基于最小生成树的异构传感器网络抗共谋优化方案

马春光[①③④] 戴膺赞[①②] 王九如[*①] 王慧强[①]
[①](哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)
[②](中国人民解放军 93062 部队 89 分队 吉林 132102)
[③](北京邮电大学网络与交换技术国家重点实验室 北京 100876)
[④](哈尔滨工程大学国家保密学院 哈尔滨 150001)

摘 要：基于 EBS (Exclusion Basis Systems)的密钥管理协议，以安全性高、动态性和扩展性好，较适用于异构传感器网络，但却存在共谋问题。该文提出了一种基于 MST (Minimum Spanning Tree)的密钥共谋问题优化方案。该方案利用 Prim 算法对由簇内感知节点所构成的无向连通图进行最小生成树求解，并对该树进行遍历，根据所得节点遍历顺序进行密钥的指派与分配，使得相邻节点间所含的密钥重叠程度增大，发生共谋的可能性得到降低。实验结果表明：同比于密钥随机分配方案与 SHELL 方案，所提方案有效提高了网络的抗捕获能力。

关键词：异构传感器网络；密钥管理；共谋问题；最小生成树(MST)；EBS
中图分类号：TP393 **文献标识码**： A **文章编号**：1009-5896(2011)12-3046-05
DOI: 10.3724/SP.J.1146.2010.01367

A Minimum Spanning Tree Based Optimization Scheme of Collusion Restraining in Heterogeneous Sensor Networks

Ma Chun-guang[①③④] Dai Ying-zan[①②] Wang Jiu-ru[①] Wang Hui-qiang[①]
[①](*College of Computer Science and Technology*, *Harbin Engineering University*, *Harbin* 150001, *China*)
[②](*Squad* 89, *Troop* 93062 *of PLA*, *Jilin* 132102, *China*)
[③](*State Key Laboratory of Networking and Switching Technology*,
Beijing University of Posts and Telecommunications, *Beijing* 100876, *China*)
[④](*College of National Secrecy*, *Harbin Engineering University*, *Harbin* 150001, *China*)

Abstract: Owing to the better security, dynamic and extensibility, Exclusion Basis Systems (EBS) based key management applies to security of heterogeneous sensor networks, but it suffers from the collusion. This paper introduces a Minimum Spanning Tree (MST) based optimization scheme of key collusion restraining, which uses Prim algorithm to create MST from undirected graph constituted by nodes in cluster. Traversing the tree gets a sequence of nodes. The sequence is used to design and distribute keys in the scheme. It improves the repeated degrees of keys in adjacent nodes and reduces the possibility of key collusion. The experimental results show that the optimization scheme effectively improves the resistant of networks' capture, comparing with SHELL and random distribution method.

Key words: Heterogeneous Sensor Networks (HSN); Key management; Collusion issue; Minimum Spanning Tree (MST); Exclusion Basis Systems (EBS)

1 引言

随着对传感器网络的深入研究和对其安全的考虑，由不同类型节点所构成的异构传感器网络(Heterogeneous Sensor Networks, HSN)成为了近年国内外学者们研究的热点[1,2]。在 HSN 中，不同类型的节点在计算能力、存储容量，以及能耗水平等方面因需要而有所不同，通常可分为基站、簇头和感知节点 3 类[3]。由于受无线通信等特性限制，对于数据机密性、完整性和可靠性的安全性保证显得尤为重要。通常假设基站是可信的，即不能被捕获或失效；簇头具有比感知节点更强的存储、计算和通信

2010-12-13 收到，2011-10-08 改回
国家自然科学基金(60973027, 61170241)，中央高校基本科研业务费专项资金(HEUCF100601)，博士后科研人员落户黑龙江科研启动资助金(LBH-Q10141)，北京邮电大学网络与交换技术国家重点实验室开放课题(SKLNST-2009-1-10)和黑龙江省教育厅科学技术研究项目(12513049)资助课题
*通信作者：王九如 jiuruwang@163.com

能力和更高的安全性；感知节点数量大、分布广，且安全性能较弱，在整个网络中容易失效甚至被捕获。因此本文只针对感知节点的安全性问题进行讨论。基于 EBS(Exclusion Basis Systems)[4]的密钥管理方法由于安全性高和扩展性好，在近年国内外的一些研究成果 [5−8] 中被广泛应用于 HSN 中，但却存在共谋问题[9]，即敌方可通过捕获节点的方式来获得节点内的密钥，共享并扩大这些被捕获节点对于密钥的获取，进而破坏整个密钥系统。它是影响基于 EBS 的 HSN 密钥管理系统安全性的主要因素。

对于共谋问题的防范，近年国内外学者曾提出了几种解决方案 [10−13]，但却较为片面。为此，本文从遏制共谋成因的角度出发，设计了一种旨在解决该问题的优化方案，即通过增加共谋群中节点数量，使相邻节点间发生共谋的概率得到降低。实验结果表明：该方案有效增强了网络抵御共谋攻击的能力，提高了安全性。

2　抗共谋优化方案

方案设计的主要宗旨在于优化 HSN 中任意区域内相邻节点管理密钥组合，尽可能减小节点间的海明码距。

2.1 符号及定义说明

在介绍优化方案前，先将符号及定义表述如表 1 所示。

表 1 符号说明

符号	含义	符号	含义
N	节点数量	C_i	密钥组合
n_α	感知节点 α	K_β	感知节点内密钥
k	节点内密钥数量	$A(\alpha,\beta)$	EBS 正则矩阵，α 表节点，β 表密钥
m	更新密钥的消息数	Ksch	感知节点与簇头间通信密钥
k+m	密钥总数	T_i	连通图生成的最小生成树子树

定义 1　密钥重叠度　不同节点间所含相同密钥的程度。

定义 2　共谋群　当一个捕获节点的集合所拥有的密钥总数为全部密钥空间时，该捕获节点集合称为共谋群。其中，形成共谋群所需节点数量最少的称为最小共谋群。

2.2 理论依据

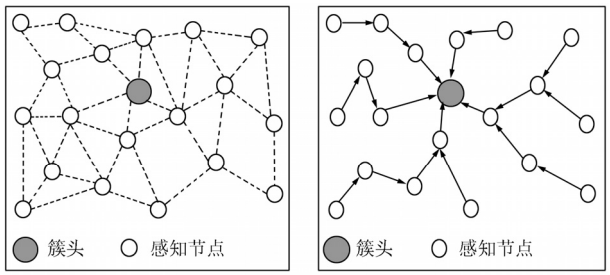
在实际应用中敌方往往根据被捕获节点的通信代价来寻找下一个被捕获的目标，通信代价相对较小的节点易成为被捕获目标。在相同密钥空间的情况下，密钥重叠度越大，妥协节点发生共谋的概率越小。显然，在 HSN 中节点数量最小的共谋群是网络安全的最薄弱环节[7]。共谋群大小与节点密钥分配方案有关，对同一个网络和密钥空间而言，不同的密钥分配方案会得到不同的最小共谋群。因此，在设计基于 EBS 的 HSN 密钥分配方案时，增大相邻节点内密钥重叠度，扩大共谋群中节点数量，使得在簇内任何一个区域内而又距离相近的节点间发生共谋的概率得到降低，是共谋问题优化方案的主要设计思想。HSN 密钥管理流程大致可分为密钥的分析、指派、产生和分配 4 个环节，本方案即对密钥指派这一环节进行优化，任意两列海明码的码距最小值为 2。

2.3 方案设计

假设 HSN 所有节点随机分布在矩形监测区域内，从图论的角度将 HSN 中的一个簇抽象为由簇头和感知节点构成的连通图，节点间优化方法变为解决连通图的相关问题。因此，我们从最小生成树能够解决连通图相关问题中得到启示，将遍历最小生成树所得结点顺序与 HSN 中的密钥分配顺序相关联。在对 HSN 簇内感知节点的实际遍历中，Prim 算法的时间复杂度为 $O(n^2)$，且与边数 E 无关，更适合于求边数较多的带权无向连通图的最小生成树。而对于树的 3 种遍历方法均适用于本方案，只需将簇头从遍历所得顺序列表中删除。实际应用中，可采用先通过每个感知节点在自己所知的局部图中构造以自己为根节点的局部最小生成树(Local Minimum Spanning Tree, LMST)[1]，再向簇头汇总的办法，这实际上是对全局最小生成树算法的一种分布式近似最优实现。

以单簇内节点连通情况为例，图 1 所示为经 Prim 算法前后，单簇内由簇头和感知节点所构成的连通图。当单簇内以节点间通信代价为权值的最小生成树形成之后，与簇头邻近且单跳通信的感知节点为各子树的根节点。簇头根据与其实现单跳通信的感知节点的位置坐标，以某一节点为起始，按照顺(逆)时针的方向进行扫描，得到的顺序即为子树的遍历顺序。

当簇中各感知节点所构成的连通图生产 MST 后，对其进行遍历，得到由感知节点构成的顺序列表。簇头将利用基于海明码距的方法产生 EBS 矩阵表，并与之前生成的感知节点前序列表一一对应，对感知节点的密钥指派即根据此对应关系确定。在 HSN 的密钥分配过程中，簇头根据此密钥指派表，向感知节点分配管理密钥，即可实现扩大相邻节点间密钥重叠度，有效抵御共谋攻击的目的。



(a) Prim 算法前单簇内节点无向连通图　(b) 经 Prim 算法后单簇内节点有向连通图

图 1 单簇内节点连通示意图

2.4 实现步骤

优化方案的具体实现处于网络初始化阶段。在节点部署之前的密钥管理中，应用基于对称密码体制的密钥预分配方法，分配 HSN 中不同类型节点间的通信密钥；在节点部署之后的密钥管理中，应用基于密钥分发中心(KDC)的密钥分配方法，分配 HSN 中的管理密钥。根据上一小节内容对优化方案的设计，其实现步骤设计如下：

步骤 1　待所布置的各节点就位之后，感知节点和簇头分别与基站建立联系，请求身份认证，并向基站提供各自的信息(包括 ID 和地理位置等)；

步骤 2　基站根据感知节点的通信能力范围和地理位置对其进行分簇，并向感知节点和簇头分发它们之间的通信密钥 Ksch。

步骤 3　簇头与簇内所属感知节点建立联系，根据感知节点数量，确定 k 与 m 的取值，并利用海明码距的方法，建立本簇的 EBS 矩阵表。

步骤 4　簇内的每个感知节点，以通信代价为权值，利用 Prim 算法生成以簇头为根的最小生成树，簇头对其进行遍历，得到感知节点遍历顺序。

步骤 5　簇头将上述遍历所得感知节点顺序与基于海明码距方法生成的 EBS 矩阵表一一对应，为簇内每个感知节点指派密钥 K_β 组合，使得排序相邻的两个感知节点中所含密钥重叠度最大。

步骤 6　经簇头与感知节点的通信密钥 Ksch 加密后，簇头向簇内每个感知节点分配 k 个管理密钥。

3 有效性验证

实验平台采用边长为 150 m 的正方形区域，随机布置 20 至 60 个感知节点，节点的通信半径为 20 m，实验结果在进行 20 次之后取平均值。EBS(N,k, m)规定每个节点拥有 k=2~7 个密钥，$k+m$=8, 12。随着被捕获节点数量的增加，敌方获知的密钥数量也会不断增大，网络安全性将不断下降。通常以敌方捕获的节点数目与敌方获知的密钥数量之间的关系来表示网络抗捕获能力，而以最小共谋群中节点数量来表示使网络安全体系失效的难易程度，它们都是 HSN 密钥体系安全性的重要参数。该优化方案将在这两方面与密钥随机分配方案[14]和 SHELL 方案[15]进行验证和比较。

3.1 网络抗捕获能力

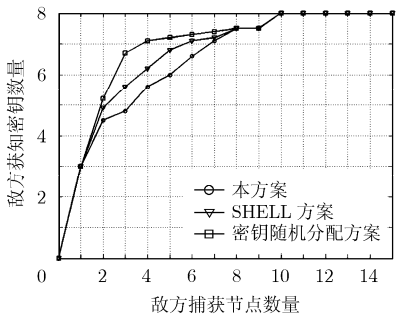
在节点数量 N 和节点密钥数量 k 的取值相同，而密钥空间 $k+m$ 的取值不同的情况下，采用密钥随机分配方案、SHELL 密钥分配方案与本方案所得到的网络抗捕获能力如图 2 所示。假设 N=50, k=3, $k+m$=8, 12。从实验结果可知，在敌方捕获少量节点的情况下，3 种方案的网络抗捕获能力水平相当。随着敌方捕获节点数量的增大，获知的密钥数量将不断增大，整个网络的密钥空间被获知的概率逐渐提高，本方案对于 SHELL 密钥分配方案和密钥随机分配方案的优势逐渐趋于明显，这种优势在密钥空间 $k+m$ 增大的情况下也会随之增大。采用本方案后，相邻节点中密钥重叠度得到了提高，在相同条件下，整体网络被敌方捕获的平均次数少于其它两种密钥分配方案，网络抗捕获能力获得增强。

3.2 最小共谋群节点数量

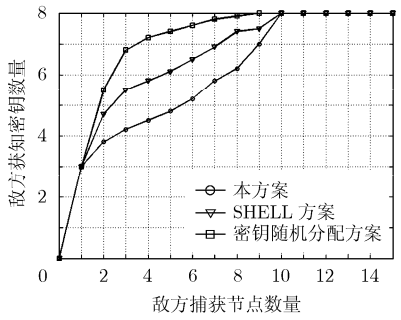
在节点数量 N 和节点密钥数量 k 的取值不同，而密钥空间 $k+m$ 的取值相同的情况下，采用密钥随机分配方案、SHELL 密钥分配方案和本方案所得到的最小共谋群节点数量如图 3 所示。假设 $k+m$=8, N=20，若 k 增加，则捕获单个节点获得的密钥信息量会增大，因此在 3 种密钥分配方案中，最小共谋群节点数量都会随着 k 的增大而减少。假设 $k+m$=8, k=3，若 N 增大，网络中节点密度变大，各节点的邻居数增加，使得共谋更容易形成，最小共谋群节点数量也会因此而变小。从实验所得结果可知，本方案明显优于其它两种密钥分配方案，特别在 N 和 k 的取值较小时。

4 结论

基于EBS的密钥管理理论丰富了HSN安全策略的内容，在拓展网络规模的同时，节省了密钥的存储空间，但由于其建立在组合理论的基础上，易发生共谋问题，即敌方可通过捕获少量节点来获取全部密钥空间，这对HSN安全构成威胁。本文对此问题提出了一种旨在降低共谋问题发生概率的优化方案，即对于由簇内感知节点所抽象成的无向连通图进行最小生成树求解，并根据对树的遍历所得节点顺序进行密钥的指派与分配，从而增大密钥重叠度，使得在簇内相邻节点间发生共谋的可能性得到降低。实验结果表明：与密钥随机分配方案和SHELL方案相比，所提方案可有效提高网络抵御共谋攻击的能力，并增强了安全性。

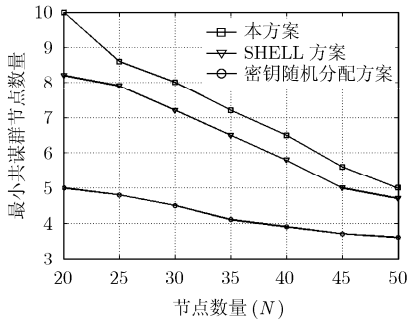


(a) k+m=8

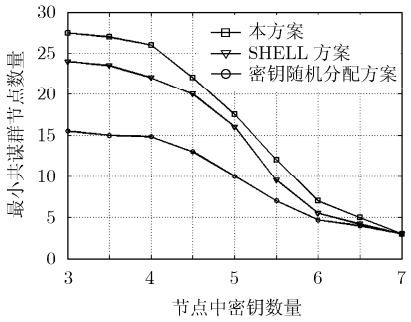


(b) k+m=12

图2 网络抗捕获能力



(a) k+m=8, N=20



(b) k+m=8, N=3

图3 最小共谋群中节点数量

参 考 文 献

[1] Samundiswary P, Priyadarshini P, and Dananjayan P. Performance evaluation of heterogeneous sensor networks[C]. Proceedings of ICFCC, Kuala Lumpur, Malaysia, April 3–5, 2009: 264–267.

[2] Liu Zhi-hong, Ma Jian-feng, Huang Qi-ping, *et al*.. A pairwise key establishment scheme for heterogeneous sensor networks[C]. Proceedings of the International Symposium on Mobile Ad hoc Networking and Computing, Hong Kong, 2008: 53–60.

[3] Younis M, Ghumman K, and Eltoweissy M. Key management in wireless Ad hoc networks: collusion analysis and prevention[C]. Proceedings of the 24th IEEE International Performance, Computing and Communications Conference, Phoenix, Arizona USA, April 7–9, 2005: 199–203.

[4] Eltoweissy M, Heydari H, Morales L, *et al*.. Combinatorial optimization of key management in group communications[J]. *Journal of Network and Systems Management*, 2004, 12(1): 33–50.

[5] Wang Huan-zhao, Luo Dong-wei, and Guo Yu-fei. TLKMS: a dynamic keys management scheme for large-scale wireless sensor networks[C]. Proceedings of ICCSA, Kuala Lumpur, Malaysia, August 26–29, 2007: 559–572.

[6] Kim Jong-Myoung, Cho Joon-Sic, Jung Sung-Min, *et al*.. An energy-efficient dynamic key management in wireless sensor networks[C]. Proceedings of the 9th ICACT, Phoenix Park, Korea, 2007: 2148–2153.

[7] 孔繁瑞, 李春文, 丁青青, 等. 一种基于EBS的无线传感器网络动态密钥管理方法[J]. 电子与信息学报, 2009, 31(5): 1045–1048.

Kong Fan-rui, Li Chun-wen, Ding Qing-qing, *et al*.. An EBS-based dynamic key management scheme for wireless sensor networks [J]. *Journal of Electronics & Information Technology*, 2009, 31(5): 1045–1048.

[8] Lo Chi-chun, Huang Chun-chieh, and Chen Shu-wen. An efficient and scalable EBS-based batch rekeying scheme for secure group communications[C]. Proceedings of IEEE MILCOM, Boston, USA, October 18–21, 2009: 1–7.

[9] Eltoweissy M, Moharrum M, and Mukkamala R. Dynamic key management in sensor networks[J]. *IEEE Communications Magazine*, 2006, 44(4): 122–130.

[10] Ma Chun-guang, Geng Gui-ning, and Wang Hui-qiang. Location-aware and secret-share based dynamic key management scheme for wireless sensor network[C]. Proceedings of NSWCTC, Wuhan, China, April 25–26, 2009: 770–773.

[11] 孔繁瑞, 李春文, 丁青青. 基于EBS的动态密钥管理方法共谋问题[J]. 软件学报, 2009, 20(9): 2531–2541.

Kong Fan-rui, Li Chun-wen, and Ding Qing-qing. Collusion problem of the EBS-based dynamic key management scheme

[J]. *Journal of Software*, 2009, 20(9): 2531–2541.

[12] 王巍, 赵文红, 李凤华. 无线传感器网络中基于EBS的高效安全的群组密钥管理方案[J]. 通信学报, 2009, 30(9): 76–82.
Wang Wei, Zhao Wen-hong, and Li Feng-hua. EBS-based efficient and secure group key management in wireless sensor networks[J]. *Journal on Communications*, 2009, 30(9): 76–82.

[13] 吴亮, 曹晓梅, 杨庚. 一种有效的无线传感器网络广播密钥管理方案[J]. 电子与信息学报, 2010, 32(6): 1480–1484.
Wu Liang, Cao Xiao-mei, and Yang Geng. An efficient broadcast key management policy in wireless sensor networks [J]. *Journal of Electronics & Information Technology*, 2010, 32(6): 1480–1484.

[14] Eschenauer L and Gligor D. A key management scheme for distributed sensor networks[C]. Proceedings of the 9th ACM Conference on Computer and Communication Security, Washington, USA, November 18–22, 2002: 41–47.

[15] Younis M, Ghumman K, and Eltoweissy M. Location-aware combinatorial key management scheme for clustered sensor networks[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2006, 17(8): 865–882.

马春光： 男，1974年生，教授，博士，博士生导师，研究领域为密码学、信息安全、传感网与物联网、网络编码.

戴膺赞： 男，1980年生，工程师，硕士，研究领域为信息安全、传感网与物联网.

王九如： 男，1983年生，博士生，研究方向为信息安全、传感网与物联网.

王慧强： 男，1960年生，教授，博士，博士生导师，研究领域为网络与信息安全、认知网络.