一种有效的无线传感器网络广播密钥管理方案

吴 亮 曹晓梅 杨 庚 李大伟
(南京邮电大学计算机学院 南京 210003)

摘 要：无线传感器网络具有自组织、自管理和能量有限等特性，使其安全性面临严峻的挑战。该文在分析现存组播密钥管理方案的基础上，提出了一种基于 BIP(Broadcast Incremental Protocol)和 EBS(Exclusion Basis Systems)算法的广播密钥管理方案 EBKMP。该方案对生成的广播树进行分组，根据相邻组间海明距离尽量小的原则分配密钥，增强安全性同时有效降低了组成员异动引起的密钥更新消耗。通过与几种经典密钥管理方案对比，证明 EBKMP 在通信、存储性能和抗合谋攻击能力等方面有显著改善。

关键词：无线传感器网络；广播；密钥管理；BIP；EBS
中图分类号：TP393; TP309.7 **文献标识码**： A **文章编号**：1009-5896(2010)06-1480-05
DOI: 10.3724/SP.J.1146.2009.00892

An Efficient Broadcast Key Management Policy in Wireless Sensor Networks

Wu Liang Cao Xiao-mei Yang Geng Li Da-wei
(*College of Computer*, *Nanjing University of Posts & Telecommunications*, *Nanjing* 210003, *China*)

Abstract: With the characteristics of self-organizing, self-management and limited energy of WSN, the security is a great challenge. In this paper, a novel Efficient Broadcast Key Management Policy named as EBKMP is proposed. It divides broadcast trees into groups, and the principle of minimizing the hamming distance between neighbor groups is adopted in keys distribution, which enhances security and reduces the overhead caused by the changes of group members. Compared with present key management policies, EBKMP can improve the efficiency in communication and storage, and resist collusion attack effectively.

Key words: Wireless Sensor Networks(WSN); Broadcasting; Key management; Broadcast Incremental Protocol (BIP); Exclusion Basis Systems(EBS)

1 引言

广播是无线传感器网络(Wireless Sensor Networks, WSN)数据传输的主要方式之一[1]，WSN 中的广播通信包括全局广播和局部组播。无线通信因为其开放式的特点使其容易受到数据窃听等攻击，同时为屏蔽不在广播组中节点和保证数据的完整性、可靠性，数据的保密性就显得尤为重要。受到节点性能的各种限制，WSN 主要采用对称加密方式。安全广播要求同一广播组内合法节点拥有一个或多个组内密钥，最常用的方法是节点通过广播密钥 S 解密广播包同时使用多个管理密钥更新 S，这种方法的研究难点是当节点动态加入或退出组时，如何高效地更新广播密钥 S 以达到向前(向后)保密性。寻找一种适合组播广播，并且针对成员动态加入和退出的、高效密钥管理协议和加密方法是 WSN 研究的重要内容[2−6]。

μTESLA[7] 方案是通过延迟泄漏计算 MAC 所用密钥来模拟公钥算法达到对广播信息进行认证的目的。但是，该方案需要基站和各节点间保持同步，同时需要节点消耗一定数量的内存来缓存所接收到的广播信息，这对于内存资源紧张的传感节点来说，是对内存空间的极大浪费。Waller 等[8]和 Wong 等[9]分别提出了基于逻辑树层次的组播密钥管理机制 LKH(Logical Key Hierarchy)。在 LKH 中，组管理员(GC)维护一棵逻辑密钥树，中间节点代表管理密钥(KEK)，叶节点代表组成员，每个成员节点保存从自身到根节点(GC)路径上的所有密钥。以一棵二叉平衡树为例，节点需要保存 $\log_2 N+1$ 个密钥，N 表示组成员数。当一个新节点加入时，需要发送 $2\log_2 N-1$ 个更新消息。Canetti 等[10]提出了一种采用伪随机生成树的单向函数协议 OFT(One-way Function Protocol)，在 OFT 中，中间节点密钥从兄弟节点密钥生成，更新所需消息数从 $2\log_2 N$ 降低

2009-06-19 收到，2009-09-28 改回
国家自然科学基金(60873231)，江苏省高校自然科学基金(08KJB520006)和江苏省“六大人才高峰”基金(06-E-044)资助课题
通信作者：曹晓梅 caoxm@njupt.edu.cn

到$\log_2 N$。Chang 等[11]将布尔函数化简技术应用到二叉树中，降低了更新通信量和 GC 存储量，同时文章研究了多用户撤销，但是这种方案复杂性太低对合谋攻击的抵抗性较差，很容易将整个网络暴露给攻击者。Perrig 等[12]设计了一种有效的大规模密钥协议 ELK(Efficient Large-group Key)。ELK 协议采用伪随机函数生成和维护层次式树形密钥结构，和 OFT 相似，父节点根据两个子节点的密钥生成自身管理密钥。当节点加入时 ELK 不需要发送组播消息，它采用周期性的本地更新。当节点退出时，其更新消息数为$\log_2 N$。Son 等[13]对 LKH 进行了改进并用于 WSN，提出了一种基于节点位置的拓扑树层次 TKH(Topological Key Hierarchy)。TKH 将地理上相邻的节点置于同一子树上，在发送更新消息的时候可以降低广播消息量。这种方法将树形结构固定在 4 层，KEK(Key Encryption Key)被分为 TK(Tree Key)和 SK(Sibling Key)，分别表示子树和兄弟拓扑结构。但是，节点异动时的更新消息数与具体的拓扑结构有关，当节点规模较大时消耗会大大增加，同时它也存在不能抵抗合谋攻击的问题。

上述方案都是基于树形结构[8−13]，恶意节点只要与任意一条分支中的节点合谋就可以获取发送的更新消息包，不同分支中的节点合谋，即可掌握整个网络中的密钥，而且这种结构动态性太差，无法满足大规模网络的要求。高效的 WSN 安全机制必然要求在安全性和资源使用间达到平衡，本文主要工作包括：(1)通过构建广播树优化更新数据包传输路径，同时使用 EBS[14](Exclusion Basis Systems)使节点保存密钥和更新数据包数相平衡；(2)进一步通过对 EBS 的改进来实现对合谋攻击的抵抗机制；(3)能满足广播组成员高频率的加入和退出，同时使节点存储的密钥不会随网络规模扩大而动态增加；(4)对提出方案通信、存储要求及对合谋攻击的抵抗性进行了分析，结果表明这种方案完全满足需要。

2　预备知识

EBKMP 根据抽象出的 BIP(Broadcast Incremental Protocol)结构，以子树上兄弟节点为分组，将子树分为数量近似相等的子组，然后采用基于海明距离的 EBS 系统配置节点管理密钥。

2.1 广播树形结构

文献[15]提出了构建高效组播广播树的算法 BIP，其核心思想充分发挥无线广播优势。BIP 根据最小增加能耗(incremental cost)动态构造广播树(类似于 Prim 算法)。假设节点 i 已经在树中(它要么是中间节点，要么是叶子节点)，节点 j 还未加入，那么根据 $P_{ij}^{'} = P_{ij} - P(i)$ (其中 $P_{ij} = r_{ij}^{\alpha}$ 代表连接 i 和 j 需要消耗的能量，$P(i)$ 代表节点 i 当前传输消耗的能量(如果 i 为叶子则=0))显示了将 j 连至 i 所增加的能耗。产生最小 $P_{ij}^{'}$ 的节点对$\{i,j\}$被选出，它们之间的连接构成广播树的一条分支。这就是 BIP 构建广播树的过程。

2.2 基于排除法的密钥分发系统(EBS)

假设一个广播组中包含 N 个节点，组成集合 $1,\cdots,N$，EBS 试图寻找节点集合 A 中的 k 个子集 $(A_1,\cdots,A_k)$，使得当每个节点 t 退出组时，剩余节点组成的集合是 A 中 m 个集合的子集，即$[1,\cdots,N]-[t]=\sum_{i=1}^{m}A_i$，如果每个子集 A_i 使用一个密钥 K_i。EBS 可以表示为(N,k,m)形式，k 为每个节点需要保存的密钥数量，m 为一个节点退出组时，需要发送的用于更新组密钥的消息数[7]。对于 EBS(N,k,m)，从长度为 $k+m$ 的位串中选择 m 位置为 0，其他位置为 1，枚举所有可能的位串集合即可，例如对于 EBS (8,3,2)，构造结果如表 1。表中每一列表示一次枚举过程，共 $C_{k+m}^{m}=10$ 列。

因为 N=8，M9 和 M10 暂时不用，所以在表 1 中子集 A_1=[5,6,7,8]，A_2=[2,3,4,8]，A_3=[1,3,4,6,7]，A_4=[1,2,4,5,7]，A_5=[1,2,3,5,6,8]。容易验证：$[1,\cdots,8]-[1]=A_1\cup A_2$，$[1,\cdots,8]-[2]=A_1\cup A_3$，$[1,\cdots,8]-[3]=A_1\cup A_4$，当任何一个节点退出网络时，只需要向相应两个集合中的节点发送密钥更新消息就可以完成组密钥的更新，而且仅需产生 5 个管理密钥。

表 1 EBS(8,3,2)规划枚举结果

	$M1$	$M2$	$M3$	$M4$	$M5$	$M6$	$M7$	$M8$	$M9$	$M10$
A_1	0	0	0	0	1	1	1	1	1	1
A_2	0	1	1	1	0	0	0	1	1	1
A_3	1	0	1	1	0	1	1	0	0	1
A_4	1	1	0	1	1	0	1	0	1	0
A_5	1	1	1	0	1	1	0	1	0	0

3 EBKMP—有效密钥管理方案

EBKMP的主要设计目的就是，优化节点存储需求和密钥更新消耗，同时通过增加攻击者得到网络中所有管理密钥所需入侵节点的数量，减少网络被捕获的可能性。采用使相邻节点掌握的密钥组合间的海明距离应尽量小的密钥分配策略，令相互连接的几个组掌握尽量少的管理密钥，即寻找最大的b，使得一个组内的所有传感器节点只需掌握$k+m-b$个管理密钥，而不需要掌握所有的$k+m$个管理密钥。

3.1 假设前提

每个节点需要保存EBS(N,k,m)中的k个管理密钥AK_i，广播密钥S，与Sink间的对称密钥PK_i，以及用于本地更新密钥的散列函数F，节点通信能力在一定范围内可调(保证BIP过程)。

3.2 初始化过程

网络结构初始化完毕后，Sink节点从相邻子树中随机选择KDC(Key Distribute Center)(可根据实际网络状况决定个数)，建立KDC与当前子树节点间的对称密钥TK_i。如图1所示，图1(a)、1(b)分别表示从节点分布中抽象出的BIP树形结构和广播组结构。子树a分为{2,3,4}，{5,6}，{1,7,8}3个组，为EBS管理密钥分配做准备(在产生分组时，可根据分组数，采用具有邻接关系子集合相并的方式)，广播路径为1→{2,3,4}，3→{5,6}，4→{7,8}。

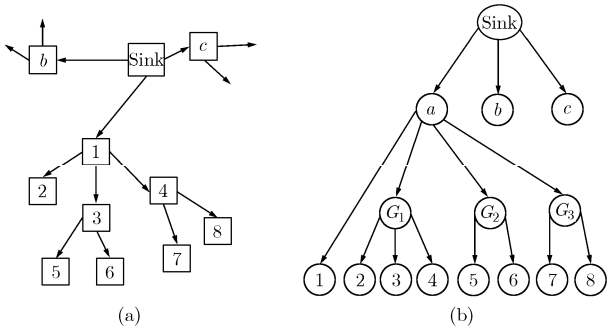

图1 EBKMP网络模型

3.3 生成管理密钥

KDC根据每个子树的节点数N和分组情况构造($k+m$)个管理密钥，然后按照相邻组集合掌握的管理密钥数量尽量少的思想，给每个节点发送数据包$\{AK_i\}_{TK_i}$。具体方法如下：

首先，寻找满足式(1)的b_1，其中$\binom{k+m-b_1}{k}$为组合数、G为组内最多节点数量。

$$\max_{b_1}\left(\binom{k+m-b_1}{k}\geq G\right) \tag{1}$$

进一步，令相互连接的i个组掌握尽量少的管理密钥，即找到满足式(2)的b_i。

$$\max_{\substack{b_i\\ 1\leq i\leq\lfloor N/G\rfloor}}\left(\binom{k+m-b_i}{k}\geq i\times G\right) \tag{2}$$

由式(2)可以得到每一对(k, m)与b_i的对应值，分为如下3个步骤：

步骤1 令k=m=1；

步骤2 计算组合数$\binom{k+m}{k}$

若$\binom{k+m}{k}<N$，则令m=m+1，转步骤2。否则记录二元组(k, m)，令k=k+1；

若k<N–1，则令m=1，重复骤2。否则转步骤3；

步骤3 对每一对二元组(k, m)，计算满足式(2)的b_i。

从结果中寻找令$k+m$最小的二元组(k, m)，若有多个满足$k+m$最小的二元组(k, m)，在其中选择k值最小的二元组作为管理密钥数量和密钥更新消息数量的取值。此后可以用此二元组对应的b_i值指定i个组掌握的管理密钥的数量。

3.4 密钥更新

为减少更新时的通信量，节点在本地根据新广播密钥S'计算生成新的管理密钥$AK_i^{'}=F(S', AK_i)$。

(1)节点加入 由于BIP和EBS算法具有递增特性，当有节点加入和退出时不会对当前网络造成影响，只需调整节点所处分组即可。

(a)当有新节点加入时，若$N+1\leq\binom{k+m}{k}$，不需要生成新管理密钥，按照3.1节叙述，在节点中放置PK_i，k个管理密钥(满足海明距离)，哈希函数F，广播密钥S'。然后Sink节点向全网广播数据包$\{S'\}_S$，原网络中节点在本地生成新管理密钥。

(b)若$N+1>\binom{k+m}{k}$，则由KDC重新选择EBS(N,k,m)，然后给各分组中节点分配新的管理密钥，最后Sink节点向全网广播数据包$\{S'\}_S$。

为增加网络动态性，假设在配置EBS系统之初适当的增加k和m值，这样当节点加入时，满足$N\leq\binom{k+m}{k}$，在一定程度上可以减少生成新管理密钥频率。

(2)节点退出 当有节点退出时，按照3.2节中描述的BIP广播路径，依据EBS算法，发送包含新

广播密钥 S' 的 m 个数据包。节点在接收到广播消息后本地更新退出节点掌握的管理密钥。因为网络中管理密钥越多，分布密度越小，这样抗合谋攻击效果越好，所以，即使 N 远小于 $\binom{k+m}{k}$ 时，也不必更新 k 和 m 的值。

如图 1，以子树 a(Tree1)为例，节点{2,3,4}，{5,6}，{1,7,8}分别构成了 3 个子集，根据 2.2 节分析有 EBS(8,3,2)，每个节点掌握 3 个管理密钥，节点离开时需要发送 2 个广播包。当节点 2 退出时，根据 Ak_1=[5,6,7,8]，Ak_2=[2,3,4,8]，Ak_3=[1,3,4,6,7]，Ak_4=[1,2,4,5,7]，Ak_5=[1,2,3,5,6,8]，$[1,\cdots,8]-[2]=Ak_1\cup Ak_3$。只需广播 $\{S'\}Ak_1$ 和 $\{S'\}Ak_2$ 即可完成对 S' 和 Ak_3，Ak_4，Ak_5 的更新，3 次转发广播路径为 1→{3,4}，3→{5,6}，4→{7,8}。显然，本方案与 LKH 相比在各方面性能上都有很大的优势。

4　有效性分析

为了验证方案的有效性，本文对EBKMP的安全性和系统开销两方面进行了分析和比较。安全性方面主要评估EBKMP抵抗合谋攻击的效率，通过合谋链的长度来评估网络被捕获的可能性。在对提出方案的系统开销进行分析时，主要考虑节点密钥存储量和加入事件、离开事件中的消耗。

4.1 安全性分析

按照平面结构，将N个节点的网络划分为S叉LKH树，树的高度，即管理节点路径长度为 $h=\log_S N$。最少需要每个分支中的一个节点即可获得整个网络管理密钥，概率为 $\alpha=S^{N/S}/C_N^{N/S}$。可见在LKH中分支越多，节点存储的密钥数越少，网络风险性越高。以二叉树，8个节点为例，$h=\log_2 8=3$，$\alpha=2^4/C_8^4=8/35$。

根据 3.3 节分析：假设将网络分为 $g=k+1$ 个组，组内成员数不超过 $G=C_{k+m-b_i}^k$，任意(g–1)个组需要的管理密钥仅次于所有密钥，每个单独的组掌握的管理密钥不超过 $C_{k+m-b_{g-1}}^k$。根据 EBS 密钥组合特点，仅需从第 1 组中选出两个密钥组合，其余每组选 1 个，即可覆盖此组掌握的所有密钥，$P=C_G^m\times\prod_{2\le i\le g}C_{G_i}^1$。掌握整个网络管理密钥的概率为 $\alpha=P/C_{KN}^{k+m}$ ($KN=C_{k+m}^k$ 表示总密钥个数)。以表 1 为例，共 $KN=10$ 个管理密钥，分为 4 组：{ $M1$，$M2$，$M3$，$M4$}，{ $M5$，$M6$，$M7$}，{ $M8$，$M9$}，{ $M10$}。$\alpha=(6\times3\times2\times1)/C_{10}^5=1/7$。

实验的结果是 10 次运行的平均值，在每一次实验中，使用不同的随机种子来产生随机网络拓扑，分别对具有 10，25，50，75，120，200 个传感器节点的 WSN 进行实验。

图 2 给出了不同网络规模下分别使用 LKH 和 EBKMP 捕获网络所需合谋链的长度比较图。从曲线可以看出，在节点数量增大的过程中 LKH 合谋链长度持续增长，但增幅较小。EBKMP 呈锯齿状上升，这是因为当节点数量增加到一定阶段时，密钥组合的增加比例小于节点增加比例，密钥组合分布密度增加，从而导致合谋链长度下降。如图所示，在大部分区域中 EBKMP 合谋链长度远大于 LKH，说明本文提出的方案对安全性的改进与前述分析一致。

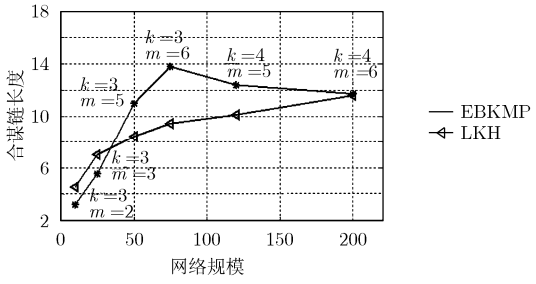

图 2 使用 LKH 和本文方案合谋链的长度比较图

4.2 密钥更新代价

假设 WSN 使用了 EBS(N, k, m)系统，则每个传感节点需要存储 k 个管理密钥、1 个对称私钥和 1 个广播密钥，共 k+2 个密钥。控制节点需要存储所有的 k+m 个管理密钥、N 个传感节点的对称私钥和广播密钥。在加入事件中，控制节点发送 1 条密钥更新广播。在离开事件中，广播的密钥更新消息为 m 条。

令 T 表示一个高为 $h=\log_S N$ 的 S 叉 LKH 密钥管理树，每个叶节点需要保存从自己到根节点路径上的所有 $\log_S N+1$ (N: 组成员节点数)个管理密钥，用于组密钥的更新，但组控制节点需要保存 $2N-1$ 个密钥。

表 2 给出了本文方案与各种方案的性能比较，(n_1+n_2) 代表 ELK 密钥长度。因为 EBKMP 采用基于组合数的 EBS 密钥系统，当网络规模增加时 k，m 值增加幅度较小并且可以根据实际需求调整。相对而言，采用基于树型结构的另外几种方案，通信和存储消耗呈线性增长。

5　总结

无线传感器网络正得到快速发展和广泛应用，

表 2 本文提出方案与 LKH 等的性能比较

	密钥更新消息数量			存储密钥数量	
	加入事件		离开事件	传感节点	控制节点
	组播	点对点			
EBKMP	1	1	m	$k+2$	$k+m+N+1$
LKH	$2h-1$	$h+1$	$2h$	$h+1$	$2N-1$
OFT	$h+1$	$h+1$	$h+1$	$h+1$	$2N-1$
ELK	0	$h+1$	$h(n_1+n_2)$	$h+1$	$2N-1$

但由于传感器节点大多被部署在无人照看或者敌方区域，很容易被入侵且这些节点的能量、存储量和计算能力受到严格的限制，因此，保证无线传感器网络广播通信的安全性是一个挑战。本文设计了一种广播密钥管理方案来解决无线传感器网络中的性能要求和合谋攻击问题，主要手段就是减少通信量和管理密钥分布密度，在存储、计算和通信间达到最优平衡，最终达到延长网络生存期的目的。在性能分析阶段，通过实验对合谋攻击的可能性和入侵节点数量对网络抵抗合谋攻击能力的影响进行分析。实验结果表明提出方案是一种有效而且具有一定安全性的广播密钥管理方案。

参 考 文 献

[1] 邱慧敏, 杨义先, 钮心忻. 无线传感器网络中广播通信的安全协议设计[J]. 北京邮电大学学报, 2006, 29(5): 53–57.
Qiu H M, Yang Y X, and Niu X X. Security protocol design about broadcast in wireless sensor network[J]. *Journal of Beiing University of Posts and Telecommunications*, 2006 29(5): 53–57.

[2] Boukerche A, Ren Y L, and Samarah S. A secure key management scheme for wireless and mobile Ad hoc networks using frequency-based approach: proof and correctness. IEEE GLOBECOM 2008 NEW ORLEANS, LA, USA, Dec., 2008: 1–5.

[3] Lu K J, Qian Y, Guizani M, and Chen H H. A framework for a distributed key management scheme in heterogeneous wireless sensor networks. *IEEE Transactions on Wireless Communications*, 2008, 7(2): 639–647.

[4] Aparna R and Amberker B B. Authenticated secure group communication using broadcast encryption key computation. ITNG 2008. Fifth International Conference on Las Vegas, Nevada, USA, 2008: 348–353.

[5] Yan J Z, Ma J F, and Liu H Y. Key hierarchies for hierarchical access control in secure group communications. *Computer Networks*: *The International Journal of Computer and Telecommunications Networking*, 2009, 53(3): 353–364.

[6] Boneh D and Hamburg M. Generalized identity based and broadcast encryption schemes. Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology 2008, Melbourne, Australia, December 2008: 455–470.

[7] 沈玉龙, 裴庆祺, 马建峰. MMμTESLA: 多基站传感器网络广播认证协议[J]. 计算机学报, 2007, 30(4): 539–546.
Shen Y L, Pei Q Q, and Ma J F. MMμTESLA: Broadcast authentication protocol for Multiple-Base-Station sensor networks[J]. *Chinese Journal of Computer*, 2007, 30(4): 539–546.

[8] Wallner D, Harder E, and Agee R. Keymanagement for multicast: Issues and Architectures. RFC 2627, June 1999.

[9] Wong C K and Lam S. Secure group communications using key graphs. Proc. ACM SIGCOMM '98 Conference in Vancouver, 1998: 68–79.

[10] Canetti R, Garay J, Itkis G, Micciancio K, and Naor M. Multicast security: a taxonomy and some efficient constructions. Proc. INFOCOM'99, New York, NY, 1999: 708–716.

[11] Chang I, Engel R, Pendarakis D, and Saha D. Key management for secure internet multicast using boolean function minimization techniques. Proc. INFOCOM'99, New York, NY, 1999: 689–698.

[12] Perrig A, Song D, and Tygar J D. ELK. A new protocol for efficient large group key distribution. IEEE Security and Privacy 2001, Oakland, California, USA, 2001: 247–262.

[13] Son J H, Lee J S, and Seo S W. Energy efficient group key management scheme for wireless sensor networks. COMSWARE 2007. 2nd International Conference Bangalore, India, Jan. 7–12, 2007: 1–9.

[14] Mohamed E, Ashraf W, and Stephan O, *et al*.. Group key management scheme for large-scale sensor networks. *Ad hoc Networks*, 2005, 3(5): 668–688.

[15] Jeffery E W and Gam D N. Energy-efficient broadcast and multicast trees in wireless networks. *Mobile Networks and Applications*, 2002, 7(6): 481–492

吴 亮： 男，1985 年生，硕士生，研究方向为计算机通信与网络、信息安全.

曹晓梅： 女，1974 年生，博士，讲师，研究方向为无线网络安全.

杨 庚： 男，1961 年生，教授，博士生导师，研究方向为计算机通信与网络、网络安全、分布与并行计算等.

李大伟： 男，1981 年生，博士生，研究方向为计算机通信网与安全、密钥管理.