(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108848074 A
(43)申请公布日 2018.11.20

(21)申请号 201810550433.2

(22)申请日 2018.05.31

(71)申请人 西安电子科技大学
地址 710071 陕西省西安市雁塔区太白南路2号

(72)发明人 马文平 高阳

(74)专利代理机构 陕西电子工业专利中心 61205
代理人 田文英 王品华

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/30(2006.01)

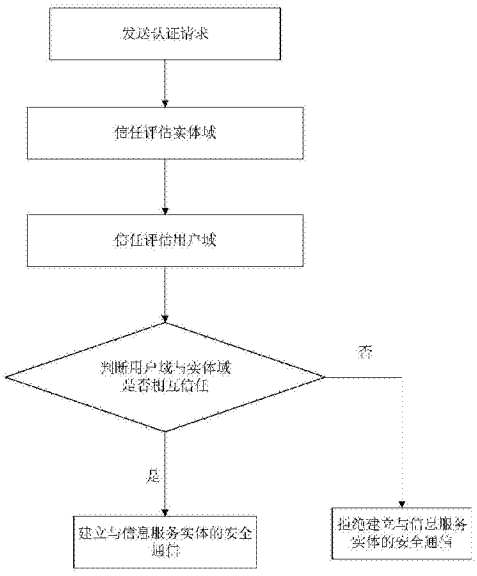
权利要求书4页 说明书8页 附图2页

(54)发明名称

基于域代理信任值的信息服务实体跨域认证方法

(57)摘要

本发明公开一种基于域代理信任值的信息服务实体跨域认证方法，主要解决当前跨域认证过程中，计算复杂度高，通信开销大和基于公钥基础设施证书管理复杂的问题，其技术方案为：采用基于身份的签名算法验证用户身份的合法性，使用连接算子，连接从域代理的交易信息表中提取的直接信任向量，用合并算子合并多条推荐路径上的信任向量，从而判断域代理之间是否相互信任。本发明克服了现有技术在跨域认证过程中，基于公钥基础设施认证体系证书管理复杂，计算复杂度高，通信开销大的问题，在保证域代理之间认证准确度的同时提高了跨域认证过程的实用性和高效性。



CN 108848074 A

1.一种基于域代理信任值的信息服务实体跨域认证方法，其特征在于，将收到请求消息域代理中对目标域代理的每个直接信任向量，用连接算子连接为一个推荐信任向量，用合并算子将多条推荐路径上的推荐信任向量合成为一个信任向量；该方法的具体步骤包括如下：

(1)发送认证请求：

(1a)利用身份签名算法，用户域中发送请求的用户对消息进行签名，得到消息的杂凑值和签名消息；

(1b)用户域内发送请求的用户将消息、消息的杂凑值和签名消息发送给用户域的域代理；

(1c)用户域的域代理验证用户的身份是否合法，若是，则执行步骤(2)，否则，中止认证；

(2)用户域的域代理对实体域的域代理进行信任评估：

(2a)将用户域的域代理作为发送方，实体域的域代理作为请求方，利用双向信任响应的方法，得到关于实体域的域代理的各个直接信任向量；

(2b)按照下式，计算用户域的域代理对实体域的域代理的直接推荐信任向量：

$$dt_1^2 = t_1^k \otimes t_k^2$$

其中，dt_1^2表示用户域的域代理对实体域的域代理的直接推荐信任向量，t_1^k表示用户域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^2表示其中一个收到请求消息的域代理对实体域的域代理的直接信任向量，$\otimes$表示连接操作；

(2c)按照下式，用户域的域代理对实体域的域代理的间接推荐信任向量：

$$it_1^2 = t_1^k \otimes t_k^m \otimes t_m^2$$

其中，it_1^2表示用户域的域代理对实体域的域代理的间接推荐信任向量，t_1^k表示用户域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^m表示其中一个收到请求消息的域代理对其交易信息表中的一个域代理的直接信任向量，t_m^2表示收到请求消息域代理交易信息表中的一个域代理对用实体域的域代理的直接信任向量，$\otimes$表示连接操作；

(2d)按照下式，计算用户域的域代理对实体域的域代理的推荐信任向量：

$$rt_1^2 = dt_1^2 \oplus it_1^2$$

其中，rt_1^2表示用户域的域代理对实体域的域代理的推荐信任向量，dt_1^2表示用户域的域代理对实体域的域代理的直接推荐信任向量，it_1^2表示用户域的域代理对实体域的域代理的间接推荐信任向量，$\oplus$表示合并操作；

(2e)按照下式，计算用户域的域代理对实体域的域代理的综合信任向量：

$$ct_1^2 = dt_1^2 \oplus rt_1^2$$

其中，ct_1^2表示用户域的域代理对实体域的域代理的综合信任向量，dt_1^2表示用户域的域代理对实体域的域代理的直接信任向量，rt_1^2表示用户域的域代理对实体域的域代理的推荐信任向量，$\oplus$表示合并操作；

(2f)判断用户域的域代理对实体域的域代理的综合信任向量的最大分量是否大于

0.5，若是，执行步骤(2g)，否则，执行步骤(6)；

(2g)将用户域的域代理对实体域的域代理信任评估的结果，发送给用户域中的发送请求用户；

(3)实体域的域代理对用户域的域代理进行信任评估：

(3a)将实体域的域代理作为发送方，用户域的域代理作为验证方，利用双向信任响应的方法，得到关于用户域的域代理的各个直接信任向量；

(3b)按照下式，计算实体域的域代理对用户域的域代理的直接推荐信任向量：

$$dt_1^2 = t_1^k \otimes t_k^2$$

其中，dt_1^2表示实体域的域代理对用户域的域代理的直接推荐信任向量，t_1^k表示实体域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^2表示其中一个收到请求消息的域代理对用户域的域代理的直接信任向量，$\otimes$表示连接操作；

(3c)按照下式，实体域的域代理对用户域的域代理的间接推荐信任向量：

$$it_1^2 = t_1^k \otimes t_k^m \otimes t_m^2$$

其中，it_1^2表示实体域的域代理对用户域的域代理的间接推荐信任向量，t_1^k表示实体域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^m表示其中一个收到请求消息的域代理对其交易信息表中的一个域代理的直接信任向量，t_m^2表示收到请求消息域代理交易信息表中的一个域代理对用户域的域代理的直接信任向量，$\otimes$表示连接操作；

(3d)按照下式，计算实体域的域代理对实体域的域代理的推荐信任向量：

$$rt_1^2 = dt_1^2 \oplus it_1^2$$

其中，rt_1^2表示实体域的域代理对用户域的域代理的推荐信任向量，dt_1^2表示实体域的域代理对用户域的域代理的直接推荐信任向量，it_1^2表示实体域的域代理对用户域的域代理的间接推荐信任向量，$\oplus$表示合并操作；

(3e)按照下式，计算实体域的域代理对用户域的域代理的综合信任向量：

$$ct_1^2 = dt_1^2 \oplus rt_1^2$$

其中，ct_1^2表示实体域的域代理对用户域的域代理的综合信任向量，dt_1^2表示实体域的域代理对用户域的域代理的直接信任向量，rt_1^2表示实体域的域代理对用户域的域代理的推荐信任向量，$\oplus$表示合并操作；

(3f)判断实体域的域代理对用户域的域代理的综合信任向量的最大分量是否大于0.5，若是，执行步骤(3g)，否则，执行步骤(6)；

(3g)将实体域的域代理对用户域的域代理信任评估的结果，发送给用户域中的发送请求的用户；

(4)判断用户域与实体域是否满足相互信任条件，若是，则执行步骤(5)，否则，执行步骤(6)；

(5)用户域中发送请求的用户访问实体域中的信息服务实体；

(6)用户域中发送请求的用户拒绝访问实体域中的信息服务实体。

2.根据权利要求1所述的基于域代理信任值的信息服务实体跨域认证方法，其特征在于，步骤(1a)中所述的消息包括用户域中发送请求的时间戳、用户的身份标识、实体域中被

访问的信息服务实体的身份标识。

3.根据权利要求1所述的基于域代理信任值的信息服务实体跨域认证方法，其特征在于，步骤(1a)中所述身份签名算法的具体步骤如下：

第一步，使用密码杂凑函数，将消息转化成一个杂凑值；

第二步，密钥生成中心产生一个随机数作为系统的主密钥，s∈[1,N-1]，其中，s表示由密钥生成中心产生的随机数，∈表示属于符号，N表示一个乘法循环群的阶数；

第三步，密钥生成中心随机选择并公开一个字节，将所选字节作为用户的私钥生成函数识别符；

第四步，按照下式，生成用户域中发送请求用户的私钥：

$$d = P \times \frac{s}{H(ID \| i) + s}$$

其中，d表示用户域中发送请求用户的私钥，P表示N阶乘法循环群的生成元，s表示基于身份的密码体制系统的主密钥，H(ID||i)表示用哈希函数将输入的用户域中发送请求用户的身份标识ID和用户私钥生成函数识别符i连接的比特串输出为一个整数；

第五步，按照下式，生成用户域中发送请求用户的公钥：

Q=H(ID||i)×P+s×P

其中，Q表示用户域中发送请求用户的公钥，H(ID||i)表示用哈希函数将输入的用户域中发送请求用户的身份标识ID和用户私钥生成函数识别符i连接的比特串输出为一个整数，P表示N阶乘法循环群的生成元，s表示基于身份的密码体制系统的主密钥；

第六步，发送请求的用户产生一个随机数，1≤r≤N-1，r表示由发送请求用户产生的随机数，N表示一个乘法循环群的阶数；

第七步，按照下式，生成请求用户对消息的签名：

S=d×[(r-h)modN]

其中，S表示请求的用户对消息的签名，d表示发送请求用户的私钥，r表示发送请求用户产生的随机数，h表示消息杂凑值，mod表示取余操作，[·]表示取整操作。

4.根据权利要求1所述的基于域代理信任值的信息服务实体跨域认证方法，其特征在于，步骤(1c)中所述的用户的身份合法是指，按照下式，用户域的域代理计算消息杂凑值，将用户域的域代理所计算出的消息杂凑值与用户域的域代理收到的消息杂凑值相等的发送请求用户判定为身份合法的用户：

$$h_2 = H_2(M_1, e(Q, S_1) \times e(P, sP)^{h_1})$$

其中，h_2表示用户域的域代理计算的消息杂凑值，$H_2(\cdot)$表示哈希函数，M_1表示用户域的域代理收到的消息，$e(\cdot)$表示双线性对操作，Q表示发送请求用户的公钥，S_1表示用户域的域代理收到的签名消息，P表示生成乘法循环群的生成元，s表示由密钥生成中心产生的随机数，h_1表示用户域的域代理收到的消息杂凑值。

5.根据权利要求1所述的基于域代理信任值的信息服务实体跨域认证方法，其特征在于，步骤(2a)、步骤(3a)中所述的双向信任响应的方法的具体步骤如下：

第一步，请求方从自身存储的交易信息表中查找验证方的信息，存在，则直接取出对验证方的直接信任向量；

第二步，请求方将评估验证方的请求消息发送给交易信息表中除验证方以外的其他域

代理；

第三步，收到请求消息域代理从其交易信息表中取出对验证方的直接信任向量，并发送给请求方；

第四步，收到请求消息的域代理将评估验证方的请求消息发送给其交易信息表中除验证方以外的其他域代理；

第五步，收到请求消息的域代理从自身的交易信息表中取出对验证方的直接信任向量，并发送给该域代理的发送方，该域代理的发送方再发送给请求方。

6.根据权利要求1所述的基于域代理信任值的信息服务实体跨域认证方法，其特征在于，步骤(4)中所述相互信任条件是指同时满足以下两个条件的情形：

条件1，用户域的域代理对实体域的域代理的综合信任向量的最大分量大于0.5；

条件2，用户域的域代理对实体域的域代理的综合信任向量的最大分量大于0.5。

基于域代理信任值的信息服务实体跨域认证方法

技术领域

[0001] 本发明属于通信技术领域，更进一步涉及网络通信技术领域中的一种基于域代理DA(Domain agent)信任值的信息服务实体ISE(Information System Entity)跨域认证方法。本发明可在资源受限的分布式的网络环境下，通过计算域代理之间的信任值，建立信任域之间的信任关系，为一个信任域的用户跨域访问信息服务实体的资源提供安全保障。

背景技术

[0002] 建立域代理之间的信任关系是提高网络中用户个人信息的保密性和安全性的重要步骤，跨域认证是指不同域的域代理之间相互认证的技术和过程。近年来，随着密码学理论、模糊集合理论在跨域认证领域应用的不断深入，许多新的方法和思想被应用于跨域认证。在其中，跨信任域的认证框架主要有公钥基础设施PKI(Public Key Infrastructure)认证框架和基于身份的公钥密码体制IBC(Identity-Based Cryptography)认证框架，这些方法能够有效的实现跨域的认证。但是PKI认证框架的证书管理开销较大，且当跨域访问资源过于繁重时容易造成认证中心网络瓶颈的问题，IBC认证框架要求不同的域使用相同的系统参数，这在工程上显然是不切实际的。因此，想要实现安全高效的跨域认证，仍然有很多需要改进的地方。

[0003] 浙江省人大常委会办公厅信息中心在其申请的专利文献“一种基于信任的跨域认证方法”(申请号201010228998.2，申请公布号CN 101888297A)中提出了一种基于信任的跨域认证方法。该方法的步骤是，首先根据各个信任域采用的认证体制，第一信任域的第一认证服务器采用证书、口令或者证书和口令相结合的方式对第一实体进行身份验证，并将认证结果发送给第二认证服务器。然后将不同信任域的认证服务器归属到基于PKI认证体系中的同一信任认证中心CA(Center Agent)，该信任认证中心CA为每个认证服务器颁发证书，这样就建立起认证服务器之间的信任关系，第二认证服务器利用预先建立的基于PKI认证体系的信任关系验证第一服务器的合法性。最后，第二认证服务器根据判断的认证结果再决定跨域认证是否成功，认证结果为认证通过则表示跨域验证成功，否则为失败。该方法存在的不足之处有两个，第一，由于该方法没有考虑第二信任域中第二认证服务器对第二实体的身份认证，忽略了第二信任域的第二实体也可能具有欺骗性，在第一信任域的第一实体访问第二信任域的第二实体过程中会引起信息的泄露的问题。第二，该方法使用PKI认证体系建立信任域之间信任关系，而PKI认证体系的缺点是，当信任域较多时认证服务器证书的管理开销很大，跨域认证的效率低。

[0004] 西南交通大学在其申请的专利文献“IBC域内的用户访问PKI域内的资源的认证密钥协商方法”(申请号201710081516.7，公开号106789042A)中公开了一种IBC域的用户访问PKI域的资源的认证密钥协商方法。该方法的步骤是，首先利用哈希值的运算和基于椭圆曲线的点乘运算计算用户的临时身份，IBC域的用户使用IBC域的认证服务器的公钥采用基于身份的加密操作向本域的认证服务器发送访问PKI域的资源的请求，IBC域认证服务器通过认证用户的合法性后转发用户的访问请求给PKI域认证服务器。然后PKI域认证服务器对

IBC域认证服务器进行身份的合法性认证，生成访问授权票据并发送给IBC域的用户。最后使用基于身份的加解密算法实现IBC域的用户和PKI域的资源的双向身份认证，从而建立协商会话密钥，其中会话密钥是由会话密钥的认证服务器部分和填充后的用户部分进行异或处理得到的。该方法存在的不足之处是，由于该方法中包括多次身份的验证和基于身份的加解密，而身份的验证和基于身份的加解密使用了双线对和基于椭圆曲线点乘的运算，双线性对和点乘运算的时间复杂度太高，从而使得跨域认证的时间效率降低，增大通信开销。

发明内容

[0005] 本发明的目的在于针对上述现有技术的不足，提出基于域代理信任值的信息服务实体跨域认证方法，以解决跨域认证过程中基于公钥基础设施认证体系证书管理复杂，时间效率低和通信开销过大的问题。

[0006] 实现本发明目的的思路是，采用基于身份的签名算法向本域的域代理证明用户是本域的合法用户，将收到请求消息域代理中对目标域代理的每个直接信任向量，用连接算子连接为一个推荐信任向量，用合并算子将多条推荐路径上的推荐信任向量合成为一个信任向量，计算域代理之间的信任向量，实现域间的双向信任评估，将信任评估的结果发送给用户域中的发送请求的用户，用户域中发送请求的用户决定与实体域中的信息服务实体是否建立安全通信。

[0007] 本发明的具体步骤包括如下：

[0008] (1)发送认证请求：

[0009] (1a)利用身份签名算法，用户域中发送请求的用户对消息进行签名，得到消息的杂凑值和签名消息；

[0010] (1b)用户域内发送请求的用户将消息、消息的杂凑值和签名消息发送给用户域的域代理；

[0011] (1c)用户域的域代理验证用户的身份是否合法，若是，则执行步骤(2)，否则，中止认证；

[0012] (2)用户域的域代理对实体域的域代理进行信任评估：

[0013] (2a)将用户域的域代理作为发送方，实体域的域代理作为请求方，利用双向信任响应的方法，得到关于实体域的域代理的各个直接信任向量；

[0014] (2b)按照下式，计算用户域的域代理对实体域的域代理的直接推荐信任向量：

[0015] $$dt_1^2 = t_1^k \otimes t_k^2$$

[0016] 其中，dt_1^2表示用户域的域代理对实体域的域代理的直接推荐信任向量，t_1^k表示用户域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^2表示其中一个收到请求消息的域代理对实体域的域代理的直接信任向量，$\otimes$表示连接操作；

[0017] (2c)按照下式，用户域的域代理对实体域的域代理的间接推荐信任向量：

[0018] $$it_1^2 = t_1^k \otimes t_k^m \otimes t_m^2$$

[0019] 其中，it_1^2表示用户域的域代理对实体域的域代理的间接推荐信任向量，t_1^k表示用户域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^m表示其中一个收到请求消息的域代理对其交易信息表中的一个域代理的直接信任向量，t_m^2表示收到请求消息域

代理交易信息表中的一个域代理对用实体域的域代理的直接信任向量，⊗表示连接操作；

[0020] (2d)按照下式，计算用户域的域代理对实体域的域代理的推荐信任向量：

[0021] $rt_1^2 = dt_1^2 \oplus it_1^2$

[0022] 其中，rt_1^2表示用户域的域代理对实体域的域代理的推荐信任向量，dt_1^2表示用户域的域代理对实体域的域代理的直接推荐信任向量，it_1^2表示用户域的域代理对实体域的域代理的间接推荐信任向量，⊕表示合并操作；

[0023] (2e)按照下式，计算用户域的域代理对实体域的域代理的综合信任向量：

[0024] $ct_1^2 = dt_1^2 \oplus rt_1^2$

[0025] 其中，ct_1^2表示用户域的域代理对实体域的域代理的综合信任向量，dt_1^2表示用户域的域代理对实体域的域代理的直接信任向量，rt_1^2表示用户域的域代理对实体域的域代理的推荐信任向量，⊕表示合并操作；

[0026] (2f)判断用户域的域代理对实体域的域代理的综合信任向量的最大分量是否大于0.5，若是，执行步骤(2f)，否则，执行步骤(6)；

[0027] (2g)将用户域的域代理对实体域的域代理信任评估的结果，发送给用户域中的发送请求用户；

[0028] (3)实体域的域代理对用户域的域代理进行信任评估：

[0029] (3a)将实体域的域代理作为发送方，用户域的域代理作为验证方，利用双向信任响应的方法，得到关于用户域域代理的各个直接信任向量；

[0030] (3b)按照下式，计算实体域的域代理对用户域的域代理的直接推荐信任向量：

[0031] $dt_1^2 = t_1^k \otimes t_k^2$

[0032] 其中，dt_1^2表示实体域的域代理对用户域的域代理的直接推荐信任向量，t_1^k表示实体域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^2表示其中一个收到请求消息的域代理对用户域的域代理的直接信任向量，⊗表示连接操作；

[0033] (3c)按照下式，实体域的域代理对用户域的域代理的间接推荐信任向量：

[0034] $it_1^2 = t_1^k \otimes t_k^m \otimes t_m^2$

[0035] 其中，it_1^2表示实体域的域代理对用户域的域代理的间接推荐信任向量，t_1^k表示实体域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^m表示其中一个收到请求消息的域代理对其交易信息表中的一个域代理的直接信任向量，t_m^2表示收到请求消息域代理交易信息表中的一个域代理对用户域的域代理的直接信任向量，⊗表示连接操作；

[0036] (3d)按照下式，计算实体域的域代理对实体域的域代理的推荐信任向量：

[0037] $rt_1^2 = dt_1^2 \oplus it_1^2$

[0038] 其中，rt_1^2表示实体域的域代理对用户域的域代理的推荐信任向量，dt_1^2表示实体域的域代理对用户域的域代理的直接推荐信任向量，it_1^2表示实体域的域代理对用户域的域代理的间接推荐信任向量，⊕表示合并操作；

[0039] (3e)按照下式，计算实体域的域代理对用户域的域代理的综合信任向量：

[0040] $ct_1^2 = dt_1^2 \oplus rt_1^2$

[0041] 其中，ct_1^2表示实体域的域代理对用户域的域代理的综合信任向量，dt_1^2表示实体域的域代理对用户域的域代理的直接信任向量，rt_1^2表示实体域的域代理对用户域的域代理的推荐信任向量，⊕表示合并操作；

[0042] (3f)判断实体域的域代理对用户域的域代理的综合信任向量的最大分量是否大于0.5，若是，执行步骤(3f)，否则，执行步骤(6)；

[0043] (3g)将实体域的域代理对用户域的域代理信任评估的结果，发送给用户域中的发送请求的用户；

[0044] (4)判断用户域与实体域是否满足相互信任条件，若是，则执行步骤(5)，否则，执行步骤(6)；

[0045] (5)用户域中发送请求的用户访问实体域中的信息服务实体；

[0046] (6)用户域中发送请求的用户拒绝访问实体域中的信息服务实体。

[0047] 本发明与现有的技术相比具有以下优点：

[0048] 第一，由于本发明通过评估域代理之间的信任度，实现域之间的双向认证，克服了现有技术在实现域代理之间的认证时，基于公钥基础设施认证体系证书管理复杂的问题，使得本发明在实现域代理之间的认证过程中具有高效性的优点。

[0049] 第二，由于本发明通过评估域代理之间的信任度，实现域之间的双向信任，克服了现有技术在基于身份的跨域认证过程，事先确定不同的域使用相同的系统参数，从而导致实用性差的问题，使得本发明在实现跨域认证的过程中具有高实用性的优点。

[0050] 第三，由于本发明使用了一次基于身份的签名验证算法，克服了现有技术在跨域认证过程中，使用大量基于椭圆曲线点乘和双线对运算，从而造成时间复杂度高和认证过程复杂的问题，使得本发明在跨域认证的过程中具有计算量少，通信开销低的优点。

附图说明

[0051] 图1为本发明的流程图；

[0052] 图2为本发明仿真实验结果图。

具体实施方式

[0053] 下面结合附图对本发明做进一步的描述。

[0054] 参照图1，本发明的具体实施步骤做进一步的描述。

[0055] 步骤1，发送认证请求：

[0056] 利用身份签名算法，用户域中发送请求的用户对消息进行签名，得到消息的杂凑值和签名消息。

[0057] 所述的消息包括用户域中发送请求的时间戳、用户的身份标识、实体域中被访问的信息服务实体的身份标识。

[0058] 所述的身份签名算法的具体步骤如下：

[0059] 第1步，将用户域中发送请求的时间戳、用户的身份标识、实体域中被访问的信息服务实体的身份标识组成消息；

[0060] 第2步，使用密码杂凑函数，将消息转化成一个杂凑值；

[0061] 第3步，密钥生成中心产生一个随机数作为系统的主密钥，$s\in[1,N-1]$，其中，s表

示由密钥生成中心产生的随机数，∈表示属于符号，N表示一个乘法循环群的阶数；

[0062] 第4步，密钥生成中心随机选择并公开一个字节，将所选字节作为用户的私钥生成函数识别符；

[0063] 第5步，按照下式，生成用户域中发送请求用户的私钥：

[0064] $$d = P \times \frac{s}{H(ID||i)+s}$$

[0065] 其中，d表示用户域中发送请求用户的私钥，P表示N阶乘法循环群的生成元，s表示基于身份的密码体制系统的主密钥，H(ID||i)表示用哈希函数将输入的用户域中发送请求用户的身份标识ID和用户私钥生成函数识别符i连接的比特串输出为一个整数；

[0066] 第6步，按照下式，生成用户域中发送请求用户的公钥：

[0067] Q＝H(ID||i)×P+s×P

[0068] 其中，Q表示用户域中发送请求用户的公钥，H(ID||i)表示用哈希函数将输入的用户域中发送请求用户的身份标识ID和用户私钥生成函数识别符i连接的比特串输出为一个整数，P表示N阶乘法循环群的生成元，s表示基于身份的密码体制系统的主密钥；

[0069] 第7步，发送请求的用户产生一个随机数，1≤r≤N-1，r表示由发送请求用户产生的随机数，N表示一个乘法循环群的阶数；

[0070] 第8步，按照下式，生成请求用户对消息的签名：

[0071] S＝d×[(r-h)modN]

[0072] 其中，S表示请求的用户对消息的签名，d表示发送请求用户的私钥，r表示发送请求用户产生的随机数，h表示消息杂凑值，mod表示取余操作，[●]表示取整操作。

[0073] 用户域内发送请求的用户将消息、消息的杂凑值和签名消息发送给用户域的域代理。

[0074] 用户域的域代理验证用户的身份是否合法，若是，则执行步骤(2)，否则，中止认证。

[0075] 用户域的域代理按照下式计算消息杂凑值，将所计算出的消息杂凑值与收到的消息杂凑值相等的发送请求用户判定为身份合法的用户：

[0076] $$h_2 = H_2(M_1, e(Q,S_1)\times e(P,sP)^h)$$

[0077] 其中，h_2表示用户域的域代理计算的消息杂凑值，$H_2(\bullet)$表示哈希函数，M_1表示用户域的域代理收到的消息，e(•)表示双线性对操作，Q表示发送请求用户的公钥，S_1表示用户域的域代理收到的签名消息，P表示生成乘法循环群的生成元，s表示由密钥生成中心产生的随机数，h_1表示用户域的域代理收到的消息杂凑值。

[0078] 步骤2，用户域的域代理对实体域的域代理进行评估。

[0079] 将用户域的域代理作为发送方，实体域的域代理作为请求方，利用双向信任响应的方法，得到关于实体域的域代理的各个直接信任向量。

[0080] 所述的双向信任响应的方法的具体步骤如下：

[0081] 第1步，用户域的域代理从自身存储的交易信息表中查找实体域的域代理的信息，存在，则直接取出对实体域的域代理的直接信任向量；

[0082] 第2步，用户域的域代理将评估实体域的域代理的请求消息发送给交易信息表中除实体域的域代理以外的其他域代理；

[0083] 第3步，收到请求消息域代理从其交易信息表中取出对实体域的域代理的直接信任向量，并发送给用户域的域代理；

[0084] 第4步，收到请求消息的域代理将信任评估验证方的请求消息发送给其交易信息表中除实体域的域代理以外的其他域代理；

[0085] 第5步，收到请求消息的域代理从自身的交易信息表中取出对实体域的域代理的直接信任向量，并发送给该域代理的发送方，该域代理的发送方再发送给用户域的域代理。

[0086] 按照下式，计算用户域的域代理对实体域的域代理的直接推荐信任向量：

[0087] $$dt_1^2 = t_1^k \otimes t_k^2$$

[0088] 其中，dt_1^2表示用户域的域代理对实体域的域代理的直接推荐信任向量，t_1^k表示用户域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^2表示其中一个收到请求消息的域代理对实体域的域代理的直接信任向量，$\otimes$表示连接操作。

[0089] 按照下式，用户域的域代理对实体域的域代理的间接推荐信任向量：

[0090] $$it_1^2 = t_1^k \otimes t_k^m \otimes t_m^2$$

[0091] 其中，it_1^2表示用户域的域代理对实体域的域代理的间接推荐信任向量，t_1^k表示用户域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^m表示其中一个收到请求消息的域代理对其交易信息表中的一个域代理的直接信任向量，t_m^2表示收到请求消息域代理交易信息表中的一个域代理对用实体域的域代理的直接信任向量，$\otimes$表示连接操作。

[0092] 按照下式，计算用户域的域代理对实体域的域代理的推荐信任向量：

[0093] $$rt_1^2 = dt_1^2 \oplus it_1^2$$

[0094] 其中，rt_1^2表示用户域的域代理对实体域的域代理的推荐信任向量，dt_1^2表示用户域的域代理对实体域的域代理的直接推荐信任向量，it_1^2表示用户域的域代理对实体域的域代理的间接推荐信任向量，$\oplus$表示合并操作。

[0095] 按照下式，计算用户域的域代理对实体域的域代理的综合信任向量：

[0096] $$ct_1^2 = dt_1^2 \oplus rt_1^2$$

[0097] 其中，ct_1^2表示用户域的域代理对实体域的域代理的综合信任向量，dt_1^2表示用户域的域代理对实体域的域代理的直接信任向量，rt_1^2表示用户域的域代理对实体域的域代理的推荐信任向量，$\oplus$表示合并操作。

[0098] 判断用户域的域代理对实体域的域代理的综合信任向量的最大分量是否大于0.5，若是，执行步骤3，否则，执行步骤6。

[0099] 步骤3，实体域的域代理对用户域的域代理的信任度进行评估。

[0100] 将实体域的域代理作为发送方，用户域的域代理作为验证方，利用双向信任响应的方法，得到关于用户域的域代理的各个直接信任向量。

[0101] 所述的双向信任响应的方法的具体步骤如下：

[0102] 第1步，实体域的域代理从自身存储的交易信息表中查找用户域的域代理的信息，存在，则直接取出对用户域的域代理的直接信任向量；

[0103] 第2步，实体域的域代理将评估用户域的域代理的请求消息发送给交易信息表中

除用户域的域代理以外的其他域代理；

[0104] 第3步，收到请求消息域代理从其交易信息表中取出对用户域的域代理的直接信任向量，并发送给实体域的域代理；

[0105] 第4步，收到请求消息的域代理将信任评估用户域的域代理的请求消息发送给其交易信息表中除用户域的域代理以外的其他域代理；

[0106] 第5步，收到请求消息的域代理从自身的交易信息表中取出对用户域的域代理的直接信任向量，并发送给该域代理的发送方，该域代理的发送方再发送给实体域的域代理。

[0107] 按照下式，计算实体域的域代理对用户域的域代理的直接推荐信任向量：

[0108] $$dt_1^2 = t_1^k \otimes t_k^2$$

[0109] 其中，dt_1^2表示实体域的域代理对用户域的域代理的直接推荐信任向量，t_1^k表示实体域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^2表示其中一个收到请求消息的域代理对用户域的域代理的直接信任向量，⊗表示连接操作；

[0110] 按照下式，实体域的域代理对用户域的域代理的间接推荐信任向量：

[0111] $$it_1^2 = t_1^k \otimes t_k^m \otimes t_m^2$$

[0112] 其中，it_1^2表示实体域的域代理对用户域的域代理的间接推荐信任向量，t_1^k表示实体域的域代理对其中一个收到请求消息的域代理的直接信任向量，t_k^m表示其中一个收到请求消息的域代理对其交易信息表中的一个域代理的直接信任向量，t_m^2表示收到请求消息域代理交易信息表中的一个域代理对用户域的域代理的直接信任向量，⊗表示连接操作。

[0113] 按照下式，计算实体域的域代理对实体域的域代理的推荐信任向量：

[0114] $$rt_1^2 = dt_1^2 \oplus it_1^2$$

[0115] 其中，rt_1^2表示实体域的域代理对用户域的域代理的推荐信任向量，dt_1^2表示实体域的域代理对用户域的域代理的直接推荐信任向量，it_1^2表示实体域的域代理对用户域的域代理的间接推荐信任向量，⊕表示合并操作。

[0116] 按照下式，计算实体域的域代理对用户域的域代理的综合信任向量：

[0117] $$ct_1^2 = dt_1^2 \oplus rt_1^2$$

[0118] 其中，ct_1^2表示实体域的域代理对用户域的域代理的综合信任向量，dt_1^2表示实体域的域代理对用户域的域代理的直接信任向量，rt_1^2表示实体域的域代理对用户域的域代理的推荐信任向量，⊕表示合并操作。

[0119] 判断实体域的域代理对用户域的域代理的综合信任向量的最大分量是否大于0.5，执行步骤4，否则，执行步骤6。

[0120] 步骤4，用户域中的发送请求的用户判断用户域与实体域是否满足相互信任条件，若是，执行步骤5，否则，执行步骤6。

[0121] 所述相互信任条件是指同时满足以下两个条件的情形：

[0122] 条件1，用户域的域代理对实体域的域代理的综合信任向量的最大分量大于0.5；

[0123] 条件2，用户域域代理对实体域的域代理的综合信任向量的最大分量大于0.5。

[0124] 步骤5，用户域中发送请求的用户访问实体域中的信息服务实体。

[0125] 步骤6，用户域中发送请求的用户拒绝访问实体域中的信息服务实体。

[0126] 本发明的效果可以通过下述仿真实验得到验证。

[0127] 1.仿真条件：

[0128] 本发明的仿真实验条件为:MATLAB R2016a,3.20GHz的Intel Pentium(R)Dual-Core CPU,内存8G,Windows7旗舰版。

[0129] 2.仿真内容：

[0130] 本发明的仿真实验是采用本发明的合并连接算子和现有信任评估技术的普通算子的计算推荐信任向量最大分量的方法,对本发明所选取的各个域代理的直接信任向量进行推荐信任向量最大分量的计算。将采用本发明的合并连接算子所计算的推荐信任向量的最大分量,与使用现有信任评估技术的普通算子计算的推荐信任向量的最大分量进行对比,得到如图2所示的两条曲线。

[0131] 3.仿真结果分析：

[0132] 图2是本发明的合并连接算子与现有信任评估技术的普通算子计算推荐信任向量的最大分量随推荐域代理数量变化的曲线图,其中,图2中的横坐标表示推荐域代理的数量,纵坐标表示推进信任向量的最大分量。图2中以实线表示采用本发明的合并连接算子计算的推荐信任向量的最大分量曲线,图2中以虚线表示采用现有信任评估技术的普通算子计算的推荐信任向量的最大分量曲线。

[0133] 由图2可见,在横坐标表示的相同数量推荐域代理的条件下,采用本发明的合并连接算子计算的推荐信任向量的最大分量,比现有信任评估技术的普通算子计算的推荐信任向量的最大分量小很多,说明采用本发明的合并连接算子比现有信任评估技术的普通算子的信任评估更加精确。

[0134] 由以上的仿真结果表明:本发明由于采用连接算子,连接从域代理的交易信息表中提取的直接信任向量,用合并算子合并多条推荐路径上的信任向量,以便计算精确的推荐信任向量最大分量,从而有效的评估了域代理之间的信任度,提高了域代理之间认证的准确度,实现了用户对信息服务实体安全有效的跨域认证。

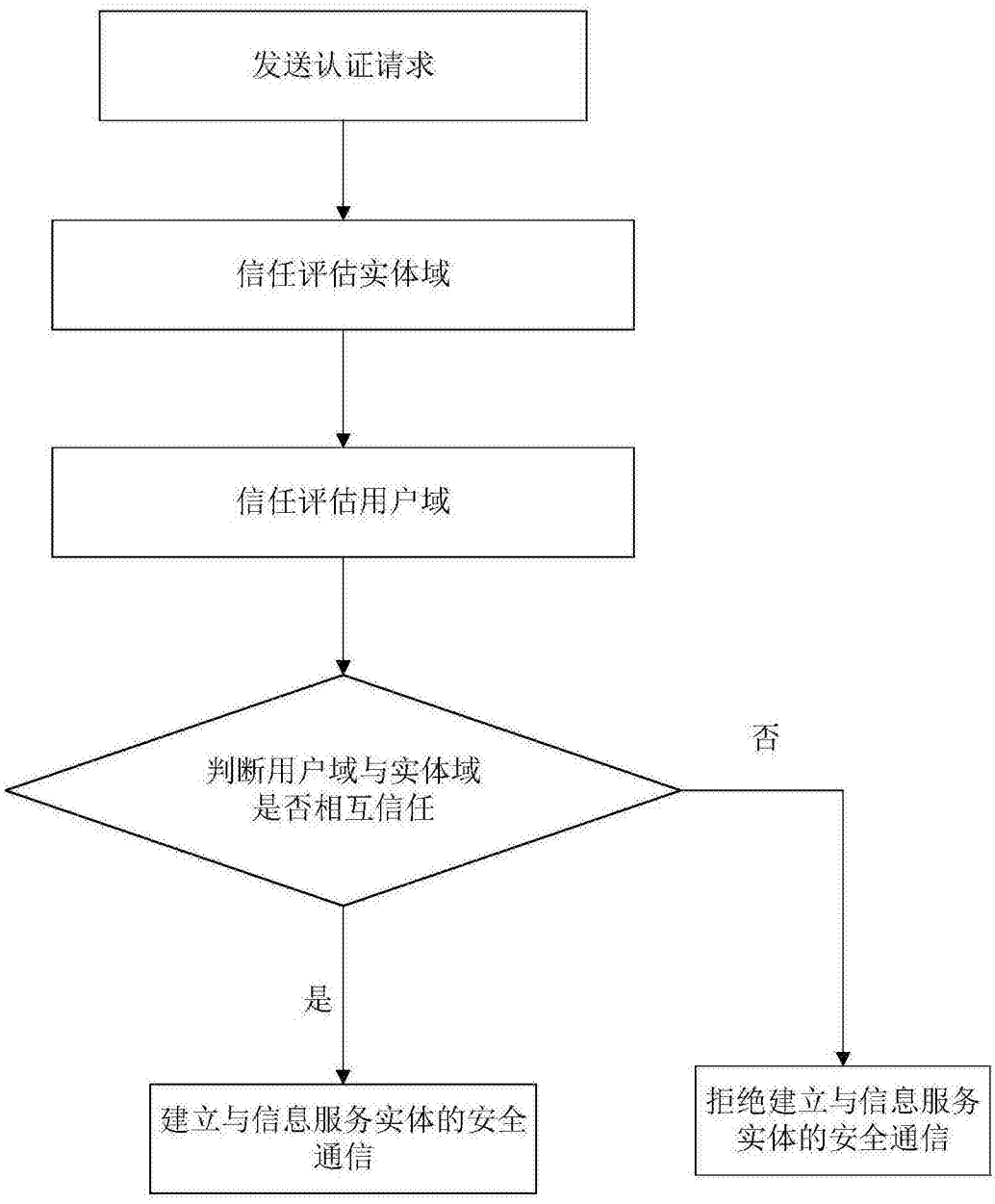

发送认证请求
信任评估实体域
信任评估用户域
判断用户域与实体域
是否相互信任
否
是
建立与信息服务实体的安全
通信
拒绝建立与信息服务
实体的安全通信

图1

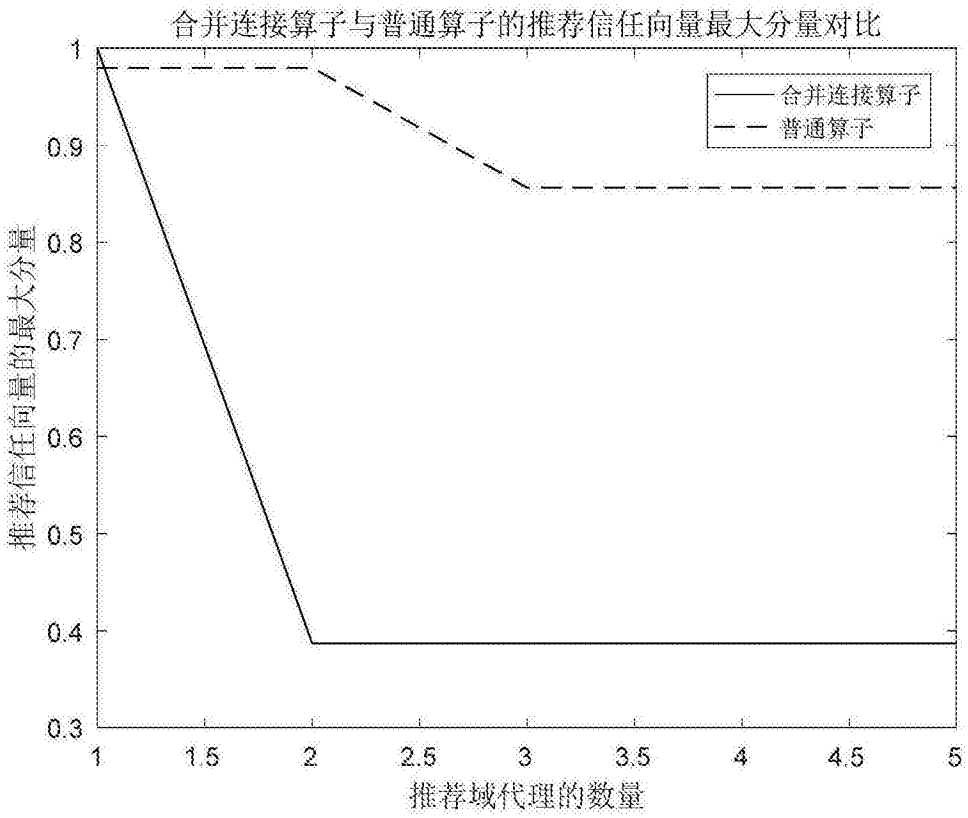

合并连接算子与普通算子的推荐信任向量最大分量对比
合并连接算子
普通算子
推荐信任向量的最大分量
推荐域代理的数量
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
1
1.5
2
2.5
3
3.5
4
4.5
5

图2