基于矩阵的无线传感器网络密钥预分配 *

郑亚红[1], 王彩芬[1], 李 旭[1], 杜秋菊[2]
(1. 西北师范大学 计算机科学与工程学院, 兰州 730070; 2. 西安电子科技大学附中, 西安 710071)

摘 要: 为了提高邻居节点建立共享密钥的概率,减少无线传感器网络资源的消耗,从而进一步提高无线传感器网络中的连通性,提出了一种基于矩阵的无线传感器网络的随机密钥部署方案。该方案在无线传感器的目标划分区域中采用 3 ×3 矩阵的方式进行密钥预分配,使邻居节点共享直接密钥的个数为 q,提高了节点间共享密钥的阈值,减少了节点存储冗余密钥的数量。数据分析和仿真结果表明,该方案不但在存储密钥数量和安全性方面有较好的性能,而且连通率为 100% 。

关键词: 无线传感器网络; 密钥预分配; 部署信息; 共享密钥阈值; 连通性; 抗毁性
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2013)09-2799-03
doi:10.3969/j.issn.1001-3695.2013.09.060

Key pre-distribution scheme for wireless sensor network using matrix deployed knowledge

ZHENG Ya-hong[1], WANG Cai-fen[1], LI Xu[1], DU Qiu-ju[2]
(1. *College of Computer Science & Engineering, Northwest Normal University, Lanzhou* 730070, *China*; 2. *Middle School Affiliated to Xidian University, Xi'an* 710071, *China*)

Abstract: In order to enhance the probability of common keys in neighbor nodes, reduce wireless sensor networks resource cost and further enhance connectivity of wireless sensor networks (WSNs), this paper proposed a key management scheme using matrix deployment and communication key for wireless sensor networks. It used way of 3 ×3 matrix to distribute the keys so as to the neighbor nodes have q common keys. In square grid using matrix deployment could enhance the threshold of common keys and reduce redundancy keys in each of node. Theoretic studies and figures of simulation show that the proposed scheme not only provides better performance in connectivity and security, but also obtains up to 100% reduction in the number keys.

Key words: wireless sensor network (WSN); key pre-distribution; deployment knowledge; common threshold; connectivity; invulnerability

0 引言

无线传感器网络(WSN)的应用非常广泛,它可以用于军事目标追踪、环境监测、空间探索、医疗健康等[1,2]很多方面,对人类的生活产生重大的影响。无线传感器网络经常需要部署在人迹罕至的恶劣环境中,节点会面临各种安全威胁。例如,恶劣的自然环境会使节点失效,遭受到重放、伪造、窜改等攻击会对整个网络造成破坏,因此无线传感器网络安全的研究显得尤为重要,其中密钥管理是研究热点。密钥管理通过为传感器的邻居节点建立共享密钥为它们之间的通信进行加密和认证来提供安全可靠的保密通信。

鉴于传感器网络自身如电池供电、计算能力有限、存储容量小和通信距离有限等特点,密钥管理技术面临许多困难和挑战。传统的密钥管理技术,如公钥加密体系已不再适用。随机密钥预分配技术是一个很好的选择。为了满足无线传感器网络的特殊需求,研究人员已提出了多种密钥预分配方案[3~10]。Eschenauer 等人[4]提出了随机密钥预分配 E-G 方案,为后来提出的各种改进方案提供了一种可行的思路。方案中每个节点预分配一定数量的密钥,节点之间通过预分配的相同密钥建立安全通信。但是此方案会造成节点中存放大量无用的密钥,浪费节点内存,而且冗余的信息使攻击者在捕获少数的节点后就可获得大份额的密钥,抗毁性差。为降低该方案的任意两对节点通信密钥相同的概率,文献[5]提出了 q-composite 随机密钥预分配方案,其中任意两个节点至少拥有 q 个相同的密钥,该方案抵抗小规模节点受损攻击能力强于 E-G 方案,在一定范围内提高了网络的安全性。根据 E-G 方案的随机密钥预分配的思想,Du 等人[6,7]把网络中的节点划分成若干个组,每个组对应分布到一个目标区域中,这种方法使位于相同组节点有共享密钥的概率得到提高,同时在一定程度上也使网络的安全性得到保证。为了更好地提高分组部署时无线传感器网络的覆盖率及整个网络的连通性等性能,文献[8]提出了六边形与双变量多项式相结合的随机密钥预分配方案,该方案采用六边形划分无线传感器网络区域,适用于大型网络且有很高的网络连通性。文献[9]利用部署信息提出了一种无线传感器网络密

收稿日期: 2012-12-13; **修回日期**: 2013-01-30 **基金项目**: 国家自然科学基金资助项目(61163038,61063041,61202395);西北师范大学青年教师科研能力提升计划项目(NWNU-LKQN-12-32);甘肃省自然科学基金资助项目(2011GS04466);国家教育部"新世纪优秀人才计划"资助项目(NCET-12-0620);国家人才资源和社会保障部留学回国人员择优资助项目

作者简介:郑亚红(1987-),女,硕士研究生,主要研究方向为信息安全与密码学(879081988@qq.com);王彩芬,教授,博导;李旭(1985-),男,硕士研究生,主要研究方向为信息安全与密码学;杜秋菊(1979-),女,二级教师,主要研究方向为信息技术及应用.

钥预分配方案。

在随机密钥预分配技术中,从大的密钥空间中随机选取一组密钥作为密钥池,传感器网络中的每个节点在部署之前先从密钥池中随机选取一定数量的密钥,通过这种方法,两个节点有可能从事先选取的密钥中找到共享的密钥来建立通信信道[11]。但这种随机密钥预分配方法也存在缺陷,如任何两个节点有共享密钥的概率很低,网络的连通性不强,安全也不能得到很好的保证。

本文提出了一种新的基于矩阵的无线传感器网络随机密钥预分配方案,利用部署信息将节点以组的形式进行分配,邻居节点有共享密钥的概率为1,很大程度上增强了网络的抗毁性。本方案将目标区域分为若干个正方形的子区域,对应若干个密钥池,每个正方形区域中采用矩阵的方式进行密钥预分配。给每个节点预先分发少量的密钥信息,提高了节点间共享密钥的阈值,减少了节点存储的冗余密钥的数量,消耗节点的内存减少,同时随着共享密钥阈值的增大,攻击者破坏安全链路的难度呈指数增大。

1 网络模型

本方案具有很强的通用性和实用性。将无线传感器的目标区域用正方形进行划分,每个正方形子区域对应一个传感器节点的位置,分别部署密钥。在部署密钥时,对同样划分的密钥的每个正方形子区域再划分为 3×3 的矩阵,模型如图1所示。

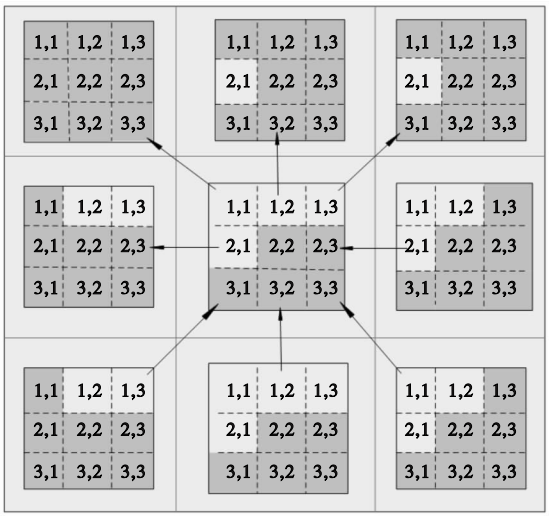

图1 网络模型

2 密钥预分配及共享

本方案中,有一个主密钥池在部署之前由系统生成,称为 S,里面包括密钥和对应的 ID,无线传感器网络中所有节点的密钥都从 S 中选取。

2.1 密钥预分配方案

在密钥分配前先将无线传感器网络区域分成若干个正方形的子区域,对应节点的位置,密钥池子区域中的 3×3 矩阵对应该位置节点的密钥分配。本方案相邻节点至少共享 q 个密钥,由本文的仿真得出,当 $q \leqslant 5$ 时连通性与安全性能较好。m 为传感器节点存储的密钥数,n 为分组密钥池中的密钥总数,因为本文考虑到相邻节点之间的上、下、左、右、左上、左下、右上、右下以及中间这九个方位,所以 m 和 n 取值为 $9q$。

分组密钥池 $S_{(i,j)}$ 的密钥分配步骤如下:

a)将密钥池 S 分成 $t \times n$ 个 $S_{(i,j)}$ ($i=1,2,\cdots,t$;$j=1,2,\cdots,n$)。每个密钥池的大小为 n 且 $n=9q$。

b)再将 $S_{(i,j)}$ 分成 3×3 的矩阵,用 $S_{(i,j)}^{(x,y)}$ 表示($x=1,2,3$;$y=1,2,3$),每个部分数量大小为 q。

c)对于 $S_{(1,1)}$,从 S 中随机选取 $9q$ 个密钥分配给 $S_{(1,1)}^{(x,y)}$。

d)对于 $S_{(1,j)}$,将 $S_{(1,j-1)}^{(2,3)}$ 的 q 个密钥复制给 $S_{(1,j)}^{(2,1)}$,剩下的 $8q$ 个密钥从 S 中随机选取分配给 $S_{(1,j)}^{(x,y)}$,其中$(x,y) \neq (2,1)$且 $j \neq 1$。

e)对于 $S_{(i,1)}$ ($i \neq 1$),将 $S_{(i-1,1)}^{(3,2)}$ 中的 q 个密钥复制给 $S_{(i,1)}^{(1,2)}$,将 $S_{(i-1,2)}^{(3,1)}$ 的 q 个密钥复制给 $S_{(i,1)}^{(1,3)}$,剩下的 $7q$ 个密钥从 S 中随机选取。

f)对于 $S_{(i,j)}$ ($i \neq 1, j \neq 1$)。当 $j \neq n$ 时,将 $S_{(i,j-1)}^{(2,3)}$ 的 q 个密钥复制给 $S_{(i,j)}^{(2,1)}$,将 $S_{(i-1,j-1)}^{(3,3)}$ 的 q 个密钥复制给 $S_{(i,j)}^{(1,1)}$,将 $S_{(i-1,j)}^{(3,2)}$ 的 q 个密钥复制给 $S_{(i,j)}^{(1,2)}$,将 $S_{(i-1,j+1)}^{(3,1)}$ 的 q 个密钥复制给 $S_{(i,j)}^{(1,3)}$,剩下的 $5q$ 个密钥从 S 中随机选取;当 $j=n$ 时(位于 i 行最后一列),将 $S_{(i,j-1)}^{(2,3)}$ 的 q 个密钥复制给 $S_{(i,j)}^{(2,1)}$,将 $S_{(i-1,j-1)}^{(3,3)}$ 的 q 个密钥复制给 $S_{(i,j)}^{(1,1)}$,将 $S_{(i-1,j)}^{(3,2)}$ 的 q 个密钥复制给 $S_{(i,j)}^{(1,2)}$,剩下的 $6q$ 个密钥从 S 中随机选取。

上述步骤完成后,将每个分组中的密钥分发给对应的节点并定期重分发,以保证网络和节点的安全性。

以图1为例,对该密钥预分配过程举例描述。

a)对于 $S_{(1,1)}$,从 S 中随机选取 $9q$ 个密钥分配给 $S_{(1,1)}^{(x,y)}$。

b)对于 $S_{(1,2)}$,将 $S_{(1,1)}^{(2,3)}$ 的 q 个密钥复制给 $S_{(1,2)}^{(2,1)}$,剩下的 $8q$ 个密钥从 S 中随机选取,再分配给 $S_{(1,2)}^{(x,y)}$,其中$(x,y) \neq (2,1)$。

c)对于 $S_{(1,3)}$,将 $S_{(1,2)}^{(2,3)}$ 的 q 个密钥复制给 $S_{(1,3)}^{(2,1)}$,剩下的 $8q$ 个密钥从 S 中随机选取,再分配给 $S_{(1,3)}^{(x,y)}$,其中$(x,y) \neq (2,1)$。

d)对于 $S_{(2,1)}$,将 $S_{(1,1)}^{(3,2)}$ 的 q 个密钥复制给 $S_{(2,1)}^{(1,2)}$,将 $S_{(1,2)}^{(3,1)}$ 的 q 个密钥复制给 $S_{(2,1)}^{(1,3)}$,剩下的 $7q$ 个密钥从 S 中随机选取。

e)对于 $S_{(2,2)}$,将 $S_{(1,1)}^{(3,3)}$ 的 q 个密钥复制给 $S_{(2,2)}^{(1,1)}$,将 $S_{(1,2)}^{(3,2)}$ 的 q 个密钥复制给 $S_{(2,2)}^{(1,2)}$,将 $S_{(1,3)}^{(3,1)}$ 的 q 个密钥复制给 $S_{(2,2)}^{(1,3)}$,将 $S_{(2,1)}^{(2,3)}$ 的 q 个密钥复制给 $S_{(2,2)}^{(2,1)}$,剩下的 $5q$ 个密钥从 S 中随机选取。

f)对于 $S_{(2,3)}$,将 $S_{(2,2)}^{(2,3)}$ 的 q 个密钥复制给 $S_{(2,3)}^{(2,1)}$,将 $S_{(1,2)}^{(3,3)}$ 的 q 个密钥复制给 $S_{(2,3)}^{(1,1)}$,将 $S_{(1,3)}^{(3,2)}$ 的 q 个密钥复制给 $S_{(2,3)}^{(1,2)}$,剩下的 $6q$ 个密钥从 S 中随机选取。

g)对于 $S_{(3,1)} \sim S_{(3,3)}$,重复步骤 d) ~ f)。

至此将图1的密钥分配完毕。

2.2 密钥共享分析

在本文方案中,由于节点的密钥中有部分是从它的相邻节点复制过去的,保证了相邻节点间共享密钥的个数大于等于 q 个。当有共享密钥的两个节点进行通信时,就可以在共享的密钥中随机选择其中一个进行通信,这样在每次通信时使用不同的共享密钥,既提高了网络的安全性,同时也增强了网络的抗毁性。如图1所示,灰色分组中的密钥从 S 中选取,白色分组中的密钥从相应邻居节点中复制。可以看出,一个 $S_{(i,j)}$ 中最多有四部分是从相应邻居节点复制的,剩下都是从 S 中选取的。这样不仅保证了相邻节点共享至少 q 个密钥,而且具有更好的抵抗捕获节点的回弹性。

3 性能分析

3.1 通信和计算需求

通信和计算需求分析在无线传感器网络资源受限的环境中显得尤为重要。由于本文方案中相邻节点至少共享 q 个密钥,故密钥建立的概率为1。显然,邻居节点直接共享 q 个密

钥,相互只需一跳就能进行通信,有效地减少了通信负载。假设发送和接收一条消息的能量消耗为 e_s 和 e_r,计算消耗为 e_l,密钥建立概率为 p。表 1 为本方案和 E-G 方案、TGKP 方案在通信消耗和计算消耗的对比。

表 1　节点能量消耗

方案	通信消耗	计算消耗
E-G 方案	$e_s + ce_r + (1-p)ce_s$	pce_l
本方案	$e_s + ce_r$	ce_l
TGKP 方案	$e_s + ce_r + (1-p)ce_s$	pce_l

通过表 1 可以看出,本文方案的通信消耗是最低的,计算消耗略高。但研究表明,无线传感器网络中传输消耗比计算消耗要大得多,将 1 bit 信息传至 100 m 外的消耗与运行三千条指令大致相当。总的来说,本方案在能量消耗方面优于其他方案。

3.2　连通性

全局连通性是指传感器网络的所有节点最大连接部分占整个网络的比例。如果全局连通性为 99%,就意味着在无线传感器网络中有 99% 的节点相互之间是连通的。因此,全局连通性可以衡量无线传感器网络中的节点由于无法连通而浪费的比例。本地连通性表示一个网络中任意两个节点至少共享一个密钥的概率。从 2.2 节可以看出,在本文方案中任意两个节点至少共享一个密钥的概率为 1,即本地连通性为 1。假设 n' 为每个节点的邻居节点数,r 为节点的通信半径,P_l 为本地连通性,P_g 为全局连通性,N 为节点总数,节点的度 d 指有共享密钥的节点的个数,则有

$$n' = (\pi \times r^2 \times N)/(t \times n)$$

$$d = n' \times p_l = (N-1) \times (\ln(N) + c)/N$$

$$P_g = e^{-e^{-c}}$$

则 P_l 与 P_g 满足

$$P_l = \frac{t \times n \times (N-1) \times (\log_e(N) - \log_e(-\log_e(P_g)))}{\pi \times r^2 \times N^2}$$

在本方案中有如下配置 $r = 40$ m,$t = n = 1\ 000$ m,$N = 10\ 000$。表 2 列出了矩形方案和六边形方案 P_l 与 P_g 的关系。

表 2　矩形方案与六边形方案本地连通性与全局连通性

P_g	0.1	0.4	0.7	0.9	0.99
矩形方案的 P_l	0.166 6	0.184 9	0.203 6	0.227 9	0.274 6
六边形方案的 P_l	0.266 3	0.295 6	0.325 6	0.364 4	0.439 1

通过计算可以得出,本方案的全局连通性约等于 1,明显高于传统的矩形和六边形方案。

3.3 安全性分析

假设当节点部署在目标区域后会遭受到敌手的物理攻击,敌手会捕获节点并获取节点内存中的信息。当敌手捕获一定数量的节点时,对传感器网络中通信链路破坏的比例可以衡量无线传感器网络的安全性。捕获一定数量的节点,对网络中通信链路影响的比例越小说明方案越安全。假设被捕获节点的数量为 x,网络被俘通信链路的比例可用下式定义:

$$P_{att} = 1 - [1 - \frac{m}{|S|}]^x$$

经过分析和统计,在大部分方案中无线传感器网络的全局连通性为 0.6 左右,本方案中全局连通性和本地连通性均为 1,提高了节点间共享密钥的阈值,同时减少了节点存储的冗余密钥。随着共享密钥阈值的增大,攻击者破坏安全链路的难度呈指数增大,同时保证了较高的网络安全连通性。当捕获相同数量的节点时,被俘的通信链路比例低于其他方案,有效地提高了网络的抗毁性。图 2 为几种密钥预分配方案的安全性能对比。

从图 2 可以看出,本文方案不但有 100% 的连通概率,同时也保证了很好的安全性能,当捕获相同数量的节点时,破坏网络中安全链路的比例与 E-G 方案和矩形、六边形方案相比更低。另外,由于本文方案相邻节点共享至少 q 个密钥,在有共享密钥的节点中进行通信时,可以随机选择其中一个共享密钥建立安全链路,每次通信所用密钥不同,可以进一步增强无线传感器网络的安全性。

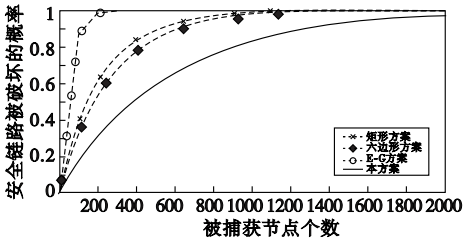

图2　节点抗捕获能力分析

4　结束语

本文提出了运用部署信息的基于矩阵的无线传感器网络随机密钥预分配方案。该方案的每个传感器节点与其他方案相比仅需要存储少量密钥就能达到相同的安全性能,同时还能保证百分之百的连通率。这对于具有有限资源的传感器来说,是十分必要的。通过数据分析和仿真表明,只要相应参数满足要求,邻居节点之间共享 q 个密钥的概率均为 1,在通信时随机选择其中一个共享密钥就能建立安全链路,提高了节点间共享密钥的阈值,减少了节点存储的冗余密钥,在保证很高网络连通性的同时减少了节点的存储消耗。

参考文献:

[1] YICK J, MUKHERJEE B, GHOSAL D. Wireless sensor network survey[J]. IEEE Computer Networks, 2008, 52(12): 2292-2300.

[2] MAO Guo-qiang, FIDAN B, ANDERSON B D O. Wireless sensor network localization techniques[J]. IEEE Computer Networks, 2007, 51(1): 2529-2553.

[3] DU Wen-liang, DENG Jing, HAN Y S, *et al*. A key management scheme for wireless sensor networks using deployment knowledge[C]//Proc of IEEE International Conference on Computer Communications. 2004.

[4] ESCHENAUER L, GLIGOR V. A key management scheme for distributed sensor networks[C]//Proc of the 9th ACM Conference on Computer and Communications Security. New York: ACM Press, 2002: 41-47.

[5] CHAN Hao-wen, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]//Proc of IEEE Symposium on Security and Privacy. 2003: 197-213.

[6] LIU Dong-gang, NING Peng, DU Wen-liang. Group-based key predistribution for wireless sensor networks[J]. ACM Trans on Sensor Networks, 2008, 4(2): 1-30.

[7] DU Wen-liang, DENG Jing, HAN Y S, *et al*. A key pre-distribution scheme for sensor networks using deployment knowledge[C]//Proc of IEEE INFOCOM. 2004: 586-597.

[8] KONG Bei-bei, CHEN Hong-yang. Key pre-distribution schemes for large-scale wireless sensor networks using hexagon partition[C]//Proc of Wireless Communications and Networking Conference. 2010: 18-21.

[9] 余旺科. 无线传感器网络密钥管理方案研究[D]. 西安:西安电子科技大学, 2011.

[10] YU Zhen, GUAN Yong. A key management scheme using deployment knowledge for wireless sensor networks[J]. IEEE Trans on Parallel and Distributed Systems, 2008, 19(10): 1411-1425.

[11] 余旺科,马文平. 无线传感器网络密钥预分配方案研究[J]. 网络安全技术与应用, 2010, 10(5): 19-21.