无线传感器网络上基于Tate对的身份认证方案设计与实现

王卫红 崔义玲 陈铁明
(浙江工业大学软件学院 杭州 310023)

摘 要 身份密码学已在安全认证中得到了较广泛的应用。双线性对是近几年发展起来的一个构造密码体制的重要工具。在研究双线性对构造密码体制的基础上,提出了一个基于ID的标准身份认证方案。该方案在被动攻击下可防止冒充,同时在性能上比较高效。在TinyOS的传感器网络环境下实现了该身份认证方案。仿真结果证明该认证方案有效可行。

关键词 无线传感器网络,双线性对,基于ID身份认证,TinyOs
中图法分类号 TP393.08 **文献标识码** A

Design and Implementation of a Standard Identity-based Authentication Protocol on Wireless Sensor Network

WANG Wei-hong CUI Yi-ling CHEN Tie-ming
(College of Software, Zhejiang Technology University, Hangzhou 310023, China)

Abstract Identity cryptography has been widely used in Security Authentication. Bilinear pairing is an important tool for constructing the cryptography developed in recent years. Based on the research of the bilinear pairing, this paper proposed a standard identity-based authentication protocol. This protocol is secure against impersonation under passive attack and has high efficiency. This paper also implemented the authentication protocol in the platform of TinyOs. Finally, the simulation results show that the authentication protocol is effective in the wireless sensor network.

Keywords Wireless sensor network, Bilinear pairing, Identity-based authentication protocol, TinyOs

1 引言

无线传感器网络是由大量的无线传感器节点组成的无线自组网络,它具有自组织的特点,节点一旦分布,多数情况下无法人为干预,所以无线传感器网络的安全问题与传统的网络安全问题有很大的不同。在传感器网络中,敌方节点很可能通过冒充节点的方式对消息进行注入或发送伪冒消息,接收者必须确认消息是从正确的节点发送过来的,然后才能对其进行处理,因此需要对发信方的身份进行认证,同时当有新节点加入时,也必须验证其身份后才能进行通信。

公钥技术是信息安全领域最广泛采用的手段之一。许多学者研究公钥算法在传感器节点上的实现,取得了一定的成果。最早Gura等在8位微控制器上实现了ECC和RSA算法[1]。2002年,R. Watro等人提出了基于低指数级RSA的TinyPK实体认证方案[2]。2007年,在An Liu, Peng Ning等人开发的TinyECC基础上[4],Leonardo B等5位巴西学者实现了Tate对在传感器节点上的运算[5],这是基于Tate对的密码学在传感器网络上的首次实现。本文在研究双线性对理论的基础上,结合身份认证的密码学基础,提出了一种基于ID的身份认证方案,并在TinyOS环境下,基于TinyECC和TinyTate实现了该方案。

2 背景知识

2.1 双线性对基本理论

双线性对是近几年发展起来的一个构造密码体制的重要工具。可以通过椭圆曲线性质构造出Weil对或Tate对。

$(G_1,+)$和$(G_2,\cdot)$是阶q的两个群,q是大素数,G_1是加法群,G_2是乘法群。基于G_1和G_2可构造双向性映射e:$G_1\times G_1->G_2$。该映射必须满足下面的属性:

1)双线性:我们说一个映射$e:G_1\times G_1->G_2$是双线性的,如果$e(aP,bQ)=e(P,Q)^{ab}$,则对于所有的$P,Q\in G_1$且$a,b\in Z$成立。

2)非退化性:若P是G_1的生成元,则$e(P,P)$是G_2的生成元;存在$P\in G_1$,满足$e(P,P)\neq 1$。

3)可计算性:有一个有效的算法计算$e(P,Q)$,对于任意的$P,Q\in G_1$。

2.2 密码学中的几个困难问题

所有的密码体制都是基于某些困难问题的,比如RSA基于大数分解难题,而ECC基于离散对数难题。而所有基于双线性对密码体制也是基于离散对数难题的。

定义1(椭圆曲线离散对数难题,ECDLP) 给定定义在有限域F_p上的椭圆曲线E,基点$P\in E(F_q)$,阶为n。$Q\in E$

到稿日期:2009-02-25 返修日期:2009-05-12 本文受国家863高新技术计划项目(2006AA10Z235),国家自然科学基金项目(60773115),浙江省自然科学基金项目(Y106290)资助。

王卫红(1969-),男,博士,教授,主要研究领域为计算机应用、信息安全,E-mail:wwh@zjut.edu.cn;崔义玲(1986-),女,硕士,主要研究领域为网络信息安全、密码学;陈铁明(1978-),男,博士,讲师,主要研究领域为网络信息安全、密码学。

(F_q)，其中 $Q=IP, I\in n$，计算 I 是困难的。

根据上述定义，在 l 足够大的情况下，无法轻易通过 Q 和 P 计算得到 l。

定义 2（计算 Diffie-Hellman 问题） 给定 $aP, bP, P\in G_1$，对于 $a, b\in Z_n^*$，计算 abP 是困难的。

我们称计算 Diffie-Hellman 问题为 CDH 问题，该问题依赖于 G_1 上的 ECDLP 问题的困难性，目前还没有有效的方法解决该问题。

定义 3（双线性 Diffie-Hellman 问题） 对于给定的 aP, $bP, cP\in G_1$ 计算 $e(P,P)^{abc}$，其中 $a, b, c\in Z_n^*$ 未知。

我们称双线性 Diffie-Hellman 问题为 BDH 问题，该问题依赖于 G_1 上的 CDH 问题的困难性。显然，目前还没有有效的方法可以解决该问题。

2.3 TinyOs 环境简介

TinyOS 是加州大学 Berkeley 分校为无线传感器网络开发的一种微型嵌入式操作系统。针对无线传感器网络内节点众多以及多并发操作的工作方式，该操作系统采用了轻量级线程、主动消息通信技术、事件驱动模式和组件化编程技术的体系结构，有助于提高传感器网络的性能，发挥硬件的特点，降低功耗并简化了应用的开发。

TinyOS 是由 NesC 语言编写和实现的。NesC 是一种类 C 语法的、基于组件的编程语言。所以 TinyOs 采用组件模型，其组件自底向上分为：硬件抽象组件、合成组件和高层次的软件组件。

TinyECC 是北卡罗莱纳州立大学（NCSU） An Liu, Peng Ning 等人开发提供的一个基于 TinyOS，由 Nesc 编写的椭圆曲线密码体制的基本运算库。该库主要由两部分组成：

大数运算：大数运算由 RSAEF2.0 修改而来，主要包括大数的加减乘除及相关的取模运算等。对于不同的节点平台提供了不同的汇编指令优化速度。

椭圆曲线基本运算：该功能基于大数运算，实现了椭圆曲线上的一些基本运算，如点加、倍点和标量乘等。其基本结构如图 1 所示。

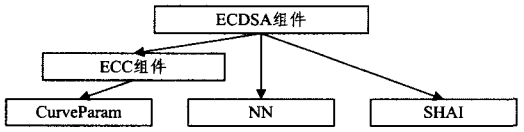

图 1 TinyECC 结构

ECDSA 是基于 ECC 的一个签名协议。其中 ECC 组件是 TinyECC 的核心，它通过调用 CurveParam 接口来初始化一条椭圆曲线，通过 NN 大数操作接口来实现其内部相关的大数运算。

TinyTate 是由巴西坎皮纳斯大学 Leonardo B 等五位学者在一个传感器上的 Tate 对运算的一个实现。它基于 TinyECC 所提供的椭圆曲线的基本运算，利用优化的 Miller 算法，在传感器网络上实现了 Tate 对的运算。并在 MICA2 节点上进行了测试，其效率如表 1 所列[5]。

表 1 Tate 对在 Mica2 节点上的运行效率

时间(seconds)	RAM(Bytes)	ROM(bytes)
30.21	1831	18484

随着硬件速度提高、预分发机制的应用和对该双线性映射运算次数的控制，该负担在传感器上将逐渐被接受。

3 基于 ID 的标准身份认证方案

3.1 方案设计

基于身份的密码体制由 Shamir 于 1984 年最早提出[6]。Boneh 和 Franklin 在 2001 年以 weil 对构造出了基于身份密码体制（Identity-Based Encryption）[7]。Boneh-Boyen 利用双线性对提出了一个标准模型下的短签名方案[8]。D. Boneh, B. Lynn 和 H. Shacham 提出了基于双线性对的 BLS 签名系统[9]。基于双线性对的密码体制近年来成为密码学的一个研究热点。

一个规范的身份认证方案由承诺、询问和应答 3 个部分组成。本文基于双线性对提出了一个基于 ID 的标准单向身份认证方案。方案设计分为如下 3 个阶段。

1）系统初始化

运行系统初始化算法，生成两个阶为 q 的点群 G_1, G_2 以及双线性映射 $e: G_1\times G_1=G_2$。其中 $(G_1, +)$ 和 $(G_2, \cdot)$ 是阶 q 的两个群，q 是大素数。G_1 是加法群，G_2 是乘法群。

随机选择点群 G_1 上的点 P 作为生成元。选择 $s\in Z_p$ 为系统主密钥。计算 $P_s=s*P$ 作为系统公钥。通过 P_s 和 P 来计算主密钥 s 是一例 CDH 难题。

选择一个哈希函数 H_1。H_1 为任何字符串到 G_1 的映射：$H_1=\{0,1\}^*->G_1$。得到系统参数如下：

$Params=\{G_1, G_2, e, P, n, H_1, s, P_s\}$

系统主密钥由系统保存，其它作为公共参数公布。

2）公私钥提取

用户 A 通过其 ID 哈希映射得到其公钥 $D_a=H_1(ID)$，并公布该信息作为其公钥。并由系统通过主密钥计算 $P_a=sD_a$ 作为其私钥，分发给 A，由 A 自己保存。所有的节点都通过这样一个过程获取公私钥。

3）身份认证

假设两个节点 Alice(A) 和 Bob(B) 进行通信，A 作为示证方，B 作为验证方。那么 A 和 B 的通信方案数据流程如图 2 所示。

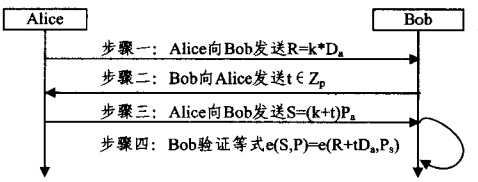

图 2 方案数据流程图

详细过程如下：

第一步 A 随机选择数 $k\in Z_p$，利用其公钥 D_a 计算 $R=k*D_a$，并向 B 发送 R。

第二步 B 收到 R 后随机选择数 $t\in Z_p$，并向 A 发送 t。

第三步 A 收到 t 后，利用其私钥 P_a 和 t 计算 $S=(k+t)P_a$，并向 B 发送密文 S。

第四步 B 收到 S 后计算 $e(S,P)$ 是否与 $e(R+tD_a, P_s)$ 相等，以完成对 A 的认证。显然若是式子成立则完成了对 A 的身份确认。验证过程如下：

(1) $e(S,P)=e((k+t)P_a, P)=e(kP_a, P)*e(tP_a, P)$

(2) $e(kP_a, P)*e(tP_a, P)=e(R, P_s)e(tD_a, P_s)=e(R+tD_a, P_s)$

3.2 安全性讨论

讨论该方案在被动攻击下满足不可冒充性。

定义 4 被动攻击主要是指敌者收集信息不是通过访问来获取数据。数据的合法用户对这种活动一点也不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。

首先，攻击者无法获得系统的主密钥，因为通过 P_s，P 和 $P_s=s*P$ 来计算主密钥 s 是一例 CDH 难题。

其次，攻击者若想要冒充节点 A，则必须获得私钥 P_a。攻击者若要通过 S,t 和 $S=(k+t)P_a$ 来计算 P_a，就需要知道 k。它若想通过 R 计算 k 从而计算 P_a，就遇到了 ECDLP 问题，即它无法通过 R,D_a 和 $R=k*D_a$ 来计算 k，从而无法得到 A 的私钥 P_a。

最后，如果攻击者通过两次监听和收集信息，可以获得第二步的两个不同的 t_1,t_2，并且获得两个不同的 S_1,S_2，则想通过 $S_1=(k_1+t_1)P_a$ 和 $S_2=(k_2+t_2)P_a$ 来计算 P_a，但是由于 R 是随机选择的，在 k 的范围足够大的情况下，攻击者很难截获两次相同的 R，因此无法通过 $P_a=(t_1-t_2)^{-1}(S_1-S_2)$ 来计算 P_a。

可见，攻击者若想要冒充节点 A，它就必须能先解决 CDH 问题、ECDLP 问题和大数分解问题中的一个问题。显然，这些问题在现有情况下认为是难解问题，所以该方案在被动攻击下是节点无法冒充的，从而保证了身份认证的安全性。

3.3 性能分析

整个方案中所需的主要运算是椭圆曲线点乘和双线性映射。其中双线性映射过程消耗最大。观察整个协议流程的主要运算在节点的分布如表 2 所列。

表 2 节点所需运算次数

节点	点乘运算(次)	双线性映射运算(次)
示证方	2	0
验证方	0	2

对于示证方的 2 次点乘运算和验证方 2 个双线性映射运算完成一个标准认证是比较省时的。方案过程通过 3 次通信完成符合认证也是符合标准的。

4 方案实现和结果分析

方案分为系统初始化、公私钥分发和身份认证 3 个阶段。考虑在传感器上实现，节点资源有限，所以在本方案不设置 PKG 中心来分发私钥。最终通过节点 ID 进行预先分发的机制来实现。系统初始化在 PC 上实现，系统公开参数预先分发给节点。并同时根据节点的 ID 对节点的公私钥预先分发。这样减少了一个 PKG 的消耗，也解决了私钥分发的问题，对于传感器网络来说是一个比较合理的选择。

在 TinyOS 环境下，基于 TinyECC 和 TinyTate 完成了该方案的实现。整个代码的组件调用关系结构如图 3 所示。

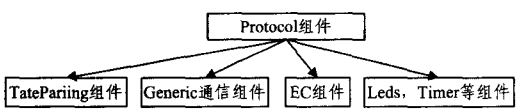

图 3 组件调用关系图

观察整个方案可以发现最为关键的两个运算是双线性映射和椭圆曲线点乘。Protocol 组件是协议方案的核心，实现了认证方案的整个流程。通过调用 Tate Pairing 组件实现了 Tate 配对映射的运算。通过调用 ECC 实现了点乘运算。而通过调用 TinyOs 自带的 Generic 通信组件实现了节点间的通信。通过 Leds 组件控制指示灯和 Timer 组件实现了定时触发功能。

程序在 PC 上使用 TOSSIM 模拟的结果和过程如图 4—图 7 所示。

1)Alice 产生随机数 r 并向 Bob 发送 R。

图 4 Alice 向 Bob 发送 R

2)Bob 随机选择 $t\in Z_p$，并向 B 发送 t。

图 5 Bob 发送随机数 k

3)A 利用其私钥 P_a 计算 $S=(k+t)P_a$，并向 B 发送 S。

图 6 Alice 发送 $S=(k+t)P_a$

4)B 计算 $e(S,P)$ 是否等于 $e(R+tD_a,P_s)$。

图 7 Bob 计算 $e(S,P)$ 和 $e(R+tD_a,P_s)$ 是否相等

协议通过 3 次通信，最后，由验证方 Bob 通过计算 $e(S,P)$ 与 $e(R+tD_a,P_s)$ 是否相等来完成对 Alice 的验证。

结束语 本文对 TinyOs 平台，TinyECC，TinyTate 做了一个简单介绍。给出了一个基于 ID 的标准身份认证方案，证明了其在被动攻击下可防止冒充，同时性能上比较可行。最后基于 TinyECC 和 TinyTate，实现了该身份认证方案，分析其结果确实可行。基于对的密码学应用能提供更多灵活的密码学应用。下一步工作将在传感器网络上寻找和设计更多高效的方案，以期为传感器网络安全提供更多的解决途径。

参 考 文 献

[1] Gura N, Patel A, Wander A. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[C]// Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004). August 2004

[2] Watro R, et al. TinyPK: secuting sensor networks with public key technology[A]//Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks[C]. 2005:135-142

[3] Ning Peng, Liu An, Du Wenliang. Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Network [R]. North Carolina State University, Department of Computer Science, Revised September 2006

[4] Liu An, Ning Peng. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks[C]//Proceedings of the 7th International Conference on Information Processing n Sensor Networks (IPSN 2008). SPOTS Track, April 2008

(下转第 141 页)

增大而增大。

4.2 仿真结果

我们通过仿真试验来比较网络编码传输与传统网络传输的性能差异。试验中假设信道传输可靠，对于不可靠的情况，由于通告机制的存在，系统可以依据通告的信息再次进行编码，编码算法一样，从而使得网络编码在信道损失情况下，同样体现其性能增益。在仿真模拟试验中，首先假定链路存在概率 $p=0.75$ 的情况下，网络节点数为 30 时信息源节点数的变化对编码性能增益的影响；而后考虑在信息源节点数 K 一定的情况下，链路存在概率的变化对编码性能增益的影响。

4.2.1 信息源节点数对编码性能的影响

在此仿真试验中，首先通过节点之间的链路存在概率 p 随机生成 50 个网络拓扑矩阵，随后依据不同的信息源节点数随机选择信息源节点构建前 K 个时隙的接收矩阵(假定中心节点在接收到所有信息源节点的消息后进行编码传输)，再用贪心近似编码算法进行编码传输，并在此过程中依据命题 1 对编码最优值进行统计。依据到节点链路存在概率 $p=0.75$、不同的信息源节点数，得到的网络编码传输策略与传统策略的比较如图 5 所示。图 6 是对应设置下网络编码传输策略相对传统策略的增益图。

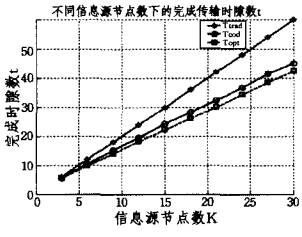

图 5 不同信息源节点下完成传输时隙对比图

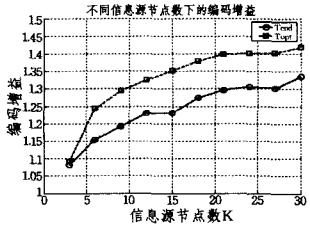

图 6 不同信息源节点下网络编码传输增益

从图 5 中可以看出，随着信息源节点的增加，由于需要传输的消息的增加，两种传输策略完成所有消息的传输的时隙也相应增加，但是在网络编码传输策略下，其增长的速率较低。从图 6 中可以看出网络编码的增益区间为(1.2,1.5)，并且增益随着信息源节点的增加而增大，这是由于更多的信息源分组，可以使得编码的效率更高。

4.2.2 链路存在概率对编码性能的影响

图 7 是参与节点数为 30、信息源节点数为 18 时，不同的链路编码概率条件下，网络编码传输策略与传统策略的比较图。图 8 是对应设置下网络编码传输策略相对传统传输策略的增益图。从图中可以看出，网络编码传输的次数随着节点之间的链路存在概率增大而减小，也即网络编码的增益随着节点之间链路存在概率的增大而增大。同时在链路存在概率大于 0.7 时，网络编码的增益可以达到 30%之上。此外，从图 5—图 8 中可以看出，本文贪心编码算法的编码效果较为接近理论的最优编码增益。

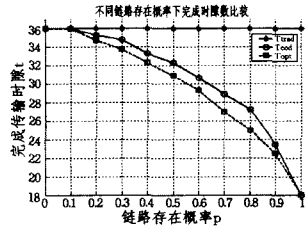

图 7 不同链路存在概率下传输完成时间图

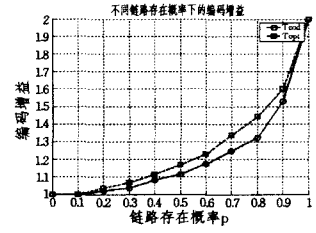

图 8 不同链路存在概率下的编码增益

结束语 本文针对战场中基于中心的作战应用网络场景，抽象出 Many-to-all 的实时业务模型，并将网络编码应用于此模型中。基于适合作战人员决策应用的性能指标：所有节点完成接收到所有信息源信息的时间，分析得出了基于中心的网络中仅在中心节点进行编码操作能达到编码的最优性能的结论，这在很大程度上简化了在实际作战应用中的实现问题。同时针对中心节点的编码操作，提出了贪心算法，并对其性能进行了分析。最后通过仿真试验验证了贪心算法所获得的性能增益与理论增益相近，证明了网路编码传输策略能够在信息实时多播应用中取得很好的效果。

参 考 文 献

[1] Ahlswede R, et al. Network Information Flow[J]. IEEE Transactions on Information Theory, 2000, 46(4)

[2] Fragouli C, et al. Wireless Network Coding: Opportunities and Challenges[C]//MILCOM. 2007

[3] Chachulski S, et al. MORE: Trading Structure for Randomness in Wireless Opportunistic Routing[C]//SIGCOMM 07. 2007

[4] Basel K J, et al. Application of Network Coding in Tactical Data Networks[C]//MILCOM 08. 2008

[5] Kim M, et al. Integrating Network Coding into Heterogeneous Wireless Networks[C]//MILCOM 08. 2008

[6] Katti S, et al. XORs in The Air: Practical Wireless Network Coding[C]//SIGCOMM. 2006

[7] Rouayheb S Y E, et al. On the Minimum Number of Tran smissions in Single-Hop Wireless Coding Networks[C]//Proceeding of IEEE Information Theroy Workshop. 2007: 120-125

[8] 许胤龙，等. Ad hoc 网络中基于网络编码的可靠组播[J]. 中国科学技术大学学报，2008，38(7)：860-868

[9] J T C, et al. Automated Synthesis of Data Paths in Digital Systems[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and systems, 1986, 5(3): 379-395

(上接第 74 页)

[5] Oliveira L B, Aranha D, Morais E, et al. TinyTate: Identity-Based Encryption for Sensor Networks[D]. University of Campinas, Brazil

[6] Kashmir. Identity-based Cryptosystems and signatures Schemes [C]//Proceeding of Crypto'84. 1985: 47-53

[7] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing[C]// Kilian J, ed. Advances in Cryptology—Crypto 2001. Berlin, Heidelberg: Springer-Verlag, 2001: 213-229

[8] Boneh D, Boyen X. Short signatures without random oraches [A]// Advances in Cryptology- EUROCRYPT 2004[C]. Berlin: Springer-Verlag, 2004: 56-73

[9] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[C] // Advances in Cryptology-Asiacrypt'01, LNCS 2248. Springer-Verlag, 2001: 514-532