计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2017,26(8):29−34 [doi: 10.15888/j.cnki.csa.005918]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于虹膜特征密钥的无线传感器网络安全数据融合①

李　敏[1], 王　旭[2], 周　俊[3], 刘书俊[1]

[1](解放军后勤工程学院 训练部装备处, 重庆 401311)
[2](四川外国语大学 国际商学院, 重庆 400031)
[3](96162 部队, 赣州 341000)

摘　要: 本文针对无线传感器网络中的数据融合操作面临严重的安全隐患, 提出了一种基于虹膜特征密钥的数据融合加密方案, 该方案不仅解决了在数据融合过程中密钥记忆和存储难的问题,而且也避免了中间节点攻击数据融合结果的问题. 通过抗攻击能力仿真实验分析, 该方案相比于传统的数据融合方案较为合理, 减少了节点能量消耗, 延长了网络生存周期.

关键词: 无线传感器网络; 安全; 数据融合; 虹膜特征; 密钥

引用格式: 李敏,王旭,周俊,刘书俊.基于虹膜特征密钥的无线传感器网络安全数据融合.计算机系统应用,2017,26(8):29–34. http://www.c-s-a.org.cn/1003-3254/5918.html

New Secure Data Aggregation Scheme of Wireless Sensor Networks Based on Iris Features Key

LI Min[1], WANG Xu[2], ZHOU Jun[3], LIU Shu-Jun[1]

[1](Training Department, Logistic Engineering Department of PLA, Chongqing 401311, China)
[2](International Business School, Sichuan International Studies University, Chongqing 400031, China)
[3](96162 Force, Ganzhou 341000, China)

Abstract: Aiming at the serious hidden danger of data fusion in wireless sensor networks, this paper proposes a data fusion and encryption scheme based on iris signature key. This scheme does not only solve the problem of key memory and storage during data fusion, it also avoids the attack of the intermediate nodes on the data fusion result. Simulation results show that the scheme is more reasonable than the traditional data fusion scheme, which reduces the node energy consumption and prolongs the network life cycle.

Key words: wireless sensor network; safety; data fusion; iris feature; key

1　引言

海防工程在长达几十年, 甚至上百年的服役过程中, 高盐高温高湿环境侵蚀、材料老化和荷载效应、人为的或自然的突变效应等灾害因素的耦合作用将不可避免地导致结构的损伤累计和抗力衰减, 从而使得抵抗自然灾害、正常荷载以及环境作用的能力下降, 引发灾难性的突发事故. 因此, 实时监测海防工程结构的健康状况信息, 及时发现危及安全的隐患, 为海防工程的急造、抢修抢建等保障活动赢取时间, 避免因海防工程设施损伤, 致使武器装备遭受重大经济损失.

近年来, 工程结构健康监测的研究与应用受到了广泛的关注并取得了显著的进展, 基于无线传感器网络[1](wireless sensor network, WSN)的工程结构健康监测已成为目前该学科最活跃的研究领域之一. 随着信息网络技术的发展, 具有部署简单、可快速组网及无需人工维护等诸多优点的无线传感器网络, 通常被部署在通信基础设施薄弱或电力供应匮乏的陌生区域, 但是网络内的传感器节点极易脱离整个网络的监控,

① 收稿时间: 2016-11-30; 采用时间: 2017-01-05

使得网络中的数据在进行融合操作时将面临严重的安全隐患. 此外, 为了延长网络的生命周期, 系统需要经常在网内进行数据融合操作, 然而被捕获的节点及容易发送伪造数据来改变整个融合结果, 这就会引发数据融合结果的不确定性. 因此, 为了有效解决数据融合过程中传感器节点被攻击者捕获以及确保数据融合的准确性, 有必要对数据融合方案的安全机制进行研究[2]. 然而安全机制研究的基础是加密算法, 加密算法的核心则是密钥管理. 因此, 本文从改进网络数据融合的安全性角度出发, 提出了一种基于虹膜特征密钥的无线传感器网络安全数据融合方案, 该方案可确保网络采集的信息在进行数据融合时, 满足数据认证、完整及保密等方面安全需求, 这对维护数据的可靠性和可用性至关重要.

2 系统概述

无线传感器网络安全需求主要包括 5 个方面[3], 即数据的机密性、完整性、新鲜性、源端认证、可用性, 其相互关系如图 1 所示[4].

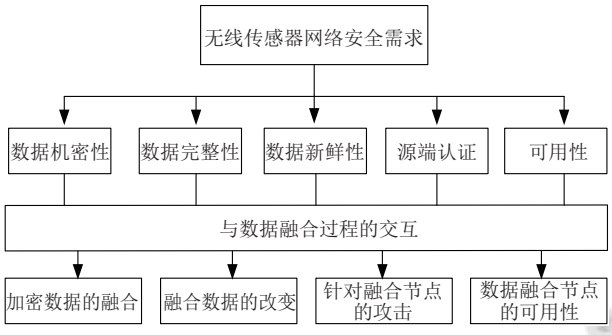

图 1 数据融合与安全需求之间的相互关系

传统网络的密钥管理方案已经研究了许多年, 也取得了丰富的成果. 但是由于无线传感器网络与传统网络的存储能力、计算能力以及能耗限制相差甚大, 无法直接应用于无线传感器网络中. 因此, 许多学者纷纷提出了多种针对无线传感器网络的密钥管理方案.

Cheng[5]等提出一种预置所有共享密钥方案, 该方案中所有的传感器节点均预配置一个共同的密钥, 所有的节点采集数据后均利用该密钥进行加密. 该方案计算简单, 安全性好, 但是对于大规模网络部署而言, 则需要大量存储空间, 同时也不利于增加新的节点.

Castelluccia[6]等提出一种基于流密钥的加性同态加密算法, 该方案是引入流密钥机制, 采用一次一密的加密方式, 并直接采用移位密码来实现同态加密, 使其加密方案的弹性得到了加强. 该算法假设各个节点均与基站共同享有一套伪随机函数和密钥种子, 且密钥在每次数据融合过程中均不相同. 该方案简单高效, 但存在问题是基站需要了解参与融合操作的节点 ID 号, 从而加大了节点的传输开销.

Girao[7]等提出 CDA(concealed data aggregation)算法, 该算法是将同态算法引入到无线传感器网络的数据融合领域, 利用加乘法同态加密体制完成对秘密数据的融合, 以保护数据的机密性. 其主要思想是传感器节点与基站共享一对公共的对称密钥, 并对中间融合节点保密, 融合节点只需对加密数据进行融合操作, 不需进行加解密, 并支持节点与基站之间进行端到端加密传输. 该方案存在的问题是算法的安全弹性较差, 主要是由于采用对称密钥加密方案, 且使用相同密钥.

Castelluccia[8]等提出一种多重加密方案, 该方案在数据融合开始前, 传感器节点将其拥有的密钥通知距该节点 t 跳的上游节点, 开始后, 节点均采用自己拥有的密钥对数据融合结果进行加密处理.

Feng[9]等提出的方案是采用节点之间的反应结果来进行数据融合, 从而使得数据融合结果更加精确. 其过程为节点先将其密钥发送至邻近节点, 若发现邻近节点未反应, 则将该邻近节点密钥传播.

Mykletun[10]提出的数据融合同态加密算法是基于公钥密码学, 该算法的传输和计算开销非常大.

黄廷辉等[11]针对密钥泄露问题, 提出了根据现有的 LEACH 协议, 通过管理节点预分发密钥, 加密和成对密钥的建立则是采用哈希函数, 以此来保证网络的安全性.

吴旭婧等[12]提出将传感器网络进行网络化, 划分为多个较小区域, 并将区域内的密钥种子池继续分成若干个与其一一对应的子密钥种子池, 区域内种子生成模式和文本由对应的节点进行选择, 通过指纹函数值建立匹配成功时的通信密钥.

李兰英等[13]针对网络密钥管理中存在扩展性差和连通率低等问题, 按照监测网络内的簇头节点以基站作为三方服务, 簇头与簇成员节点采用新方案通信, 而提出一种可扩展性强、网络连通率较高的密钥预分配方案.

张新帅[14]在对基于非对称密码体系的网络密钥管理技术深入研究的基础上, 通过实现公钥的合法性验

证和采用 Bloom filter 技术, 提出了一种基于身份密码体系的高效的密钥管理方案. 该方案不仅能够避免复杂的认证过程, 而且还能节省大量的存储空间, 确保密钥分配过程的安全性.

赵慎[15]针对无线传感器网络在资源有限的情况下, 结合网络自身特点与实际应用需求, 重新设计了密钥管理协议, 提出了一种基于整数模运算和连通图理论的密钥管理机制, 确保高效地完成整个网络会话密钥的管理.

付帅等[16]针对在 WSN 环境中, 隐私保护是数据融合技术中最具有挑战性的安全问题之一, 提出了一种隐私保护数据融合方案, 该方案采用 2 次不同形式的数据扰动, 不仅实现数据对基站的隐私保护, 而且也实现了对网内其他节点的隐私保护, 具有较好的抗数据丢失能力.

以上学者提出的方案是从不同角度改进网络数据融合的安全性, 可是它们的不足之处在于密钥存在记忆困难、不易存储等问题. 简单的口令虽然容易记忆, 但容易被破解, 而且也不安全; 复杂的密钥难于记忆, 只能存于计算机、智能卡等存储介质中, 而且还容易丢失.

虹膜由于具有可采集性、非侵犯性、稳定性, 特别是拥有唯一性等特点, 现在常常用来作为一种重要的身份识别特征, 且与密钥结合比其它生物特征与密钥结合更容易实现[17]. 本文提出的基于虹膜特征的密钥源自人体本身, 密钥可动态生成, 用户不仅无需记忆或存储密钥, 而且也不需要保存虹膜特征信息, 在确保数据融合安全性能的同时, 大大降低了节点存储空间, 并节约了网络的通信能量.

3 安全数据融合方案

部署在网络中的传感器节点需要不间断的采集大量数据, 故本方案中节点与基站之间采用计算量小、速度快的对称密码体制, 这对于存储能力和计算能力都很弱的传感器节点来说是十分重要的. 其方案的实施步骤示意图如图 2 所示.

图 2 安全的数据融合方案实施步骤示意图

Step1. 系统初始化. 由于基于预置的密钥管理方案[18]思想非常适合无线传感器网络, 因而在部署传感器节点之前, 将私钥或其相关信息提前置入到节点中, 待部署完并形成自组织网络之后, 节点将其 ID 号或预置信息进行广播, 网络内的其它节点通过计算接收到信息, 从而计算得出共享密钥.

Step2. 密钥生成与分发. 采用基于 KDC(Key Distribution Center)的密钥管理方案[19]思想, 用于产生虹膜特征密钥的一个可信第三方 KDC, 一般可用 Sink 节点作为 KDC. 其基本思想是 KDC 首先对虹膜进行预处理, 以便提取虹膜特征和完成二进制编码, 最后生成所需的虹膜特征密钥. 基于 KDC 的密钥管理方案采用对称密码体制, 使用逻辑密钥分级结构来有效分配密钥. KDC 负责整个网络的密钥分发, 并用公钥对密钥进行加密, 并向无线传感器网络广播密钥密文, 各个传感器节点接收到密钥密文之后, 用私钥进行解密, 以获取虹膜密钥.

Step3. 加密与解密. 当网络内出现数据融合操作, 节点立刻采用获取的虹膜特征密钥对采集到的数据进行加密, 然后将密文上传至上层节点. 中间融合节点在接收到子节点上传的数据后, 无需对数据加解密, 而是直接对传递的密文进行融合和统计分析, 并将融合结果向上转发. 基站直接将整个网络数据融合结果传送至数据处理中心, 最后通过虹膜特征密钥进行解密, 以获取数据融合结果.

3.1 虹膜特征密钥生成

3.1.1 虹膜预处理[20]

这个过程主要包括图像采集、虹膜定位、归一化等几个步骤, 如图 3 所示, 目的是对虹膜有效区域进行处理以供特征提取. 图像采集除虹膜外, 还应包括眼睑睫毛和瞳孔, 因此, 虹膜定位在去除眼睑、睫毛和光斑等干扰外, 重点在于提取虹膜环状纹理.

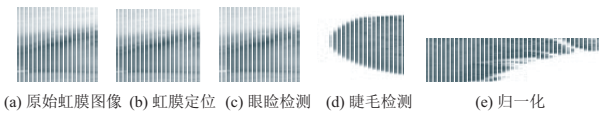

图 3 虹膜预处理

3.1.2 虹膜特征提取及编码

对图 3(e)中的虹膜进行归一化图像分析, 如图 4 所示. 由于 $R1$、$R2$ 区域受眼睑干扰较严重, 故选择 $R3$ 区域为特征提取区域.

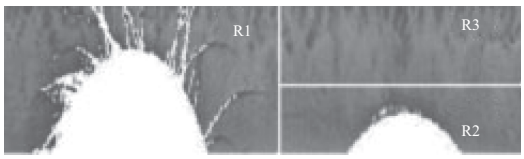

图 4 特征提取区域选取

本文采用 2D Haar 小波对 $R3$ 区域进行四级分解, 以便提取虹膜特征, 如图 5 所示. 由于虹膜特征分量主要集中在第四层, 因此提取第四层的高频子图 LH_4、HL_4 和 HH_4 作为虹膜特征.

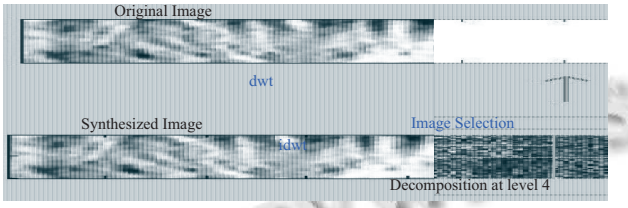

图 5 Haar 小波四级分解图

小波系数表示小波与分解信号的相似程度, 具有正小波系数与负小波系数描述的相似程度截然不同的性质, 利用该性质对获得的 117 个特征系数二值化为二进制编码. 设 $C=\{LH_4, HL_4, HH_4\}$为虹膜特征空间, 其元素 $C(i)$的编码规则如式(1):

$$\begin{cases} C(i)=0 & \text{if} \quad C(i)<0 \\ C(i)=1 & \text{if} \quad C(i)\geq 0 \end{cases} \quad 1\leq i\leq 117 \qquad (1)$$

经过以上编码规则, 可以得到 117 bit 的虹膜特征码, 如图 6 所示.

```
Columns 1 through 10
  1  0  1  1  1  1  1  0  1  1
Columns 11 through 20
  1  1  0  1  1  0  1  1  1  0
Columns 21 through 30
  1  1  1  1  1  0  1  1  0  1
Columns 31 through 40
  0  0  1  1  1  1  1  1  1  0
Columns 41 through 50
  1  1  0  1  1  0  1  1  0  1
Columns 51 through 60
  1  0  1  1  0  1  1  0  1  1
Columns 61 through 70
  0  0  1  0  0  1  0  0  1  0
Columns 71 through 80
  1  1  0  0  1  0  0  1  1  1
Columns 81 through 90
  1  1  0  0  1  0  0  1  1  0
Columns 91 through 100
  0  0  0  0  1  1  1  1  1  1
Columns 101 through 110
  1  0  1  1  0  0  1  1  1  1
Columns 111 through 117
  1  0  0  0  1  1  1
```

图 6 117 bit 虹膜特征码

3.1.3 DES 密钥提取

DES(Data Encryption Standard)算法是一种用 56 位密钥来加密 64 位数据的方法, 虽然 DES 算法已经被新的加密算法所取代, 但是由于无线传感器网络节点存在计算能力弱、能量有限等特点. 因此, 把 DES 算法应用于无线传感器网络中, 仍具有举足轻重的作用.

采用 DES 算法对传感器节点传送的融合数据进行加密, 其密钥源自于 117bit 的虹膜特征码. 假设 117bit 虹膜特征码序列为 $K=\{k_1, \ldots, k_i, \ldots, k_m\}$, 提取的 64 位密钥序列为 $R=\{r_1, \ldots, r_i, \ldots, r_m\}$. DES 密钥是通过映射函数 $f:R\rightarrow K$ 从集合 K 中按照 R 的自然排列顺序逐一选取, 这里定义映射函数 $f(j)$为:

$$f(j)=[(m-j+z_r) \bmod m]+1, z_r\in Z \qquad (2)$$

其中, z_r 为采用线性同余法产生伪随机整数, 且 $0<z_r<10^7$.

为了提高数据融合所需密钥的安全性, 随机函数 f 把密钥组序列 j 映射到虹膜特征码序列 K, 即 $r_j=k_i$. 经过对虹膜处理后, 提取的虹膜特征码为 117 bit, 即 $m=117$, 通过式(2)映射得到 64 bit 的 DES 密钥 R, 如图 7 所示.

```
Columns 1 through 19
  1  1  0  0  1  0  1  1  1  0  1  1  1  0  1  0  1  1  1
Columns 20 through 38
  0  0  0  0  1  1  1  1  0  1  1  0  0  1  1  0  0  0  0
Columns 39 through 57
  1  1  1  1  1  1  1  1  1  1  1  0  1  1  1  1  0  0  1
Columns 58 through 64
  1  1  1  0  1  0  0
```

图 7 从虹膜特征码中提取出的 64 bit DES 密钥 R

3.2 虹膜特征密钥分发

假设网络部署完毕后, 每个节点都被赋予唯一的网络标识号, 并通过网络标识号知道该节点在整个网络中的逻辑位置. 网络拓扑基于分簇型数据融合方式, 如图 8 所示. 数据融合开始后, 当簇成员节点需要从虹膜特征密钥池中取得所需密钥时, 基站就采用基于 KDC 的密钥管理方案, 使用公钥加密来广播虹膜特征密钥, 如式(3)所示:

$$S\rightarrow *: type, E_p[ID_s, Msg] \qquad (3)$$

其中, $type$ 表示传输为广播消息, 其它节点可选择私钥解密信息, 以获取虹膜特征密钥.

3.3 虹膜特征密钥加解密

数据融合操作开始之后, 通信双方应用虹膜特征密钥和 DES 算法进行加、解密. 首先, 簇成员节点根据接收到的虹膜特征密钥计算出簇成员节点探测数据的消息鉴别码 MAC[21], 然后将数据及 MAC 值一起传

送至簇头节点. 如图 8 中簇成员 A 和 B, 通过式(4)进行加密处理.

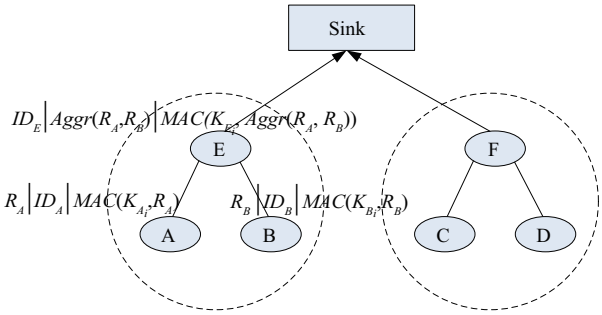

图 8 分簇型数据融合方式

$$A \to E \quad R_A \left| ID_A \right| MAC(K_{A_i}, R_A) \tag{4}$$

其中, R_A 是簇成员节点 A 产生的数据, ID_A 是节点 A 的标识, K_{Ai} 是在某一时间段上, A 与基站共享的虹膜特征密钥. 簇头节点在收到簇内成员节点上传数据后, 进行数据融合操作, 并将结果及其 MAC 值上传至 $Sink$ 节点, 如图 8 中簇头节点 E, 通过式(5)进行数据融合操作.

$$E \to S \quad ID_E \left| Aggr(R_A, R_B) \right| MAC(K_{E_i}, Aggr(R_A, R_B)) \tag{5}$$

4 方案抗攻击能力分析

本文提出的安全数据融合方案只是从密钥生成、密钥长度及管理等 3 个方面进行了考虑, 而在能耗方面未能表现出突出优势. 因此, 本节主要对方案的抗攻击能力进行了分析, 并用 Matlab 进行了模拟仿真, 其实验环境设置为攻击者对节点捕获是随机的, 且只分析在密钥建立阶段系统抵抗攻击的能力.

安全连通概率 P 是指, 在通信范围内, 融合节点与其所有相邻节点之间至少拥有一个虹膜特征密钥的概率[22], 如式(6)所示:

$$P = (1 - p_s^2) \times \frac{\binom{w-t}{t}}{\binom{w}{t}} \tag{6}$$

其中, P_s 为安全节点的比例数, w 为虹膜特征密钥池的大小, t 为普通节点从 w 中选取的密钥数. P 不仅是无线传感器网络密钥管理方案中一个重要指标, 而且还决定了节点密钥协商的跳数.

当网络中传感器节点部署完毕后, 仍然存在节点间的链路受到攻击, 其根本原因在于攻击者可以物理捕获节点的所有密钥信息. 在本方案设计中, 由于引入了具有抗碰撞性和单向运行性的 Hash 函数, 因此节点密钥是依据节点的 ID 号从虹膜特征密钥池中通过 Hash 函数计算得出的. 由于计算得出的密钥不尽相同, 因此, 攻击者无法从捕获的密钥推算出其它密钥以及原始密钥信息. 根据密钥管理方案可知, 所有节点收到虹膜特征密钥后都将转为安全节点, 这时整个网络系统具有完全抗攻击能力. 因此, 本节仅分析在密钥建立阶段时网络的抗攻击性.

本文假设网络中节点被捕获是随机的, 可以得出普通节点在 n 个已被捕获节点中的个数为 $n(1\text{-}P_s)$, 相邻节点间的安全连通概率 P=0.33[23]. 假设虹膜特征密钥池的大小为 w 时, 普通节点从中选取的密钥数为 t, 概率为 t/w. 因此, 当 n 个节点被捕获时, 安全链路被攻击的比例 P_b 如式(7)所示:

$$P_b = (1 - \left(1 - \frac{t}{w}\right)^{n(1-P_s)} \tag{7}$$

相邻节点间的安全连通概率 P=0.33.

图 9 是当传感器节点上保存密钥数 t=100 时, 在方案 P_s 不同的情况下, 节点抗攻击能力变化示意图. 可以得出, 在一定的连通概率下, 当 P_s 增加到某种程度, 网络抗攻击能力趋于平衡. 这是由于随 P_s 增加, 虹膜特征密钥池中的密钥数则会相应减少, 泄露密钥的概率则会增加. 图 10 可以得出, 当虹膜特征密钥池中的密钥数一定时, 随着 P_s 的增加, P_b 则会相应的增加, 即网络的抗攻击能力是随着 P_s 的增加一直增大. 这是因为在数据融合的整个过程中, 都不需要保存虹膜特征信息, 即使攻击者得到了节点存储的信息, 也不能获取虹膜特征密钥.

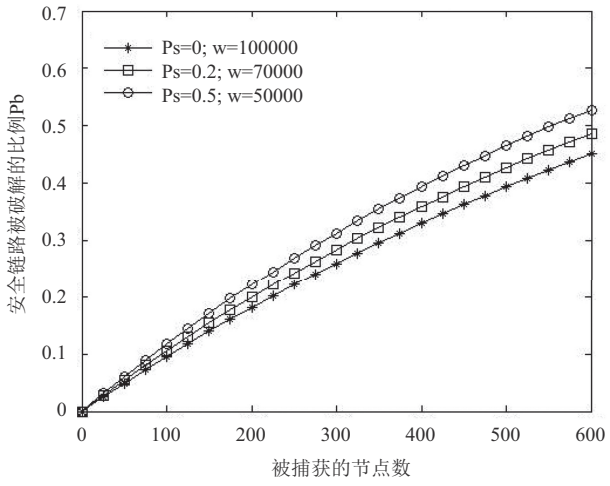

图 9 被捕获的节点数与安全链路被破解比例之间的关系

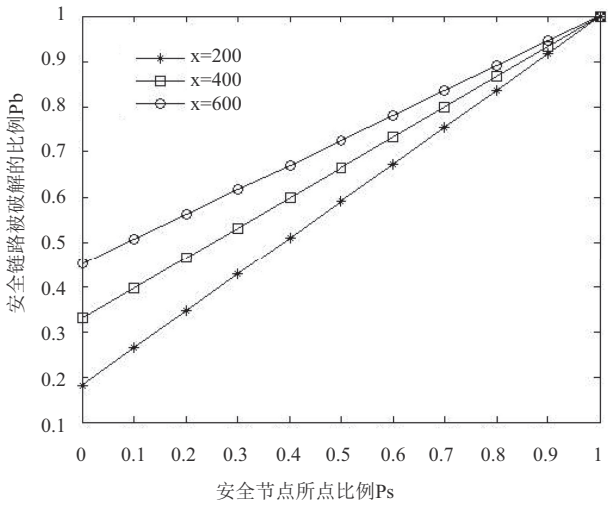

图 10 安全节点所占的比例与安全链路被破解比例之间的关系

5 结束语

无线传感器网络技术是当前信息领域的研究热点, 将其应用于远离大陆、基础通信设施薄弱及电力供应缺乏的南海岛礁海防工程监测领域, 有着巨大的应用前景. 本文提出的方案对于数据融合的安全性和高效性起到了一定的作用, 其优点在于可以方便地采用一次一密加密技术, 即使密钥泄露, 整个网络的安全性也不会遭到破坏, 抗毁性能强. 但该方案由于采用对称密钥, 且所有簇成员节点同时共享同一密钥, 安全弹性较差.

参考文献

1 孙利民, 李建中. 无线传感器网络. 北京: 清华大学出版社, 2005.

2 周强, 杨庚, 李森, 等. 一种可检测数据完整性的隐私数据融合算法. 电子与信息学报, 2013, 35(6): 1277–1283.

3 魏利利. 无线传感器网络轻量级安全数据融合方案的研究[硕士学位论文]. 南京: 南京邮电大学, 2013.

4 Ozdemir S, Xiao Y. Secure data aggregation in wireless sensor networks: A comprehensive overview. Computer Networks, 2009, 53(12): 2022–2037. [doi: 10.1016/j.comnet.2009.02.023]

5 Lai BC, Kim S, Verbauwhede I. Scalable session key construction protocol for wireless sensor networks. Proc. of IEEE Workshop on Large Scale Real-Time and Embedded Systems (LARTES). Austin, USA. 2002.

6 Castelluccia C, Mykletun E, Tsudik G. Efficient aggregation of encrypted data in wireless sensor networks. Proc. of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services. San Diego, CA, USA. 2005. 109–117.

7 Westhoff D, Girao J, Acharya M. Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation. IEEE Trans. on Mobile Computing, 2006, 5(10): 1417–1431. [doi: 10.1109/TMC.2006.144]

8 Castelluccia C. Securing very dynamic groups and data aggregation in wireless sensor networks. Proc. of IEEE International Conference on Mobile Adhoc and Sensor Systems. Pisa, Italy. 2007. 1–9.

9 Feng TM, Wang C, Zhang WS, *et al*. Confidentiality protection for distributed sensor data aggregation. Proc. of the 27th Conference on Computer Communications. Phoenix, AZ, USA. 2008. 56–60.

10 Mykletun E, Girao J, Westhoff D. Public key based cryptoschemes for data concealment in wireless sensor networks. Proc. of IEEE International Conference on Communications. Istanbul, Turkey. 2006. 2288–2295.

11 黄廷辉, 杨旻, 崔更申, 等. 基于 LEACH 协议的无线传感器网络密钥管理路由方案. 传感技术学报, 2014, 27(8): 1143–1146.

12 吴旭婧, 许勇, 张亚楠. 基于指纹模式匹配的无线传感器网络密钥预分配方案. 计算机工程, 2015, 41(3): 106–109.

13 李兰英, 易春焕, 孙建达, 等. 基于单位元的无线传感器网络密钥管理方案. 计算机工程与应用, 2015, 51(2): 94–98.

14 张新帅. 基于非对称密码体制的无线传感器网络密钥管理研究[硕士学位论文]. 南京: 东南大学, 2015.

15 赵慎. 基于整数取模的无线传感器网络密钥管理机制的研究[硕士学位论文]. 北京: 北京理工大学, 2016.

16 付帅, 姜奇, 马建峰. 一种无线传感器网络隐私保护数据聚合方案. 计算机研究与发展, 2016, 53(9): 2030–2038.

17 史春蕾, 杨丹丹, 韩飞. 虹膜识别综述. 科技展望, 2016, (5): 307.

18 Karlof C, Sastry N, Wagner D. TinySec: A link layer security architecture for wireless sensor networks. Proc. of the 2nd International Conference on Embedded Networked Sensor Systems. Baltimore, MD, USA. 2004. 162–175.

19 周俊, 罗挺, 王帅, 等. 不均匀光照下的虹膜定位算法研究. 后勤工程学院学报, 2010, 26(6): 78–86.

20 Chan HW, Perrig A, Song D. Key distribution techniques for sensor networks. Wireless Networks, 2004, 6(2): 277–303.

21 Hu LX, Evans D. Secure aggregation for wireless networks. Proc. of 2003 Symposium on Applications and the Internet Workshops Washington DC, USA. 2003. 384.

22 张建民. 智能建筑中无线传感器网络安全研究[博士学位论文]. 武汉: 华中科技大学, 2007.

23 Chan HW, Perrig A, Song D. Random key predistribution schemes for sensor networks. Proc. of 2003 Symposium on Security and Privacy. Berkeley, CA, USA. 2003. 197–213.