \{A_1, A_2, A_3, A_4, A_5\}$，密钥分配如下：$A_1 = \{5,6,7,8\}$，$A_2 = \{2,3,4,8\}$，$A_3 = \{1,3,4,6,7,8\}$，$A_4 = \{1,2,4,5,7\}$，$A_5 = \{1,2,3,4,5,6,7\}$。以节点 5 为例，可以知道它具有 3 个共享密钥：A_1, A_4, A_5，且不具备的密钥 A_2、A_3，而 A_2、A_3 拥有的节点包含 $\{1,2,3,4,6,7,8\}$。当它被捕获，可以通过不具备的 2 个密钥 A_2、A_3 来更新其他节点，以排除节点 5，具体步骤如下：(1)创建一个新的密钥系列 key'。(2) A_1' 代替 A_1，分别用 A_2、A_3 加密。(3) A_4' 代替 A_4，分别用 A_2、A_3 加密。(4) A_5' 代替 A_5，分别用 A_2、A_3 加密。(5)分 2 条路径发送给所有节点：$En_{A_2}(key', A_1(A_1'), A_4(A_4'), A_5(A_5'))$，$En_{A_3}(key', A_1(A_1'), A_4(A_4'), A_5(A_5'))$。

由于节点 5 没有密钥 A_2、A_3，无法获取更新信息，因此最终将节点 5 排除。

3　EBS-GL 无线传感器网络密钥管理策略

EBS 密钥分配策略为多路径传输提供了优越的条件，但是基于 EBS 的多路径密钥管理方案使用不多。同时，基于 MDS 的 JERT 多路径信息管理策略在计算信息分发大小和信息验证时，过分依赖 WSN 的环境，且安全性能不高，可恢复性不好。为减少密钥管理策略对 WSN 的环境的依赖，增强基站对信息验错、排错的成功率，提高节点之间通信安全性和 WSN 的可恢复性，本文提出基于 EBS 的分组、分层的无线传感器网络管理策略。EBS-GL 密钥管理流程如图 3 所示。

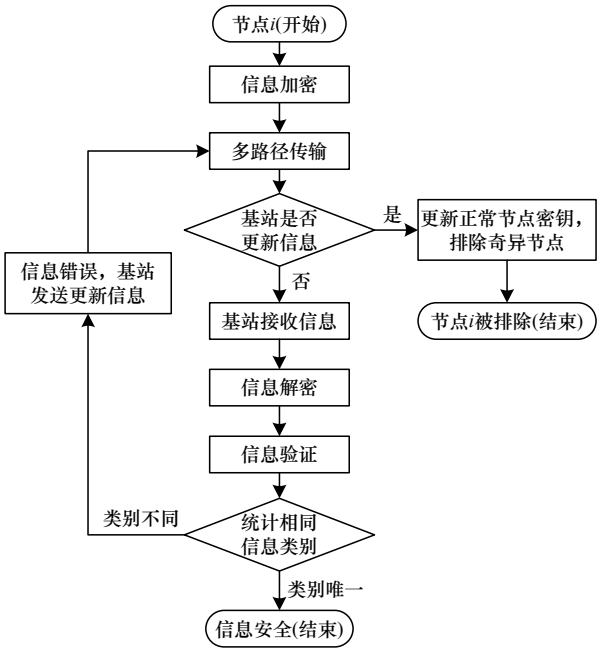

图 3　EBS-GL 密钥管理流程

本文策略中的符号定义如下：

(1) $EBS(n,k,m)$：具有 n 个节点，每个节点包含 k 个共享密钥，且不包含 m 个密钥的排他系统。

(2) A：密钥池；A_i：密钥池中第 i 号密钥。

(3) $Node_i$：节点 i。

(4) C：节点需要传输的信息，$C \neq C_1 + C_2 + \cdots + C_k$。

(5) N_i：路径 i 传输信息 C 时，随机截取 C 的信息长度(C_i 信息长度)就是 N_i 的值。N_i 的位数是基站规定的，并且位数固定，但是其值是随机的。

(6) C_i：对于路径 i，以 C 二进制编码第一位开始向后截取 $k(k=N_i)$位的二进制代码的信息量，$C_i = c_1, c_2, \cdots, c_k$。

(7) C_i'：路径 i 剩余信息量，$C_i' = C - C_i$。

(8) $En_{A_i}(C_j)$：表示用密钥 A_i 加密信息 C_j。

(9) S：所有路径加密后的信息总量，$S=\sum_{i=1}^{i=k}S_i$。

(10) S_i：路径 i 以密钥 A_i、A_j 加密后的信息，$S_i=En_{A_i}(C_i,A_j(C_i^{'}),N_i)$。

(11) CS：基站解密后信息总量，$CS=\sum_{i=1}^{i=k}CS_i$。

(12) CS_i：路径 i 被解密后的信息。

(13) M_i：基站发出的第 i 条更新密钥信息。

(14) A_e：被捕获的密钥。

(15) $A_i(A_i^{'})$：密钥 A_i (被捕获)被更新为 $A_i^{'}$。

3.1 EBS-GL 系统的构建

系统构建过程如下：

(1)密钥预分配：生成密钥池 $A:\{A_1,A_2,\cdots,A_y\}$，并对其中每个密钥进行位置编码，然后分配密钥组给各个节点，构建 $EBS(n,k,m)$，最后将各个节点相关信息保存在基站中。

(2)网络路径分化：通过节点 $Node_i$ 的 k 个共享密钥，构建到达基站的 k 条逻辑密钥路径(加密路径)，并使每条逻辑密钥路径编码与密钥位置进行一一匹配(基站通过路径编码找到被捕获密钥)，记录在基站中。

3.2 信息加密、通信与解密

假设任意节点 $Node_i$ 与基站通信，以及基站知道密钥池 A 的所有密钥和每个节点到基站的逻辑密钥路径。

3.2.1 信息加密

图 4 表示了节点一次加密过程，具体描述了路径 P_i 的 C_i 和 S_i，具体步骤如下(其他路径同理)：

(1)截取 i(i 为节点共享密钥数)次信息 C，每次截取信息位数为 N_i 的值(注意：不是 N_i 的位数)，将 C 变换成 i 段信息(即 $C\rightarrow C_1+C_2+\cdots+C_i$，第 i 条路径表示为 P_i)，每段信息 C_i 对应一个加密密钥 A_i。

(2)对于任意路径 P_i，计算 $C_i^{'}=C-C_i$，并通过 A_j 加密 $C_i^{'}$(即 $C_i^{'}=En_{A_j}(C_i^{'})$)。

(3)将 C_i、$En_{A_j}(C_i^{'})$ 和 N_i 通过 A_i 加密，获得路径 P_i 的传输信息 $S_i=En_{A_i}(C_i,En_{A_j}(C_i^{'}),N_i)$。

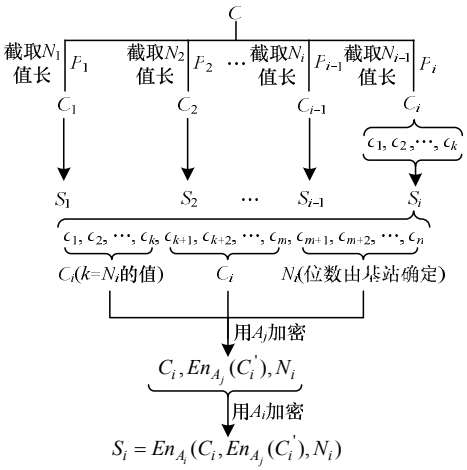

图 4 加密过程

3.2.2 通信

通信过程如下：

(1)节点 $Node_i$ 通过 i 条路径分别发送加密后的信息 $S_1,S_2,\cdots,S_{i-1},S_i$。对任意信息 S_i，只有拥有共享密钥 A_i 才能解密，而完全解密信息必须同时知道密钥 A_i、A_j 以及 N_i。

(2)节点 $Node_i$ 拥有共享密钥 A_i，解密接收到的 S_i，在此转发 S_i 并用 A_i 加密，不再做其他变动。

(3)经过多次转发加、解密，S_i 被转发到了基站，基站接收到后用每个密钥逐一解密。

3.2.3 信息解密

对信息进行解密时，基站得到由路径 i 发来的信息 CS_i 后将其保存下来，同时基站还收到路径 j 发来的信息 CS_j，最终基站接收到所有路径传来的信息 CS。解密过程如图 5 所示。

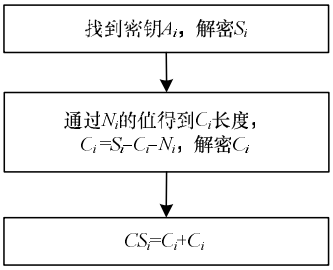

图 5 解密过程

3.3 信息验证机制与纠错、排错策略

对于一次通信，$Node_i$ 发送来的 CS 应共有 k 条(k=i，表示节点 $Node_i$ 发送到基站的路径数目)，基站对所有接收的 CS 条数做如下判断：

(1)如果不等于 k 条，则此信息不安全，丢掉此信息或命令源节点重发此信息。

(2)如果等于 k 条，基站按 CS_i 分类，相同信息会被分在一起($CS_i=CS_j$，如果全部 CS_i 都不同，则有 i 类)。

(3)若信息类别只有 1 类，则信息安全，基站可以使用。否则计算出各类的 CS_i 总数(路径条数)，找出总数最大的一类，而其余类对应的传输路径判定为损毁路径。进行如下排除：

1)通过 CS_i 的路径与密钥一一对应关系，找出源节点不具备的 m 个密钥 $A_{k+1}A_{k+2}\cdots A_{k+m}$ 以及源节点被捕获的 k 个密钥 $A_{e1}A_{e2}\cdots A_{ek}$。

2)基站计算出更新密钥 $A_{e1}^{'}A_{e2}^{'}\cdots A_{ek}^{'}$，用 $A_{k+1}A_{k+2}\cdots A_{k+m}$ 依次加密所有更新信息 $M_1M_2\cdots M_m$：

$$M_1=En_{A_{k+1}}(A_{e1}(A_{e1}^{'}),A_{e2}(A_{e2}^{'}),\cdots,A_{ek}(A_{ek}^{'}))$$

$$M_2=En_{A_{k+2}}(A_{e1}(A_{e1}^{'}),A_{e2}(A_{e2}^{'}),\cdots,A_{ek}(A_{ek}^{'}))$$

$$\cdots$$

$$M_m=En_{A_{k+m}}(A_{e1}(A_{e1}^{'}),A_{e2}(A_{e2}^{'}),\cdots,A_{ek}(A_{ek}^{'}))$$

由于源节点没有 $A_{k+1}A_{k+2}\cdots A_{k+m}$ 这 m 个密钥，因此

无法解密基站发出的 m 条信息，而其余所有节点都会接收到对应更新信息，从而改变与损坏节点共享的密钥 $A_e \to A_e^{'}$，最终排除损坏节点。

4　安全性与性能分析

实验通过 Omnetpp-4.2 仿真平台模拟 WSN 基站通信模型，从而对本文策略的安全性与性能进行分析。

4.1　安全性

EBS-GL 利用分组、分层加密策略完成信息通信。所以，要捕获一个节点的信息，必须同时捕获 2 层密钥以及随机数 N_i 的值。首先推得同时捕获 2 层密钥的概率为：

$$\left(\frac{1}{|A|}\right)\times\left(\frac{1}{|A|-1}\right)=\left(\frac{1}{|A|(|A|-1)}\right) \tag{1}$$

设 EBS-GL 编码码字 $Code=c_1c_2\cdots c_{x-1}c_x$ 存在 x 位。传输过程中可能存在的误码位数为 e 位，对任意 e 位误码来说都有一种可能是正确序列，而其余都是错误序列。则发生 e 位误码的错误序列的概率为：

$$p_c(e,x)=\frac{1}{C_x^e-1} \tag{2}$$

由于加密过程中 N_i 长度固定为 N 位，因此可能发生 $1\to N$ 位误码。令 $e\in[1,N]$，则捕获 N_i 的概率为：

$$\sum_{e=1}^{e=N}p_c(e,N)=\frac{1}{C_N^1-1}+\frac{1}{C_N^2-1}+\cdots+\frac{1}{C_N^{N-1}-1}+\frac{1}{C_N^N-1} \tag{3}$$

推出 EBS-GL 的安全系数为：

$$p_{\text{EBS-GL}}=1-\left(\frac{1}{|A|(|A|-1)}\right)\times\sum_{e=1}^{e=N}p_c(e,N) \tag{4}$$

当 N=2，$|A|$=2 时，EBS-GL 的安全系数为 0.5，安全性最差。随着密钥池和随机数 N_i 的提高，EBS-GL 的安全性提高明显。

由于 JERT 是通过多路径单密钥加密传输，因此，其安全系数为：

$$p_{\text{JERT}}=1-\left(\frac{1}{|A|}\right)^{path_{\text{muti}}} \tag{5}$$

其中，$path_{\text{muti}}$ 为多路径传输条数。

同理，与 EBS-GL 一样，JERT 安全系数为 0.5，安全性最差。

实验对比了 JERT 在 p=4、p=6(多路径条数)与 EBS-GL 在 N=16、N=24 的情况下，安全系数随密钥池规模增大的变化情况，如图 6 所示。其中，密钥池大小即密钥数量。可以看出，虽然在性能方面两者的安全系数都很高，但 JERT 的安全系数依赖于传输路径。当路径较多时，JERT 安全系数较高，表明其依赖于 WSN 环境，是难以控制、不可预测且不灵活的；而 EBS-GL 是基于码字随机数，对 WSN 环境没有太多依赖，对每次传输的码字是可控、可预测且灵活的，对其配置也较为方便。

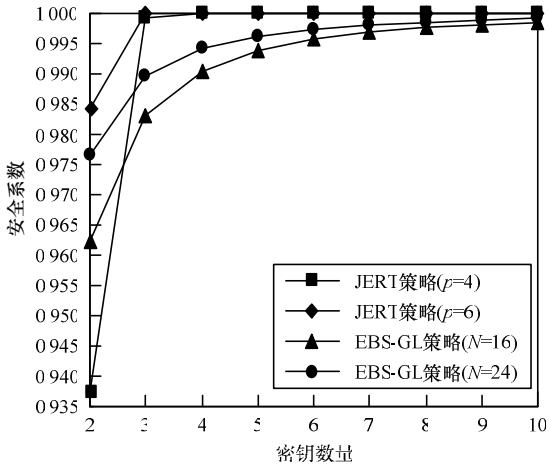

图 6　安全系数对比

4.2　验错成功率

假设传输路径被捕获率为 p_e，路径条数为 k。可以知道被捕获路径条数为 p_ek，正确路径为 $k(1-p_e)$。只有当 $p_ek>k(1-p_e)$ 时，即 $p_e\geqslant 0.5$，才有可能存在验错失败。

设每次通过分组、分层加密后的码字序列长度为 L 位。由于可能发生 $1\to L$ 位误码，令 $e\in[1,L]$，利用式(2)，推得任意一种可能的误码 e，使 p_ek 条(全部被捕获路径)错误序列全部相同的概率为：$\left(p_c(e,L)\right)^{p_ek}$。则发生 $1\to L$ 位误码，且错误序列全部相同的概率 p_{es}：

$$p_{es}=\sum_{e=1}^{e=L}\left(\frac{1}{C_L^e-1}\right)^{p_ek} \tag{6}$$

当且仅当 $p_{es}>1-p_e$ 时，存在 EBS-GL 验错失败。

实验对比了 JERT 和 EBS-GL 在 k=10、k=20 情况下，验错成功率与路径损毁率的关系，如图 7 所示。可以看出，由于 JERT 是基于 MDS 的多项式信息编码方式，因此路径损毁率提高后，对其影响不大。而 EBS-GL 是基于信息汇总机制，当路径损毁率高于 0.5 时，验错成功率就开始产生波动。但当路径损毁率小于 0.5 时，EBS-GL 的验错成功率明显大于 JERT，且波动较小。虽然 JERT 对路径损毁率的依赖不强，但总体来说对信息的验错效率不高。

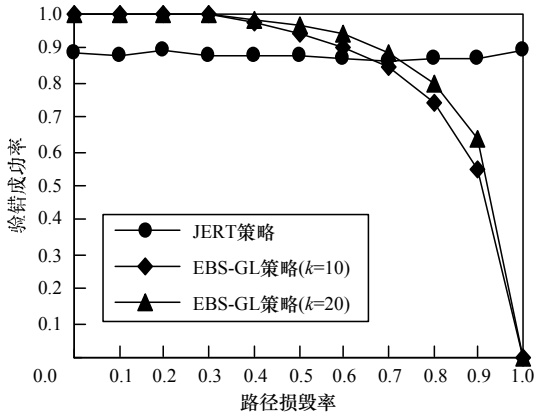

图 7　路径损毁率与验错成功率的关系

4.3 排错成功率

基站排错时共发出 m 条排错更新信息，因此，捕获到每条信息的概率为：

$$p_{\text{avg}}=\frac{1}{m} \tag{7}$$

由于每个节点拥有 k 个共享密钥，如果要使某个节点排错失败，则必须同时捕获发给该节点的 k 条信息，概率为：$\left(\frac{1}{m}\right)^k$。同时还需要捕获该节点拥有的 k 个共享密钥，概率为：

$$\prod_{i=0}^{i=k-1}\left(\frac{1}{|A|-i}\right)=\frac{1}{|A|}\times\frac{1}{|A|-1}\times\cdots\times\frac{1}{|A|-k+2}\times\frac{1}{|A|-k+1} \tag{8}$$

则可推出 EBS-GL 排错失败的概率为：

$$p_{e\text{-remove}}=\left(\frac{1}{m}\right)^k\times\prod_{i=0}^{i=k-1}\left(\frac{1}{|A|-i}\right) \tag{9}$$

由于 $m\geqslant 1,k\geqslant 2\Rightarrow|A|\geqslant 3$，因此 EBS-GL 排错性能最差为 $1-\frac{1}{6}$。

实验比较 EBS-GL 在 k=3, m=3、k=3,m=6、k=6, m=6 的情况下，排错成功率与密钥池大小的关系，如图 8 所示。可以看出，EBS-GL 在密钥池较小时排错成功率较低，随着密钥池增大，排错成功率显著增大。

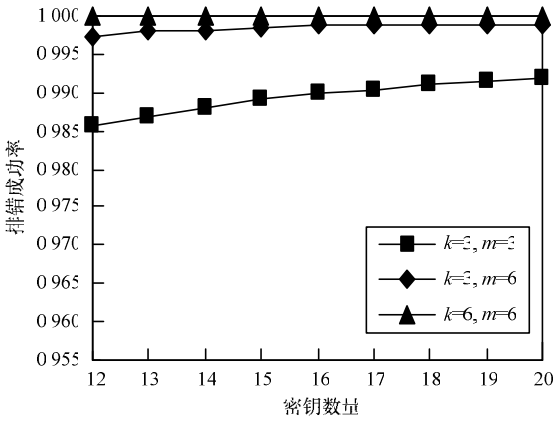

图 8 排错成功率

5 结束语

在 WSN 密钥管理中，基于 EBS 的密钥预分配方案能够提高系统的连通性和可恢复性，有利于实现基于分组的多路径传输方案。根据上述特点，本文提出一种基于 EBS 的分组分层密钥管理策略(EBS-GL)。仿真结果表明，该策略可提高系统通信的安全性；在路径损毁率小于 0.5 的情况下，EBS-GL 信息认证成功率明显高于 JERT 策略，且较为稳定，同时还能有效、稳定地排除各类被捕获节点。但该策略也存在一些不足，如要求路径损毁率较小、未考虑信道质量(如信道衰减、干扰等导致的误码)等，下一步将对此进行改进。

参考文献

[1] Akyildiz I F, Su Weilian, Sankarasubramamiam Y, et al. A Survey on Sensor Networks[J]. Computer Networks, 2002, 38(4): 393-422.

[2] 赵忠华, 皇甫伟, 孙利民, 等. 无线传感器网络管理技术[J]. 计算机科学, 2011, 38(1): 8-14.

[3] Manju V C. Study of Security Issues in Wireless Sensor Network[J]. International Journal of Engineering Science and Technology, 2011, 3(10): 7347-7352.

[4] Perrig A, Stankovic J, Wagner D. Security in Sensor Networks[J]. Communications of the ACM, 2004, 47(6): 53-57.

[5] 毕 斌, 王金一, 陈文亮, 等. 无线传感器网络管理综述[J]. 计算机系统应用, 2010, 19(12): 265-270.

[6] Eschenauer L, Gligor V D. A Key Management Scheme for Distributed Sensor Networks[C]//Proc. of ACM Conference on Computer and Communications Security. Washington D. C., USA: ACM Press, 2002.

[7] 石军峰, 钟先信, 陈 帅, 等. 无线传感器网络结构及特点分析[J]. 重庆大学学报: 自然科学版, 2005, 28(2): 16-19.

[8] Mhatre V, Catherine R. Design Guidelines for Wireless Sensor Networks: Communication, Clustering and Aggregation[J]. Ad Hoc Network, 2004, 2(1): 45-63.

[9] Chan H, Perrig A, Song D. Random Key Pre-distribution Schemes for Sensor Networks[C]//Proc. of IEEE Symposium on Security and Privacy. Berkeley, USA, IEEE Press, 2003.

[10] Gu Wenjun, Bai Xiaole, Chellappan S, et al. Network Decoupling: A Methodology for Secure Communications in Wireless Sensor Networks[C]//Proc. of the 14th IEEE International Workshop on Quality of Service. New Haven, USA: IEEE Press, 2006.

[11] Mahadevaswamy U B, Shanmukhaswamya M N. Reliable and Load Balanced Multi-path Routing for Multiple Sinks in Wireless Sensor Networks[J]. International Journal of Computer Applications, 2012, 50(12): 14-21.

[12] Deng Jing, Han Y S. Multi-path Key Establishment for Wireless Sensor Networking Using Just-enough Redundancy Transmission[J]. IEEE Trans. on Dependable and Secure Computing, 2008, 5(3): 177-190.

[13] Eltoweissy M, Heydari M H, Morales L, et al. Combinatorial Optimization of Group Key Management[J]. Journal of Network and Systems Management, 2004, 12(1): 33-50.

[14] Shailaja P, Mukeh Z. MDS and Trilateration Based Localization in Wireless Sensor Network[J]. Wireless Sensor Network, 2011, 3(6): 198-208.

[15] Deng Jing, Han Y S. Using MDS Codes for the Key Establishment of Wireless Sensor Networks[C]//Proc. of International Conference on Mobile Ad-hoc and Sensor Networks. Wuhan, China: [s. n.], 2005.

编辑 金胡考