doi: 10.7694/jdxblxb20130328

适用于无线传感器网络密钥管理LEAP方案的改进与优化

余宜诚[1]，张文才[2]，胡 亮[1]，吴方明[1]，初剑峰[1]
(1. 吉林大学 计算机科学与技术学院，长春 130012；2. 吉林省公安厅 交通警察总队，长春 130028)

摘要：针对无线传感器网络密钥管理LEAP方案的缺点，提出一种通过引入秘密信息验证节点合法性的方法，并利用Diffie-Hellman算法生成节点间配对密钥来保障密钥的安全. 由安全性、节点开销等方面对原LEAP方案与改进方案进行对比分析结果表明，改进方案在计算代价上略有增加，但提高了网络的安全性.

关键词：无线传感器网络；密钥管理；安全性；Diffie-Hellman算法
中图分类号：TP309 **文献标志码**：A **文章编号**：1671-5489(2013)03-0483-04

Improvement and Optimization of LEAP Scheme for Key Management in Wireless Sensor Networks

YU Yi-cheng[1], ZHANG Wen-cai[2], HU Liang[1], WU Fang-ming[1], CHU Jian-feng[1]
(1. *College of Computer Science and Technology, Jilin University, Changchun* 130012, *China*;
2. *Traffic Police Headquarter Department, Public Security of Jilin Province, Changchun* 130028, *China*)

Abstract: The method to use secret information to verify the legitimacy of the nodes was presented and Diffie-Hellman algorithm was used to generate the shared key for guaranteeing the security of the key so as to overcome the weakness of localized encryption and authentication protocol. The analysis of the original scheme and the improved scheme from the security and node overhead shows that the computational cost is slightly increased in the improved scheme, but the security of the network is improved.

Key words: wireless sensor network; key management; security; Diffie-Hellman algorithm

无线传感器网络(wireless sensor networks, WSN)广泛应用于环境监控、军事、医疗、交通控制、森林防火等领域[1-3]，但由于传感器节点大多数部署在无人触及、易受损、易被俘获的环境下，因此保证无线传感器网络的安全性十分重要[4-6].

为实现WSN中节点通信的机密性、完整性和可认证性等安全特性，人们提出了许多密钥管理方案，如E-G方案[7]、基于E-G模型的实现方案[8]、基于多项式的密钥管理方案[9]、基于部署信息的方案[10]、LEAP方案[11]和基于椭圆曲线点加的方案[12]等.

本文提出一种基于LEAP方案改进的密钥管理方案，通过引入秘密信息验证节点的合法性，用

收稿日期：2013-04-09.

作者简介：余宜诚(1990—)，男，汉族，硕士研究生，从事通信协议安全的研究，E-mail：yycitb@vip.qq.com. 通信作者：胡 亮(1968—)，男，汉族，博士，教授，博士生导师，从事网格计算与网络安全的研究，E-mail：hul@jlu.edu.cn；初剑峰(1978—)，男，汉族，博士，副教授，从事计算机系统结构的研究，E-mail：chujf@jlu.edu.cn.

基金项目：国家自然科学基金(批准号：61073009).

Diffie-Hellman算法生成配对密钥以增强方案的安全性，与LEAP方案相比，本文提出的方案在计算代价上略有增加，但能克服LEAP方案的缺点.

1 预备知识

1.1 LEAP方案

LEAP方案是基于单一密钥机制无法实现无线传感器网络安全通信思想而提出的，该方案的优点是当网络中的节点被俘获时，不会对其他节点的安全产生威胁，但在节点部署后特定的时间段内，节点需要保存WSN全网通用的主密钥，而一旦该密钥暴露，网络的安全极其危险.

LEAP方案的提出基于如下假设：攻击者想要俘获WSN中的传感器节点，至少需要花费$T_{\min}$时间，而新节点部署后，寻找邻居节点并产生与邻居节点的配对密钥需花费T_{est}时间($T_{\min}>T_{est}$). 该方案根据网络中传送的消息包类别和安全级别，将网络中的通信密钥分为4种类型：基站与节点进行通信的唯一密钥、簇头节点间通信的对偶密钥、簇内节点间通信的簇密钥和全组通信的组密钥.

1.2 Diffie-Hellman算法

1) 存在两个全局公开的参数：素数q和整数α，α是q的一个原根.

2) 假设A,B用户需要交换一个密钥，A用户生成一个随机数$X_A<q$并计算$Y_A=\alpha^{X_A} \bmod q$，A保密存储X_A而公开将Y_A发送给B. 类似地，B用户同样生成一个随机数$X_B<q$并计算$Y_B=\alpha^{X_B} \bmod q$，B保密存储X_B而公开将Y_B发送给A.

3) 用户A以$K=(Y_B)^{X_A} \bmod q$产生共享密钥. 同样，用户B产生共享密钥$K=(Y_A)^{X_B} \bmod q$，

$$K=(Y_B)^{X_A} \bmod q=(\alpha^{X_B} \bmod q)^{X_A} \bmod q=(\alpha^{X_B})^{X_A} \bmod q=\alpha^{X_B X_A} \bmod q=$$
$$(\alpha^{X_A})^{X_B} \bmod q=(\alpha^{X_A} \bmod q)^{X_B} \bmod q=(Y_A)^{X_B} \bmod q,$$

因此双方能够得到相同的共享密钥.

由于计算以素数为模的指数相对容易，而计算离散对数较难，因此用Diffie-Hellman算法计算配对密钥能保证密钥的安全性.

2 改进方案

设u,v表示传感器节点中的普通节点；K_i表示基站与节点间的通信密钥；$E_k(M)$表示用密钥K对消息M进行加密；MAC(K,M)表示消息M使用对称密钥K返回的消息认证码；$h(x)$表示对x求其哈希值.

在无线传感器网络中，由于基站、簇头和普通节点在计算能力、存储空间等方面存在较大差距，因此它们在WSN中的作用也不同.

2.1 方案初始化

在网络部署前，每个节点先预存自身的ID、与基站的通信密钥K_i及大素数p和p的本原根α.

2.2 密钥的建立

簇内普通节点密钥分配过程分为如下4个阶段.

1) 主密钥分配阶段.

① 各节点生成一个随机数$r_i \in Z_p^*$，通过哈希函数$H_i=h(\mathrm{ID}_i \| r_i) \bmod p$计算秘密信息，用$K_i$进行加密，将$E_{K_i}(H_i \| ID_i)$发送给基站，并删除$K_i$；

② 基站收齐所有节点的秘密信息后，用与各节点相对应的K_i进行解密，得到各节点的秘密信息H_i和节点ID，计算

$$p(x)=(x-H_1)(x-H_2)\cdots(x-H_n) \bmod p;$$

基站生成主密钥K，计算

$$g(x)=[p(x)+K] \bmod p,$$

将$g(x)$广播发送给WSN中的所有传感器节点；

③ 节点收到$g(x)$，将各自的秘密信息H_i代入$g(x)$进行计算得到主密钥K，删除自身的秘

密信息 H_i.

2）簇内发现邻居节点阶段.

传感器节点部署到网络后都将初始化一个计时器，时间一旦超过 $T_{\min}$ 便会报警. 节点广播包含其节点 ID 的 Hello 消息，节点 u 等待每个邻居节点 v 以其 ID 号作为回应消息，消息均通过主密钥 K 进行加密及解密，其中：

$$u \rightarrow *: E_K(u);$$

$$v \rightarrow u: E_K(v, \mathrm{MAC}(K, u \mid v)).$$

如图 1 所示.

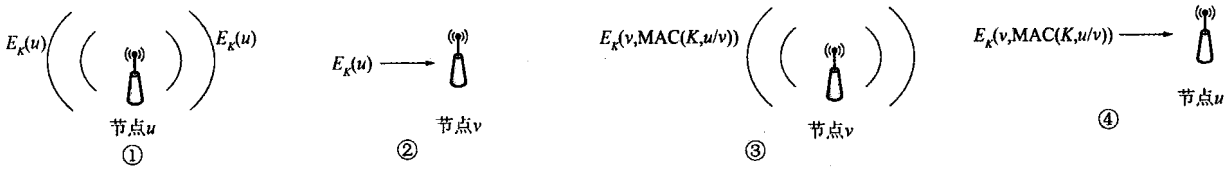

图 1　节点 u 发现邻居节点的过程

Fig. 1　Process of neighbor discovery

3）配对密钥生成阶段.

节点 u 生成一个随机数 $X_u < q$，并计算 $Y_u = \alpha^{X_u} \bmod q$，将 Y_u 发送给节点 v，节点 v 同样生成一个随机数 $X_v < q$，计算 $Y_v = \alpha^{X_v} \bmod q$，发送给节点 u，从而节点 u，v 便得到其相同的配对密钥

$$K_{u,v} = (Y_v)^{X_u} \bmod q = \alpha^{X_v X_u} \bmod q = (Y_u)^{X_v} \bmod q.$$

4）密钥信息删除阶段.

节点中的定时器时间一超过 T_{est}，节点 u 便删除主密钥 K、大素数 p 和 p 的本原根 α.

3　性能分析

3.1　安全性分析

在 LEAP 方案中，当 $T_{\mathrm{est}} > T_{\min}$ 时，攻击者即可能获取初始化密钥 K_I，而在本文改进方案中，合法节点存有基站与其通信的密钥 K_i，并用其对 H_i 进行加密，发送给基站. 攻击者没有 K_i，发送的非法秘密信息无法通过基站认证，从而保证了秘密信息的合法性，且只有合法节点才能通过 $g(x)$ 计算出主密钥 K，保证了密钥安全，且在发现邻居节点阶段，节点间的合法性认证可通过主密钥 K 的加解密实现，能有效识别非法节点，因此本文改进方案也能抵抗 Hello Message 攻击. 在配对密钥生成阶段，通信双方通过 Diffie-Hellman 密钥交换算法获得会话密钥，即使交换的中间参数被攻击者获取，会话密钥也不会暴露. 因此，本文改进方案的安全性强于 LEAP 方案.

3.2　节点开销分析

3.2.1　*存储开销*　在 LEAP 方案中，普通节点只需存储初始化密钥 K_I 和节点标志 ID，而本文改进方案中，虽然每个节点需存储的信息有与基站通信的密钥 K_i、节点标志 ID、自身的秘密信息 H_i、本原根 α、大素数 p 及与邻居节点间的会话密钥，但在密钥分配完成过程中，这些信息都先后被删除了，所以两个方案在存储代价上相等.

3.2.2　*计算开销*　与 LEAP 方案相比，本文改进方案在主密钥分配阶段，进行了一次哈希运算和一次加密运算；在邻居发现阶段发送的信息经过主密钥 K 加密，收到的信息也经过主密匙 K 进行解密；在生成配对密钥阶段，节点生成 Y_u，进行了一次指数运算，在生成配对密钥时，又进行了一次指数运算得到配对密钥. 虽然本文改进方案的计算开销大于 LEAP 方案，但考虑到指数运算只在生成或更新配对密钥时才需进行，故本文改进方案的计算开销可以接受.

3.2.3　*通信开销*　本文改进方案只在主密钥分配时，普通节点将秘密信息 H_i 发送给基站，比 LEAP 方案多一次通信，但在系统中仅发生一次，因此，两个方案的通信代价相等.

表 1 列出了本文改进方案与原 LEAP 方案的对比结果.

表1 本文改进方案与原LEAP方案的对比

Table 1 Comparison of this scheme and LEAP scheme

方 案	安全性	存储开销	计算开销	通信开销
原LEAP方案	弱	相同	低	相同
本文改进方案	强	相同	高	相同

综上所述，本文提出了一种基于LEAP方案改进的密钥管理方案，通过引入一个节点秘密信息验证节点合法性的方法，计算网络中的主密钥，利用Diffie-Hellman算法生成节点间配对密钥，保障了密钥的安全性. 性能分析结果表明，与LEAP方案相比，本文改进方案的存储开销和通信开销与原方案相同，在计算代价上略有增加，但能克服LEAP方案的缺点，提高了网络的安全性.

参 考 文 献

[1] Badescu A M, Fratu O, Frujina A, et al. Wireless Sensor Network for Wildlife Monitoring [J]. Environmental Engineering and Management Journal, 2011, 10(11): 1625-1634.

[2] Sidek O, Quadri S A, Kabir S, et al. Application of Carbon Nanotube in Wireless Sensor Network to Monitor Carbon Dioxide [J]. Journal of Experimental Nanoscience, 2013, 8(2): 154-161.

[3] Jiménez V P G, Armada A G. Field Measurements and Guidelines for the Application of Wireless Sensor Networks to the Environment and Security [J]. Sensors, 2009, 9(12): 10309-10325.

[4] Ameen M A, LIU Jing-wen, Kwak K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Application [J]. Journal of Medical Systems, 2012, 36(1): 93-101.

[5] Islam K, SHEN Wei-ming, WANG Xian-bin. Wireless Sensor Network Reliability and Security in Factory Automation: A Survey [J]. IEEE Transactions on Systems, Man and Cybernetics, Part C: Appliactions and Reviews, 2012, 42(6): 1243-1256.

[6] Kumar H, Sarma D, Kar A. Security Threats in Wireless Sensor Networks [J]. IEEE Aerospace and Electronic Systems Magazine, 2008, 23(6): 39-45.

[7] Eschenauer L, Gligor V D. A Key Management Scheme for Distributed Sensor Networks [C]//Proceedings of the 9th ACM Conference on Computer and Communication Security. New York: ACM Press, 2002: 41-47.

[8] WANG Hao, YANG Jian, WANG Ping, et al. Efficient Pairwise Key Establishment Scheme Based on Random Pre-distribution Keys in WSN [C]//International Conference on Computational Science and Its Applications. Berlin: Springer, 2010: 291-304.

[9] LIU Dong-gang, NING Peng. Establishing Pairwise Keys in Distributed Sensor Networks [C]//Proceedings of the 10th ACM Conference on Computer and Communication Security. New York: ACM Press, 2003: 52-61.

[10] LIU Dong-gang, NING Peng. Location-Based Pairwise Key Establishments for Static Sensor Networks [C]//Proc of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2003: 72-82.

[11] ZHU Sen-cun, Setia S, Jajodia S. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks [C]//Proceedings of the 10th ACM Conference on Computer and Communication Security. New York: ACM Press, 2003: 62-72.

[12] Rajendiran K, Sankararajan R, Palaniappan R. A Secure Key Predistribution Scheme for WSN Using Elliptic Curve Cryptography [J]. ETRI Journal, 2011, 33(5): 791-801.

(责任编辑：韩 啸)