一种基于 EBS 的无线传感器网络动态密钥管理方法

孔繁瑞[①] 李春文[①③] 丁青青[②] 崔光照[③] 崔昺祎[④]
[①](清华大学自动化系 北京 100084)
[②](清华大学电机工程与应用电子技术系电力系统及发电设备控制和仿真国家重点实验室 北京 100084)
[③](郑州轻工业学院河南省信息化电器重点实验室 郑州 450002)
[④](南京大学物理系 南京 210093)

摘 要：设计安全合理的密钥管理方法是解决无线传感器网络安全性问题的核心内容。基于Exclusion Basis System (EBS)的动态密钥管理方法由于安全性高，动态性能好，节约存储资源，受到了广泛关注。但同时存在共谋问题，即对于被捕获节点通过共享各自信息实施的联合攻击抵抗性较差。针对这一问题，该文利用一种特殊形式的三元多项式(同化三元多项式)密钥取代EBS系统中的普通密钥，并在分簇式的网络拓扑结构基础上，设计了一种基于EBS的无线传感器网络动态密钥管理方法。仿真与分析结果表明，相比于采用普通密钥或是二元多项式密钥的方法，该文方法不仅可以有效地解决共谋问题，提高网络对被捕获节点的抵抗性，而且显著减低了更新密钥过程中的能量消耗。

关键词：无线传感器网络；安全性；EBS；动态密钥管理方法；多项式密钥
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2009)05-1045-04

An EBS-Based Dynamic Key Management Scheme for Wireless Sensor Networks

Kong Fan-rui[①] Li Chun-wen[①③] Ding Qing-qing[②] Cui Guang-zhao[③] Cui Bing-yi[④]
[①](*Department of Automation*, *Tsinghua University*, *Beijing* 100084, *China*)
[②](*State Key Lab of Power Systems*, *Department of Electrical Engineering*, *Tsinghua University*, *Beijing* 100084, *China*)
[③](*Key Laboratory of Informationed Electric Apparatus in Henan State*, *Zhengzhou University of Light Industry*, *Zhengzhou* 450002, *China*)
[④](*Department of Physics*, *Nanjing University*, *Nanjing* 210093, *China*)

Abstract: Security of wireless sensor networks has attracted much attention in recent years and key management is a critical issue of it. EBS-based dynamic key management scheme is a new approach for wireless sensor networks. The major advantages of EBS-based dynamic key management scheme are enhanced network survivability, high dynamic performance and better support for network expansion. But it suffers from the collusion problem, which means it is prone to the coordinated attack of the compromised nodes. In this paper, a special kind of polynomial, the common trivariate polynomial, is presented, which can guarantee that all the nodes having the same polynomial can get the same key. The common trivariate polynomial keys are used in stead of the normal keys in EBS system and a new dynamic key management scheme is designed for clustered wireless sensor networks. Analytical and simulation results show that compared with the former works, the proposed scheme can greatly improve the network resilience to the attack of the compromised nodes and decrease the energy consumption in the process of updating the administration and session keys.

Key words: Wireless sensor networks; Security; Exclusion Basis System (EBS); Dynamic key management; Polynomial keys

1 引言

无线传感器网络是一种由大量传感器节点构成的，自组织的新型无线通信网络[1−3]。为确保网络中数据的完整性、准确性、私密性，近年来网络安全已逐步得到网络架构人员和研究人员的重视。2006 年 Eltoweissy 在传感器网络的分簇结构和 EBS[4]的基础上提出了动态密钥管理的概念[5]，与静态密钥管理[6]相比，其主要优点在于：(1)可以动态取消被捕获节点所拥有的全部密钥，使网络不受被捕获节点的独立攻击。(2)动态性能好，适合于使用寿命长，拓扑结构变化频繁

2008-04-17 收到，2008-07-24 改回
国家自然科学基金(69774011)资助课题

的网络。(3)可扩展性强，适合于大范围，冗余布置的网络。但是基于 EBS 的动态密钥管理方法中存在共谋问题[7]，即对被捕获节点通过共享各自信息实施的联合攻击抵抗性较差，是影响其安全性的主要因素。针对这一问题，本文提出了同化三元多项式密钥，可以使所有拥有同一多项式的节点得到相同的密钥，从而既提高了网络对于被捕获节点的抵抗性能，又降低了通信开销。

2 EBS 和基于 EBS 的无线传感器网络动态密钥管理方法

EBS 是由 Eltoweissy 等于 2004 年提出的一种基于组合原理的组通信密钥管理方法[4]。一个 EBS 被定义为以用户子集为元素构成的一个特殊集合，在 EBS(n,k,m)中， n 表示节点数目， k 表示分配给每个节点的密钥个数， $k+m$ 表示密钥总数。可以证明[4,8]：

(1)当 $C_{k+m}^{k} \geq n$ 时， C_{k+m}^{k} 中的任意 n 个组合方式均可构成 EBS(n,k,m)，进而形成一个密钥分配方案。

(2)可以通过广播最多 m 个数据包实现动态取消并更新任意一个节点所拥有的全部密钥，从而驱逐该节点。

例如当 $n=8,k=3,m=2$ 时，密钥分配方案如表 1 中的 EBS 矩阵 $\boldsymbol{M}$ 所示，其中 $M(i,j)$ 为 1 表示将密钥 K_i 分配给节点 N_j 。

表 1 EBS 矩阵

	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8
K_1	0	0	0	0	1	1	1	1
K_2	0	1	1	1	0	0	0	1
K_3	1	0	1	1	0	1	1	0
K_4	1	1	0	1	1	0	1	0
K_5	1	1	1	0	1	1	0	1

若要取消并更新节点 N_1 所具有的 3 个密钥 K_3,K_4,K_5 ，则只需广播以下 2 个数据包：(1) $E_{K_1}(S',E_{K_3}(K_3'),E_{K_4}(K_4'),E_{K_5}(K_5'))$ ，(2) $E_{K_2}(S',E_{K_3}(K_3'),E_{K_4}(K_4'),E_{K_5}(K_5'))$ 。其中 $E_{K_i}(x)$ 表示以密钥 K_i 对数据 x 进行加密， K_i' 表示密钥 K_i 的更新， S' 为新的会话密钥。

3 同化三元多项式密钥

定义 1 (同化三元多项式) $f(x_1,x_2,x_3)$ 为 $t+1$ 阶同化三元多项式，若 $f(x_1,x_2,x_3)=C+\sum_{i_1=1}^{t+1}\sum_{i_2=1}^{t+1}\sum_{i_3=1}^{t+1}a_{i_1i_2i_3}x_1^{i_1}x_2^{i_2}(x_3-x_c)^{i_3}$ ，其中 x_c 为一常数， $C,a_{i_1i_2i_3}$ 属于有限域 F_q ， q 为一可以容纳通信密钥的足够大的质数。显然同化三元多项式具有一条重要的性质： $\forall x_1,x_2 \quad f(x_1,x_2,x_c)=C$ ，意味着只要变量 x_3 取值为 x_c 时，多项式 $f(x_1,x_2,x_3)$ 将得到一个常数。

在布置网络之前，可以将所有节点的序号设定为一个唯一的二元组，因此任意被分配了多项式 f 的节点 N_i 都可以得到同一个共享密钥 $\text{key}=f(\text{ID}_{i1},\text{ID}_{i2},x_c)=C$ ，其中 $(\text{ID}_{i1},\text{ID}_{i2})$ 为 N_i 的序号。可以证明基于 $t+1$ 阶同化三元多项式的密钥是 t^2 -安全的，即当捕获不超过 t^2 个被分配了某一同化三元多项式的节点时，即使它们共享信息，该多项式仍是不可破解的，利用该多项式得到的共享密钥仍是安全的。

4 基于同化三元多项式密钥的无线传感器网络动态密钥管理方法

本文提出的是基于 EBS 的动态密钥管理方法，利用同化三元多项式密钥取代了普通密钥。网络采用分簇式结构，每个簇内形成一个 EBS。本文主要研究的是簇内密钥的管理方法，包括多项式预分配，初始化会话密钥，密钥更新，驱逐被捕获的节点 4 个主要组成部分，而分簇的方式可以采用已有的结果，如文献[5,7]中的方法。

4.1 多项式预分配

设网络中采用的 EBS 为 EBS(n,k,m)。首先簇头节点随机生成 $k+m$ 个 $t+1$ 阶同化三元多项式 $f_i(x_1,x_2,x_3)=C_i+\sum_{i_1=1}^{t+1}\sum_{i_2=1}^{t+1}\sum_{i_3=1}^{t+1}a_{ii_1i_2i_3}x_1^{i_1}x_2^{i_2}(x_3-x_{ic})^{i_3}$ ， i=1,2,⋯,$k+m$ ，其中 x_{ic} 互不相同。对于任意节点 N_a ，簇头节点根据 EBS 矩阵分配给它 k 个多项式 $f_{a_j}(x_1,x_2,x_3)$ ， $j=1,2,\cdots,k$ ， $a_j\in\{1,2,\cdots,k+m\}$ ，最后将 $f_{a_j}(x_1,x_2,x_3)$ 的一部分 $f_{a_j}(\text{ID}_{a1},\text{ID}_{a2},x_2)$ 存储在节点 N_a 中，其中 $(\text{ID}_{a1},\text{ID}_{a2})$ 为 N_a 的节点序号数组。实际上，每个节点存储了 k 个一元 $t+1$ 阶多项式，本文定义其为 $f_{a_j,\text{ID}_{a1},\text{ID}_{a2}}(x_3)$ 。显然网络中被分配了某一同化三元多项式 f_i 的所有节点可以形成一个相同的共享密钥 $\text{key}_i=f_{i,\text{ID}_1,\text{ID}_2}(x_c)=C_i$ ，其中 $(\text{ID}_1,\text{ID}_2)$ 为节点的序号。

4.2 初始化会话密钥

网络布置完毕后，需要初始化会话密钥。可以通过簇头节点广播 $k+m$ 个数据包达到初始化会话密钥的目的。它们分别为 $x_{ic}\|E_{C_i}(S_0)$ ， $i=1,\cdots,k+m$ 。节点收到这些数据包后，将 x_{ic} 作为变量值代入存储在其上的一元多项式中即可得到 C_i ，最后利用 C_i 解密数据包的 $E_{C_i}(S_0)$ 部分得到会话密钥 S_0 。

4.3 更新密钥

与初始化会话密钥类似，更新密钥同样要广播 $k+m$ 个数据包。它们分别为 $x_{ic}\|E_{C_i}(E_s(S'),f_i')$ ， $i=1,\cdots,k+m$ ，其中 S 为旧的会话密钥， S',f_i' 分别为新的会话密钥和同化三元多项式。节点将自己的序号数组作为变量代入 f_i' 中得到新的一元多项式连同 S' 存储起来，完成更新密钥的过程。

4.4 驱逐被捕获的节点

假设网络中节点 N_a 被捕获或疑似被捕获，可以通过簇头节点广播最多 m 个数据包驱逐 N_a ，即更新被分配给 N_a 的全部 k 个同化三元多项式 f_{a_j} ， $j=1,\cdots,k$ ， $a_j\in\{1,2,\cdots,$

$k+m\}$。这 m 个数据包为：$x_{b_l c}||E_{C_{b_l}}[x_{a_1 c}||E_{C_{a_1}}(f'_{a_1}),\cdots,x_{a_k c}||E_{C_{a_k}}(f'_{a_k})]$，其中 $l=1,2,\cdots,m$，$\{b_1,b_2,\cdots,b_m\}=\{1,2,\cdots,k+m\}-\{a_1,a_2,\cdots,a_k\}$，$f'_{a_j}$ 为新的同化三元多项式。若先后有 y 个节点被捕获，可以逐一地按照上面的方法驱逐它们。当 y 个节点被同时捕获，但没有形成联合攻击，即没有共享他们的信息时，可以证明通过广播最多 m^y 个数据包同时驱逐 y 个节点[9]。

5　性能分析与比较

下面从网络对被捕获节点的抵抗性，更新密钥和驱逐节点过程中的能耗和密钥所占存储空间三方面对本文提出的方法与文献[4,5]两种方法进行了比较，它们均为基于 EBS 的动态密钥管理方法，其中文献[4]中采用的是普通密钥，而文献[5]中采用的是基于一般二元多项式的密钥。最后还针对 3 种方法进行了计算复杂性的分析。

5.1 对捕获节点的抵抗性

设网络中全部节点数为 N，被分配了多项式 f_i 的节点个数为 N_i，被捕获的节点数为 N_c（$N_c>t^2$），多项式 f_i 被破解的概率为 Ω。捕获 N_c 个节点，其中有 p 个节点被分配了 f_i 的概率为 $\varphi(p)$，则

$$N_c>N-N_i\text{ 时，}\varphi(p)=\begin{cases}0, & p<N_c-(N-N_i)\\ \dfrac{C_{N_i}^{p}C_{N-N_i}^{N_c-p}}{C_N^{N_c}}, & p\geq N_c-(N-N_i)\end{cases};$$

$$N_c\leq N-N_i\text{ 时，}\varphi(p)=\frac{C_{N_i}^{p}C_{N-N_i}^{N_c-p}}{C_N^{N_c}}。$$

由于 $t+1$ 阶同化三元多项式密钥是 t^2-安全的，所以 $\Omega=1-\sum_{p=0}^{t^2}\varphi(p)$。

由于 f_i 是任意选取的多项式，所以通过捕获 N_c 个节点可以破解的密钥占全部密钥的比例也为 Ω [10]。图 1 为在 $k=3,\ m=5,N=56$ 的条件下 3 种方法中，被破解密钥比例与被捕获节点数的关系曲线。从图中可以发现，本文方法中被破解密钥比例远好于文献[4,5]中的结果。

图 2 为采用本文方法，破解密钥比例与被捕获节点数的关系曲线随 t 的变化情况。由图 2 可知当 $t\geq 5$ 时，被破解的密钥比例近似为 0，但付出的代价是存储空间占有量变大。

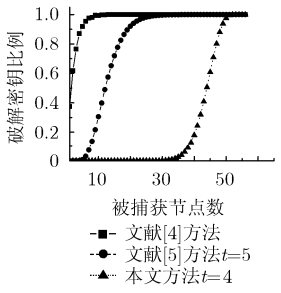

图 1 破解密钥比例与被捕获节点数的关系曲线

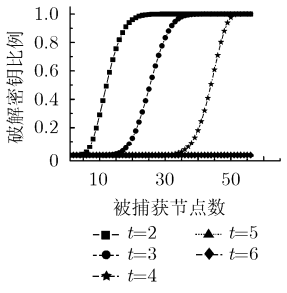

图 2 不同 t 的条件下破解密钥比例与被捕获节点数的关系曲线

5.2 密钥存储空间

同为 EBS(n,k,m)，由于文献[4]是基于普通密钥的，所以需要存储的密钥个数为 k，而本文和文献[5]是基于多项式的，所以它们需要存储的密钥个数分别为 $k(t+2)$ 和 $k(t+1)$ 个。图 3 为本文与文献[4–6]的节点需存储密钥数目比较情况，其中文献[6]是在保证连通度为 0.999，且破解全部密钥所需节点个数和本文方法相同的条件下进行比较的。

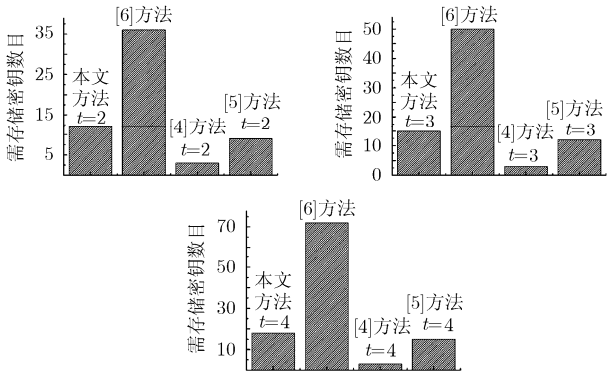

图 3 文献[4–6]与本文方法（$n=56,k=3,m=5$）密钥存储空间比较

5.3 更新密钥和驱逐节点过程中的能耗

本文利用 Ns2 对 3 种方法的更新和驱逐节点过程进行了仿真。在一个 50m×50m 的区域内，随机布置 56 个节点形成一个簇，节点通信半径为 20m。设更新密钥的频率为 10 次/min，网络运行时间为 10min。图 4 为 3 种方法更新密钥过程中节点的平均能耗曲线。由于文献[4]中采用的是普通密钥，所以能耗与 t 无关，本文方法能耗明显低于文献[5]，这是因为本文方法中的密钥是在所有被分配了同一个多项式的节点之间共享的，所以只需要广播 $k+m$ 个包即可。类似地，在驱逐节点的过程中，本文方法的能耗与文献[4]接近，明显优于文献[5]。图 5 为 3 种方法驱逐节点过程中节点的平均能耗曲线。仿真条件为每 1min 随机驱逐一个节点。

5.4 计算复杂度

文献[4]采用的是普通密钥，因此不涉及计算密钥的计算复杂度问题，而本文与文献[5]采用的是基于多项式的密钥，其密钥计算复杂度为相应的多项式求值的复杂度。多项式求

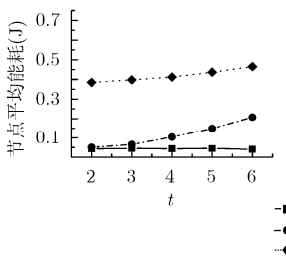

图 4 3 种方法更新密钥过程中节点的平均能耗

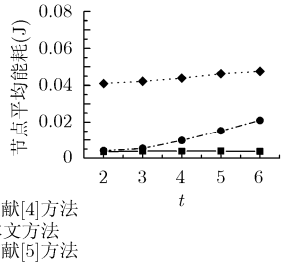

图 5 3 种方法驱逐节点过程中节点的平均能耗

值的方法很多，其适用性和复杂度也各不相同，本文利用最简单的直接求值的方法来对本文和文献[5]这两种密钥方案进行计算复杂度分析。

直接计算 $a_i x^i$ 需要 i 次乘法运算，文献[5]中的密钥是通过计算形如 $\sum_{i=0}^{t} a_i x^i$ 的一元 t 次多项式得到的，因此需要 $\frac{t(t+1)}{2}$ 次乘法运算和 t 次加法运算。本文方法中，密钥计算分为两个步骤：

(1)利用节点序号数组 $(\mathrm{ID}_1, \mathrm{ID}_2)$，通过同化三元多项式 $f(x_1,x_2,x_3) = C + \sum_{i_1=1}^{t+1}\sum_{i_2=1}^{t+1}\sum_{i_3=1}^{t+1} a_{i_1 i_2 i_3} x_1^{i_1} x_2^{i_2} (x_3 - x_c)^{i_3}$ 得到形如 $C + \sum_{i=1}^{t+1} a_i (x - x_c)^i$ 的一元 t 次多项式。

(2)利用 x_c，通过步骤(1)中得到的一元 t 次多项式得到密钥。

步骤(1)中需要 $(t+1)^2(t+2)$ 次乘法运算和 $(t+1)^3$ 次加法运算；步骤(2)中需要 $\frac{(t+1)(t+2)}{2}$ 次乘法运算和 $t+2$ 次加法运算。实际上，本文方法最终的计算复杂度，并不是两个步骤的简单相加，因为只有在同化三元多项式被捕获的时候，步骤(1)才会发生，而步骤(2)是常用的密钥计算过程，如密钥更新等。因此，本文方法的密钥计算复杂度主要由步骤(2)所决定，而它又是与文献[5]近似的。

6 结束语

密钥管理是无线传感器网络安全的核心问题，本文以基于 EBS 的密钥管理方法为基础，利用同化三元多项式密钥取代普通密钥，针对分簇式网络结构，设计了一种新型的无线传感器网络动态密钥管理方法。分析结果表明，本文方法与传统的基于 EBS 的密钥管理方法相比，可有效地解决共谋问题，提高网络对被捕获节点的抵抗性，并节约了更新密钥和驱逐节点过程中的能耗。在存储空间占有量方面虽略有增加，但是相比于静态密钥管理方法所需的存储空间仍是少量的。

参 考 文 献

[1] Akyildiz I F, Su W, and Sankarasubramaniam Y. Wireless sensor networks: A survey[J]. *Computer Networks*, 2002, 38(4): 393–422.

[2] Qi H, Iyengarb S, and Chakrabartyk K. Distributed sensor networks-a review of recent research[J]. *Journal of the Franklin Institute*, 2001, 338(6): 655–668.

[3] Aboelaze M and Aloul F. Current and future trends in sensor networks: A survey[C]. Second International Conference on Wireless and Optical Communications Networks (IFIP 2005). Sydney: IEEE Press, 2005: 551–555.

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

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

[6] Eschenauer L and Gligor V D. A key-management scheme for distributed sensor networks[C]. Proceedings of the 9th ACM conference on Computer and communications security. Washing D.C: ACM Press., 2002: 41–47.

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

[8] Mohamed Eltoweissy, Ashraf Wadaa, Stephan Olariu, and Larry Wilson. Group key management scheme for large-scale sensor networks [J]. *Ad hoc Networks*, 2005, 3(5): 668–688.

[9] Chorzempa Michael and Park Jung-Min, *et al.*. Key management for long-lived sensor networks in hostile environments [J]. *Computer communications*, 2007, 30(3): 1964–1979.

[10] Liu D and Ning P. Establishing pairwise keys in distributed sensor networks[C]. CCS'03, Washington DC, 2003: 52–61.

孔繁瑞： 男，1981 年生，博士生，研究方向为无线传感器网络.

李春文： 男，1958 年生，教授，研究方向为无线传感器网络、网络化运动控制.

丁青青： 女，1963 年生，副教授，研究方向为电器与系统测控技术.