

引用格式:袁驰. 基于特征向量的非随机 WSN 密钥预分配方法[J]. 微电子学与计算机, 2020, 37(11): 6-12. [YUAN C. Eigenvector-based assignable key predistribution method for wireless sensor networks[J]. Microelectronics & Computer, 2020, 37(11): 6-12.]

基于特征向量的非随机 WSN 密钥预分配方法

袁 驰

(中国人民大学 信息学院, 北京 100872)

摘 要: 针对无线传感器网络(WSN)密钥预分配过程中存在的门限共谋及概率连通问题,提出了一种非随机的(即确定的)基于矩阵特征向量的 EBSC 方案,利用一个生成矩阵 A,根据申请节点的不同类型,可动态生成 2N 个相异的秘密矩阵. 不同于其他基于概率的随机密钥预分配方案,EBSC 方案解决了经典 BLOM 方案存在的门限共谋问题,也解决了随机方案(称之为:RDMS 方案)中存在的概率连通问题,可以实现 WSN 网络的全连通(即:网络中任意两个节点可直接通信). 不仅如此,EBSC 方案利用特征值和特征向量的性质,在节点申请时采用单次身份认证,大大提高的网络的安全性能. 通过比较分析表明,新方案在节点存储量、运算量和网络通信能量消耗方面均有优势. 特别地,在网络后续更新较大的情况下,新方案通过简单的赋值操作,以轻量级的通信消耗,便可实现规模为 N 的全网更新,避免了复杂的矩阵扩容运算,更适合能量受限的 WSN 网络.

关键词: 特征向量;特征值;密钥预分配;网络全连通;门限

中图分类号: TP393.1

文献标识码: A

文章编号: 1000—7180(2020)11—0006—07

Eigenvector-based assignable key predistribution method for wireless sensor networks

YUAN Chi

(School of Information, Renmin University of China, Beijing 100872, China)

Abstract: Aiming at the threshold collusion and probabilistic connectivity problems in the process of wireless sensor network (WSN) key pre-distribution, an scheme based on matrix eigenvector (EBSC) is proposed. By using a generating matrix A, 2N secret matrices can be dynamically generated according to the different types of application nodes. The problem of threshold collusion in classical BLOM scheme and probabilistic connectivity in probabilistic is sloved. Full connectivity of WSN network (that is, any two nodes in the network can communicate directly) can be realized. Moreover, utilizing the properties of eigenvalues and eigenvectors in the EBSC scheme, a single authentication is used in the application of nodes, which greatly improves the security performance of the network. The comparison analysis shows that the new scheme has advantages in node storage, computation and network communication energy consumption. Especially, in the case of large network updates, the new scheme can realize the whole network updates of scale N by simple assignment operation and lightweight communication consumption, avoiding complex matrix expansion operation. This shows that EBSC algorithm is more suitable for energy-constrained WSN networks.

Key words: eigenvector; eigenvalue; key pre-distribution; fully connected network; threshold

1 引言

无线传感器网络(WSN)的应用目前已经广泛存在于人们的日常生活工作中^[1-2],也被定义为一种任务型网络^[3-4].人们在这方面的研究一直在进行着(见下章),其中较为典型的是1984年Blom提出的方案^[5],但由于其方案设计的初衷并不是针对WSN网络,加之方案还存在门限共谋风险,因此有学者对此方案进行了改进.其中有一类方案较为典型,即随机分配方案(RDMS),它主要通过使用多个随机小秘密矩阵(或格,或多空间)的方法,可以保证任意两个节点之间都可以连通,但也带来了新的问题.一是占用资源较大.每一个节点都需要存储 τ 个小秘密矩阵 D' ,在每次通信时均要进行公共小秘密矩阵的对比查找.二是仍然存在共谋风险.在极端情况下,如果每次节点通信时候恰好都选到了同一个小秘密矩阵 D' ,RDMS方案就等同于Blom方案.三是网络的扩展性不好.在新节点加入网络时,还需要重新对 G 矩阵进行扩充,并再次分发.

针对此,本文提出一种EBSC方案.该方案利用特征向量性质,根据申请节点的类型,针对性地进行秘密矩阵的动态生成,既解决了门限共谋问题,也解决了上述随机方案(RDMS)中的部分连通问题,实现了网络的全连通,同时,方案还引入了节点单次身份认证,大提高了网络的安全性能,特别是在网络规模更新阶段,优势更加明显.

2 研究现状

近年来,不少研究者开始研究如何利用混沌系统进行WSN网络密钥管理,文献[6]设计出一种FEIS-TEL网络下的定长8bit运算单元的混沌密钥管理系统.文献[7]提出一种DSK(dynamic sub key)混沌密钥管理方案.近年来,基于矩阵的密钥协议设计和分析也成为研究热点之一^[8-11].在典型的概率分配方案(RDMS)中,Du等人提出方案^[12]首次将概率论的观点应用到改进方案中.王杨子等人提出了多空间的密钥预分配方案^[13].王淑华等人提出了基于格的密钥预分配方案^[14],以概率方式输出认证消息,利用较少的步骤就能进行较高概率的密钥协商.

3 算法介绍

3.1 密钥分配过程

3.1.1 系统初始化阶段

(1)BS选取 n 个实向量 $\{a_1, a_2, \dots, a_n\}$,组成 $n \times$

n 对称矩阵 A ,形如:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} (a_{ij} = a_{ji})$$

(2) 计算矩阵 A 的迹 $Tr_a = \sum_{i=1}^n (a_{ii})$;

(3) 对 A 进行特征值分解,可得到 n 个的实特征值 $v_i, i \in (1, n)$,其中允许有重根 $v_i = v_j (i \neq j)$,过程如下:

$$A = QVQ^T = \begin{bmatrix} q_{i1} & q_{j1} \\ q_{i2} & q_{j2} \\ \vdots & \vdots \\ q_{in} & q_{jn} \end{bmatrix} \cdot \begin{bmatrix} v_1 & 0 \\ v_i & \\ v_j & \\ 0 & v_n \end{bmatrix} \cdot \begin{bmatrix} q_{i1} & q_{i2} & \cdots & q_{in} \\ q_{j1} & q_{j2} & \cdots & q_{jn} \\ \vdots & \vdots & \ddots & \vdots \end{bmatrix}$$

(4) 将得到的实数特征值 v_i 分别赋值给 n 个节点(单独发送),使得每个节点有且只有一个特征值,其中 $i \in (1, n)$;

(5) 生成范德蒙矩阵,广播分发给 n 个节点.特别地,生成的矩阵 G 为 $n \times n$ 矩阵,而不同于Blom算法中的 $t \times n$ 矩阵.

3.1.2 节点赋值及申请通信阶段

(1) 各节点接收BS赋值信息,使 $Id_i = v_i; i \in (1, n)$;

(2) 两任意节点 i 和 j 分别发送的 $(Id_i \| j)$ 和 $(Id_j \| i)$ 至BS,申请进行通信(单次申请过程记为 a_{pl}).

3.1.3 BS验证及接受申请阶段

(1)BS接收到任意两个节点 i 和 j 要求通信的请求后,分别取 (Id_i) 和 (Id_j) 和相对应的特征向量 q_i 和 q_j ,与矩阵 A 进行乘运算,验证相应请求是否合法,取出: $\begin{cases} (q_i \cdot Id_i) = (q_i \cdot v_i) \cdot A \cdot v_i \\ (q_j \cdot Id_j) = (q_j \cdot v_j) \cdot A \cdot v_j \end{cases}$;如果验证成功,则接着进行下一步向量种子分发(此验证过程记为 v_{σ}).

(2)BS分别取 v_i 和 v_j 对应的特征向量种子 q_i 和 q_j ,计算 $q_i \times q_j^T (i < j)$ 得矩阵 D^* ,过程如下:

$$D_{ij}^* = \begin{bmatrix} q_{i1} \\ q_{i2} \\ \vdots \\ q_{in} \end{bmatrix} \cdot \begin{bmatrix} q_{j1} & q_{j2} & \cdots & q_{jn} \end{bmatrix}$$

$$= \begin{bmatrix} d_{11}^* & \cdot & d_{1(n-1)}^* & d_{1n}^* \\ d_{21}^* & \cdot & d_{2(n-1)}^* & d_{2n}^* \\ \cdot & \cdot & \cdot & \cdot \\ d_{n1}^* & \cdot & d_{n(n-1)}^* & d_{nm}^* \end{bmatrix}$$

(3) 由矩阵 $\mathbf{D}^*$, 生成秘密矩阵 $\mathbf{D}_{ij}$ (此生成过程记为 g_{ei}^+), 即:

$$\mathbf{D}_{ij}^* + (\mathbf{D}_{ij}^*)^T = \begin{bmatrix} d_{11}^* & \cdot & d_{1(n-1)}^* & d_{1n}^* \\ d_{21}^* & \cdot & d_{2(n-1)}^* & d_{2n}^* \\ \cdot & \cdot & \cdot & \cdot \\ d_{n1}^* & \cdot & d_{n(n-1)}^* & d_{nm}^* \end{bmatrix} + \begin{bmatrix} d_{11}^* & d_{21}^* & \cdot & d_{n1}^* \\ \cdot & \cdot & \cdot & \cdot \\ d_{1(n-1)}^* & d_{2(n-1)}^* & \cdot & d_{n(n-1)}^* \\ d_{1n}^* & d_{2n}^* & \cdot & d_{nm}^* \end{bmatrix}_{ij}$$

(4) 由范德蒙矩阵 $\mathbf{G}$ 结合上步生成的秘密对称矩阵 $\mathbf{D}_{ij}$ 共同产生矩阵 $\mathbf{B}$, 即:

$$\mathbf{B} = (\mathbf{D}_{ij} \cdot \mathbf{G})^T = \begin{bmatrix} d_{11}^* & \cdot & d_{1(n-1)}^* & d_{1n}^* \\ d_{21}^* & \cdot & d_{2(n-1)}^* & d_{2n}^* \\ \cdot & \cdot & \cdot & \cdot \\ d_{n1}^* & \cdot & d_{n(n-1)}^* & d_{nm}^* \end{bmatrix} \cdot \begin{bmatrix} 1 & \cdot & 1 & 1 \\ g_1^1 & \cdot & g_{(n-1)}^1 & g_n^1 \\ \cdot & \cdot & \cdot & \cdot \\ g_1^n & \cdot & g_{(n-1)}^n & g_n^n \end{bmatrix}^T$$

(5) BS 分别秘密发送矩阵 $\mathbf{B}$ 的第 i 行 b_i^{row} 、第 j 行 b_j^{row} 给节点 i 和 j (单次分发过程记为 d_{is})。

3.1.4 节点产生共同密钥阶段

(1) 节点 i 收到 BS 发送来的第 i 行元素 b_i^{row} (同 b_{ik}), 与自己掌握的矩阵 $\mathbf{G}$ 的第 j 列元素 g_{ij}^{col} (同 g_{lj}) 相乘, 得 k_{ij} (此过程记为 $k_{ij}^* \square n * n$), 如下:

$$(b_{i1}, b_{i2}, \dots, b_{in}) \cdot (g_{1j}, g_{2j}, \dots, g_{nj})^T =$$

$$\sum_{k=1}^n b_{ik} \cdot g_{kj} = k_{ij}$$

(2) 节点 j 收到 BS 发送来的第 j 行元素 b_j , 与自己掌握的矩阵 $\mathbf{G}$ 的第 i 列元素相乘, 得 k_{ji} (此过程记为 $k_{ji}^* \square n * n$), 如下:

$$(b_{j1}, b_{j2}, \dots, b_{jn}) \cdot (g_{1i}, g_{2i}, \dots, g_{ni})^T = \sum_{k=1}^n b_{jk} \cdot g_{ki} = k_{ji}$$

(3) 由于 $k_{ij} = k_{ji}$ (见后节正确性证明), 节点 i 和节点 j 便获得共同密钥, 可以进行通信。

3.2 网络更新过程

3.2.1 赋值阶段

如果有新节点加入, 则从 Id_n 开始, 新加入的第一个节点编号为 $Id_{(n+1)}$, 依次递增, 直至编号 $Id_{(2n-1)}$, 即, 保证新增加的节点数据不大于 $(n-1)$

个, 也即节点规模始终小于 $2n$ 。同时, 将 $Id_{(i)}$ 的特征值 v_i 也赋值给 $Id_{(n+i)}$ (赋值过程记为 a_{ss})。

3.2.2 扩充阶段

若新增节点数据超过 n , 即网络规模达到 $2n$ 时, 则需要重新初始化网络, 即对初始矩阵 $\mathbf{A}$ 的规模进行扩充, 对 n 的数量重新定义。

3.2.3 秘密矩阵生成阶段

对于节点更新后的申请者, 分为以下三种情况来产生秘密对称矩阵 $\mathbf{D}_{ij}$:

(1) 若申请通信双方节点编号 i 和 j 均小于或等于 n , 即两个申请者都不属于系统初始化后的新增节点, 则按上节 BS 验证及接受申请阶段中的方法生成秘密矩阵并最终产生共同密钥, 不再重复描述;

(2) 若申请通信双方其中一个节点编号 i 小于等于 n , 另外一个节点编号 $(n+j)$ 大于 n , 则对节点 i 按 BS 验证及接受申请阶段中的方法验证, 对节点 $(n+j)$ 则进行初步范围验证即可, 即验证 $Id_{(n+j)} = v_j \cdot \in \{v_1, v_2, \dots, v_n\}$, 若通过, 则进行下步秘密矩阵生成 $\mathbf{D}^*$, 再用前述方法生成秘密对称矩阵 $\mathbf{D}$, 并最终产生共同密钥, 不再重复描述;

(3) 若申请通信双方两个节点编号 $(n+i)$ 与 $(n+j)$ 均大于 n , 说明两个申请者均为新增加节点, 对两个节点均进行初步范围验证, 即验证 $Id_{(n+i)} = v_i \cdot \in \{v_1, v_2, \dots, v_n\}$, $Id_{(n+j)} = v_j \cdot \in \{v_1, v_2, \dots, v_n\}$, 若通过, 则进行下步秘密矩阵生成 $\mathbf{D}^*$ (此生成过程记为 g_{en}^*), 再用前述方法生成秘密对称矩阵 $\mathbf{D}$, 并最终产生共同密钥, 不再重复描述。

3.2.4 假冒节点排查阶段

(1) 在节点更新之后, 系统会在节点申请通信时候对每一个节点先进行单独认证, 对于节点编号小于等于初始规模 N 的节点, 利用特征向量及特征值的性质 $(q_i \cdot v_i) = A \cdot v_i$ 进行验证; 对于节点编号大于初始规模 N 的新增节点, 进行初步的范围验证 $Id_{(n+i)} = v_i \cdot \in \{v_1, v_2, \dots, v_n\}$ 。

(2) 由系统基站 BS 定期对系统内全部节点所拥有的特征值 (v_i) 进行不重复统计, 不需要进行节点编号比较。如果有 $Tr_a < \sum_{i=1}^{2n} (ID_i)$, 则说明系统内有假冒节点, 此时需对系统进行重新初始化, 由 BS 重新选定初始对称矩阵 $\mathbf{A}$, 并确定新的网络规模 N , 按 EBSC 算法进行共同密钥的生成。

4 性能分析

4.1 正确性

定理 1: 利用 EBSC 算法, 由节点 i 和节点 j 所对应的特征值, 结合匹配的特征向量, 可以产生出可以保证节点 i 和 j 正常通信的共同密钥。

证明: 由 Blom 算法可知, 若矩阵 $\mathbf{D}_{ij}$ 为对称矩阵, 则有矩阵 $\mathbf{B}$ 和范德蒙矩阵 $\mathbf{G}$ 生成最终的对称矩阵 $\mathbf{K}$ 也为对称矩阵, 即:

$$\begin{aligned}\mathbf{K} &= \mathbf{B} \times \mathbf{G} = (\mathbf{D}_{ij} \times \mathbf{G})^T \times \mathbf{G} = \mathbf{G}^T \times \mathbf{D}_{ij}^T \times \mathbf{G} \\ &= \mathbf{G}^T \times \mathbf{D}_{ij} \times \mathbf{G} \\ &= (\mathbf{B} \times \mathbf{G})^T\end{aligned}$$

because $\mathbf{D}_{ij} = \mathbf{D}_{ij}^* + (\mathbf{D}_{ij}^*)^T$

$$\begin{aligned}&= \begin{bmatrix} d_{11}^* & \cdot & d_{1(n-1)}^* & d_{1n}^* \\ d_{21}^* & \cdot & d_{2(n-1)}^* & d_{2n}^* \\ \cdot & \cdot & \cdot & \cdot \\ d_{n1}^* & \cdot & d_{n(n-1)}^* & d_n^* \end{bmatrix} + \begin{bmatrix} d_{11}^* & d_{21}^* & \cdot & d_{n1}^* \\ \cdot & \cdot & \cdot & \cdot \\ d_{1(n-1)}^* & d_{2(n-1)}^* & \cdot & d_{n(n-1)}^* \\ d_{1n}^* & d_{2n}^* & \cdot & d_n^* \end{bmatrix} \\ &= \begin{bmatrix} d_{11}^{ij} & \cdot & d_{1(n-1)}^{ij} & d_{1n}^{ij} \\ d_{21}^{ij} & \cdot & d_{2(n-1)}^{ij} & d_{2n}^{ij} \\ \cdot & \cdot & \cdot & \cdot \\ d_{n1}^{ij} & \cdot & d_{n(n-1)}^{ij} & d_n^{ij} \end{bmatrix} \\ \text{so } \begin{cases} d_{kl}^{ij} = d_{kl}^* + d_{kl}^* = 2 * d_{kl}^* (k = l) \\ d_{kl}^{ij} = d_{kl}^* + d_{lk}^* = d_{lk}^* (k \neq l) \end{cases}\end{aligned}$$

可以看出, 矩阵 $\mathbf{D}_{ij}$ 为对称矩阵. 再根据 Blom 算法, 矩阵 $\mathbf{K}$ 亦为对称矩阵, 必有 $k_{ij} = k_{ji}$. 证毕。

定理 2: 利用 EBSC 算法, 任意两个节点间申请通信时 BS 均能通过全局矩阵 $\mathbf{A}$ 生成一个秘密矩阵 $\mathbf{D}_{ij}$, 并且任意两对节点生成的秘密矩阵 $\mathbf{D}_{ij}$ 互不相同 (即: 能保证网络的强连通性)。

证明:

(1) 首先证明存在性:

根据特征值的定义, 有: $\mathbf{A} \cdot \mathbf{q}_i = v_i \cdot \mathbf{q}_i$;

由于“实对称矩阵的特征值 v_i 必为实数, 其中 $i \in (1, n)$ (定理, 不重复证明)”;

所以必定存在特征向量 $\mathbf{q}_i$ 与特征值 v_i 相对应, 且不唯一, 比如向量 $(k \cdot \mathbf{q}_i)$ 。

(2) 再证明强连通性:

选定与各不同 $v_i \neq v_j (i \neq j)$ 特征值 $\{v_1, v_2, \dots, v_n\}$ 所对应的特征向量 $\{q_1, q_2, \dots, q_n\}$ 。

设特征向量 $\{q_1, q_2, \dots, q_n\}$ 线性相关, 并且其极大无关组为 $\{q_1, q_2, \dots, q_m, 1 \leq m \leq n-1\}$

选定一组整数 $\{k_1, k_2, \dots, k_{m+1}, 1 \leq m \leq n-1\}$, 使得:

$$k_1 q_1 + k_2 q_2 + \dots + k_{m+1} q_{m+1} = 0 \quad (1)$$

由于 $\mathbf{A} \cdot \mathbf{q}_i = v_i \cdot \mathbf{q}_i$, 可得:

$$\begin{aligned}\mathbf{A} \cdot (k_1 q_1 + k_2 q_2 + \dots + k_{m+1} q_{m+1}) &= \mathbf{A} \cdot 0 \\ \Leftrightarrow v_1 k_1 q_1 + v_2 k_2 q_2 + \dots + v_{m+1} k_{m+1} q_{m+1} &= 0\end{aligned} \quad (2)$$

又因为:

$$\begin{aligned}v_{m+1} \cdot (k_1 q_1 + k_2 q_2 + \dots + k_{m+1} q_{m+1}) \\ = v_{m+1} \cdot 0 \Leftrightarrow v_{m+1} k_1 q_1 + v_{m+1} k_2 q_2 + \dots + \\ v_{m+1} k_{m+1} q_{m+1} = 0\end{aligned} \quad (3)$$

式(3) ~ 式(2) 得:

$$\begin{aligned}(v_{m+1} - v_1) \cdot k_1 q_1 + (v_{m+1} - v_2) \cdot k_2 q_2 + \dots \\ + (v_{m+1} - v_{m+1}) \cdot k_{m+1} q_{m+1} = 0\end{aligned}$$

即:

$$\begin{aligned}(v_{m+1} - v_1) \cdot k_1 q_1 + (v_{m+1} - v_2) \cdot k_2 q_2 + \\ \dots + (v_m - v_m) \cdot k_m q_m = 0\end{aligned}$$

由前面假设条件知, $\{q_1, q_2, \dots, q_m\}$ 为极大无关组, 且 $v_i \neq v_j (i \neq j)$, 可得:

$$k_1 = k_2 = \dots = k_m = 0; \text{ 代入式(1), 得:}$$

$$k_{m+1} q_{m+1} = 0 \quad (4)$$

又因为: $q_{m+1} \neq 0$, 所以 $k_{m+1} = 0$; 由此可得: $\{q_1, q_2, \dots, q_{m+1}\}$ 线性无关, 这与 $\{q_1, q_2, \dots, q_m\}$ 为极大无关组相矛盾。

因此假设不成立. 故:

$\{q_1, q_2, \dots, q_n\}$ 线性无关, 由任意两个线性无关的特征向量必然可产生不同的秘密矩阵 $\mathbf{D}_{ij}$. 证毕。

4.2 EBSC 方案优点

4.2.1 无门限值约束

在 EBSC 网络中, 每一对单独的申请者, 其对应的秘密矩阵 $\mathbf{D}_{ij}$ 却是动态生成并且唯一的, 有三种情况:

对于前两种情况 (即: 申请通信双方节点编号 i 和 j 均小于或等于 n , 或申请双方其中一个节点编号 i 小于等于 n , 另外一个节点编号 $(n+j)$ 大于 n), 由于秘密矩阵的生成是由特征向量运算动态生成, 即: 发送给每对申请者的行信息来源于不同的矩阵 $\mathbf{B}$, 因此节点共谋无法得出秘密矩阵。

对于第三种情况 (即: 申请通信双方两个节点编号 $(n+i)$ 与 $(n+j)$ 均大于 n), 此时由于 $\mathbf{A}$ 为 $n \times n$ 矩阵, 若要有共谋出现, 节点数量应该为 N , 而 ENSC 算法要求更新阶段全部新增节点数量不能超过 N (网络总规模小于 $2N$), 所以新增节点也不可能形成共谋. 因此, EBSC 网络没有门限值约束。

4.2.2 网络内强连通

对于网络中的任意两个节点,不管是更新前节点还是更新后节点,采用 EBSC 方案均能产生出唯一的秘密矩阵(结合上述密钥分配过程以及证明),结合范德蒙矩阵 $\mathbf{G}$,必定能最终生成相同的共有密钥 k_{ij} (or k_{ji}),从而实现网络的强连通.

4.2.3 网络扩容性强

EBSC 方案针对更新前和更新后情况,动态生成秘密矩阵,由于其无门限值约束,直接生成的是秘密矩阵 $\mathbf{D}$ 和矩阵 $\mathbf{G}$,同时,对新加入的节点(更新后)按次序利用原有特征值进行二次赋值即可,不需要重新对 $\mathbf{G}$ 进行扩充,即 $[(\lambda+1) \times (n)] \rightarrow [(\lambda+1) \times (n+i)]$,网络中原有节点存储矩阵信息不需改变.

4.2.4 算法效率较高

在 EBSC 方案中,特征向量和秘密矩阵的生成,以及对节点身份的认证等都是在 BS 端进行,对于网络中节点,在更新前只需存储矩阵 $\mathbf{D}$ 信息和 BS 赋予自身的编号和特征值,更新后并不需要额外的矩阵信息,占用资源较少,算法效率得到提提高,更适合于 WSN 网络环境.

4.2.5 网络安全性能提升

网络中对更新前的节点(即:节点编号 i 小于或等于 n),利用特征向量的性质 $(q_i \cdot v_i) = A \cdot v_i$ 进行验证;对更新后的节点(即:节点编号 i 大于 n),采用初步范围验证,能有效防止节点的假冒攻击,大大提升网络的安全性能.

4.3 性能比较

结合上述分析,本文从网络连通率、门限、身份认证及矩阵数量等五个方面进行比较;在网络更新阶段,EBSC 方案性能及原理与后二者差别较大,为保证比较结果的普遍性,假定有编号为 $(n+i)$ 及 $(n+j)$ 的 2 个节点新加入网络,并申请相互通信,在此条件约束下,比较结果如表 1 所示.

其中部分对比较结果无影响的数据在上表中不再列出,比较用到的计算量、存储量符号统一归纳如表 2 所示.从对比可以看出,EBSC 方案在无门限共谋风险的基础上,实现了网络的全连通(任意两个节点均可直接通信,无需借助第三方),综合了 RDMS 方案和 BLOM 方案各自的优点.不仅如此,EBSC 方案在实现了单次申请认证,大大提高了网络的安全性,并且在一个源矩阵 $\mathbf{A}$ 的基础上,通过特征向量特性,产生的秘密矩阵 $\mathbf{D}$ (相异)数量最多,为 $2n$ 个,可以保证任意两节点间安全通信.

表 1 性能比较

	EBSC	RDMS	BLOM
任意连通	Y	N	Y
共谋风险	N	N	Y
单次认证	Y	N	N
秘密矩阵数	$2n$	ω	1
A 矩阵数	1	NULL	NULL
BS 存储量	$A; (n \times n), G; (n \times n), D^*, D_{ij}, B$	$\omega * D'(\lambda+1) \times (\lambda+1), G; (\lambda+1) \times n, B; (\lambda+1) \times n$	$1 * D(\lambda+1) \times (\lambda+1), G; (\lambda+1) \times n, B; (\lambda+1) \times n$
BS 计算量	$v_{or} + a_{ss} + g_{or}^+ (\rightarrow D^*) + g_{or}^+$	$e_{xp}^{k_{n+i}} + g_{or}^+ (\rightarrow B^T) + g_{or}^+ (\rightarrow K^{ij})$	$e_{xp}^{k_{n+i}} + g_{or}^+ (\rightarrow B^T) + g_{or}^+ (\rightarrow K^{ij})$
网络更新阶段	$G; (n \times n), Id_{(n+i)}, Id_{(n+j)}, b_i^{row}(n) + b_j^{row}(n) + k_{ij} + k_{ji}$	$G; (\lambda+1) \times n, \tau * D'; (\lambda+1) \times (\lambda+1), b_i^{row}(\lambda+1) + b_j^{row}(\lambda+1) + k_{ij} + k_{ji}$	$G; (\lambda+1) \times n, b_i^{row}(\lambda+1) + b_j^{row}(\lambda+1) + k_{ij} + k_{ji}$
节点存储量	$k_{ij}^* [n * n] + k_{ji}^* [n * n]$	$k_{ij}^* [(\lambda+1) * (\lambda+1)] + k_{ji}^* [(\lambda+1) * (\lambda+1)] + k_{ji}^* [(\lambda+1) * (\lambda+1)]$	$k_{ij}^* [(\lambda+1) * (\lambda+1)] + k_{ji}^* [(\lambda+1) * (\lambda+1)]$
节点计算量	$k_{ij}^* [n * n] + k_{ji}^* [n * n]$	$k_{ij}^* [(\lambda+1) * (\lambda+1)] + k_{ji}^* [(\lambda+1) * (\lambda+1)] + k_{ji}^* [(\lambda+1) * (\lambda+1)]$	$k_{ij}^* [(\lambda+1) * (\lambda+1)] + k_{ji}^* [(\lambda+1) * (\lambda+1)]$
BS 通信量	$2 * (d_{is} + a_{pl})$	$(n+2) * d_{is} + 2 * a_{pl}$	$(n+2) * d_{is} + 2 * a_{pl}$

表 2 符号定义

Notations Guide	
$e_{xp}^{k_{n+i}}$	矩阵扩充
a_{ss}	一次赋值过程
d_{is}	BS 分发一次信息
a_{pl}	节点申请一次通信
v_{or}	对节点身份验证
g_{or}^*	向量相乘
g_{or}^+	叠加生成秘密矩阵 D_{ij}
$b_i^{row}(n)$	规模为 (n) 的向量
$k_{ij}^* [n * n]$	向量相乘生成共同密钥 k (计算规模为 $n * n$)

对 BS 而言,在存储量方面,EBSC 方案和 BLOM 方案差距不大,但 RDMS 方案为了保证网络连通率,存储了多个秘密矩阵,相对来说对 BS 存储空间占用较多.在计算量方面,EBSC 方案优势明显,这主要是由于三者秘密矩阵的生成方式不同,EBSC 方案通过简单的赋值运算即可实现规模 $2n$ 网络的更新,而 RDMS 和 BLOM 方案仍然为传统的 $(\lambda+1) \times (\lambda+1)$ 和 $(\lambda+1) \times (n)$ 规模,后续更新阶段需大量的矩阵扩展和矩阵乘法计算.

对网络普通节点而言,EBSC 方案中普通节点存储的信息变化仅限于赋值后的数值变化,存储量变化不大,而在 RDMS 和 BLOM 方案中,更新后的

范德蒙矩阵由原来的 n 列变为 $(n+2)$ 列(对比设定场景为增加 2 个节点 i 和 j), 全部网络节点均需存储相应的增加项, 导致普通节点存储量加大, 若考虑网络扩容较大的情况, 对 G 矩阵要增加多列, 则对应的普通节点存储量将增加较大, 同时为了传送这些更新后的信息, 网络的通信量也将增大, 特别地, 对于规模较大的能量受限网络, 这是不能接受的. 需要指出的是, 在 EBSC 方案中, 普通节点的计算量 $k_{ij}^* [n * n]$ 要大于 RDMS 和 BLOM 方案的计算量 $k_{ij}^* [(\lambda+1) * (\lambda+1)]$, 但这一计算操作是相对简单的向量内积运算, 与计算复杂的矩阵乘法运算、扩容运算以及资源消耗较大的通信过程相比, 此内积运算量的增加可以忽略.

总体看来, EBSC 算法无论在存储占用上, 还是在运算量上, 都要优于 RDMS 和 BLOM 方案, 更加适合于 WSN 环境.

5 结束语

本文提出的 EBSC 密钥预分配方案, 利用特征向量性质, 仅使用一个源矩阵 A , 可动态生成 $2n$ 个各不相同的秘密矩阵, 解决了门限共谋攻击问题, 同时保证了网络的全连通(任意两个节点间可直接通信), 在保证通信效率的前提下, 引入了申请节点的单次身份验证, 网络的安全性得到了大幅提高. 通过对比分析, 相对于有门限约束的经典 BLOM 方案和非全连通的 RDMS 方案, EBSC 方案更具优势. 特别在网络的更新阶段, 当有新网络节点加入时, EBSC 方案通过简单的赋值操作便可完成网络的扩容, 而经典的 BLOM 方案和 RDMS 方案则需对矩阵进行扩充并下发至网络才能完成, 在极端情况下, 网络新加入节点体量较大时, 这种对矩阵的扩充方案会极大的增加网络普通节点的负荷, 也会导致网络的通信效率下降, 而新提出的 EBSC 方案则不存在上述缺点, 因此新方案更加适合于资源受限的 WSN 网络.

参考文献:

- [1] 任丰原, 黄海宁, 林闯. 无线传感器网络[J]. 软件学报, 2003, 14(7): 1282-1291.
- REN F Y, HUANG H N, LIN C. Wireless sensor networks[J]. Journal of Software, 2003, 14(7): 1282-1291.
- [2] 蒋华, 王瑶, 王慧娇, 等. 基于模糊逻辑的 WSNs 能量高效分簇路由算法[J]. 微电子学与计算机, 2020, 37(7): 25-30.

- JIANG H, WANG Y, WANG H J, et al. Energy-efficient clustering routing algorithm for WSNs based on fuzzy logic[J]. Microelectronics & Computer, 2020, 37(7): 25-30.
- [3] 关志涛, 徐月, 伍军. 传感器网络中基于三元多项式的密钥管理方案[J]. 通信学报, 2013, 34(12): 71-78. DOI: 10.3969/j.issn.1000-436x.2013.12.008.
- GUAN Z T, XU Y, WU J. Ternary polynomial based key management scheme for wireless sensor network[J]. Journal on Communications, 2013, 34(12): 71-78. DOI: 10.3969/j.issn.1000-436x.2013.12.008.
- [4] MSOLLI A, AMEUR H. A new secure key management scheme for wireless sensor network[C]//Proceedings of 2017 International Conference on Control, Automation and Diagnosis (ICCAD). Hammamet, Tunisia: IEEE, 2017: 254-257. DOI: 10.1109/CADI-AG.2017.8075666.
- [5] KAUR G, DEEPALI, KALRA R. Improvement and analys security of WSN from passive attack[C]//Proceedings of the 5th International Conference on Reliability, Infocom Technologies and Optimization. Noida, India: IEEE, 2016: 420-425. DOI: 10.1109/ICRITO.2016.7784992.
- [6] BLOM R. An optimal class of symmetric key generation systems[EB/OL]. (1984-01-06). [2020-03-06]. https://link.springer.com/chapter/10.1007%2F3-540-39757-4_22.
- [7] 佟晓筠, 左科, 王翥. 基于无线传感器网络的混合混沌新分组加密算法[J]. 物理学报, 2012, 61(3): 030502. DOI: 10.7498/aps.61.030502.
- TONG X J, ZUO K, WANG Z. The novel block encryption scheme based on hybrid chaotic maps for the wireless sensor networks[J]. Acta Physica Sinica, 2012, 61(3): 030502. DOI: 10.7498/aps.61.030502.
- [8] 王亚华, 凌玉华, 廖力清, 等. 基于动态子密钥的 WSN 混沌分组加密方案[J]. 通信学报, 2017, 38(12): 144-152. DOI: 10.11959/j.issn.1000-436x.2017292.
- WANG Y H, LING Y H, LIAO L Q, et al. Novel chaotic block encryption scheme for WSN based on dynamic sub key[J]. Journal on Communications, 2017, 38(12): 144-152. DOI: 10.11959/j.issn.1000-436x.2017292.
- [9] YUAN C, CHEN W P, LI D Y. A hierarchical identity-based signcryption scheme in underwater wireless sensor Network[C]//Proceedings of the 11th China Conference on Wireless Sensor Network. Tianjin, China: Springer, 2017. DOI: 10.1007/978-981-10-8123-

- 1_5.
- [10] LIU J H, ZHANG H G, JIA J W, et al. Cryptanalysis of an asymmetric cipher protocol using a matrix decomposition problem[J]. Science China Information Sciences, 2016, 59(5): 052109. DOI: 10.1007/s11432-015-5443-2.
- [11] YUAN C, CHEN W P, LI D Y. A hierarchical matrix decomposition-based signcryption without key-recovery in large-scale WSN[J]. Wireless Communications and Mobile Computing, 2018: 5929828. DOI: 10.1155/2018/5929828.
- [12] DU W L, DENG J, HAN Y S, et al. A pairwise key pre-distribution scheme for wireless sensor networks[C]//Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington: ACM Press, 2003: 42-51.
- [13] 王杨子, 管有庆. 无线传感器网络的多空间密钥预分配方案[J]. 电信快报, 2019(4): 42-62.
- WANG Y Z, GUAN Y Q. Multi-space key pre-distribution scheme for wireless sensor networks[J]. Telecommunications Information, 2019(4): 42-62.
- [14] 王淑华, 陈振龙. 基于格的无线传感器网络密钥协商协议[J]. 传感技术学报, 2019, 32(2): 283-289. DOI: 10.3969/j.issn.1004-1699.2019.02.020.
- WANG S H, CHEN Z L. Lattice-based key agreement protocols for wireless sensor networks[J]. Chinese Journal of Sensors and Actuators, 2019, 32(2): 283-289. DOI: 10.3969/j.issn.1004-1699.2019.02.020.
- 作者简介:**
- 袁 驰(通讯作者) 男,(1980-),博士研究生,高级工程师.研究方向为传感器网络信息安全.
E-mail:chiyuan@ruc.edu.cn.
-
- (上接第 5 页)
- [5] WU Y H, SCHUSTER M, CHEN Z F, et al. Google's neural machine translation system: bridging the gap between human and machine translation[EB/OL]. [2020-01-16]. <https://arxiv.org/pdf/1609.08144.pdf>.
- [6] SILFA F, DOT G, ARNAU J M, et al. E-PUR: an energy-efficient processing unit for recurrent neural networks[C]//Proceedings of the 27th International Conference on Parallel Architectures and Compilation Techniques (PACT). Limassol, Cyprus. ACM, 2018: 1-12.
- [7] LI S C, WU C P, LI H, et al. FPGA acceleration of recurrent neural network based language model[C]//Proceedings of the IEEE 23rd Annual International Symposium on Field-Programmable Custom Computing Machines(FCCM). Vancouver. IEEE, 2015: 111-118. DOI: 10.1109/FCCM.2015.50.
- [8] GUAN Y J, LIANG H, XU N Y, et al. FP-DNN: an automated framework for mapping deep neural networks onto FPGAs with RTL-HLS hybrid templates[C]//Proceedings of the 25th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM). Napa. IEEE, 2017: 152-159. DOI: 10.1109/FCCM.2017.25.
- 作者简介:**
- 范 军 男,(1995-),硕士研究生.研究方向为深度学习加速器设计.
- 巩 杰 男,(1995-),硕士研究生.研究方向为深度学习加速器设计.
- 吴茜凤 女,(1997-),硕士研究生.研究方向为深度学习加速器设计.
- 何 虎(通讯作者) 男,(1974-),博士,副研究员.研究方向为高性能数字信号处理器、嵌入式高性能 CPU IP 设计.
E-mail: hehu@tsinghua.edu.cn