基于零知识证明的安全认证方案*

陈 渊[1] 王欣蕾[2] 叶 清[1] 姜洪海[3]
(1. 海军工程大学信息安全系 武汉 430033)(2. 92001 部队 青岛 266021)
(3. 青岛市香港西路 11 号 35 号信箱 青岛 266074)

摘 要 为满足无线传感器网络的安全认证需求,针对传统认证方案中可能遭受的重放、中间人攻击的问题,提出了一种基于零知识证明的安全认证方案。网络中的合法节点与请求认证的节点间运行零知识证明协议,根据请求者的回答来验证请求节点的身份。分析表明,敌手无法从认证中获取关于秘密的信息,方案可以抵抗重放,中间人和节点间的合谋攻击,在能耗上也较小,适合资源受限的无线传感器网络。

关键词 无线传感器网络;零知识证明;安全认证
中图分类号 TP393 **DOI**:10.3969/j.issn1672-9722.2015.07.026

Security Authentication Scheme Based on Zero Knowledge Proof

CHEN Yuan[1] WANG Xinlei[2] YE Qing[1] JIANG Honghai[3]
(1. Department of Information Security, Navy University of Engineering, Wuhan 430033)
(2. No. 92001 Troops of PLA, Qingdao 266021)
(3. NO. 65 Box, NO. 11 West of Hongkong Road, Qingdao 266074)

Abstract In order to satisfy the safety certification requirements of wireless sensor networks, and solve the replay and man in the middle attack problem in traditional authentication, a security authentication scheme based on zero knowledge proof is proposed. In the scheme, the zero knowledge protocol is launched between the request node and the legal nodes, which can identify the identity of the request node according to the answers. It is analyzed that our scheme can resist replay attacks, man in the middle attack and collusion attack, while the attacker cannot gain any information about the secret. The consumption of the scheme is light, which can apply to the source limited wireless sensor networks.

Key Words wireless sensor networks, zero knowledge proof, security authentication
Class Number TP393

1 引言

随着微电子技术、计算机技术和无线通信技术的不断发展,无线传感器网络作为一个新的应用领域,已成为研究的热点。但是由于无线传感器网络具有节点能量有限、处理能力弱、存储空间小等特点,使其容易遭受各方面的威胁。主要有物理破坏、节点注入、窃听、重放、欺骗等,为了保障传感器网络的安全,必须对接入网络的节点合法性进行认证。

目前,在无线传感器网络安全认证方面主要有以下几种方法:1) 采用对称密码体制[1],基本思想是使用一定的方法使通信节点间得到相同的会话密钥;2) 采用非对称密码体制[2],相比对称密码体制安全性高,但是计算较复杂;3) 基于身份的密码体制[3],将身份作为公钥,避免了公钥体制中获取公钥的困难;4) 分布式认证方案[4],采用秘密共享的思想对秘密进行分割,由多个节点共同参与认证。但是这些认证方式在证明自己身份的同时,或多或少会暴露自己的秘密信息,这些信息可能会给

* **收稿日期**:2015 年 1 月 18 日,**修回日期**:2015 年 2 月 23 日
基金项目:湖北省自然科学基金(编号:2011CDB052);中国博士后科学基金(编号:2012M512132)资助。
作者简介:陈渊,男,硕士研究生,研究方向:无线传感器网络安全。王欣蕾,女,助理工程师,研究方向:网络安全。叶清,男,博士,副教授,硕士生导师,研究方向:信息与网络安全。姜洪海,男,工程师,研究方向:网络安全。

恶意攻击者可乘之机。零知识证明可以在证明自己知道某秘密的情况下使验证者无法从认证中获得关于秘密的任何信息。

本文提出了一种基于零知识证明的安全认证方案,方案采用了基于离散对数难题的零知识证明协议,被认证节点同多个节点进行零知识证明协议交互,每同一个节点进行交互就相当于执行了一轮零知识证明协议,那么执行 m 轮零知识证明协议就相当于被 m 个节点进行认证。

2 相关基础知识

2.1 零知识证明的基本原理

可以通过一个洞穴问题来解释零知识证明的基本原理[5],如图1所示。C 和 D 之间存在一个密门,并且只有知道咒语的人才能打开。P 知道咒语并想对 V 证明,但证明过程中不想泄露咒语。

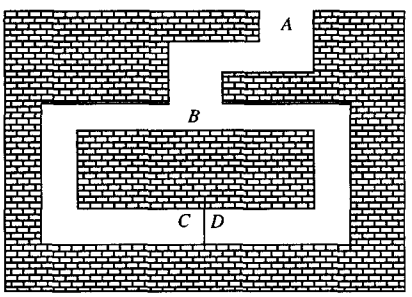

图1 零知识洞穴问题示意

步骤如下:

1) V 站在 A 点;

2) P 一直走进洞穴,到达 C 点或者 D 点;

3) 在 P 消失在洞穴中之后,V 走到 B 点;

4) V 随机选择左通道或者右通道,要求 P 从该通道出来;

5) P 从 V 要求的通道出来,如果有必要就用咒语打开密门;

6) P 和 V 重复步骤1)至5)m 次。

如果 P 不知道这个咒语,那么只能从进去的路出来,如果在协议的每一轮中 P 都能按 V 要求的通道出来,那么 P 所有 m 次都猜中的概率是 $1/2^m$。经过16轮后,P 只有1/65536的机会猜中。于是 V 可以假定,如果所有16次 P 的证明都是有效的,那么他一定知道开启 C 点和 D 点间的密门的咒语。

目前关于零知识证明的协议主要是用于进行数字签名[6~8],近几年随着无线传感器网络的发展,零知识证明也逐渐被应用到无线传感器网络的认证中[9~12]。下面介绍本文用到的一种基于椭圆曲线上离散对数难题的零知识证明方案。

2.2 零知识证明方案

设 F_q 为一个有限域,椭圆曲线为 E,Q 为椭圆曲线 E 上的一个点,且 $Q=nP$,n 为秘密。公开点 P,Q 和椭圆曲线 E。具体方案如下[13]:

设 P 与 V 分别是证明者和验证者。P 想向 V 证明他知道秘密 n,但又不想暴露它,他们可以按下列步骤来进行:

Step1:P 随机选择一整数 r,$r<q$。计算 $P_1=rP$,$P_2=(n-r)P$,并将 P_1 和 P_2 发送给验证者 V。

Step2:V 随机要求 P 发送 r_i,$i=1,2$,其中 $r_1=r$,$r_2=n-r$。

Step3:V 收到 r_i 后,验证 $P_i=r_iP$ 和 $P_1+P_2=Q$ 是否成立。

重复以上三步 m 次,直到 V 相信 P 知道秘密 n。

可以证明 P 每轮能够成功欺骗 V 的概率为1/2,因为若 P 不知道秘密 n,P 要想成功欺骗 V,P 可以进行如下过程:

P 选择一个整数 r,并记 $P_1=rP$,$P_2=Q-P_1$,然后按上述步骤发送给 V,假设 V 要求 P 传送 $r_1=r$,它恰好可以提供 r,这时 P 成功欺骗了 V。假设 V 要求传送与 P_2 对应的数 r_2,因为 P 不知道秘密 n,而通过 P_2 得到对应的数 r_2 是一个基于椭圆曲线上的离散对数问题,所以 P 无论如何也得不到 r_2。因此,P 在每一轮能够成功欺骗 V 的概率为1/2,经过 m 轮后,P 能成功欺骗 V 的概率为 $1/2^m$。所以经过充分大的次数后,如果 P 每次均能正确回答,则 V 相信 P 知道秘密 n。

经过上述过程,P 向 V 证明了自己知道秘密 n 而没有向 V 透露关于 n 的任何信息。

3 安全认证方案

传统的安全认证方案通常在证明自己身份的同时,交互过程中的信息可能被攻击者利用进行重放、冒充,零知识证明可以在证明自己知道某秘密的情况下而不暴露自己的秘密,同时验证者不能从认证过程中得到关于秘密的任何信息,鉴于这一特性,本文提出了一种基于零知识证明的安全认证方案。具体方案如下:

假设 Q 是请求被认证的节点,B 是基站节点,S 是其他合法节点。具体的认证过程如下:

1) 认证初始化:节点基站为每个节点设置唯一的身份ID,并预置系统参数,系统参数设置如下:令 p 为一个大素数,$F_p=\{0,1,2,\cdots,p-1\}$ 是模 p 的有限域,E 是定义在有限域 F_p 上的椭圆曲线,P 是 $E(F_p)$ 上的基点,阶为 q,则系统参数为 p,

E,q,P;

节点部署前，基站根据节点的身份 ID 为所有传感器节点生成秘密 N，具体生成过程如下：设某节点 C 的身份标识符为 ID_C，则节点 C 的秘密为 $N_C=hash(ID_C \| K)$，其中 K 为基站的主密钥，该秘密作为节点加入网络进行认证的凭证。

2) 认证过程：

(1)当节点 P 请求加入网络时，P 向基站提交自己的身份 ID_P，基站生成 P 的公开秘密 $Q=sP$ 其中 $s=hash(ID_P \| K)$。将 Q 进行广播。

(2)节点 P 按照上述零知识证明协议生成随机数 r，计算 $P_1=rP$，$P_2=(s-r)P$，并将 P_1 和 P_2 进行广播。

(3)假设与 P 邻近的 t 个节点 $V_1,V_2,\cdots,V_t$ 收到了 P 的广播，$V_1,V_2,\cdots,V_t$，首先验证 $P_1+P_2=Q$ 是否成立，若有一个节点验证不成立，则向其簇首或者基站发送验证失败消息，认证失败，拒绝 P 加入网络。否则，$V_1,V_2,\cdots,V_t$ 各自随机选择 $i=1$ 或 2，发送给节点 P。

(4)节点 P 按收到消息的顺序依次回复 r_i($i=1$ 或 2 为收到 $V_1,V_2,\cdots,V_t$ 的问询)。

(5)$V_1,V_2,\cdots,V_t$ 收到应答后，验证 $P_i=r_iP$ 是否成立。若有一个节点验证失败，则拒绝 P 加入网络，P 认证失败。

每一个节点的认证过程流程图如图 2 所示。

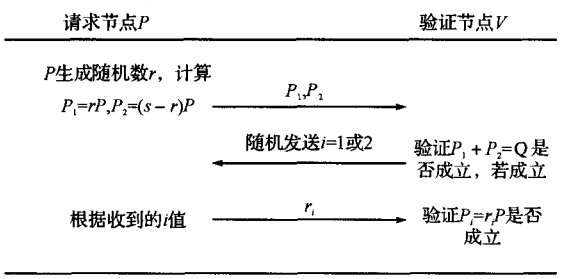

图 2　认证过程图

4　方案性能分析

4.1　安全性分析

1) 本文采用的零知识证明方案是基于椭圆曲线上的离散对数难题来设计实现的，经过 m 次协议交互后验证者 P 能成功欺骗验证者 V 的概率为 $1/2^m$，要通过 16 个节点的认证的概率为 1/65536，所以通过零知识证明协议能够认证节点 P 的身份，同时整个认证过程中，验证节点或者恶意节点无法从认证中获取任何有关节点 P 的秘密信息，因此，本文的认证方案是安全的。

2) 部署前基站根据节点的身份为每个节点预置了秘密信息，即使某个节点被捕获也不会威胁到整个网络的安全，节点之间的安全性是相互独立的，认证过程中的消息交互也没有传输关于秘密任何信息或信息的变体，节点的秘密参与的计算始终在本地进行，因此，本文的认证方案可以抵抗重放、冒充和中间人攻击。

3) 方案采用多个节点对请求者执行零知识证明协议，可以有效避免了恶意节点为了扩大势力进行的合谋攻击，多个节点中只要有一个节点没有通过认证，请求者就无法加入网络，所以方案是抗合谋攻击的。

4.2　效率分析

在计算量上，由于在每轮零知识证明协议中，请求者和验证者均只需要进行两次椭圆曲线上的加法运算，每次认证需进行 m 轮零知识证明协议，因此完成一次认证需要进行 $4m$ 次椭圆曲线上的加法运算，没有复杂的点乘运算和幂指数运算，运算开销较小。

在存储空间上，每个节点只需存储系统公共参数和自身的秘密信息，没有复杂的公钥和证书，存储开销较小。

在通信开销上，每轮完整的零知识协议交互，验证节点只需进行一次发送和两次接收消息，通信开销不大。对于请求节点，由于需要进行 m 轮零知识证明协议主，通信开销是验证节点的 m 倍，因此，整体来讲，一次认证对网络的能耗不大。

5　结语

本文针对传统认证方案中可能遭遇重放、中间人攻击的问题，提出了一种基于零知识证明的安全认证方案，网络中的多个合法节点对请求加入网络的节点进行零知识证明协议交互，验证节点的身份，在确认节点身份的同时，验证者和恶意节点无法从认证中获取任何请求节点的秘密信息，方案可以抵抗重放和中间人攻击，也是抗合谋攻击的，协议在计算、存储、能耗方面的性能上也有一定优势。

参 考 文 献

[1] Qiu Y, Zhou J Y, Baek J, et al. Authentication and Key Establishment in Dynamic Wireless Sensor Networks[J]. Sensors, 2010: 3718-3731.

[2] Yeh H L, Chan T H, Liu P C, et al. A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography[J]. Sensors, 2011: 4767-4779.

[3] Peng S W. An ID Based multiple authentication

schemes against attacks in wireless sensor networks [C]//Proceedings of IEEE CCIS,2012:1436-1439.

[4] Bauer K, Lee H. A distributed authentication scheme for a wireless sensing system[C]//Proceedings of the 2th International Workshop on Networked Sensing Systems, San Diego,2005:210-215.

[5] 吴世忠,祝世雄,张文政,等译. 应用密码学[M]. 北京:机械工业出版社,2006:71-72.

[6] 汤鹏志,李彪. Schnorr 数字签名的零知识证明[J]. 微电子学与计算机,2012,29(6):177-179.
TANG Pengzhi, LI Biao. Zero-knowledge proof Scheme of Schnorr digital Signature[J]. Microelectronics & Computer,2012,29(6):177-179.

[7] 王平水. 基于零知识证明的签名方案研究[J]. 计算机工程与设计,2007,28(16):3834-3836.
WANG Pingshui. Study on signature schemes based on zero-knowledge proof[J]. Computer Engineering and Design,2007,28(16):3834-3836.

[8] 舒麟,廖闻剑,彭艳兵. 拥有 DSA 数字签名的零知识证明[J]. 计算机工程与应用,2011,47(16):120-121.
SHU Lin, LIAO Wenjian, PENG Yanbing. Zero-knowledge proof scheme of possessing DSA digital signature[J]. Computer Engineering and Applications, 2011,47(16):120-121.

[9] Keith S, Lin S. Zero-knowledge proofs as authentication method in wireless sensor networks[J]. Cryptography and Network Security Final Project Report, 2007:1-5.

[10] Parbat V, Manikrao T, Tayade N, et al. Zero Knowledge Protocol to design security model for threats in WSN[J]. International Journal of Engineering Research and Applications (IJERA), 2012: 1533-1537.

[11] VamsiRam K, Venkateswarlu B L. Network Security Management in Wireless Networks through Zero Knowledge Proof[J]. International Journal of Advanced Research in Computer Science and Software Engineering,2012,2(9):185-191.

[12] Udgata S K, Mubeen A, Sabat S L. Wireless Sensor Network Security Model using Zero Knowledge Protocol[C]//Communications(ICC), 2011 IEEE International Conference on IEEE,2011:1-5.

[13] 韩德,郑素文. 基于椭圆曲线群上的零知识证明[J]. 装甲兵工程学院学报,2010,24(6):92-94.
HAN De, ZHENG Suwen. Zero-knowledge Proof Schemes Based on Elliptic Curve Groups[J]. Journal of Academy of Armored Force Engineering, 2010, 24 (6):92-94.

(上接第 1269 页)

[5] 董晓明,等. 美海军 DDG-1000 全舰计算环境体系结构探析[J]. 中国舰船研究,2012,7(6):7-14.
DONG Xiaoming, SHI Chaoming, HUANG Kun, et al. Analysis on the Architecture of USN DDG-1000 Total Ship Computing Environment[J]. Chinese Journal of Ship Research,2012,7(6):7-14.

[6] 李乔,郑啸. 云计算研究现状综述[J]. 计算机科学,2011,38(4):32-37.
LI Qiao, ZHENG Xiao. Research Survey of Cloud Computing[J]. Computer Science,2011,38(4):32-37.

[7] 孔飞. 构建军事云计算体系提升军队信息化水平[J]. 地面防空武器,2011,42(1):25-28.
KONG Fei. Build a Military Cloud Computing System and Enhance the level of Military information [J]. Land-Based Air Defence Weapons,2011,42(1):25-28.

[8] 李昭锐,吴学智,何如龙. 浅析云计算的军事应用[J]. 通信技术,2011,44(9):120-122.
LI Zhaori, WU Xuezhi, HE Rulong. Cloud Computing in Military Application[J]. Communications Technology,2011,44(9):120-122.

[9] 赵菲,刘俊杰. 云计算在指挥信息系统建设中的应用[J]. 通信技术,2012,45(4):7-9.
ZHAO Fei, LIU Junjie. Application of Cloud Computing in Construction of Command Information System [J]. Communications Technology,2012,45(4):7-9.

[10] 张秋江,王澎. 云计算的安全问题探讨[J]. 信息安全与通信保密,2011,44(5):94-95.
ZHANG Qiujiang, WANG Pen. Cloud computing security issues discussed[J]. Information security and communication security,2011,44(5):94-95.