一种新的基于身份的 Ad hoc 认证和密钥协商方案

霍士伟 杨文静 李景智 申金山
(国防科技大学信息通信学院 西安 710106) (西安通信学院 西安 710106)

摘 要 现有 Ad hoc 网络中基于身份的认证和密钥协商方案是基于双线性对实现的,计算开销较大,并且存在密钥托管问题。针对该问题,提出了一种新的基于身份的认证和密钥协商方案。方案中,节点之间通过无双线性对的基于身份签名算法实现身份认证,通过 Diffie-Hellman 密钥协商技术建立会话密钥。分析表明,该方案不存在密钥托管问题,并且具有更高的执行效率。

关键词 Ad hoc 网络,认证,密钥协商,基于身份的密码体制
中图法分类号 TP309 **文献标识码** A

New Identity-based Authentication and Key Agreement Scheme in Ad hoc Networks

HUO Shi-wei YANG Wen-jing LI Jing-zhi SHEN Jin-shan
(Institute of Information and Communications, National University of Defense Technology, Xi'an 710106, China)
(Xi'an Communications Institute, Xi'an 710106, China)

Abstract The available identity-based authentication and key agreement schemes in Ad hoc networks are based on bilinear pairing with high computation cost, and the schemes also have the problem of key escrow. Considering the problem, a new identity-based authentication and key agreement scheme was proposed. Identity authentication was realized using identity-based signature without bilinear pairing. The session key was established using diffie-hellman key exchange technology. It is shown that the proposed scheme avoids the problem of key escrow, and has higher efficiency.

Keywords Ad hoc networks, Authentication, Key agreement, Identity-based cryptography

1 引言

Ad hoc 网络是一种移动多跳的无线网络,不依赖于固定的基础设施,通过移动节点的相互协作进行组网,具有资源受限和网络结构动态变化的特点[1]。Ad hoc 网络被广泛应用于各领域,如军事、航空和智能城市等。Ad hoc 网络具有链路开放、节点资源受限的特点,相比于传统网络,其面临更多的安全威胁。因此,安全是 Ad hoc 网络能否实施的关键。

认证和密钥协商是实现 Ad hoc 网络安全通信的基础,对构建安全的 Ad hoc 网络具有重要意义[1]。早期的 Ad hoc 网络认证和密钥协商方案大都利用传统基于证书的公钥体制来设计,能够提供较高的安全性[2-3]。但是,传统基于证书的公钥体制中由于需要复杂的证书管理过程,会造成较大的计算和通信开销。基于身份的公钥体制中由于公钥可以由公开信息直接推导得出,无需公钥证书对身份和公钥进行绑定,因此其计算和通信开销较小,适合在 Ad hoc 网络中应用[4]。近年来,一些采用基于身份公钥体制的 Ad hoc 网络认证与密钥协商方案被相继提出[4-5]。文献[4]提出了基于身份的 Ad hoc 网络密钥协商方案,其中通信双方只要一次交互就能建立会话密钥。但是,密钥协商过程中没有双向身份认证机制,同时密钥建立过程中由通信方提供密钥协商参数,通信方能够控制会话密钥是一个预先选择的值。文献[5]提出了一个更加安全的基于身份的 Ad hoc 密钥协商方案,该方案在密钥协商过程中提供了完善的双向身份认证机制,并且会话密钥协商参数由通信双方共同产生。上述基于身份的认证和密钥协商方案都是基于双线性对实现的,在密钥协商过程中,节点需要进行多次双线性对运算,计算开销过大。另外,基于身份的公钥体制具有密钥托管的缺陷,系统的主密钥如果被攻击者获得,攻击者就可以假冒网络中的合法节点,因此主密钥成为了系统安全的瓶颈。文献[6]提出了一种更加高效和安全的基于身份的签名算法,其只需要进行加法群上的点乘操作,避免了复杂的双线性对运算,具有较高的执行效率;同时,该算法不存在密钥托管问题,攻击者即使获得了系统主密钥,也无法获得完整的用户私钥,从而无法假冒合法节点。基于文献[6]中的基于身份的签名算法,本文设计了一种新的 Ad hoc 网络认证和密钥协商方案,节点不需要进行复杂的双线性对运算,并且不存在密钥托管问题,兼具安全性和性能上的优势。

2 基于身份的认证和密钥协商方案

本方案利用文献[6]中的基于身份的签名算法对密钥协商参数进行签名,节点之间通过验证签名来认证对方身份,然后利用 Diffie-Hellman 密钥协商技术建立会话密钥。假设网络中存在一个离线的私钥生成中心(Private Key Generate, PKG),PKG 在网络初始化时为节点生成了基于身份的公私钥对。假设每个网络节点拥有唯一的身份标识。方案包括系统初始化、认证与密钥协商两个阶段。

2.1 系统初始化

(1)给定安全参数 k,PKG 选择椭圆曲线 $E(F_p)$ 上的 q 阶

霍士伟(1985-),男,硕士,讲师,主要研究方向为无线网络技术,E-mail:shiweihuo@163.com;杨文静(1975-),女,博士,主要研究方向为体系结构建模;李景智(1987-),男,硕士,讲师,主要研究方向为网络管理技术;申金山(1984-),男,硕士,主要研究方向为无线网络技术。

循环加法群 G，G 的生成元为 P。随机选择 $s\in Z_q^*$ 作为系统主密钥，系统公钥为 $P_{pub}=sP\in G$。定义以下安全哈希函数：$H_1:\{0,1\}^*\times G\rightarrow Z_q^*$，$H_2:\{0,1\}^*\rightarrow Z_q^*$，$H_3:G\rightarrow\{0,1\}^*$。PKG 妥善保管 s，公开系统参数$\{G,q,P,P_{pub},H_1,H_2,H_3\}$。

(2)假设每个节点拥有唯一的身份标识 $ID_i\in\{0,1\}^n$，节点 ID_i 随机选择 $s_i\in Z_q^*$ 作为秘密数，计算 $R_1=s_iP$，然后将 R_1 和 ID_i 发送给 PKG；PKG 可以通过零知识证明方法确认节点 ID_i 具有与 R_1 对应的秘密数 s_i。PKG 对节点身份和 R_1 鉴定后，按如下步骤计算节点 ID_i 的部分私钥。

1)随机选择 $r_i\in Z_q^*$，计算 $R_2=r_iP$，$R_i=R_1+R_2$；

2)令 $h=H_1(ID_i,R_i)$，计算部分私钥 $d_i=r_i+sh$。

PKG 将 R_i 和 d_i 发送给节点 ID_i；节点 ID_i 通过检验 $(d_i+s_i)P=R_i+H_1(ID_i,R_i)P_{pub}$ 是否成立来验证部分私钥的正确性。

2.2　认证与密钥协商

当节点 A 与节点 B 通信时，通过以下步骤进行相互认证并协商安全的会话密钥。

(1)节点 A 选择 $x_A,y_A\in Z_q^*$，计算 $Y_A=y_AP$，$X_A=x_AP$，获取当前时戳 T_A，计算 $e_A=H_2(T_A,X_A,ID_A,R_A,Y_A)$ 和对 T_A 和 X_A 的签名 $z_A=y_A+e_A(d_A+s_A)$，然后发送消息$\langle ID_A,R_A,X_A,T_A,e_A,z_A\rangle$给节点 B。

(2)节点 B 收到消息后，检查时戳 T_A 的新鲜性。若 T_A 是新鲜的，则计算 $h_A=H_1(ID_A,R_A)$，$Y_A'=z_AP-e_A(R_A+h_AP_{pub})$，并验证 $e_A=H_2(T_A,X_A,ID_A,R_A,Y_A')$ 是否成立，若成立，则通过对节点 A 的认证。然后，节点 B 选择 $x_B,y_B\in Z_q^*$，计算 $Y_B=y_BP$，$X_B=x_BP$，获取当前时戳 T_B，计算 $e_B=H_2(T_B,X_B,ID_B,R_B,Y_B)$ 和对 T_B 和 X_B 的签名 $z_B=y_B+e_B(d_B+s_B)$，并发送消息$\langle ID_B,R_B,X_B,T_B,e_B,z_B\rangle$给节点 A。最后，节点 B 计算 $k_{AB}=H_3(x_BX_A)$作为会话密钥。

(3)节点 A 收到消息后，检查时戳 T_B 的新鲜性。若 T_B 是新鲜的，则计算 $h_B=H_1(ID_B,R_B)$，$Y_B'=z_BP-e_B(R_B+h_BP_{pub})$，并验证 $e_B=H_2(T_B,X_B,ID_B,R_B,Y_B')$ 是否成立，若成立，则通过对节点 B 的认证。然后，节点 A 计算 $k_{AB}=H_3(x_AX_B)$作为会话密钥。

通过上述过程，节点 A 与节点 B 能够确认对方为合法节点，并建立了会话密钥 $k_{AB}=H_3(x_AX_B)=H_3(x_BX_A)$。

3　方案分析

3.1　正确性分析

节点之间通过验证对方的签名，可以正确地认证对方的身份。以节点 B 对节点 A 进行认证为例，B 通过验证 $e_A=H_2(T_A,X_A,ID_A,R_A,Y_A')$ 是否成立来确认节点 A 身份的合法性。因为：

$$z_A=y_A+e(d_A+s_A) \tag{1}$$

式(1)两边同乘以 P，得：

$$z_AP=y_AP+e(d_A+s_A)P \tag{2}$$

由式(2)得：

$$z_AP=Y_A+e_A(r_A+s_A+sh_A)P \tag{3}$$

由式(3)得：

$$z_AP=Y_A+e_A(r_AP+s_AP+sh_AP) \tag{4}$$

由式(4)得：

$$z_AP=Y_A+e_A(R_A+h_AP_{pub}) \tag{5}$$

由式(5)得：

$$Y_A=z_AP-e_A(R_A+h_AP_{pub}) \tag{6}$$

由于：

$$Y_A'=z_AP-e_A(R_A+h_AP_{pub}) \tag{7}$$

由由式(6)、式(7)可得：

$$Y_A=Y_A'$$

因此：

$$\begin{aligned}e_A&=H_2(T_A,X_A,ID_A,R_A,Y_A)\\&=H_2(T_A,X_A,ID_A,R_A,Y_A')\end{aligned} \tag{8}$$

通过上述证明，可知式(8)成立，因此认证过程是正确的。

3.2　安全性分析

本方案利用基于身份的公钥密码体制，实现了 Ad hoc 网络节点之间的双向认证，并协商了安全的会话密钥。方案满足以下安全属性。

(1)已知会话密钥安全：本方案中节点 A 和节点 B 每次都会生成不同的会话密钥，并且每次协商密钥都选择了新的密钥协商参数 x_A 和 x_B，因此会话密钥之间是独立的，一个密钥的泄露不会影响另一个密钥的安全性。如果节点 A 与节点 B 的某次会话密钥泄露，攻击者仅可在本次交互中冒充节点 A 与节点 B 通信，或是冒充节点 B 与节点 A 通信，但不会影响到节点 A 与节点 B 间其他会话的安全性。

(2)前向保密性：方案中节点 A 与节点 B 长期私钥的泄漏不会影响之前建立的密钥的安全性。攻击者即使获得了节点 A 或节点 B 的长期私钥，甚至同时获得了两者的私钥，也无法得到节点 A 与节点 B 之前的密钥。密钥中包含节点 A 与节点 B 选择的密钥协商参数 x_A 和 x_B，网络中不直接传输这两个随机的密钥协商参数，而是传送 X_A 和 X_B。由椭圆曲线上离散对数问题的难解性可知，攻击者无法由公开信息得到 x_A 和 x_B，因此无法计算出历史会话密钥。

(3)主密钥前向安全性：攻击者即使获得了 PKG 的主密钥，也无法获得节点 A 与节点 B 之前建立的会话密钥。因为，攻击者仅能利用主密钥计算出节点 A 与节点 B 的部分私钥，仍然无法获得密钥协商参数 x_A 和 x_B，从而无法计算出以前的会话密钥。

(4)抗密钥泄露伪装攻击：攻击者若获得节点 A 的长期私钥，他仅能向其他节点冒充节点 A，而无法向节点 A 冒充其他节点。本方案中，密钥协商双方需要对产生的密钥协商参数和时间戳进行签名，已掌握节点 A 私钥的攻击者无法在协议中假冒节点 B，因为他不知道节点 B 的私钥而无法计算出密钥协商参数和时间戳的正确签名。

(5)未知密钥共享安全：方案在计算会话密钥前需要通过验证签名来确认对方身份的正确性，不会在未知对方身份的情况下共享相同的会话密钥。因此，攻击者无法试图使节点 A 与节点 C 共享会话密钥，而实际上节点 A 是与节点 B 共享密钥。

(6)密钥控制安全：在密钥协商过程中，节点 A 和节点 B 分别提供了密钥协商参数 x_A 和 x_B，它们都不能单独控制会话密钥的生成。

(7)无密钥托管：本方案 PKG 只为节点生成了部分私钥 d_i，只有获得节点选择的秘密值 s_i 才能得到完整的签名私钥 d_i+s_i。因此，当 PKG 被恶意实体攻破，主密钥被恶意实体获得后，恶意实体因没有节点秘密值而无法得到节点的签名

私钥，从而无法假冒合法节点。因此，本方案具有更强的容侵能力。

由上述分析可以看出，本方案具有完善的安全特性，并且不存在密钥托管问题，在安全性上优于文献[4-5]中的方案。

3.3 效率分析

本节将对方案的计算开销进行分析，并与文献[4-5]中的方案进行比较。这 3 个方案都是采用基于身份的公钥体制实现的。在分析比较方案的计算开销时，忽略对称密钥操作和普通哈希操作，仅考虑双线性对运算(P)、指数运算(Ex)和椭圆曲线加法群上的点乘运算(Pm)。由文献[7]可知，P 的计算开销约为 Pm 的 9.6 倍，Ex 的计算开销约为 Pm 的 8 倍。由表 1 可以看出，本方案中每个节点只需要进行 6 次椭圆曲线加法群上的点乘运算，不需要进行双线性对运算，因此本方案具有更小的计算开销，更适合在 Ad hoc 网络环境中应用。

表 1 计算开销比较

方案	P	Ex	Pm
文献[4]方案	2	1	1
文献[5]方案	3	1	3
本文方案	0	0	6

结束语 本文结合无双线性对的基于身份的签名算法和 Diffie-Hellman 密钥协商技术，设计了一种新的 Ad hoc 网络认证和密钥协商方案。分析表明，方案在满足安全性要求的前提下，具有较小的计算开销，很好地适应了 Ad hoc 网络的特点和需要。

参 考 文 献

[1] ZHOU L, HAAS Z. Securing Ad Hoc Networks[J]. Microcomputer Applications, 2005, 13(6): 24-30.

[2] YI S, KRAVETS R. MOCA: MObile Certificate Authority for Wireless Ad Hoc Networks[C]// Pki Research Workshop Program. 2004: 65-79.

[3] SEN J, SUBRAMANYAM H. An Efficient Certificate Authority for Ad Hoc Networks[M]// Distributed Computing and Internet Technology. Springer Berlin Heidelberg, 2007: 97-109.

[4] 吴平，王保云，徐开勇. 基于身份的 Ad Hoc 网络密钥管理方案[J]. 计算机工程，2008，34(24)：143-145.

[5] 施荣华，樊翔宇. 基于身份认证的 Ad Hoc 密钥协商方案[J]. 中南大学学报(自然科学版)，2010，41(6)：2236-2239.

[6] DU H Z, WEN Q Y. Efficient traceable identity-based signature scheme[J]. Journal on Communications, 2009, 30(8): 56-61.

[7] 杜红珍，温巧燕. 高效的可追踪的基于 ID 的签名方案[J]. 通信学报，2009，30(8)：56-61.

[8] 周福才，徐剑，徐海芳，等. Ad hoc 网络中基于双线性配对的 STR 组密钥管理协议研究[J]. 通信学报，2008，29(10)：117-125.

(上接第 355 页)

6)透明化的特点，使得区块链需要具备更完备的隐私保护机制

区块链的开放式存储和数据透明化的特点，使得隐私保护成为重中之重。研究区块链应用的隐私保护问题，有助于解决数据泄露与滥用的问题，兼顾效率性与安全性。

7)点对点交易的模式，使得区块链应具备灵活且安全的访问控制机制

区块链技术对访问控制和身份认证机制提出了新的技术挑战，研究应用于区块链技术的访问控制机制能够有效抵抗外部攻击并避免隐私泄露的问题，从而加强区块链。

最后，随着国家支持政策与监管政策的出台，以及区块链技术的完善，2018 年区块链的应用落地会出现在各行各业。

参 考 文 献

[1] 谭磊，陈刚. 区块链 2.0[M]. 北京：电子工业出版社，2015.

[2] 隐藏在数字货币身后的力量——浅析区块链技术应用场景[EB/OL]. (2015-11-12). http://mingin.baijia.baidu.com/article/228350.

[3] RICHARD D R, GARETH O G. Rep on the block: anext generation reputation system based on the blockchain[C]// Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST). London, Britain: IEEE, 2015.

[4] GUY ZYSKIND G, NATHAN O, ALEX' A S. Decentralizing privacy: using blockchain to protect personal data[C]// Proceedings of the Security and Privacy Workshops (SPW). San Jose, USA: IEEE, 2015.

[5] 赵赫，李晓风，占礼葵，等. 基于区块链技术的采样机器人数据保护方法[J]. 华中科技大学学报，2015，43(S1)：216-219.

[6] 龚鸣. 简单谈谈究竟什么是“区块链”技术[EB/OL]. (2015-10-23). http://mt.sohu.com/20151023/n424005566.shtml.

[7] SWAN M. Blockchain thinking: the brain as a decentral-ized autonomous corporation [J]. IEEE Technology and Society Magazine, 2015, 34(4): 41-52.

[8] 刘孝男，王永涛，白云波. 区块链+时代，行业面临的机遇与挑战[J]. 中国信息安全，2017(8)：100-103.

[9] ANONYMOUS. New kid on the blockchain [J]. New Scientist, 2015, 225(3009): 7.

[10] GODSIFF P. Bitcoin: bubble or blockchain [C]// Proceedings of the 9th KES International Conference on Agent and Multi-Agent Systems: Technologies and Applications (KES-AMSTA). Sorrento, Italy: Springer, 2015: 191-203.

[11] 谢辉，王健. 区块链技术及其应用研究[J]. 信息网络安全，2016(9)：192-195.

[12] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016，42(4)：481-494.

[13] 邵宇. 区块链技术对金融监管的挑战[J]. 上海政法学院学报(法治论丛)，2017，32(4)：30-40.

[14] 黄锐. 金融区块链技术的监管研究[J]. 学术论坛，2016，39(10)：53-59.

[15] 赵田雨. 区块链技术的监管困境[J]. 经济师，2017(3)：26-27.

[16] 龚鸣. 区块链社会-解码区块链全球应用于投资方案[M]. 北京：中信出版集团，2016(3)：14-16.

[17] 杨东. 保持动态监管体制[J]. 中国经济信息，2016(5)：9-9.

[18] 杨东. 互联网金融的法律规制——基于信息工具的视角[J]. 中国社会科学，2015(4)：107-126.

[19] 杨东. 论金融领域的颠覆创新与监管重构[J]. 人民论坛·学术前沿，2016(11)：30-39.

[20] SAMUL A. Consumer Financial Servicesin Britain: New Approaches to Dispute Resolution and Avoidance[J]. European Business Organization Law Review, 2002, 3(3): 649-694.

[21] 朱岩，甘国华，邓迪，等. 区块链关键技术中的安全性研究[J]. 信息安全研究，2016，2(12)：1090-1097.