·安全技术· 文章编号：1000-3428(2015)01-0126-04 文献标识码：A 中图分类号：TP309

一种具有强匿名性的无线传感器网络访问控制方案

陈 婷，卢建朱，江俊晖

（暨南大学信息科学技术学院，广州 510632）

摘 要： 随着无线传感器网络（WSN）的应用越来越广泛，其访问控制的安全性和隐私问题已成为研究热点。将 Hash 函数、消息认证码以及椭圆曲线上的点乘计算相结合，提出一种具有强匿名性的 WSN 访问控制方案。该方案中通信双方相互认证抵抗攻击者的伪造攻击，利用消息认证码来保证数据的完整性；同时以公平的方式生成共享的会话密钥，具有较强的抵抗伪装攻击和抵抗节点捕获攻击的能力。理论分析与评估结果表明，该方案通过引入强匿名的节点请求，实现节点请求的不相关性，增强抵抗节点捕获攻击的能力。将 Hash 函数与消息认证码相结合，在相同阶的计算复杂度下不增加通信成本，增强系统的安全性。

关键词： 无线传感器网络；访问控制；强匿名性；认证；安全

中文引用格式： 陈 婷，卢建朱，江俊晖. 一种具有强匿名性的无线传感器网络访问控制方案[J]. 计算机工程，2015，41(1)：126-129.

英文引用格式： Chen Ting，Lu Jianzhu，Jiang Junhui. An Access Control Scheme with Strong Anonymity in Wireless Sensor Network[J]. Computer Engineering，2015，41(1)：126-129.

An Access Control Scheme with Strong Anonymity in Wireless Sensor Network

CHEN Ting，LU Jianzhu，JIANG Junhui

（College of Information Science and Technology，Jinan University，Guangzhou 510632，China）

【Abstract】 With the wide application of Wireless Sensor Networks（WSN），it attracts increasing attention and its security and privacy concerns of access control are becoming important research issues. This paper proposes an access control scheme with strong anonymity by utilizing a Hash function，the message authentication code and the point multiplication calculation on an elliptic curve. It uses mutual authentication in both communication sides to resist the forgery attacks，and uses the message authentication code to ensure data integrity. Meanwhile，it generates the share session key in a fair way and has a strong resistance to node capture attacks. Theoretical analysis and evaluation result shows that the scheme achieves the uncorrelated requests between nodes by introducing node requests with strong anonymity，which can enhance the ability to resist the node capture attacks. In particular，compared with the existing schemes，combining the message authentication code with the Hash function，it is more secure and efficient in the same order of computational complexity and without increasing the cost of communication.

【Key words】 Wireless Sensor Network（WSN）；access control；strong anonymity；authentication；security

DOI： 10.3969/j.issn.1000-3428.2015.01.023

1 概述

随着近年来无线传感器网络（Wireless Sensor Networks，WSN）相关技术的快速发展，无线传感器节点通常可以部署到不同的环境中执行各种监测任务，可用于工业监控、生态环境等众多领域[1-2]。在 WSN 的应用中，其安全问题是需要考虑的主要问题。传感器采用电池供应能源，计算能力有限和较小的存储空间[3]。随着存储技术的提高，当前传感器的存储大小可达到 64 MB[4]。所以要尽量运用存储的信息来降低计算和通信产生的能耗。通常更换已部署的传感器的电池不方便，设计低能耗的 WSN 访问控制机制是一项富有挑战性的任务。传统的访问控制机制因计算较复杂、通信成本较高，一般不适用于 WSN。此外，传感器节点经常由于电源耗尽或周围环境等原因而失效，一些早期的研究中提出来

基金项目： 国家自然科学基金资助项目（61373125，61272415，61070164）；广东省自然科学基金资助项目（S2011010002708，2010B090400164）；暨南大学科技创新基金资助项目（11611510）。

作者简介： 陈 婷（1987－），女，硕士研究生，主研方向：信息安全，网络通信；卢建朱，副教授、博士；江俊晖，硕士。

收稿日期： 2013-12-10 **修回日期：** 2014-02-04 **E-mail：** novelting@foxmail.com

的、静态地添加新节点的方法[5-8]在抵抗节点捕获上存在明显的不足之处,此时动态添加传感器节点常常是需要的。在 WSN 的节点捕获攻击中,攻击者可读取捕获节点中的密码信息,并进行复制部署伪造的网络节点。目前,没有一种有效的方法完全制止这一攻击,但可尽量减少该攻击造成的损失。

基于椭圆曲线问题与 Hash 链,文献[9]提出了 ACP 方案,但文献[10]指出 ACP 方案的认证过程需要时间戳来保证,并且 2 个节点同时部署时需要相同的引导时间,这在实际应用中不容易实现。Huang 等人接着提出了 ACP 的改进方案 NACP。文献[11]指出,NACP 是不安全的,它不能抵抗重放攻击;并进一步做出改进,提出 ENACP 方案。文献[12]设计了一个 WSN 可抵抗节点捕获攻击的访问控制机制,利用 Hash 值对网络节点进行有限的访问授权,可较好地抵抗节点捕获攻击,并可实现传感器的动态添加。若在该机制中,节点的访问是匿名的和不可追踪的,则可进一步增加攻击者捕获节点的困难,增强系统的安全性。

本文在文献[12]的基础上,提出一种具有强匿名性的无线传感器网络访问控制方案。该方案通过引入强匿名的节点请求,实现节点请求的不相关性。

2　本文方案设计

针对 WSN 的访问控制需求,将 Diffie-Hellman 密钥协商算法、对称加密算法和安全的哈希函数相结合,提出一种具有强匿名的 WSN 访问控制方案。该方案包含 3 个阶段:系统初始化,认证和会话密钥建立以及新节点加入阶段。

2.1　系统初始化

假设在某一区域部署一个无线传感器网络。该网络由一个基站和若干个无线传感器节点组成。在部署之前,基站首先执行系统初始化,然后为传感器节点进行密钥的预分配。

在系统初始化过程中,基站选取系统公共参数 $parm=\{p,q,E(F_q),P,h(\cdot),\mathbb{K}\}$。其中,$p,q$ 为2 个大素数;$E(F_q)$是系数属于域 F_q 的椭圆曲线上的加法群;P 是群 $E(q)$的一个 q 阶生成元,$h(\cdot)$和$h'(\cdot)$是安全的 HASH 函数,$\mathbb{K}$是一个足够大的密钥空间。

初始的 WSN 网络由 N 个无线传感器节点 S_j 均匀地分布在部署的二维平面区域,节点 S_j 的位置为坐标(x_j,y_j),其身份标识符为 ID_j,$1\leqslant j\leqslant N$。在节点 S_j 部署之前,基站先选取 2 个唯一的密钥 $k_j^{(1)}\in\mathbb{K}$,$k_j^{(2)}\in Z_q$,计算 $k_j^{(2)}P$,设 $PK_j=k_j^{(2)}P$;然后,确定节点 S_j 的部署位置(x_j,y_j),选取与点(x_j,y_j)距离小于通信半径 R 的传感器节点 S_i 为内节点,$1\leqslant i\leqslant n$;利用 S_j 的每个内节点 S_i 的密钥 $k_i^{(1)}$、PK_i 和 ID_i,计算$h(ID_j||k_i^{(1)})$,将数对$(ID_i,PK_i,h(ID_j||k_i^{(1)}))$预装到节点 S_j。

2.2　认证和会话密钥建立

传感器节点只能向其内节点发起建立身份认证和会话密钥的请求。假设传感器节点 S_j 向内节点 S_i 发送会话请求,S_j 利用内部存储的信息$(ID_i,PK_i,h(ID_j||k_i^{(1)}))$,双方进行如下操作:

(1)$S_j\rightarrow S_i:M_1=\{CID_j,T_j,F_j\}$

1)S_j 选择随机数 $t_j\in Z_p^*$,计算 $T_j=t_jP=(T_{x_j},T_{y_j})$,$F_{ji}=t_jPK_i$;

2)用 F_{ji} 隐藏真实身份 ID_j,计算 $CID_j=h'(F_{ji})\oplus ID_j$;

3)生成请求的认证信息 $F_j=h(ID_j||T_{x_j}||h(ID_j||k_i^{(1)}))$。

(2)$S_i\rightarrow S_j:M_2=\{CID_i,T_i,F_i\}$

1)收到$\{CID_j,T_j,F_j\}$后,S_i 计算 $F_{ji}=k_i^{(2)}T_j$、$ID_j=CID_j\oplus h'(F_{ji})$,然后验证以下等式是否成立:

$F_j=h(ID_j||T_{x_j}||h(ID_j||k_i^{(1)}))$

若等式不成立,则拒绝该请求;否则,S_j 是合法授权节点,进行下一步;

2)S_i 选择随机数 $t_i\in Z_p^*$,计算 $T_i=t_iP=(T_{x_i},T_{y_i})$;

3)利用双方的共享秘密 F_{ji}隐藏真实身份 ID_i,计算 $CID_i=h'(F_{ji})\oplus ID_i$;

4)生成响应的认证信息 $F_i=h(ID_i||T_{x_i}||h(ID_j||k_i^{(1)}))$。

(3)$S_j\rightarrow S_i:M_3=\{Z_j\}$

1)收到$\{CID_i,T_i,F_i\}$后,S_j 利用步骤(1)的 F_{ji},根据等式 $F_i=h(ID_i||T_{x_i}||h(ID_j||k_i^{(1)}))$验证 S_i 的信息。若等式不成立,则中止该认证过程;否则,进行下一步;

2)利用步骤(1)选取的 t_j,计算 $k_{ji}=t_jT_i=(k_{x_{ji}},k_{y_{ji}})$;

3)计算认证信息 $Z_j=h(ID_j||k_{x_{ji}}||h(ID_j||k_i^{(1)}))$。

(4)$S_i\rightarrow S_j:M_4=\{Z_i\}$

1)收到 Z_j 后,S_i 根据步骤(2)选取的 t_i,结合请求信息 M_1 中的 T_j,计算会话密钥 $k_{ji}=t_iT_j=(k_{x_{ji}},k_{x_{ji}})$;

2)若 Z_j 与 $h(ID_j||k_{x_{ji}}||h(ID_j||k_i^{(1)}))$相等,则会话密钥 k_{ji}是正确的,否则,退出认证过程;

3)生成认证信息 $Z_i=h(ID_i||k_{x_{ji}}||h(ID_j||k_i^{(1)}))$,表示 S_i 已得到正确的会话密钥 k_{ji}。

(5)S_j 收到 M_4 后,进行验证 Z_i 是否等于 $h(ID_i||k_{x_{ji}}||h(ID_j||k_i^{(1)}))$。若等式成立,则保存会话密钥 k_{ji},

用于未来的通信;否则,重复步骤(1)~步骤(5)。

S_j 与 S_i 建立认证和会话密钥过程如图 1 所示。

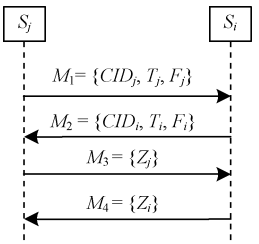

图 1 S_j 与 S_i 的认证和会话密钥过程

2.3 新节点加入

在 WSN 的应用中,根据实际情况的需求(如检测区域的扩大或提高感知数据的精度),有时需要加入新的传感器节点。假设 WSN 现已部署 N' 个传感器节点,需在位置为 $(x_{N'+1}, y_{N'+1})$ 加入新的传感器节点 $S_{N'+1}$。具体操作如下:

(1)基站为它产生 2 个唯一密钥:$k_{N'+1}^{(1)}$ 和 $k_{N'+1}^{(2)}$,身份标识符为 $ID_{N'+1}$,$PK_{N'+1}=k_{N'+1}^{(2)}P$;

(2)$S_{N'+1}$ 装载与它有关的内节点 S_i 的数对集合 $(ID_i, PK_i, h(ID_{N'+1}||k_i^{(1)}))$,其中,$ID_i$ 是 S_i 的身份标识,PK_i 用于隐藏身份标识;

(3)预装载上述数据后,将节点 $S_{N'+1}$ 部署到 $(x_{N'+1}, y_{N'+1})$;由 $S_{N'+1}$ 向其他节点发起 2.2 节中的认证和会话密钥建立。

3 安全性分析与性能分析

3.1 安全性分析

本文方案的安全性是基于安全的哈希函数单向性和椭圆曲线上的离散对数问题。将具体分析传感器节点密钥的机密性、通信双方会话密钥的安全性、认证过程的不可伪造性及其传输数据的完整性、抗节点捕获攻击的能力。

(1)传感器节点密钥的机密性是基于安全的哈希函数的单向性和椭圆曲线上的离散对数问题。

在初始化阶段,每个传感器节点 S_i 被分配 2 个密钥 $(k_i^{(1)}, k_i^{(2)})$,分别用于生成隐藏自己的身份标识 $PK_i=k_i^{(2)}P$ 和作为节点 S_j 内节点的预装载信息 $h(ID_j||k_i^{(1)})$。攻击者通过捕获 S_j,可从 S_j 获取其存储的内节点 S_i 的信息 $(ID_i, PK_i, h(ID_j||k_i^{(1)}))$;利用 PK_i 获取密钥 $k_i^{(2)}$,攻击者面临求解椭圆曲线上的离散对数问题。此外,根据捕获节点 S_j 中的数据 $h(ID_j||k_i^{(1)})$,攻击者欲求解 S_i 的密钥 $k_i^{(1)}$;由于哈希函数 $h(\cdot)$ 的单向性,攻击者成功的概率十分小。

(2)通信双方相互认证抵抗攻击者的伪造攻击,利用消息认证码来保证数据的完整性。

传感器节点 S_j 向其内节点 S_i 发送请求信息,S_i 先认证 S_j 的合法性,再认证与合法 S_j 的会话密钥的正确性。根据请求信息 $M_1=\{CID_j, T_j, F_j\}$,S_i 利用第二个密钥 $k_i^{(2)}$ 恢复出 S_j 的真实身份 $ID_j=CID_j\oplus h'(k_i^{(2)}T_j)$,再检查 S_j 是否为合法的授权节点。若 $F_j=h(ID_j||T_{x_j}||h(ID_j||k_i^{(1)}))$,则表明在基站将 $(ID_i, PK_i, h(ID_j||k_i^{(1)}))$ 预装到了节点 S_j,S_j 是一个合法的授权节点,且 S_i 是它的一个内节点;否则,S_j 是一个非法节点,S_i 拒绝这一请求。若传感器节点 $\overline{S}_j$ 的内节点不包含 S_i,攻击者利用 $\overline{S}_j$ 生成一个关于 S_i 的合法请求,必须获取 $h(ID_j||k_i^{(1)})$;若攻击者已知 ID_j,然后随机选取一个 $\overline{k}_i^{(1)}\in \mathrm{K}$,计算 $h(ID_j||\overline{k}_i^{(1)})$,生成对应的请求信息;那么,攻击者能生成一个被 S_i 接受的请求的概率是 $\frac{1}{|\mathrm{K}|}$。此外,本文方案是匿名的,攻击者不知道其授权内节点之外的节点的身份标识,这进一步降低了攻击者的成功率。

对于合法的授权节点 S_j 的应答信息 $M_3=\{Z_j\}$,S_i 通过 $Z_j=h(ID_j||k_{x_{ji}}||h(ID_j||k_i^{(1)}))$ 验证会话密钥 k_{ji} 的正确性,其中 $k_{ji}=t_iT_j=t_jT_i=(k_{x_{ji}}, k_{x_{ji}})$,$t_i$ 和 t_j 分别是 2.2 节中 S_i 和 S_j 选取的随机数。根据 Diffie-Hellman 密钥协商算法可知,除 S_i 和 S_j 外,攻击者根据 T_i 和 T_j 计算 k_{ji} 的概率是可忽略不计的。且由 $h(\cdot)$ 函数输出的随机性,没有正确的会话密钥 k_{ji},攻击者得到正确 Z_j 的概率是小于 $\frac{1}{p}$。这样,攻击者伪造 M_3 的成功概率很小。

接收内节点 S_i 的响应信息后,节点 S_j 生成合法内节点的应答信息;再根据 S_i 关于会话密钥建立成功的信息,计算共享的会话密钥。S_j 根据等式 $F_i=h(ID_i||T_{x_i}||h(ID_j||k_i^{(1)}))$,验证内节点 S_i 的响应 M_2 的正确性,其中,$T_i=t_iP=(T_{x_i}, T_{y_i})$,$h(ID_j||k_i^{(1)})$ 是 S_j 预装载的内节点信息。若攻击者不是 S_j 请求的内节点 S_i,不持有密钥 $k_i^{(1)}$;这时,攻击者得到正确值 $h(ID_j||k_i^{(1)})$ 的概率小于 $\max\{\frac{1}{p}, \frac{1}{|\mathbb{K}|}\}$。类似应答信息 $M_3=\{Z_j\}$ 的正确性分析,攻击者伪造信息 $M_4=\{Z_i\}$ 的成功率是可忽略不计的。

(3)以公平的方式生成正确性的共享的会话密钥。

节点 S_i 和 S_j 之间会话密钥的建立是基于 Diffie-Hellman 密钥协商算法,生成共享的会话密钥 $k_{ji}=(t_it_j)P$。在 $(t_it_j)P$ 中,t_i 是 S_i 选择的随机数,t_j 是 S_j 随机选取的整数,即 k_{ji} 是由 S_i 和 S_j 共同协商产生的一次性会话密钥。其他用户或攻击者不知道 t_i 和 t_j,只能通过窃听获取传输信息中的 T_i 和 T_j。由 Diffie-Hellman 密钥协商算法的安全性可知,直接从 T_i 和 T_j 计算 k_{ji} 是十分困难的;而根据 T_i 和 T_j 求

整数 t_i 和 t_j,面临求解离散对数问题。

(4)本文方案中节点具有良好的抗捕获攻击的能力。

假设节点 S_j 被捕获,攻击者可以获取 S_j 存储的所有数据,即有关内节点 S_i 用于隐藏身份标识的 $PK_i = k_i^{(2)}P$ 和捕获节点与内节点的第 1 个密钥串接结果的哈希值 $h_{ji} = h(ID_j \| k_i^{(1)})$。由哈希函数输出结果的随机性,攻击者从 h_{ji} 求 $k_i^{(1)}$ 的成功概率十分小;从 PK_i 获取 S_i 的第 2 个密钥 $k_i^{(2)}$,攻击者面临求解离散对数问题。由此可知,攻击者捕获 S_j 获取内节点密钥成功的概率是十分小的,本文方案具有较好的抗捕获攻击的能力。

3.2　性能分析

本文方案与文献[5]都是基于椭圆曲线上的 Diffie-Hellman 密钥协商算法。相对于椭圆曲线上的点乘计算,异或运算和哈希计算的耗时可忽略不计。又系统的初始化只在部署传感器节点时执行一次,下文只讨论传感器节点中间的认证阶段的时间复杂性和通信成本的复杂性。

在认证阶段,传感器节点 S_j 在生成请求消息需要计算 $T_j = t_jP$ 和 $F_{ji} = t_jPK_i$;在接受 S_i 的应答后计算 $k_{ji} = t_jT_i$ 生成认证信息 z_j。节点 S_j 一共需要执行 3 次点乘计算。类似地,S_j 的请求节点 S_i 也需要计算 $T_i = t_iP$,$F_{ji} = k_i^{(2)}T_j$ 和 $k_{ji} = t_iT_j$,共 3 次点乘计算。与文献[5]相比,传感器节点 S_j 和 S_i 各需要增加 1 次点乘计算,以保护信息发送者的身份隐私。从上述分析可知,本文方案中传感器节点 S_j 和 S_i 的时间复杂性与文献[5]的方案有相同的阶。

令 $|x|$ 表示二进制字符串的长度。类似于文献[5],取 $|p| = 160$ bit,$|q| = 80$ bit。进一步地,取$\mathbb{K}$的最大密钥长度为 80 bit,随机数长度为 80 bit,函数 $h(\cdot)$ 和 $h'(\cdot)$ 的输出长度为 160 bit,$h'(\cdot)$ 的结果取其高 80 位进行保存。此外,置文献[5]中身份标识符长度为 80 bit。在 S_j 与 S_i 的相互认证中,S_j 的请求信息 M_1 的长度为 $|CID_j| + |T_j| + |F_j| = 80 + 320 + 160 = 560$ bit,S_i 的响应信息 M_2 的长度为 $|CID_i| + |T_i| + |F_i| = 80 + 320 + 160 = 560$ bit,S_j 和 S_i 先后发送会话密钥的确认信息 M_3 和 M_4,它们的长度分别为 $|T_j| = |T_i| = 160$ bit。本文方案的通信成本为 $|M_1| + |M_2| + |M_3| + |M_4| = 1\,440$ bit。由此可见,在通信成本方面,本文方案和文献[5]具有相同的通信成本,进一步地本文方案实现了节点请求的匿名性和不可追踪性。

本文方案与文献[5]方案计算和通信成本对比如表 1 所示。

表 1　计算与通信成本对比

方案	计算成本/时间周期	通信成本/bit
文献[5]方案	4	1 440
本文方案	6	1 440

综上分析可知,本文提出的基于 WSN 上的具有强匿名的访问控制方案是可行的,具有良好的安全性能。

4　结束语

本文提出了一种具有强匿名性的 WSN 访问控制方案,其安全性是基于安全的哈希函数单向性和椭圆曲线上的离散对数问题。本文方案在合理的存储开销与计算复杂性下,未增加通信成本,实现了增强系统的抗捕获攻击能力。

参考文献

[1] Akyildiz F, Su Weilian, Sankarasubramaniam Y, et al. Wireless Sensor Network: A Survey [J]. Computer Networks, 2002, 38(4): 393-422.

[2] 任丰原,黄海宁,林　闯. 无线传感器网络[J]. 软件学报, 2003, 14(7): 1282-1291.

[3] 米　波,曹建秋,段书凯,等. 无线传感器网络密钥管理问题综述[J]. 计算机工程与应用, 2011, 47(13): 77-83.

[4] Nachman L, Huang J, Shahabdeen J, et al. IMOTE2: Serious Computation at the Edge [C]//Proceedings of Wireless Communications and Mobile Computing Conference. [S.1.]: IEEE Press, 2008: 1118-1123.

[5] Eschenauer L, Gligorv D. A Key-management Scheme for Distributed Sensor Networks [C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2002: 41-47.

[6] Chan H W, Perrig A, Song D. Random Key Pre-distribution Schemes for Sensor Networks [C]// Proceedings of IEEE Symposium on Security and Privacy. [S.1.]: IEEE Press, 2003: 197-213.

[7] Choi S J, Youn H Y. An Efficient Key Pre-distribution Scheme for Secure Distributed Sensor Networks [C]// Proceedings of Workshops on Embedded and Ubiquitous Computing. Berlin, Germany: Springer-Verlag, 2005: 1088-1097.

[8] Park C W, Choi S J, Youn H Y. A Noble Key Pre-distribution SScheme with LU Matrix for Secure Wireless Sensor Networks [C]//Proceedings of International Conference on Computational Intelligence and Security. Berlin, Germany: Springer-Verlag, 2005: 494-499.

[9] Zhou Yun, Zhang Yanchao, Fang Yuguang. Access Control in Wireless Sensor Networks [J]. Ad Hoc Networks, 2007, 5(1): 3-13.

[10] Huang H F. A Novel Access Control Protocol for Secure Sensor Networks [J]. Computer Standards & Interfaces, 2009, 31(3): 272-276.

[11] Kim H, Lee S. Enhanced Novel Access Control Protocol over Wireless Sensor Networks [J]. IEEE Transactions on Consumer Electronics, 2009, 55(2): 492-498.

[12] Lee H, Shin K, Lee D H. PACPs: Practical Access Control Protocols for Wireless Sensor Networks [J]. IEEE Transactions on Consumer Electronics, 2012, 58(2): 326-338.

编辑　索书志