



基于属性披露的移动信任协商方案^{*}

汪秋云, 蒋文保, 王 鸿

(北京信息科技大学信息管理学院 北京 100192)

摘 要:针对移动环境下使用传统信任协商方案存在的通信开销、存储开销及计算开销大的问题,提出一种基于属性披露的移动信任协商方案,协商时双方首先交换包含加密属性的信任证,并根据对对方的信任度评估,预先选择性地显露证书中的某些敏感属性,之后再根据协商策略多次交换属性加密密钥,逐步向对方显示自己的属性,从而完成协商过程。通过具体的应用实例说明方案的实现过程,方案性能分析表明该方案高效可行。

关键词:属性证书;移动;信任评估;信任协商

doi: 10.3969/j.issn.1000-0801.2013.10.018

Scheme of Attribute-Based Disclosure Mobile Trust Negotiation

Wang Qiuyun, Jiang Wenbao, Wang Hong

(School of Information Management, Beijing Information Science & Technology University, Beijing 100192, China)

Abstract: For it is difficult to use traditional trust negotiation on the mobile environment, which has large communication overhead, storage overhead and computational overhead, an attribute-based disclosure mobile trust negotiation scheme was proposed. In the negotiation process, two sides in trust negotiation exchange certificate which contains encrypted credential attributes firstly, then, one side in trust negotiation can selectively dispose the sensitive attributes to the other side in trust negotiation procedure based on the trust evaluation result of the other, next, two sides in trust negotiation exchange attribute encryption key based on personal security policy until the trust negotiation was completed. The implementation procedure was given in concrete application instances and the scheme was analyzed.

Key words: attribute certificate, mobile, trust negotiation, trust evaluation

1 引言

传统信任协商是在陌生的双方之间,反复呈现信任证和要求信任证,逐步建立充足的信任以便双方能够完成交易^[1,2]。目前关于传统信任协商的研究,国内外学者都进行了大量的研究^[3],如信任协商的形式化描述^[4]、信任证存储策略研究^[5]、敏感信息传输方案^[6]以及环策略依赖检测技术^[7]等,但在移动环境下,如果仍使用传统信任协

商基于证书交换的协商方式,那么协商过程中大量的证书交换对通信和存储将带来巨大的开销^[8],另外大量证书的公钥密码运算,也会给计算时间带来很大的开销,这些都表明传统信任协商不适合计算能力、网络带宽以及存储空间都有限的移动计算设备,而目前关于移动信任协商的研究还比较少。

本文在分析现有信任协商解决方案^[9-13]的基础上,提出了一种基于属性披露的移动信任协商方案,在该方案中

^{*} 国家自然科学基金资助项目(No.60873202),北京市自然科学基金资助项目(No.4132011)



协商双方的信任证包含多个属性,由信任证发行者签名颁发,信任证中的属性根据敏感度的不同设立属性信任阈值并进行对称加密,信任协商开始阶段协商双方除交换信任证以外,还根据对方的信任度预先披露一些敏感属性,如果这些属性还没有满足协商要求,那么之后的协商过程则可简化为属性匹配及其对应解密密钥的交换过程。

2 基于属性的信任证

传统数字证书中,属性可以使用有序对 $\langle AN, AV \rangle$ 表示,其中 AN 表示属性名, AV 表示属性值。在本文中,针对属性引入属性信任阈值,使用三元组 $\langle AN, AV, T \rangle$ 表示属性名称、属性值以及信任阈值,其中属性信任阈值 $T(0 \leq T \leq 100)$ 由证书持有者根据属性的敏感度定义,当某个属性属于敏感信息时,其信任阈值 $T > 0$,则在证书中该属性的属性值以密文形式存储;当某个属性属于非敏感信息即 $T = 0$ 时,则该属性的属性值以明文存储,如图1所示。

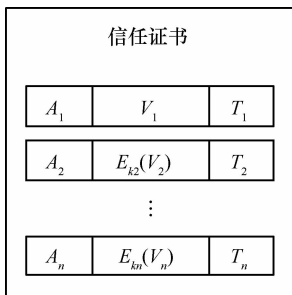


图1 基于属性的信任证

例如,Alice的证书Cre中包含 n 个属性,属性名为 $A_1, A_2, \dots, A_n$,对应的属性值为 $V_1, V_2, \dots, V_n$,如果有 $m(m \leq n)$ 个属性(下标记为 $j_1, j_2, \dots, j_k$)是敏感的,则在证书Cre中这 m 个属性的属性值以密文形式存储,而其他的 $n-m$ 个属性的属性值以明文形式存储。证书颁发者先生成证书Cre并对其进行数字签名,之后将证书Cre以及 m 个敏感属性加解密密钥通过可信信道发送给Alice。

基于属性的信任证进行协商时,双方首先交换包含加密属性的信任证,接着根据双方的访问策略交换属性加解密密钥,向对方逐步披露信任认证的加密属性,最终完成信任协商。由此可见,在基于属性的信任协商中,协商策略与访问控制策略都变成与信任证的属性相联系。为了保证安全,协商双方在开始阶段先用椭圆曲线密钥交换算法产生会话密钥,然后用该密钥加密信任证及属性加解密密钥,进行传输。

3 基于属性披露的移动信任协商方案

为便于进行形式化的描述,用Alice和Bob分别表示进行信任协商的双方,基于属性披露的移动信任协商方案的整个过程可分为3个阶段,如图2所示。第1阶段为证书生成阶段,发行者生成证书并发送给Alice;第2阶段为证书交换阶段,Alice向Bob提交证书Cre,并根据Bob的信任度生成属性开放向量 V ,向Bob显露证书Cre的部分或全部敏感属性;第3阶段为密钥交换阶段,在交换证书后,双方根据协商策略,多次交换敏感属性加解密密钥,逐步向对方显示自己的属性,从而完成协商。

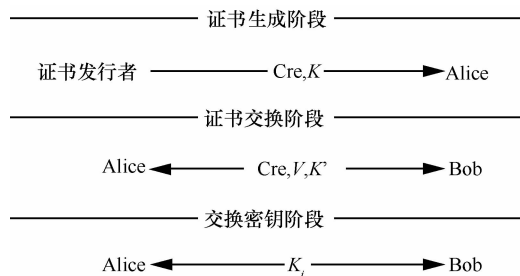


图2 基于属性披露的移动信任协商方案

3.1 证书生成阶段

在此阶段,证书发行者生成证书Cre并发送给证书的持有人Alice,主要有以下3个步骤。

(1)在证书发行者生成证书之前,Alice根据自身的情况给证书的每一个属性设定一个信任阈值。

(2)发行者根据Alice设定的属性信任阈值,生成证书Cre。在证书Cre中,设有 n 个属性,当属性的信任阈值 $T_i = 0$ ($i = 1, \dots, n$)时,表明此属性为非敏感属性,保存的是属性值的明文,即 $\langle AN, AV \rangle$;当属性的信任阈值 $T_i > 0$ 时,表明此属性为敏感属性,每个敏感属性保存的是属性值的密文,即 $\langle AN, E_{K_i}(AV) \rangle$,此处的加解密密钥 K_i 是随机选取的。

(3)证书生成之后,发行者把证书Cre和密钥 K (K 包含多个子密钥 $K_i, i = 1, \dots, N$)发送给Alice,密钥的传输通过可信信道传送。

3.2 证书交换阶段

在此阶段,为尽可能减少密钥交换阶段的密钥交换次数,协商双方在发送自己的信任证之前先对对方做一个信任评估,根据对方的信任度决定证书交换时披露的敏感属性数量,主要通过4个步骤完成。

(1)Alice根据与Bob的历史交往以及其他种种因素,对Bob的信任度为 T_{Bob} ,在Alice将证书Cre发给Bob前,

先将证书中每个属性的信任阈值 T_i 与 T_{Bob} 进行比较,若 T_{Bob} 大于第 i 个属性的信任阈值 T_i , 则产生对应的一个二进制 1,意味着该属性可以向 Bob 开放,反之产生一个二进制 0,意味着该属性不能向 Bob 开放,将这些比特按照先后顺序排列就可以得到一个属性开放向量 V , V 由这些二进制编码组成,可以节约存储空间。

(2) Alice 根据证书中属性的信任阈值大于 0 且属性开放向量中的对应二进制位为 1 的、可显露的敏感属性,组织对应的属性加密密钥 K_i ,最终得到密钥组 K' 。

(3) Alice 将证书 Cre、密钥组 K' 和属性开放向量 V 发送给 Bob,其中密钥组使用椭圆曲线密钥交换算法建立的可信信道发送。

(4) Bob 收到证书 Cre、 K' 和 V 之后,对二进制数 V 中值为 1 的位对应的可披露敏感属性进行解密,即可获得敏感属性的属性值。

3.3 交换密钥阶段

协商双方根据协商策略,多次交换敏感属性加密密钥,逐步向对方显示自己的属性,从而完成协商,步骤如下。

(1) Bob 在获得 Alice 发送的证书 Cre、 K' 和 V 之后,解密得到 Alice 的某些属性值,但并未满足 Bob 的策略要求,于是向 Alice 请求访问属性 A_i 。

(2) Alice 在 Bob 满足访问其属性 A_i 的前提下,把属性对应的加密密钥 K_i 发给 Bob。

(3) Bob 得到 K_i 后,对属性 A_i 进行解密,获得 A_i 的属性值,如此循环直至协商结束。

4 应用实例

借鉴参考文献[13]的一个实例:假设在线书店(Bookshop)对高校在校学生提供打折销售服务,访问者 Alice 向 Bookshop 要求得到学生折扣服务,Bookshop 起初并没有 Alice 的任何信息,Bookshop 的策略是只给高校在校学生提供折扣服务,因此 Bookshop 请求 Alice 出具高校学生证号以及银行信用卡号信任证,Alice 的策略是银行信用卡号只能提供给中国银行的会员单位查看。

在传统的信任协商(以吝啬策略为例)中,Alice 向 Bookshop 提供自己的高校学生信任证后,也会要求 Bookshop 提供中国银行会员的信任证,在 Bookshop 向 Alice 出示中国银行会员的信任证后,Alice 才向 Bookshop 出示自己的信用卡号凭证。如图 3 所示,为了满足双发的

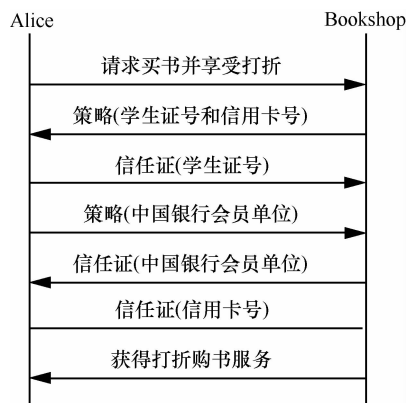


图 3 传统信任协商(吝啬策略)

协商策略,一般要多次交换信任证。

在基于属性披露的移动信任协商方案中,Alice 出示的信任证包含高校学生证号以及信用卡号两个属性,对 Alice 而言,认为高校学生证号属于非敏感属性,所以属性值存储的是明文,而信用卡号属于敏感属性,所以存储的是对称加密的密文;对 Bookshop 而言,它的信任证中中国银行会员单位属性属于非敏感属性,所以是明文存储。在 Alice 第一次将自己的信任证提交给 Bookshop 之前,Alice 评估了 Bookshop 的信任度,认为还没有达到信用卡号属性信任阈值,所以没有将信用卡号属性对应的解密密钥发给 Bookshop,这时 Bookshop 没法解密信用卡号,只能看到信任证中的高校学生证号,在 Bookshop 向 Alice 出示信任证显示中国银行会员单位属性后,Alice 才将自己信任证中信用卡号属性对应的解密密钥发给 Bookshop,Bookshop 解密获得 Alice 的信用卡号,如图 4 所示。

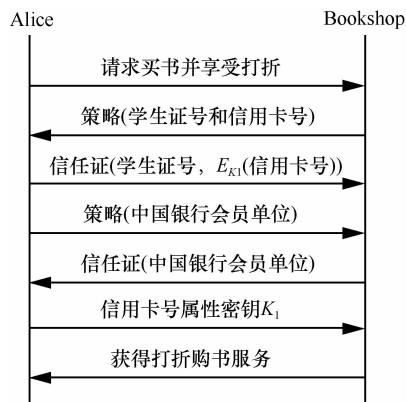


图 4 基于属性披露的移动信任协商(初次)

如果在 Alice 第一次将自己的信任证提交给在线书店之前,评估 Bookshop 的信任度达到信用卡号属性信任阈值,那么 Alice 会将信用卡号属性对应的解密密钥也发给 Bookshop,这时在线书店就可以一次性获取 Alice 的高校



学生证号及信用卡号,减少 Bookshop 发送信认证及 Alice 发送信用卡号属性解密密钥的过程,如图 5 所示。

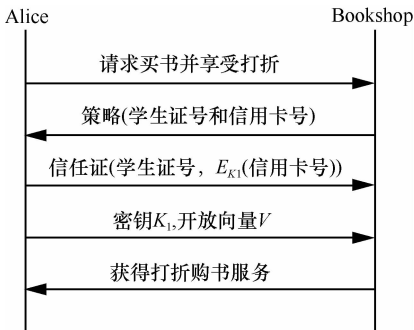


图 5 基于属性披露的移动信任协商(多次)

5 方案性能

基于属性披露的移动信任协商方案,总体思路是将传统信任协商的多次证书交换带来的非对称加解密运算,尽可能地转变为证书属性披露带来的对称加解密运算,后者的计算时间开销、存储开销以及通信开销,都要明显优于前者。表 1 列出了上述应用实例信任协商过程的开销对比数据。

下面从计算时间开销、存储开销和通信开销 3 个方面,分析基于属性披露的移动信任协商方案的性能。

(1) 时间开销

尽管相比传统信任协商方案,增加了信任度评估和证书交换中的属性开放向量计算过程,但这些过程所占用的时间开销是固定不变的,即其时间复杂度为 $O(1)$;相反,基于证书属性披露的对称加解密运算开销要比传统信任协商多次交换证书进行的非对称加解密运算开销要小很多。

(2) 通信开销

基于属性披露的移动信任协商方案中,证书生成阶段的通信开销是证书加上敏感属性的解密密钥,在证书的交换阶段,通信开销是证书、可显露敏感属性的解密密钥以及属性开放向量 V ,密钥交换阶段通信开销仅有对应属性

的解密密钥,相比传统信任协商多次证书交换的通信开销,这些是微不足道的。

(3) 存储开销

基于属性披露的移动信任协商方案的存储开销除了证书本身的开销之外,还增加了协商对方的信任度 T_{Bab} 、属性开放向量 V 以及敏感属性解密密钥的存储开销,但这些相对于传统信任协商多个证书存储开销也是微不足道的。

为了对比方案的整体时间开销,进行了一组仿真实验,结果如图 6 所示。与传统信任协商方案不同,随着协商双方的信任度越来越高,基于属性披露的移动信任协商方案在协商过程中,预先披露的属性越来越多,需要交换的密钥越来越少,协商时间开销不断下降,越是复杂的信任协商过程,这种时间开销的下降优势越明显。

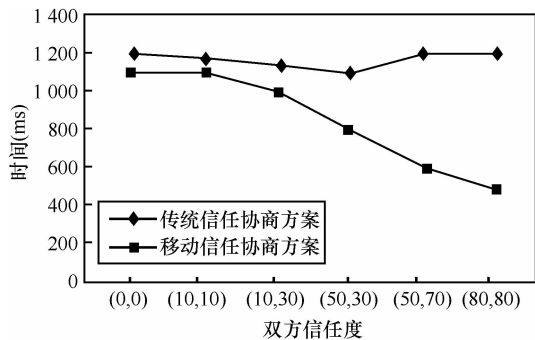


图 6 信任协商时间开销

6 结束语

本文所介绍的基于属性披露的移动信任协商方案是在分析现有传统信任协商决方案的基础上,专门针对移动环境提出的,该方案基本解决了在移动环境下进行信任协商造成的计算开销、通信开销及存储开销大的问题,但信任认证中属性的具体划分、证书链的转换以及基于属性的策略表达等问题仍需要进一步考虑。因此,下一步的工作是将该方案进行进一步完善,考虑更多因素,以适应移动环境。

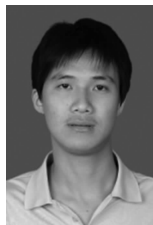
表 1 信任协商开销对比

方案	信任度计算	策略检索次数	证书交换次数	密钥交换次数	解密校验运算	
					对称	非对称
传统信任协商(齐备)	—	2	3	—	—	3
移动信任协商(初次)	1	2	1	1	1	1
移动信任协商(多次)	1	1	1	0	1	1

参考文献

- 1 Winslett M, Yu T, Seamons K, *et al.* Trust negotiation on the Web. *IEEE Internet Computing*, 2002, 6(6):30~37
- 2 Yu T, Winslett M, Seamons K E. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. *ACM Transactions on Information and System Security*, 2003, 6 (1):1~42
- 3 廖振松, 李赤松, 邹德等. 自动信任协商及其发展趋势. *软件学报*, 2006, 17(9): 1933~1948
- 4 官尚元, 伍卫国, 董小社等. 自动信任协商的形式化描述与验证研究. *通信学报*, 2011, 32(2):86~99
- 5 李健利, 高勇, 解洋等. 自动信任协商中信任证存储策略研究. *计算机工程*, 2011, 37(12): 140~143
- 6 李健利, 霍光磊, 刘博等. 基于魔方算法的自动信任协商敏感信息传输方案. *计算机应用*, 2011, 34(4): 984~988
- 7 王凯, 张红旗, 任志宇. 自动信任协商中环策略依赖检测技术. *计算机应用*, 2012, 33(3): 686~689,693
- 8 蒋文保, 陈文亮, 汪秋云. 一种自适应信任协商模型设计与分析. *四川大学学报(自然科学版)*, 2013(2):273~280
- 9 Guo S X, Jiang W B. A trust evaluation model and algorithm. *Proceedings of International Conference on Communications and Intelligence Information Security*, Nanning, China, 2010:130~134
- 10 Horst T, Sundelin T, Seamons K E, *et al.* Mobile trust negotiation authentication and authorization in dynamic mobile networks. *Proceedings of Eighth IFIP Conference on Communications and Multimedia Security*, Porto, Portugal, 2004
- 11 廖俊国, 洪帆, 李俊等. 在信任协商中保密证书的敏感属性. *通信学报*, 2008, 29(6):20~25
- 12 雷建云, 余涵, 蒋天发等. 自动信任协商中的敏感信息保护方案. *武汉理工大学学报*, 2012, 34(3):1~4
- 13 洪帆, 郭亚军. 资源限制信任协商. *华中科技大学学报: 自然科学版*, 2006, 34(5):23~25

[作者简介]



汪秋云,男,北京信息科技大学硕士研究生,主要研究方向为人工智能与信息安全。



蒋文保,男,北京信息科技大学教授,主要研究方向为网络安全监测与监控。



王鸿,男,北京信息科技大学硕士研究生,主要研究方向为物流工程与信息安全。

(收稿日期:2013-06-28)

(上接第 102 页)

- 11 罗竣友,赵军辉,廖健雄.基于混沌优化的无线定位算法研究. *电路与系统学报*,2010(1):113~119
- 12 任重远,陈佳品,李振波等.一种基于无线传感器网络的 RF 定位算法研究. *传感器与微系统*,2012(7):52~54
- 13 肖卫初,陈伟宏,龚伦峰.一种新的几何无线定位方法. *科学技术与工程*,2011,11(13):2945~2948
- 14 王慧琴.小波分析与应用.北京:北京邮电大学出版社,2011
- 15 Chan Y T, Ho K C. A simple and efficient estimation or for hyperbolic location. *IEEE Transactions on Signal Processing*, 1994, 42(8): 1905~1915
- 16 汪新凡. 小波基选择及其优化. *株洲工学院学报*,2003,17(5): 33~35
- 17 张颖.无线定位优化算法的研究.西安邮电大学硕士学位论文, 2011
- 18 张德丰. MATLAB 小波分析.北京:机械工业出版社,2012

[作者简介]



陈宝全,男,西安邮电大学硕士研究生,主要研究方向为通信信号处理、移动台定位。



毛永毅,男,博士,西安邮电大学教授、硕士生导师、研究生院副院长,主要研究方向为通信信号处理、移动台定位。

(收稿日期:2013-06-30)