第 36 卷 第 3 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.3 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)03—0142—03 文献标识码：A 中图分类号：TP393

基于 ECC 的无线传感器网络密钥管理协议

蹇 波，郭永辉，罗长远，李 伟
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：针对无线传感器网络在电量、计算能力和内存容量等方面的局限性，基于椭圆曲线密码体制，提出一种适用于无线传感器网络的密钥管理协议，给出通信密钥建立、新节点加入以及节点密钥更新与回收的实现过程。从协议的安全性、抗毁性和效能方面进行性能分析，实验结果表明该协议具有较强的可扩展性与抵抗攻击能力。

关键词：无线传感器网络；密钥管理；椭圆曲线密码体制；密钥回收

Key Management Protocol for WSN Based on ECC

JIAN Bo, GUO Yong-hui, LUO Chang-yuan, LI Wei
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Aiming at the limitation of Wireless Sensor Network(WSN) in power, computation and storage, this paper presents a key management protocol based on Elliptic Curve Cryptosystem(ECC) for WSN. It gives the accomplished courses which consists of building communication key, adding new node, renewing and recycling key. The performance of security, resilience and efficiency are analyzed, experimental results indicate that the scalability and resilience of the protocol is much better.

【Key words】 Wireless Sensor Network(WSN); key management; Elliptic Curve Cryptosystem(ECC); key recycling

1 概述

无线传感器网络(Wireless Sensor Network, WSN)是多学科高度交叉的研究热点领域，在军事和民用方面有着广泛的应用。同时，WSN 受到窃听、欺骗、注入、重放、拒绝服务(DoS)、HELLO 扩散法、陷阱区等安全威胁[1]，如何保证 WSN 安全已成为通信和信息技术领域研究的热点和难点。

密钥安全是网络安全机制的基础。由于 WSN 中节点在能量、计算能力和通信带宽等方面的限制，因此其密钥管理面临许多困难和挑战。简单的密钥分配方法是所有节点事先存储一个相同的对称密钥，每个节点均使用这个密钥进行通信，若某一个节点被攻破，则全网络都被攻破。

文献[2]提出 WSN 的随机密钥预分配方案(E-G 方案)，其主要思想是：在节点部署前，每个节点从同一密钥池中随机选取一定数量的密钥，使得任何 2 个节点之间以某一概率至少共享一个密钥，对于没有共享密钥的节点利用已建立好的安全通道迂回建立。对称密钥，具有计算量小的特点，但对称密钥需要预分配，这就限制了 WSN 增加节点和更新密钥等动态性操作。非对称密钥可以很好地满足 WSN 动态性的要求，但需要更多的资源开销。随着大规模集成技术的发展，传感器的计算能力、存储能力与能量都有了很大提高，通过有效控制，非对称密码体制中部分方法可以应用于 WSN 中。

文献[3]提出基于身份密码体制的密钥预分配方案(基于 IBC 方案)。将双线性对技术与地理信息相结合，建立配对密钥，并在此基础上生成各种通信密钥，该方案具有很强的容侵能力，任何节点的受损都不会暴露其他节点的机密信息，但该方案只适用于静态 WSN，节点位置的确定较困难。

文献[4]提出椭圆曲线密码体制(Elliptic Curve Cryptosystem, ECC)，其在相同安全强度要求下具有密钥长度短、算法速度快、占用内存少和抗攻击能力强等优点。本文以椭圆曲线密码体制为基础，提出一种适用于 WSN 的新密钥管理协议，该协议可以完成通信密钥协商，还能够动态增加节点、更新和回收密钥。

2 基于ECC的密钥管理协议

假设 WSN 中有且仅有一个基站，基站是安全的，不存在失效问题，每个节点可以感知邻近节点，在初始阶段传感器节点具有一定的抵抗外部入侵的能力(即在一定时间范围内节点是安全的)。

2.1 系统初始化

在部署 WSN 前，部署服务器为基站与每个节点进行初始化设置。选定安全的椭圆曲线 E，E 上阶为 n 的基点 G，定义曲线上的点加与标量乘运算。节点持有 $Public=\{E,G,n,H\}$（H 为单向散列函数）、公私钥对 $<PK_A, SK_A>$、临时初始密钥 K_m、节点标志(用节点公钥表示，即 $ID_A=PK_A$)以及超时计时器。基站持有除超时计时器以外普通节点的信息，同时还存储网络中所有节点的公私钥对。

2.2 通信密钥建立

节点在被布置到目标区域后，首先启动超时计时器，然后建立通信密钥，具体过程分为 3 步：

(1)节点 A 选取随机数 $d_a\in[2,n-2]$；计算 $Y_a=d_a+K_mG$，并局部广播发送消息 $\{Y_a,PK_A\}$；节点 B 做相同操作，局部广

基金项目：国家“863”计划基金资助项目(2006AAJ124)
作者简介：蹇 波(1982－)，男，硕士研究生，主研方向：无线传感器网络安全；郭永辉、罗长远，副教授、博士；李 伟，硕士研究生
收稿日期：2009-06-22 **E-mail：**jiancomnet@126.com

播发送消息 $\{Y_b, PK_B\}$。

(2)节点 B 接收消息后，通过 PK_A 判断 A 是否为 B 的邻近节点，如果不是则丢弃消息；否则解密 Y_a 得 $d_a = Y_a - K_m G$，计算通信密钥 $k_{BA} = H(d_b \oplus d_a)$。节点 A 在收到 B 的局部广播消息后，同理可以计算通信密钥 $k_{AB} = H(d_a \oplus d_b)$，显然 $k_{AB} = k_{BA}$。经一次交互，A 即可与 B 建立通信密钥。

(3)计算并保存节点的认证密钥 $W_A = H(PK_A \| K_m)$。节点计时器超时后，删除 K_m。通信密钥协商完成。

2.3 新节点加入

在新节点加入时，需要对其进行身份验证和通信密钥建立。通信密钥建立包括新节点与新节点间和老节点与新节点间 2 种情况。新节点与新节点之间由于使用相同的初始密钥，不需要身份验证，因此，通信密钥建立通过 2.2 节方式完成。新节点与老节点的通信密钥建立过程包含节点身份的验证过程，具体过程分为 3 步：

(1)节点 A 部署到区域后，随机选取 $d_a \in [2, n-2]$，计算 $W_B = H(PK_B \| K_m)$，$T_a = W_B \| d_a + W_B G$，并将消息 $\{T_a, PK_A\}$ 发送给老节点 B。

(2)老节点 B 在收到消息后，判断 A 是否是 B 的邻近节点，若不是则丢弃数据包；否则使用 W_B 解密 T_a，$W_B \| d_a = T_a - W_B G$，比较 W_B 是否相同，若不同则丢弃；否则节点 B 随机选取 $d_b \in [2, n-2]$，计算 $T_b = d_b + W_B G$，发送消息 $\{T_b, PK_B\}$ 给节点 A，然后计算通信密钥 $k_{BA} = H(d_b \oplus d_a)$。老节点 B 对新节点 A 的认证与通信密钥建立完成。

(3)节点 A 接收到消息后，利用 W_B 解密 T_b 得到 d_b，计算 $k_{AB} = H(d_a \oplus d_b)$。节点 A 完成与老节点 B 的通信密钥协商。

在新节点完成通信密钥协商后，需要基站对新节点进行身份验证，具体过程如下：

(1)节点 A 计算 $U_a = K_m \| SK_A + K_m G_a$，并将消息 $\{U_a, PK_A\}$ 发送给基站(通过单跳或者是多跳加密传输)。

(2)基站收到消息后，通过 K_m 解密 U_a 得到节点 A 的私钥 SK_A 与 K_m，判断 K_m 是否相等，如果相等则基站存储公私密钥，承认节点的合法性；否则丢弃数据信息。

在完成上述所有过程之后，节点 A 计算并存储 $W_A = H(PK_A \| K_m)$，节点计时器超时后删除 K_m。节点在网络中的增加操作完成。

2.4 密钥更新与回收

节点使用公私密钥对更新通信密钥的过程分为 2 个步骤：

(1)节点 A 随机选取 $d_a, r_a \in [2, n-2]$，计算 $R_a = r_a G$，$S_a = d_a + r_a PK_B$，发送消息 $\{R_a, S_a, PK_A\}$ 给节点 B，然后计算通信密钥 $K_{AB} = H(d_a)$。

(2)节点 B 在收到消息后，利用私钥 SK_B 与 R_a 解密 Y_a，得到 $d_a = Y_a - R_a SK_B$，计算新通信密钥 $k_{BA} = H(d_a)$，实现节点 A, B 间的通信密钥更新过程。

在 WSN 中，节点发现网络中某个节点不合法时，向基站投出对节点的不信任票，当基站收到对某个节点的不信任投票超过限定值，基站通过广播节点私钥的方式执行对节点的密钥回收，具体过程如下：

(1)基站在收到不信任节点 A 的投票数量超过某一阈值 α 时，广播发送回收消息 $recycling = \{SK_A, PK_A\}$ 到网络中。

(2)节点在收到回收消息 *recycling* 后，查找是否与 A 是邻近节点，若不是则丢弃；否则用节点 A 的私钥 SK_A 计算 $SK_A G$，将结果与 PK_A 比较，如果相同，则将节点 A 列为恶意节点，删除其通信密钥。

3 协议性能分析

本节将通过与其他 2 种密钥管理协议的比较，分析本文协议的安全性、存储开销、能量消耗和抗毁性。

3.1 安全性分析

本文协议的安全基础是椭圆曲线上离散对数问题。在通信密钥协商过程中，攻击者并不知道初始密钥，而通过截获通信密钥协商消息推导出的初始密钥是困难的。

在节点删除临时初始密钥时，必须保证是绝对删除，如果攻击者恢复初始密钥，很容易对协议其他内容进行复制；同时，超时计时器的时间设置必须在一个安全合适的范围内，以保证在密钥协商完成之后且在节点被攻击成功之前完成删除操作。

在新节点的加入过程中，老节点可以通过认证密钥验证新节点的身份，同时完成节点间通信密钥建立。

认证密钥保证了通信的安全性，如果一个节点的认证密钥泄露，只会影响到节点本身以及临近的新节点，不会破坏其他节点。基站使用 K_m 对新节点进行身份验证时，如果恶意新节点窃取认证密钥通过老节点验证，但其无法通过基站身份验证。

通信密钥的更新是通过节点的公私钥对完成的。更新操作可以让被窃取的密钥失效，同时节点私钥的机密性可以保证新的通信密钥的安全。

密钥的回收可以撤销网络中的恶意节点，此时，节点私钥的机密性确保只有基站可以发送回收消息，而其他节点是不能伪造的。

3.2 存储开销分析

理想的 WSN 存储开销是节点仅保存其邻近节点通信密钥和节点标志。假设所有密钥长度相等，网络的规模为 n，参数存储开销为 e_u，单个密钥存储开销为 e_k，k 表示平均邻近节点数量，以下对 E-G 方案、基于 IBC 方案和本文协议的存储开销进行分析比较。

在 E-G 方案中，单个节点存储密钥数量 m 与网络规模存在如下关系[2]：

$m = np = n \times (\ln n + 9.21)/k$。

因此，E-G 方案单个节点存储开销为 $n \times (\ln n + 9.21)e_k / k$。本文协议中除了存储通信密钥之外，增加了 *Public* 参数、节点公私密钥对以及认证密钥，故单个节点的存储开销为 $e_u + (k+3)e_k$。

基于 IBC 方案，增加了存储公共系统参数、系统公钥、节点公私钥以及节点标志开销，所以，单个节点的存储开销是 $e_u + (k+4)e_k$。由此可知，本文协议与基于 IBC 方案存储开销接近。

假设网络平均邻近节点数量 $k = \sqrt{n}$，对 3 种方案网络规模与存储开销关系进行分析对比，结果如图 1 所示。

从图 1 中可以看出，本文协议与基于 IBC 方案支持网络规模扩展性方面相近，E-G 方案支持网络规模可扩展性较小。

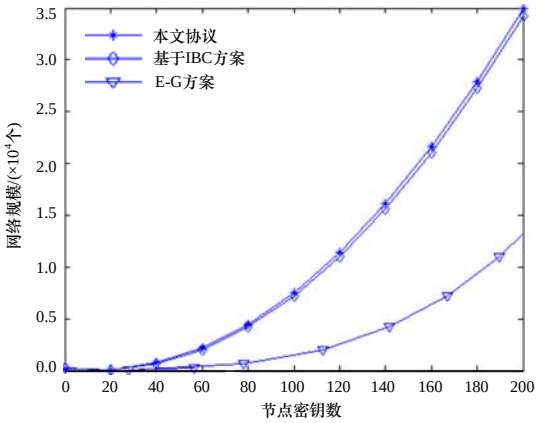

图 1　网络规模与节点内存的关系

3.3　能耗分析

传感器节点的电源能量极其有限，要求密钥管理协议的耗能要尽可能少。协议能耗主要包括通信能耗和计算能耗。

假设椭圆曲线上一次标量乘与点加运算开销为 e_1 和 e_2；e_n，e_h 表示有限域上一次模加运算开销和一次哈希运算开销；发送和接收一条消息的能耗分别为 e_S 和 e_R。表 1 为本文协议的能耗分析。

表 1　协议能耗

过程	计算能耗	通信能耗
密钥建立	$2e_1+2e_2+e_h+e_n$	e_S+e_R
节点加入	$3e_1+3e_2+2e_h+e_n$	$2e_S+e_R$
密钥更新	$2e_1+e_2+e_h$	e_S
密钥回收	e_1	e_R

从表 1 可以看出，节点通信密钥建立的计算能量开销只需要 2 次椭圆曲线上的标量乘运算和点加运算开销、一次哈希运算和加法运算开销。通信能量开销仅为一次发送和接收数据开销，因此，本文协议在通信密钥建立过程中能耗是可以接受的。协议中密钥更新与回收能耗小于通信密钥建立，虽然新节点加入能耗略大于通信密钥建立，但是新节点增加数量是有限的。

研究表明，传感器节点传输信息时要比执行计算时消耗更多电能，传感器将 1 bit 信息传输 100 m 所需要的能量大约相当于执行 3 000 条计算指令消耗的能量[5]。在 E-G 方案密钥发现过程中，哈希运算、XOR 运算和节点间的通信是必须的，当密钥环大小为 200 时，通信对能量的消耗较大，在新节点增加时，E-G 方案必须重执密钥发现过程。因此，E-G 方案与本文协议的能量消耗处于同一层次。

3.4　抗毁性分析

在无线传感器网络中，节点被捕获是一种严重安全威胁，攻击者试图通过被捕获的节点获得其他节点的密钥信息。

假设 K 为节点间没有被截获的通信密钥，网络的规模为 n，k 表示平均邻近节点数量。在 E-G 方案中，当其他节点被捕获后，K 没有被捕获的概率[2]是 $1-m/S$ (S 和 m 分别为密钥池和密钥环大小)，当 x 个节点被捕获时，K 没有被捕获的概率是 $(1-m/S)^x$。因此，在 E-G 方案中密钥被捕获的概率为 $1-(1-m/S)^x$。基于 IBC 方案和本文协议仅存储了邻近节点间的通信密钥，所以，这 2 种方案密钥被捕获的概率分别为 $1-(1-k/C_n^2)^x$ 和 $1-(1-k/C_n^2)^{(1-e)x}$ (e 为密钥回收成功率)。若 $n=400$，$m=200$，$p=0.33$，$k=\sqrt{n}$，则 $e=0.25$。

不同方案抵抗捕获攻击的能力对比结果如图 2 所示。

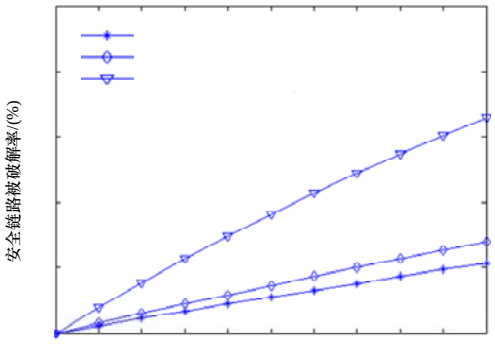

图 2　抵抗捕获攻击能力的对比结果

E-G 方案不仅存储与其直接通信节点的密钥，同时密钥环还存储其他节点密钥，这使得其网络的抗捕获攻击能力较差。本文协议与基于 IBC 方案仅存储邻近节点的密钥，但本文协议中的密钥更新与回收可以改善抵抗捕获攻击的能力，因此，其抵抗捕获攻击的能力明显好于其他 2 个方案。

4　结束语

密钥管理是无线传感器网络安全的研究热点，本文提出一种基于 ECC 的无线传感器网络密钥管理协议。通信密钥建立只要交换节点标志与密钥信息，有效地减少了通信数据，节约了节点的能量，延长了网络生存期。新节点增加、密钥更新和密钥回收协议的给出可以让无线传感器网络具有良好的可扩展性，提高了网络的抗攻击能力。通过性能分析验证了协议的有效性。

参考文献

[1] Wood A D, Stankovic J A. Denial of Service in Sensor Network[J]. IEEE Computer, 2002, 35(10): 89-95.

[2] Echenauer L, Gligor V D. A Key Management Scheme for Distributed Sensor Network[C]//Proc. of the 9th ACM Conf. on Computer and Communications Security. New York, USA: ACM Press, 2002: 41-47.

[3] Zhang Yanchao, Liu Wei, Lou Wenjing, et al. Location Based Compromise-tolerant Security Mechanisms for Wireless Sensor Networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 247-260.

[4] 向广利，朱　平，张俊红，等. 基于 ECC 的同态密钥协商[J]. 计算机工程与设计, 2007, 28(13): 374-376.

[5] 孙利民，李建中，陈　渝. 无线传感器网络[M]. 1 版. 北京: 清华大学出版社, 2005.

编辑　陆燕菲