无线传感器网络中基于 LU 分解的分簇密钥管理方法

吴 凡, 毛玉明
(电子科技大学 通信与信息工程学院, 成都 610054)

摘 要: 提出了一种基于 LU 矩阵分解的密钥管理方案。该方案借助于 LU 矩阵来完成密钥预分配,使得所有的簇头间以及节点和它的簇头间都能进行安全通信。分析表明,该方法占用较小密钥存储空间,同时支持网络的拓扑结构变化,能动态地管理密钥信息,从而解决了密钥泄露等问题。

关键词: 无线传感器网络; LU 矩阵; 密钥管理
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2010)01-0265-03
doi:10.3969/j.issn.1001-3695.2010.01.078

New clustered key-management scheme based on LU matrix for wireless sensor networks

WU Fan, MAO Yu-ming
(*School of Communication & Information Engineering, University of Electronic Science & Technology of China, Chengdu* 610054, *China*)

Abstract: This paper proposed a new key-management scheme for wireless sensor networks. Based on the LU matrix, this scheme could pre-load some key information to sensors to insure the establishment of secure link. The analysis shows that the scheme can cost lesser key storage overhead, and can delete and update key information with the network topology changes to avoid key information to be revealed.

Key words: wireless sensor networks(WSNs); LU matrix; key-management

0 引言

无线传感器网络(WSNs)综合了传感器技术、嵌入式计算技术、分布式信息处理技术和无线通信技术,能够协作地实时监测、感知和采集各种环境或监测对象的信息,并对其进行处理,可广泛应用于教育、军事、医疗、交通等诸多领域,拥有巨大的应用潜力和商业价值[1~3]。由于无线传感器网络资源限制以及无中心管理点,网络拓扑结构在分布完成前是未知的,一般处于恶劣环境、无人区域或敌方阵地,无人参与值守,传感器节点的物理安全不能保证等特性,使得任何潜在的敌手可以很容易地截取、窃听和伪造信息。安全对于无线传感器网络来说是非常重要的问题[3]。而以提供安全、可靠的保密通信为目标的密钥管理是无线传感器网络安全研究中最为重要、最为基本的内容。

针对其特殊性,现已提出了许多相应的无线传感器网络的密钥管理方案,这些方案都有不同的优缺点[3]。根据其体系结构的不同可以分为两类[3],即分布式结构和分簇式结构。分布式密钥管理的一般方式是密钥预分配,即在传感器安置前把密钥存储进传感器;在安置后,每个传感器利用存储的密钥与其邻居建立秘密链路。分布式密钥管理的特点是密钥协商通过相邻节点的相互协作来实现,具有较好的分布特性。分簇式密钥管理的特点是对普通节点的计算,存储能力要求低。

本文基于 LU 矩阵分解,结合分簇结构提出了一种新的密钥管理方案。

1 LU 密钥管理方案

在 LU 密钥预方案[4]中,提出了基于矩阵 LU 分解的密钥预分配方案,且网络中任意一对节点都能建立密钥对。其具体实施过程是:首先产生一个大小为 s 的大密钥池 P(包括对应的密钥 ID),该密钥池用于产生一个大小为 $N\times N$ 的对称矩阵 $\boldsymbol{A}$(其中:N 是网络中传感器节点数,且$(N^2-N)/2+N=s$,$\boldsymbol{A}$ 中元素 $A_{ij}(i=1,\cdots,N,j\leqslant i)$ 都是从密钥池中选择的互不相同的密钥);然后对对称矩阵 $\boldsymbol{A}$ 进行 LU 分解,产生一个 $N\times N$ 下三角矩阵 $\boldsymbol{L}$ 和 $N\times N$ 上三角矩阵 $\boldsymbol{U}$,即有 $L_{ij}=\begin{cases} l_{ij} & i\geqslant j \\ 0 & i<j \end{cases}$,$U_{ij}=\begin{cases} u_{ij} & i\leqslant j \\ 0 & i>j \end{cases}$。对于每个节点 $S_i(i=1,2,\cdots,N)$,使用下面的密钥预分配方法:

a)存储 $L_r(i)$。其中 $L_r(i)$ 表示下三角矩阵 $\boldsymbol{L}$ 的第 i 行。

b)同时存储 $U_c(i)$。其中 $U_c(i)$ 表示上三角矩阵 $\boldsymbol{U}$ 的第 i 列。

由于对于下三角矩阵的每一行和上三角矩阵的每一列多是由非零元素和零(零个或多个)组成,在存储下三角矩阵的行和上三角矩阵的列时,仅存储非零元素和含零元素个数的值。这样的存储方式对于含零元素数目多的节点是非常有利的。

当任意两个相邻节点 S_i 和 S_j 要建立密钥对时,首先交换

收稿日期: 2009-05-10; **修回日期**: 2009-06-15

作者简介:吴凡(1978-),男,四川成都人,博士研究生,主要研究方向为无线自组织网络(wufan@uestc.edu.cn);毛玉明(1956-),男,教授,博导,主要研究方向为网络体系结构与协议、宽带通信网、无线通信网等.

彼此所含的关于上三角矩阵的列的信息，然后根据这些信息还原出整个列；同时也根据自己所存的关于下三角矩阵的行，还原出整个行。然后 S_i 计算 $K_{ij}=L_r(i)\times U_c(j)$，$S_j$ 计算 $K_{ji}=L_r(j)\times U_c(i)$。易知 A 是对称矩阵，所以有 $K_{ij}=K_{ji}$，K_{ji}（或 K_{ji}）就是节点 S_i 和 S_j 的通信会话密钥。

2　基于 LU 的分簇密钥管理方案

基于矩阵 LU 分解和分簇网络体系结构如图 1 所示，提出了新的密钥管理方案。

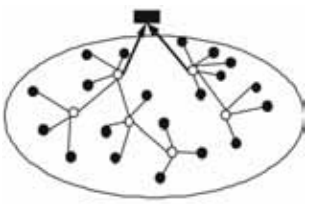

图 1　分簇网络结构

在该方案中，节点只与它自己的簇头通信，并且假设每个节点都能以单跳的方式到达簇头；簇头与基站的通信，采用多跳或单跳的方式到达。

该方案主要有密钥预分配、密钥对的建立、密钥的动态管理几个部分。

2.1　密钥预分配

基于传感器网络资源受限的特点，最好的密钥分配方法就是在部署前预先预置密钥。因此在该方案中，不同的节点将预置不同的密钥信息。

假设网络中有 $m-1$ 个簇，每个簇 $C_i(i=1,\cdots,m-1)$ 有一个簇头记为 CH_i 和 $n-1$ 个普通的簇内节点。在簇 C_i 内的每个普通节点被记为 $C_{ij}(j=1,\cdots,n-1)$，它也作为是普通节点的惟一标志符，作为簇头的节点被记为 C_{in}。

由于在所有簇头和基站组成的高级簇（假设基站为簇头 CH_m）中采用的是 LU 密钥管理方案。而在各个簇头和各自的簇内节点组成的普通簇中，采取的是密钥预分配方案。在该方案中，由于只有簇头和基站组成的高级簇才采用 LU 矩阵预分配方案，用于其中的大小为 $m\times m$ 的对称矩阵 A' 分解为

$$A'=L'U'$$

$$L'=\begin{bmatrix} l_{11} & 0 & \cdots & 0 \\ l_{21} & l_{22} & \cdots & \acute{u} \\ \acute{u} & \acute{u} & & 0 \\ l_{m1} & l_{m2} & \cdots & l_{m1} \end{bmatrix},\quad U'=\begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ 0 & u_{22} & \cdots & u_{2m} \\ \acute{u} & & & \acute{u} \\ 0 & \cdots & 0 & u_{mm} \end{bmatrix}$$

在本文中，用 $r_i(1\leqslant i\leqslant m)$ 表示所存的下三角矩阵 L' 的第 i 行的相关信息，即非零元素和零元素的个数值；同样，用 $c_i(1\leqslant i\leqslant m)$ 表示所存的上三角矩阵 U' 的第 i 列的非零元素信息。由于此时的零元素个数和下三角矩阵 L' 的第 i 行的零元素个数值是一致的，此处就不保存零元素的个数值了。那么由此可以给不同的节点分配不同的密钥信息。

基站 BS 只需存储 r_m、c_m，簇头 CH_i 存储 r_i、c_i。

对于普通的传感器节点，为了降低节点的存储空间，每个节点只需用于与自己簇头通信的密钥信息，因此对于每个簇内也将预存一些密钥信息。以簇 C_i 为例，其中的节点 C_{ij} 与簇头 CH_i 的共享密钥为 KC_{ij}，那么该共享密钥的产生方法如下：

a）基站从所有簇头中随机选取 h 个簇头。其中 $h>1$，h 为偶数。为了方便描述，将选择 $h=2$ 来说明具体的情况，即基站随机选取两个簇头 CH_a 和 CH_b（$1\leqslant a\leqslant m-1$，$1\leqslant b\leqslant m-1$，$a\neq b$）。

b）基站将存在这两个簇头中的密钥信息即 r_a、c_a 和 r_b、c_b，恢复出 $L'_r(a)$、$U'_c(a)$ 和 $L'_r(b)$、$U'_c(b)$ 来计算 KC_{ij}，$KC_{ij}=h(\kappa_1,\kappa_2,C_{ij})$。$h()$ 表示散列函数；κ_1、κ_2 分别由下式得到：$\kappa_1=L'_r(a)\times(L'_r(b))^{\mathrm{T}}$，$\kappa_2=(U'_c(a))^{\mathrm{T}}\times U'_c(b)$。

c）基站将 KC_{ij} 存在节点 c_{ij} 中，并且将与所选的元素相关的簇头对的 ID 即（CH_a，CH_b）存入该节点 C_{ij} 中。

这样，经过密钥预分配阶段，每个不同的节点都预置了不同的密钥信息。对于基站存储 $2m$ 个簇头来说，由于每个簇头所存的密钥数不一样，最小存储空间占用为 3 个，最大为 $2(m-1)+1$。对于普通节点来说一共储存 3 个密钥信息。由于散列函数的特殊性质，使得每个节点所预置的密钥即使被他人所知也不会暴露其他节点的密钥信息。

2.2　密钥对的建立

在网络配置后，每个簇头都要与其他簇头和基站建立密钥对来保证它们的通信安全。在基站和簇头间的密钥对的建立，与 LU 预分配方案中的密钥对的建立方法一致，即将基站和所有的簇头看成是一个高级簇，在这个高级簇内的两节点要通信时，交换自己所存的上三角矩阵的密钥信息，即可计算出彼此的共享密钥。

对于普通簇内的密钥对的建立，为了清楚地描述，以普通节点 C_{ij} 和它的簇头 CH_i 之间的密钥对的建立为例来说明。节点 C_{ij} 和簇头 CH_i 建立密钥对时，首先节点 C_{ij} 要将自己所存的密钥对的 ID 即（CH_a，CH_b）发送给它自己的簇头 CH_i。根据前文可知，簇头 CH_i 和 CH_a、CH_b 都能够建立安全通信。簇头 CH_a 和 CH_b 分别将 $L'_r(a)$ 和 $L'_r(b)$ 通过安全链接发送给簇头 CH_i。同时由于簇头间通信时就已经知道了 $U'_c(a)$ 和 $U'_c(b)$，簇头 CH_i 就可以根据自己的密钥信息和收到的簇头 CH_a 和 CH_b 与它分享的密钥信息来计算与 C_{ij} 的共享密钥 KC_{ij}。首先计算 $\kappa_1=L_r(a)\times(L_r(b))^{\mathrm{T}}$，$\kappa_2=(U'_c(a))^{\mathrm{T}}\times U'_c(b)$，然后簇头 CH_i 计算 $KC_{ij}=h(\kappa_1,\kappa_2,C_{ij})$，这样簇头 CH_i 和节点 C_{ij} 就能用 KC_{ij} 来保证它们的安全通信。

这样整个网络就是一个安全的、连通的网络了。

2.3　密钥的动态管理

由于无线传感器网络的传感器节点容易受到物理损坏或被俘获，把受损节点排除于网络之外或增加新的节点，动态地更新或撤回已受损的密钥是极其重要的。

2.3.1　普通节点的加入

当普通传感器节点加入时（假设这个节点标号为 s_c），首先会给它预分配一个密钥 K_c（K_c 的产生方法与 KC_{ij} 的一致）和存储与 K_c 有关的簇头对的 ID；然后由基站控制，加入一个簇内。与上面所描述的密钥对的建立方法一样，这个新加入的节点将会与它的簇头建立密钥对。

2.3.2　普通节点的删除

假设当节点被俘或受损时，节点的这些不安全性都能探测

到,并且每次探测到之后,都将激发一次相关节点的删除和密钥更新过程。

当普通传感器节点受损或能量耗尽时(假设该节点的标号为 C_{id}),基站广播该节点的不安全性,该节点的簇头收到关于该节点 C_{id} 发送的信息,则不传送给其他簇头用来计算相关的密钥,所以就不会与它建立通信。这样,该节点就被排除到网络外,不会威胁到网络的安全。

3　网络的安全分析及性能分析

3.1　安全性能分析

无线传感器网络中,节点的受损是不可避免的,因此为了保证网络的安全性,要求密钥管理方案具有较好的抗毁性能,即当部分节点受损后,尽可能少地暴露或者不暴露其他未受损节点的密钥信息[5]。在该方案中,普通节点所分配的密钥最终是由散列函数来产生,因此,即使节点被俘,也不会暴露其他节点的密钥,同时该方案能动态地管理密钥信息,以确保在节点受损时网络的安全性。

在该方案中,节点密钥信息的动态管理能及时地把受损节点排除到网络外,因此受损的节点不会暴露其他未受损节点的密钥信息。如图 2 所示,选择一个共有 200 个普通簇、共有 20 000个传感器节点的网络来进行仿真比较,与基本的随机密钥预分配方案[5]、基于 hash 函数的密钥预分配方案[6]作比较。当普通节点受损时,该方案在节点受损时是不会泄露其他密钥的,能完全保证网络的安全。

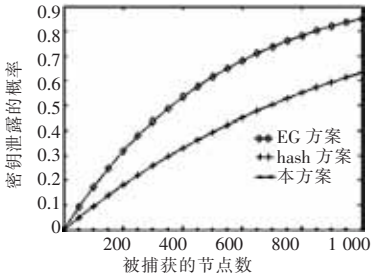

图 2　被捕获节点数与密钥泄露的概率

3.2　存储空间、通信计算开销分析

在该方案中,普通节点只需预存三个密钥,因此对于普通节点存储空间有限的特点来说很有优势。同时对于网络中的簇头来说,平均的存储空间大小为 $m+1$,而对于具有相同安全性能的改进的密钥管理方案[9]来说(即 $\lambda=m$),簇头平均存储 $m+2$ 个密钥,因此在簇头总的存储空间上有一定优势。

同时在该方案中,所有簇首和基站间都是通过单跳或者多跳来完成的,对于在一个簇首的通信范围内,与其他簇首通信也是通过多跳或者单跳结合的,普通节点只与自己的簇头节点通信,这样可以降低通信费用。在该方案中,有密钥的动态管理,涉及到密钥的更新,在一定程度上增加了计算费用;但是就密钥更新来说,对于普通节点的加入或删除,这些过程都是相对简单的,不会引入太多的计算开销和通信开销。

4　结束语

本文在 LU 密钥预分配方案的基础上,提出了一种新的改进的密钥预分配方案。该方案具有一些优势:首先,该方案中普通节点预置密钥的生成方式能使节点在被俘时不暴露其他节点的密钥信息,使得该方案具有良好的抗毁性能,同时,这种方式又降低了普通节点的存储空间;其次,该方案具有密钥的动态管理,因此能够支持网络拓扑结构的变化。根据分析 MATLAB 仿真结果可以看出,比较原有的一些密钥管理方案,该方案具有很好的抗毁性能和较小的开销。

参考文献:

[1] 于海斌,曾鹏,梁韦华. 智能无线传感器网络系统[M]. 北京:科学出版社,2006.

[2] 孙利民,李建中,陈渝,等. 无线传感器网络[M]. 北京:清华大学出版社,2005.

[3] 周贤伟,覃伯平,徐福华. 无线传感器网络与安全[M]. 北京:国防工业出版社,2007.

[4] PATHANA S K,DAI T T,HONG C S. An efficient LU decomposition-based key pre-distribution scheme for ensuring security in wireless sensor networks[C]//Proc of the 6th IEEE International Conference on the Computer and Information Technology. Los Alamitos: IEEE Computer Society,2006:227-232.

[5] 苏忠,林闯,封富君,等. 无线传感器网络密钥管理的方案和协议[J]. 软件学报,2007,18(5):1218-1231.

[6] 张建民,刘贤德,徐海峰. 基于 hash 函数的无线传感器网络密钥预分配方案[J]. 计算机应用,2007,27(8): 1904-1906.

(上接第 264 页)而 S 码要作为附加信息随水印作品一起发布的要求可能会给实际运用带来不便。为此,下一步的研究工作是考虑将 S 码加入到图像像素的 LSB 位,以及优化第三方的嵌入和检测过程以降低其业务负荷。

参考文献:

[1] PODILCHUNK C I,DELP E J. Digital watermarking:algorithms and applications[J]. IEEE Signal Processing Magazine,2001,18(4):33-46.

[2] 伍凯宁,曹汉强,朱耀庭,等. 数字水印攻击技术及对策研究[J]. 计算机应用研究,2004,21(9):153-154.

[3] 王志雄,王慧琴,李人厚. 数字水印应用中的攻击和对策综述[J]. 通信学报,2002,23(11):74-79.

[4] KIROVSKI D,MALVAR H. Embedding and detecting spread-spectrum watermarks under estimation attacks[C]//Proc of IEEE International Conference on Acoustics, Speech and Signal Processing. 2002: 1293-1296.

[5] KALKER T,LINNARTZ J R M G,DIJK M van. Watermark estimation through detector analysis[C]//Proc of International Conference on Image Processing. 1998:425-429.

[6] CRAVER S,MEMON N,YEO B L,*et al*. Resolving rightful ownerships with invisible watermarking techniques:limitations,attacks and implications[J]. IEEE Journal on Selected Areas in Communications,1998,16(4):573-586.

[7] 李昌利,卢朝阳. 数字水印的去同步攻击及其对策[J]. 中国图象图形学报,2005,10(4):403-409.

[8] PETITCOLAS F A P. Watermarking schemes evaluation[J]. IEEE Trans on Signal Processing,2000,17(5):58-64.

[9] [EB/OL]. http://www. petitcolas. net/fabien/software/StirMark-Benchmark_4_0_129. zip.