一种基于二次型的无线传感器网络密钥管理方案

王小刚,石为人,周 伟,高 鹏,蒋亿松
(重庆大学自动化学院,重庆 400044)

摘 要: 针对现有的基于多项式的密钥预分配管理方案受限于节点间密钥共享率和网络连通率等问题,文中提出了一种基于二次型的无线传感器密钥管理方案.该方案突破现有二元 t 次对称多项式建立共享密钥的思路,引入多元非对称二次型多项式,利用二次型特征值与特征向量之间的关系,分析证明二次型正交对角化的特性,生成密钥信息,节点则通过交换密钥信息实现身份认证,生成与邻居节点之间独立唯一的会话密钥.性能分析表明,与现有的密钥管理方案相比,方案在抗俘获性、连通性、可扩展性、通信开销和存储开销上有较大的改进.

关键词: 无线传感器网络; 密钥管理; 二次型; 特征值; 特征向量
中图分类号: TP393.02 **文献标识码:** A **文章编号:** 0372-2112 (2013) 02-0214-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.02.002

A Key Management Scheme Based on Quadratic Form for Wireless Sensor Network

WANG Xiao-gang, SHI Wei-ren, ZHOU Wei, GAO Pen, JIANG Yi-song
(*College of Automation, Chongqing University, Chongqing*, 400044, *China*)

Abstract: This paper presents a key management scheme based on quadratic form polynomial for wireless sensor network (WSN) for the problems that some existing key pre-distribution schemes are limited in key sharing and network connectivity probability between neighbor nodes. It beyonds the current ideas for establishing shared key based on quadratic symmetric polynomial and presents the multiple asymmetric quadratic form polynomial, and analyzes the orthogonal diagonalization properties of quadratic form to generate the key information by the relationship between eigenvalues and eigenvectors of the quadratic form, the nodes could achieve identification and generate the unique session keys between the neighbor nodes through exchanging the key information. Compared to some existing key pre-distribution schemes, the analysis of performance show that this scheme could resist captive, have good scalability and connectivity, and have a lower storage cost, a lower communication overhead.

Key words: wireless sensor network; key management; quadratic form; eigenvalues; eigenvectors

1 引言

由于传感器节点大多被部署在无人触及或容易受损或被俘获的环境中,所以保证 WSN 的安全性是应该优先考虑的问题.目前,网络安全问题已成为 WSN 的一个研究热点[1,2],而密钥管理是无线传感器网络的安全基础[3,4].提供安全、可靠的保密通信是密钥管理最重要、最基本的内容,同时也是安全路由、安全定位、广播认证、安全数据融合等安全机制解决方案的基础.

事实上,节点资源的严重受限导致现有的成熟密钥管理机制难以得到有效的应用.基于此,研究者设计了多种 WSN 密钥预分配管理方案,主要有三类:①基于密钥池的密钥预分配方案,如 Eschenauer-G1igor 随机密钥预分配方案[5]、q-composite 随机密钥预分方案[6]、随机密钥对预分配方案[7]等.这类方案,每个节点从密钥池中任意选择若干密钥,通信时只与具有相同密钥的节点通信,优点是应用简单,计算负载小,能支持网络的动态变化,但是由于节点间共享的密钥不唯一,密钥共享率低,不支持身份认证,攻击者很容易使用获得的密钥信息,有效地进行各种恶意攻击.②基于多项式密钥池的密钥预分配方案,如基于多项式的密钥预分配方案[8]、基于多密钥空间的密钥对分配方案[9]、n-conference t-secure 方案[10]、基于矩阵的密钥预分配方案[11]、基于配置知识的密钥预分配方案[12]等.这类方案一般能够抵抗俘获攻击,安全性较高,网络连通性较好,但是计算开销大,不支持邻居节点的身份认证、网络的可扩展性不强,不利于新节点的加入.③其它密钥预分配方案,如基于 Grid 模型的方案[13]、基于逻辑密钥树的密钥管理方

收稿日期:2012-05-02;修回日期:2012-08-06
基金项目:国家科技支撑计划(No.2011BAJ03B13)

案[14]等,这些方案虽然网络连通性高、存储开销小,但是网络适用性和安全性较差.

本文突破现有二元 t 次对称多项式建立共享密钥的思路,引入多元非对称二次型多项式,提出了一种基于二次型的无线传感器密钥管理方案.方案与现有的密钥管理方案相比,在抗俘获性、连通性、可扩展性、通信开销和存储开销上有较大的改进.

2 二次型特性分析

2.1 二次型定义

定义 1 设 P 是一数域,一个系数在数域 P 中的 $x_1, x_2, \cdots, x_n$ 的多元非对称二次齐次多项式

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j \tag{1}$$

称为数域 P 上的一个 n 元二次型.

把式(1)的系数排成一个 $n \times n$ 矩阵 $\boldsymbol{A}$

$$\boldsymbol{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \tag{2}$$

称 $\boldsymbol{A}$ 为二次型 $f(x_1, x_2, \cdots, x_n)$ 的矩阵,其中 $a_{ij} = a_{ji}$, $i, j = 1, \cdots, n$,即 $\boldsymbol{A} = \boldsymbol{A}^{\mathrm{T}}$ 为对称矩阵.为了简易表述 $f(x_1, x_2, \cdots, x_n)$,令 $\boldsymbol{X} = [x_1, x_2, \cdots, x_n]^{\mathrm{T}}$,则

$$f(x_1, x_2, \cdots, x_n) = \boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{X} \tag{3}$$

2.2 特征值与特征向量

定义 2 设 $\boldsymbol{A}$ 是数域 P 上的一个矩阵,如果对于数域 P 中的一数 λ,存在一个非零向量 ξ,使得

$$\boldsymbol{A}\xi = \lambda\xi \tag{4}$$

那么 λ 称为 $\boldsymbol{A}$ 的一个特征值,而 ξ 称为 $\boldsymbol{A}$ 的属于特征值 λ 的一个特征向量.

根据式(4)可以得出 $(\lambda\boldsymbol{E} - \boldsymbol{A})\xi = 0$,也说明 ξ 是方程(5)的非零解,且式(5)有非零解的充分必要条件就是 $|\lambda\boldsymbol{E} - \boldsymbol{A}| = 0$.

$$\begin{cases} (\lambda - a_{11})x_1 - a_{12}x_2 - \cdots - a_{1n}x_n = 0 \\ -a_{21}x_1 + (\lambda - a_{22})x_2 - \cdots - a_{2n}x_n = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ -a_{n1}x_1 - a_{n2}x_2 - \cdots + (\lambda - a_{nn})x_n = 0 \end{cases} \tag{5}$$

定义 3 设 $\boldsymbol{A}$ 是数域 P 上的 n 级矩阵,矩阵 $\lambda\boldsymbol{E} - \boldsymbol{A}$ 的行列式

$$|\lambda\boldsymbol{E} - \boldsymbol{A}| = \begin{vmatrix} \lambda - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n1} & -a_{n2} & \cdots & \lambda - a_{nn} \end{vmatrix} \tag{6}$$

称为 $\boldsymbol{A}$ 的特征多项式,这是数域 P 上关于 λ 的一个 n 次多项式.

为此,根据定义 2 和定义 3,确定矩阵 A 的特征值和特征向量的方法可以分成以下几步:

(a)在数域 P 上,选取一个二次齐次多项式 $f(x_1, x_2, \cdots, x_n)$,写出 $f(x_1, x_2, \cdots, x_n)$ 的矩阵 $\boldsymbol{A}$;

(b)求出 $\boldsymbol{A}$ 的特征方程 $|\lambda\boldsymbol{E} - \boldsymbol{A}| = 0$ 在数域 P 中全部的解,它们既是矩阵 $\boldsymbol{A}$ 的全部特征值;

(c)将所求得的特征值代入式(5)求解,得出一组基础解系,它们就是属于这个特征值的几个线性无关的特征向量.同样,也就得到属于每个特征值的全部线性无关的特征向量 $\{\xi_1, \xi_2, \cdots, \xi_n\}$.

2.3 矩阵 $\boldsymbol{A}$ 正交对角化

引理 1 设 $\boldsymbol{A}$ 是实对称矩阵,则在数域 P 上对任意的向量 $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, 有 $(\boldsymbol{A\alpha}, \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \boldsymbol{A\beta})$ 或 $\boldsymbol{\beta}^{\mathrm{T}}(\boldsymbol{A\alpha}) = \boldsymbol{\alpha}^{\mathrm{T}}(\boldsymbol{A\beta})$.

证明 实际上 $\boldsymbol{\beta}^{\mathrm{T}}(\boldsymbol{A\alpha}) = \boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{\alpha} = (\boldsymbol{A\beta})^{\mathrm{T}}\boldsymbol{\alpha} = \boldsymbol{\alpha}^{\mathrm{T}}(\boldsymbol{A\beta})$,也即 $(\boldsymbol{A\alpha}, \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \boldsymbol{A\beta})$.

引理 2 设 $\boldsymbol{A}$ 是实对称矩阵,则在数域 P 中属于 $\boldsymbol{A}$ 的不同特征值的特征向量必然正交.

证明 设 λ, μ 是 $\boldsymbol{A}$ 的两个不同特征值,$\boldsymbol{\alpha}, \boldsymbol{\beta}$ 分别是属于 λ, μ 的特征向量:$\boldsymbol{A\alpha} = \lambda\boldsymbol{\alpha}$, $\boldsymbol{A\beta} = \mu\boldsymbol{\beta}$.由引理 1 知,由 $(\boldsymbol{A\alpha}, \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \boldsymbol{A\beta})$,有 $(\boldsymbol{\lambda\alpha}, \boldsymbol{\beta}) = (\boldsymbol{\alpha}, \boldsymbol{\mu\beta})$,继而得出 $\lambda(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mu(\boldsymbol{\alpha}, \boldsymbol{\beta})$.而由于 $\lambda \neq \mu$,得出 $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 0$,即属于矩阵 $\boldsymbol{A}$ 的不同特征值的特征向量 $\boldsymbol{\alpha}, \boldsymbol{\beta}$ 必然正交.

定理 1 对于任意一个 $n \times n$ 级实数域的对称矩阵 $\boldsymbol{A}$,都存在一个 $n \times n$ 级正交矩阵 $\boldsymbol{B}$(其中 $\boldsymbol{B}^{\mathrm{T}} = \boldsymbol{B}^{-1}$, $\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B} = \boldsymbol{E}$),使 $\boldsymbol{B}^{\mathrm{T}}\boldsymbol{AB} = \boldsymbol{B}^{-1}\boldsymbol{AB} = \boldsymbol{C}$ 成对角矩阵.

证明 为了证明 $\boldsymbol{B}$ 的存在,假设 $\boldsymbol{B}$ 就是由矩阵 $\boldsymbol{A}$ 的特征向量组 $\{\xi_1, \xi_2, \cdots, \xi_n\}$ 组成的,即 $\boldsymbol{B} = [\xi_1, \xi_2, \cdots, \xi_n]$,则有

$$\begin{aligned} \boldsymbol{B}^{\mathrm{T}}\boldsymbol{AB} &= [\xi_1, \xi_2, \cdots, \xi_n]^{\mathrm{T}}\boldsymbol{A}[\xi_1, \xi_2, \cdots, \xi_n] \\ &= [\xi_1, \xi_2, \cdots, \xi_n]^{\mathrm{T}}[A\xi_1, A\xi_2, \cdots, A\xi_n] \\ &= [\xi_1, \xi_2, \cdots, \xi_n]^{\mathrm{T}}[\lambda_1\xi_1, \lambda_2\xi_2, \cdots, \lambda_n\xi_n] \\ &= \begin{bmatrix} \xi_1^{\mathrm{T}}\lambda_1\xi_1 & \xi_1^{\mathrm{T}}\lambda_2\xi_2 & \cdots & \xi_1^{\mathrm{T}}\lambda_n\xi_n \\ \xi_2^{\mathrm{T}}\lambda_1\xi_1 & \xi_2^{\mathrm{T}}\lambda_2\xi_2 & \cdots & \xi_2^{\mathrm{T}}\lambda_n\xi_n \\ \cdots & \cdots & \cdots & \cdots \\ \xi_n^{\mathrm{T}}\lambda_1\xi_1 & \xi_n^{\mathrm{T}}\lambda_2\xi_2 & \cdots & \xi_n^{\mathrm{T}}\lambda_n\xi_n \end{bmatrix} = \boldsymbol{C} \end{aligned} \tag{7}$$

观察矩阵 $\boldsymbol{C}$,如果 $\boldsymbol{B} = [\xi_1, \xi_2, \cdots, \xi_n]$ 是正交矩阵,则有 $(\xi_i, \xi_j) = 0$,其中 $i, j = 1, \cdots, n$, $i \neq j$,那么

$$\boldsymbol{C} = \begin{bmatrix} \xi_1^{\mathrm{T}}\lambda_1\xi_1 & 0 & \cdots & 0 \\ 0 & \xi_2^{\mathrm{T}}\lambda_2\xi_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \xi_n^{\mathrm{T}}\lambda_n\xi_n \end{bmatrix} \tag{8}$$

所以,如若要满足式(8),必须满足 $(\xi_i, \xi_j) = 0$, $i, j = 1, \cdots, n$, $i \neq j$.而由引理 2 知,在数域 P 中属于 $\boldsymbol{A}$ 的不同

特征值的特征向量必然正交.所以,目前的问题就是使矩阵 $\boldsymbol{A}$ 的属于同一特征值的特征向量正交即可.为此,本文引入 Gram-Schmidt 正交化方法[15],且 Gram-Schmidt 正交化的过程为:设初始向量组为$\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$,则

$$\beta_1=\alpha_1,\qquad \eta_1=\frac{\beta_1}{\|\beta_1\|},$$

$$\beta_2=\alpha_2-(\alpha_2,\eta_1)\eta_1,\qquad \eta_2=\frac{\beta_2}{\|\beta_2\|},$$

$$\beta_3=\alpha_3-(\alpha_3,\eta_1)\eta_1-(\alpha_3,\eta_2)\eta_2,\qquad \eta_2=\frac{\beta_2}{\|\beta_2\|},$$

$$\cdots\cdots$$

$$\beta_n=\alpha_n-\sum_{i=1}^{n-1}(\alpha_n,\eta_i)\eta_i,\qquad \eta_n=\frac{\beta_n}{\|\beta_n\|}. \tag{9}$$

这样就得到了向量组$\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$对应的一组正交向量组$\{\beta_1,\beta_2,\cdots,\beta_n\}$,以及相应的单位标准正交向量$\{\eta_1,\eta_2,\cdots,\eta_n\}$,$(\eta_i,\eta_i)=1$,其中$\|\boldsymbol{\beta}_i\|$,$i=1,\cdots,n$ 表示正交向量$\boldsymbol{\beta}_i$的模,(α_n,η_i)表示向量间的内积.

为此,本文利用 Gram-Schmidt 正交化方法将矩阵 $\boldsymbol{B}$ 中属于同一特征值的不同特征向量正交单位化,得到单位正交矩阵 $\boldsymbol{B}'=[\xi_1',\xi_2',\cdots,\xi_n']$,其中$(\xi_i',\xi_i')=1$,$(\xi_i',\xi_j')=0$,$i\neq j$,$i,j=1,\cdots,n$.

为此,如果令 $\boldsymbol{B}=\boldsymbol{B}'=[\xi_1',\xi_2',\cdots,\xi_n']$,则有

$$\boldsymbol{C}=\begin{bmatrix}\lambda_1 & 0 & \cdots & 0\\ 0 & \lambda_2 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & \lambda_n\end{bmatrix} \tag{10}$$

所以,对于任意 n 级实数域的对称矩阵$\boldsymbol{A}$,确实存在 n 级实数域单位正交矩阵 $\boldsymbol{B}=[\xi_1',\xi_2',\cdots,\xi_n']$,使 $\boldsymbol{B}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{B}=\boldsymbol{B}^{-1}\boldsymbol{A}\boldsymbol{B}=\boldsymbol{C}$ 成对角矩阵,且对角线的值为矩阵 $\boldsymbol{A}$ 的特征值.

综上所述,实现二次型 $f(x_1,x_2,\cdots,x_n)$矩阵 $\boldsymbol{A}$ 的正交对角化的方法可以分成以下几步:

(a)在数域 P 上,任选一个二次齐次多项式 $f(x_1,x_2,\cdots,x_n)$,写出 $f(x_1,x_2,\cdots,x_n)$的矩阵 $\boldsymbol{A}$;

(b)求解特征方程$|\lambda\boldsymbol{E}-\boldsymbol{A}|=0$在数域 P 上全部特征值 $\lambda_1,\lambda_2,\cdots,\lambda_n$ 及特征向量$\{\xi_1,\xi_2,\cdots,\xi_n\}$;

(c)利用 Gram-Schmidt 正交化方法对特征向量$\{\xi_1,\xi_2,\cdots,\xi_n\}$单位正交化,求得正交矩阵 $\boldsymbol{B}=[\xi_1',\xi_2',\cdots,\xi_n']$,其中 $\boldsymbol{B}^{\mathrm{T}}=\boldsymbol{B}^{-1}$,$\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B}=\boldsymbol{E}$;

(d)应用正交矩阵 $\boldsymbol{B}$ 对二次型$f(x_1,x_2,\cdots,x_n)$的矩阵 $\boldsymbol{A}$ 经过$\boldsymbol{B}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{B}$的线性替换变成对角矩阵$\boldsymbol{C}$,实现对$f(x_1,x_2,\cdots,x_n)$的标准化.

3 基于二次型的密钥管理方案

3.1 网络模型假设

为了便于讨论,本文的密钥管理方案是基于以下假设:

(a)假设网络是同构和静态的,即网络中的所有节点在软硬件的配置上完全相同,且一旦被部署就不会发生位置移动,其中网络大小为 N,存在基站和普通节点两种类型的节点.

(b)假设基站 BS 配备了充足的软硬件资源,并且通过装备大功率无线信号发射装置而使其信号传输范围能够覆盖整个网络部署区域,承担着整个网络密钥分配的中心任务.在网络部署前,基站生成一个二次型密钥池,$\{f_{\omega_i}(x_1,x_2,\cdots,x_n)=\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{X}\}$,其中,$\omega_i$ 为二次型的 ID 号,然后给每个普通节点分配一个二次型多项式;收集分析普通节点发送过来的信息;有检测出被攻破或被俘获节点的能力;存储所有普通节点的 ID 号,能够计算出普通节点之间的配对密钥.

(c)普通节点负责对周围环境数据的采集,将数据发送给邻居节点或基站.普通节点处理数据的能力较低,有限的存储空间和能量储备,通信范围小,不在通信半径之内的节点之间的通信要借助邻居节点中转.

(d)文中主要符号约定为:BS/KDS 表示基站或密钥分配中心;$S_i(1\leqslant i\leqslant n)$表示普通节点;$N_S(S_i)$表示节点 S_i 的邻居节点;$h(x)$表示单向 hash 函数;K_{pub},K_s 表示基站的公钥和私钥;$K_{a,b}$表示节点 a 与 b 之间的会话密钥;ID_i 表示节点 i 的身份标识符;$f_{\omega_i}(x_1,x_2,\cdots,x_n)$表示二次型.

3.2 密钥建立

3.2.1 方案初始化

(a)基站 BS 生成一个二次型密钥池 KDS,预存私钥 K_s 以及网络中每个普通节点的标识符 ID_i,同时记录每次分配到具体普通节点的二次型的标识符$(ID_i\|\omega_i)$;

(b)普通节点 S_i 预存基站公钥 K_{pub}、二次型 $f_{\omega_i}(x_1,x_2,\cdots,x_n)=\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{X}$.

3.2.2 建立会话密钥

不失一般性,本文重点考虑邻居节点之间的通信.由于网络的部署区域并非是安全的,邻居节点之间必须建立安全链路来保护可能发生的通信,且具体的链路建立过程如下:

(a)网络建成后,每个普通节点广播自身的 ID 信息,同时得到每个邻居节点的 ID 信息和网络拓扑结构,建立邻居列表$(ID_j\|ID_k\|\cdots\|ID_m)$,然后加密邻居列表信息 $E_{K_{pub}}(ID_i\|ID_j\|ID_k\|\cdots\|ID_m)$,$ID_i$ 为节点自身标识符,最后通过直接或邻居中转的方式(网络节点识别公钥 K_{pub}加密信息自动转发)发送到 BS,然后删除 K_{pub}.BS 通过私钥 K_s 解密列表信息,存储属于 ID_i 的邻居列表信息.

(*b*)节点 *a* 首先解析自身二次型 $f_{w_a}(x_1,x_2,\cdots,x_n)$ 的矩阵 $\boldsymbol{A}$,再根据定义 2、定义 3,求解矩阵 $\boldsymbol{A}$ 的特征值 $\lambda_1,\lambda_2,\cdots,\lambda_n$ 及特征向量 $\{\xi_1,\xi_2,\cdots,\xi_n\}$,同时取矩阵 $\boldsymbol{D}=[\xi_1,\xi_2,\cdots,\xi_n]$,然后根据推论结果定理 1 求解使 $\boldsymbol{A}$ 对角化的正交矩阵 $\boldsymbol{B}$ 和对角矩阵 $\boldsymbol{C}$,最后向所有邻居节点广播密钥信息 $(f_{w_a}(x_1,x_2,\cdots,x_n)\parallel h(\boldsymbol{B})\parallel h(\boldsymbol{C})\parallel h(\boldsymbol{D})\parallel ID_a)$. 当节点 *m* 收到邻居节点 *a* 的密钥信息时,解析 $f_{w_a}(x_1,x_2,\cdots,x_n)$ 的矩阵 $\boldsymbol{A}$,计算其特征值 $\lambda_1',\lambda_2',\cdots,\lambda_n'$ 和特征向量 $\{\xi_1',\xi_2',\cdots,\xi_n'\}$(由于计算求得的特征值可能因为顺序不同或不正确,也会影响特征向量的正确性,同时同一特征值的不同特征向量的顺序也会影响结果的正确性);所以,为了判断节点 *m* 解析的信息正确性,将 $\lambda_1',\lambda_2',\cdots,\lambda_n'$ 和 $\{\xi_1',\xi_2',\cdots,\xi_n'\}$ 代入 $h(x)$,判断结果是否与 $h(\boldsymbol{C})$ 和 $h(\boldsymbol{D})$ 分别相等,如果相等,则进一步判断 $h(\boldsymbol{B})$ 的正确性;在完成信息的判断后,也相当于完成了对节点 *a* 身份的验证,节点 *m* 才会计算与节点 *a* 之间的会话密钥,假设节点 *m* 广播的密钥信息为 $(f_{w_m}(x_1,x_2,\cdots,x_n)\parallel h(\boldsymbol{F})\parallel h(\boldsymbol{G})\parallel h(\boldsymbol{H})\parallel ID_m)$,则令节点 *m* 与 *a* 之间的会话密钥为 $K_{ma}=h(\boldsymbol{FB})$,之后删除 $(f_{w_a}(x_1,x_2,\cdots,x_n)\parallel h(\boldsymbol{B})\parallel h(\boldsymbol{C})\parallel h(\boldsymbol{D})\parallel ID_a)$.

同样,节点 *a* 收到来自邻居节点 *m* 的密钥信息 $(f_{w_m}(x_1,x_2,\cdots,x_n)\parallel h(\boldsymbol{F})\parallel h(\boldsymbol{G})\parallel h(\boldsymbol{H})\parallel ID_m)$,通过判断信息的正确性来识别节点 *m* 的身份,再令节点 *a* 与 *m* 之间的会话密钥为 $K_{am}=h(\boldsymbol{BF})$,同时删除 $(f_{w_m}(x_1,x_2,\cdots,x_n)\parallel h(\boldsymbol{F})\parallel h(\boldsymbol{G})\parallel h(\boldsymbol{H})\parallel ID_m)$. 因为矩阵正交后为标准化对角矩阵,而对角矩阵之间的计算是可交换的($\boldsymbol{BF}=\boldsymbol{FB}$),所以 $K_{am}=h(\boldsymbol{BF})=h(\boldsymbol{FB})=K_{ma}$,也说明节点 *a* 与 *m* 得到它们之间唯一的会话密钥. 同理,节点 *a* 可以得到与所有邻居节点之间的会话密钥.

(*c*)如果要实现不相邻节点 *a* 与 *f* 的通信,首先节点 *a* 通过会话密钥加密邻居列表,与邻居节点交换邻居列表,发现节点 *f* 与邻居节点 *m* 相邻;节点 *a* 再向 *m* 发送请求信息 $E_{K_{am}}(ID_a\parallel ID_f)$,节点 *m* 解析信息得知 *a* 需要和 *f* 通信,重新请求获得节点 *a* 和 *f* 的会话密钥信息,再交换转发给 *f* 和 *a*,然后自身删除这两个会话密钥信息;而节点 *a* 与 *f* 根据密钥信息计算得到会话密钥 K_{af} 与 K_{fa},然后节点 *a* 加密发送会话内容 $E_{K_{am}}(E_{K_{af}}(M)\parallel ID_a\parallel ID_f)$,节点 *m* 解析信息得知这是发往 *f* 的信息,重新加密信息发送 $E_{K_{mf}}(E_{K_{af}}(M)\parallel ID_a\parallel ID_f)$;节点 *f* 收到信息后,首先解析得知这是节点 *a* 发给它的信息,再次解密得到会话内容 *M*.

3.3 密钥更新

(*a*)网络密钥更新. 为了保障网络长期的安全性以及会话密钥的新鲜性,基站 BS 会在网络运行一段周期之后,重新给每个普通节点分配二次型,保证节点间的安全通话. 由于网络在初始化时,基站保存了每个节点的邻居列表,并且记录了初始分配到每个节点的二次型的标识符,所以基站能够计算出普通节点之间的配对密钥. 为此,基站可以参照每个节点的邻居列表,随机生成一个会话密钥,实现与节点间的通信,例如:基站 BS 为更新节点 *a* 的二次型 $f_{\omega_a}(x_1,x_2,\cdots,x_n)$,选择节点 *a* 与 *m* 之间的会话密钥 K_{am} 作为 BS 与 *a* 之间的会话密钥,然后发送 $K_{am}(f'_{\omega_a}(x_1,x_2,\cdots,x_n)\parallel K'_{pub})$,其中 K'_{pub} 为基站重新生成的公钥. 节点 *a* 在收到信息后,得知是基站更新密钥的命令,则删除原有的密钥信息(包括二次型 $f_{\omega_a}(x_1,x_2,\cdots,x_n)$),然后重新生成密钥信息 $(f'_{\omega_a}(x_1,x_2,\cdots,x_n)\parallel h(\boldsymbol{B}')\parallel h(\boldsymbol{C}')\parallel h(\boldsymbol{D}')\parallel ID_a)$ 以及与节点 *m* 的会话密钥 K'_{am},之后删除其他节点的密钥信息. 这样可以实现全网节点的密钥更新,保证网络周期性的完全换血.

(*b*)会话密钥更新. 为了保障安全通信,节点会统计自身的通信次数,对于通信过于频繁的节点,会成为网络的热点,也成了敌人俘获的重点对象. 为此,节点会在一定的通信次数后调整会话节点间的会话密钥,例如:节点 *a* 与 *m* 之间的次数大于预警次数 *R*,那么两者都会重新生成密钥信息发送给对方,其中,*a* 节点发送密钥信息 $K_{am}(f_{\omega_a}(x_1,x_2,\cdots,x_n)\parallel h(\boldsymbol{B}'')\parallel h(\boldsymbol{C}'')\parallel h(\boldsymbol{D}'')\parallel ID_a)$,信息中并没有更新二次型,只是调整了特征值与特征向量的顺序,这样就改变了正交矩阵和密钥的结果. 同样,节点 *m* 也会发送更新的密钥信息,计算新的会话密钥,然后删除对方的密钥信息,实现热点之间的安全通信. 这种方法的好处在于,节点可以自身调整节点间的会话密钥,即使敌人俘获两点的会话密钥,但在节点调整更新会话密钥时,敌人是很难完成再次对身份的验证,而暴露了自身.

(*c*)新节点加入. 假设 *a* 是新加入网络的节点,那么 *a* 已经事先预存了二次型 $f_{\omega_a}(x_1,x_2,\cdots,x_n)$ 和基站新公钥 K''_{pub},节点 *a* 通过广播信息获取自己的邻居列表,然后通过 K''_{pub} 加密发送给基站,之后删除 K''_{pub};基站在解析到信息后,删除 K''_s,存储节点 *a* 的邻居列表,同时添加修改和它相邻的所有节点的邻居列表;同时,节点 *a* 完成和邻居节点的会话密钥的建立,删除其他节点的密钥信息,这样也就完成了新节点的加入. 而新节点的加入并没有影响网络的任何通信结构,因此这种方法具有很强的扩展性.

(*d*)俘获节点删除. 假设基站 BS 检测到节点 *a* 被敌人俘获,需要删除 *a*,那么 BS 首先会广播全网 *a* 将被删除,停止所有与 *a* 的通信和删除所有与 *a* 的会话密

钥,从 a 的邻居列表中删除 ID_a;同时 BS 会用全网密钥更新的方法,实现所有与 a 相邻的节点的密钥更新,切断 a 通向全网的必经之路,孤立 a,也即把 a 从网络中删除.这种方法用最小的代价实现了全网的安全.

4 性能分析

4.1 安全性分析

(1)节点的抗俘获能力.①节点与邻居节点通过交互密钥信息生成的会话密钥是彼此独立,互不相同,即密钥只在与其配对的节点中存在一份.所以攻击者只能获知节点与其通信节点间的会话密钥(主要为邻居节点),而对未参与其通信的节点的密钥信息毫不知情,不会影响到其它未被俘获节点之间的安全通信,更不会影响网络安全.②公钥是普通节点在网络初始化前预存的密钥,而在网络建成后节点便会删除公钥,所以尽管公钥是公开的,但是在网络建成后已被删除,毫不影响网络的运行和安全.③即使被俘节点在会话密钥协商阶段泄露了自身的会话信息,但是由于节点本身所存储的身份验证信息都经过单向 hash 函数处理,攻击者是不可能破解出完整的 hash 函数处理过的信息.④基站具有检测功能,所以当基站检测到有节点被俘获时,会广播全网删除与该节点通信的会话密钥,同时更新所有与该节点相邻的节点的密钥,切断该节点通向全网的必经之路,从而提高了网络抵御节点俘获攻击的能力,确保了网络的安全通信.

(2)节点的抗合谋能力.假设网络中有多个节点被攻破或者被俘获,但是由于攻击者获得的二次型是不同的,无法借助多次获得相同的二次型通过合谋的方法破解它,俘获再多的节点对于攻击者来说是没有用的.所以,本方案能够抵抗合谋攻击.

(3)节点的抗泛洪能力.泛洪攻击中攻击者可以伪造成多个身份的节点,给节点 a 回复许多伪造的消息,节点 a 在收到这些消息后都要对收到的节点身份进行次认证.而每一次认证都需要一定的计算量,攻击者可以通过发送大量的消息,这样就可以消耗掉节点 a 的能源,进而达到攻击节点的目的.而本方案一方面攻击者没有基站预分配的公钥,是没有在基站建立邻居列表的,所以逃不过基站的伪节点检测;另一方面,攻击者没有二次型身份验证的方法,是无法计算出会话密钥的,因此是无法用密钥加密会话的.

4.2 网络的健壮性

本方案中,合法节点预存基站的公钥,并且加密节点的邻居列表发送给基站,节点的交互信息则用进行单向 hash 函数处理.因此,一方面攻击者是没有公钥的,即使将自身非法的秘密信息发送给基站,也无法通过基站认证,从而保证了秘密信息的合法性;另一方面只有合法节点才拥有身份验证的算法,实现对节点的身份验证,从而计算出会话密钥.通信双方是通过交换密钥信息来计算获得会话密钥的,因此,即使交换的中间参数被攻击者获取,也不会暴露会话密钥.此外,由于每对会话密钥均不相同,即使节点被俘获,也牵涉不到其他节点的安全,这样就保证了网络的强健壮性.

4.3 连通性分析

本方案中,网络中任意节点与邻居节点都可以通过交换密钥信息,验证节点身份,计算求得双方的会话密钥,从而建立通信连接.即使是不相邻的节点,也可以通过交换邻居列表,获得通信的链路,再通过链路中间节点实现信息的转发,实现两个节点的会话.所以网络中任意节点间都可以实现通信,即本方案网络的连通率为 1.

4.4 可扩展性分析

本方案在初始化阶段,节点只需预存自身的 ID_i、K_{pub}及二次型$f_{\omega_a}(x_1,x_2,\cdots,x_n)$.当有新节点 a 加入时,只需通过广播获取自身的邻居列表,通过 K_{pub}加密发送给基站,基站会根据列表信息修改存储与它相邻的所有节点的邻居列表;在密钥建立阶段,节点 a 通过与邻居节点完成信息交互,再通过身份认证,完成和邻居节点的会话密钥的建立,然后删除其它节点的密钥信息,这样也就完成了新节点的加入.整个过程中,其邻居节点只需在自己的密钥空间添加与新节点的会话密钥即可,不相关的节点未发生任何变化,即新节点的加入并没有影响网络的任何通信结构,因此本方案具有很强的扩展性.

4.5 开销分析

(1)计算开销.初始化阶段,每个节点向基站发送秘密信息时,需要一次加密运算;密钥建立阶段,节点需要进行一次二次型多项式的解析来获取二次型矩阵,一次特征多项式运算求解特征值,一次线性方程组运算求解特征向量,一次 Gram-Schmidt 正交化运算求解正交矩阵,三次 hash 运算用来验证身份、一次 hash 运算来形成会话密钥.虽然在初始化阶段进行了多次了运算,但是当节点间建立了会话密钥后,每次只需进行一次加密运算和一次解密运算,这种计算量还是比较小的,因此本方案的计算开销是可以接受的.

(2)存储开销.本方案中,每个节点需要存储的信息只有:身份标识符 ID_i、二次型 $f_{\omega_a}(x_1,x_2,\cdots,x_n)$、自身的密钥信息以及与邻居节点之间的会话密钥.而在 Eschenauer-G1igor 和 q-composite 方案中,节点都要保存相当数量的密钥空间才能保证较高的密钥连通性.

(3)通信开销.本方案中,节点在初始化阶段需要进行一次广播获取邻居列表;密钥建立阶段向基站发

送一个秘密信息,通知基站存储列表信息,邻居节点之间还需要进行一次广播通信生成节点与所有邻居节点之间的会话密钥;会话密钥更新时,不论是全网更新还是节点间更新,只需进行一次信息交互即可.而在随机密钥预分配方案中,节点需要与所有邻居节点进行一次通信交互才可以完成会话密钥的更新.所以,本方案的通信开销相对较小.

5 总结

本文提出了一种基于二次型的无线传感器密钥管理方案,该方案突破现有二元 t 次对称多项式建立共享密钥的思路,引入多元非对称二次型多形式,利用二次型正交对角化特性建立会话密钥,开创了基于多项式预分配方案的新研究方向.性能分析表明,与现有的密钥管理方案相比,该方案在抗俘获性、连通性、可扩展性、通信开销和存储开销上有较大的改进.

参考文献

[1] Xiaojiang Du, et al. Security in wireless sensor networks[J]. IEEE Wireless Communications, 2008, 15(4): 60 – 66.

[2] Zhang Yuan, Shen Yongluo, Lee Sangkeun. A cluster-based group key management scheme for wireless sensor networks [A]. Proceedings of the 12th International Asia Pacific Web Conference [C]. APWeb, 2010. 386 – 388.

[3] 李凤华,王巍,马建峰.适用于传感器网络的分级群组密钥管理[J].电子学报,2008,36(12):2405 – 2411.
Li Fenghua, Wang Wei, Ma Jianfeng. Leveled group key management for wireless sensor networks [J]. Acta Electronica Sinica, 2008, 36(12): 2405 – 2411. (in Chinese)

[4] 彭清泉,裴庆祺,等.无线传感器网络中自治愈的群组密钥管理方案[J].电子学报,2010,38(1):123 – 128.
Peng Qingquan, Pei Qingqi, et al. A self-healing group key management scheme in wireless sensor networks [J]. Acta Electronica Sinica, 2010, 38(1): 123 – 128. (in Chinese)

[5] Eschenauer L, Gligor V. A key management scheme for distributed sensors networks [A]. Proceedings of the 9th ACM Conference on Computer and Communications Security [C]. New York, USA: ACM Press, 2002. 41 – 47.

[6] Chan Haowen, Perrig A, Song D. Random key pre-distribution schemes for sensor network [A]. Proceedings of the IEEE Symposium On Security and Privacy [C]. Washington DC, USA: IEEE Press, 2003. 197 – 213.

[7] 阎军智,李凤华,马建峰.一种无状态的传感器网络密钥预分配方案[J].电子学报,2009,37(10):2199 – 2204.
Yan Junzhi, Li Fenghua, Ma Jianfeng. A self-healing group key management scheme in wireless sensor networks [J]. Acta Electronica Sinica, 2009, 37(10): 2199 – 2204. (in Chinese)

[8] 杨庚,王江涛,等.基于身份加密的无线传感器网络密钥分配方法[J].电子学报,2007,35(1):179 – 184.
Yang Geng, Wang Jiangtao, et al. A key establish scheme for WSN based on IBE and diffie-hellman algorithms [J]. Acta Electronica Sinica, 2007, 35(1): 179 – 184. (in Chinese)

[9] Liu Donggang, Ning Peng. Establishing pair-wise keys in distributed sensor networks [A]. Proceedings of the l0th ACM Conference on Computer and Communications Security [C]. New York, USA: ACM Press, 2003. 52 – 61.

[10] Chorzempa M, Park J M, Eltoweissy M. SECK: Survivable and efficient clustered keying for wireless sensor networks [A]. Proceedings of the IEEE International Performance, Computing and Communications Conference (Phoenix) [C]. USA: IEEE Press, 2005. 453 – 458.

[11] Choi S, et al. Key management in wireless sensor networks with inter-network sensor roaming [A]. Proceedings of the 33rd IEEE Conference on Local Computer Networks [C]. Montreal, Quebec, Canada: IEEE Press, 2008. 328 – 335.

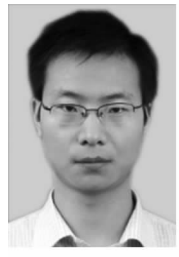
[12] Delgosha F, Fekri F. Key pre-distribution in wireless sensor networks using multivariate polynomials [A]. Proceeding of the Second Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks [C]. USA: IEEE Press, 2005. 118 – 129.

[13] Kim J M, et al. N-dimensional grid-based key pre-distribution in wireless sensor networks [A]. Proceeding of International Conference on Computational Science and its Applications [C]. Malaysia: ICCSA Press, 2007, 2. 1107 – 1120.

[14] Dutertre B, Cheung S, Levy J. Light Weight Key Management in Wireless Sensor Networks by Leveraging Initial Truest, SDL Technical Report [R]. SRI-SDL-04-02, 2004.

[15] Werneth C M, Dhar M, Maung K M, et al. Numerical gram-schmidt orthonormalization [J]. European Journal of Physics, 2010, 31(3): 693 – 700.

作者简介



王小刚　男,1984 年 2 月出生,陕西宝鸡人.2008 进入重庆大学自动化学院硕博连读,现为博士生.主要研究方向为无线传感器网络、普适计算,建筑节能等.
E-mail: wxg_zf@yahoo.com.cn; wxg_zf@163.com

石为人　男,1948 年 10 月出生,重庆市人.教授、博士生导师.主要研究方向为信息控制与智能系统、无线传感器网络及其应用、嵌入式系统、普适计算等.
E-mail: wrs@cqu.edu.cn