一种基于模糊逻辑的网络认证扩展模型 *

李 伟, 范明钰
(电子科技大学 计算机科学与工程学院, 成都 610054)

摘 要: 为了解决主体之间的信任关系一般很难用精确方式来描述这一问题,以模糊逻辑为基础对传统基于数字证书的主体认证模型进行了扩展,并对认证路径的构造和信任值计算规则进行了研究,该算法可以信任值为基础给出了信任级别的计算方法,为网络认证的研究提供了一条新思路。

关键词: 模糊逻辑; 数字证书; 认证路径
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)03-1026-03
doi:10.3969/j.issn.1001-3695.2010.03.060

Authentication extension model in networks based on fuzzy logic

LI Wei, FAN Ming-yu
(*School of Computer Science & Engineering, University of Electronic Science & Technology of China, Chengdu* 610054, *China*)

Abstract: At present the authentication process in PKI is based on digital certification, but in reality most of the users of digital certification is principal such as persons, and their trust model is difficult to depict with precise authentication. This paper proffered an extension scheme to traditional digital certification authenticate model based on fuzzy logic, and the construction of trust path and method for computation of confidence value, so proposed a new method for networks authentication.
Key words: fuzzy logic; digital certification; trust path

公钥基础设施(PKI)是目前在开放式网络环境中保障网络和信息系统安全运行的最有效的技术,利用公钥证书建立起来的信任关系可以方便地保障个人及组织在网络中秘密通信。另外 PKI 也是实施电子商务和电子政务的基础平台,也是诸多基于网络应用的新产品、新业务安全开展的基本保障。

PKI 的核心问题是解决网络中实体的信任问题,人们已经提出了很多基于 PKI 的信任模型。目前在实践中信任问题主要是通过 X.509 数字证书来解决,即信息的接收者通过共同信任的 CA 公钥来验证发送者的数字证书来决定是否信任消息发送者,数字证书通过 CA 的私钥进行签名,在公钥算法和通信协议安全的前提下任何人都不可能伪造数字证书。

在现实生活中实际存在两种信任关系,一种是客体之间的信任,即排除了人的主观因素的对象或实体(如设备等)。客体之间的信任是基于证据的,可以精确描述和验证,其基本研究方法是推理和证明,如对于安全协议的研究。另一种信任关系是主体之间的信任关系,这里的主体是指人或代表人的客体。这种信任关系具有主观性、模糊性和不确定性,很难用精确的形式来描述[1]。在现实中,证书的使用者很多情况下是人,因此有必要利用模糊认证的方式对证书认证进行扩展,使其更符合现实情况。

关于主观模糊信任研究目前已经取得了一些成果[2~5],文献[2~4]对主观信任进行了有益的探索,但是将信任的主观性和不确定性等同于随机性,使用概率模型对主观信任进行建模,因此这些信任模型存在诸多不足,无法处理信任本身的模糊性。文献[5]对这一问题进行了进一步的研究,提出了开放式网络环境的自主信任模型,但模型中需要引入一定数量的信任头(header),即各主体完全信任的节点,而这在实际网络系统中很难做到。针对上述问题,本文在这些研究成果的基础上,对具体的 PKI 网络体系中的主观信任问题进行了研究,并给出了正确的找到任意主体之间信任值和认证路径的计算规则。在此基础上计算出信任级别,对传统的基于证书的主体认证进行扩展。

1 PKI 认证模型[6]

在基于 X.509 公钥证书的 PKI 系统中,认证的过程实际上就是对证书的验证过程。假设网络中的通信实体 A 要向 B 发送消息 m,他们共同信任认证中心 CA,则其通信过程如下:$A \rightarrow B \{M, Sig_A(M), PUB_A, Cer(A)\}$。其中 $Sig_A(M)$ 是 A 利用自己的私钥对消息 M 的签名,PUB_A 是 A 的公钥,Cer(A)是 CA 用自己的私钥为 A 签发的证书。当 B 接收到上述消息之后,它首先使用 CA 公钥来验证 Cer(A)的合法性,然后再通过 PUB_A 来验证签名 $Sig_A(M)$ 来决定消息的真实性。

上述的精确模型很难解决实体之间信任关系的随意性和模糊性,为此本文提出了基于模糊逻辑的认证关系。

2 信任的度量

首先给出模糊集合及其隶属度的定义。

定义 1[1] 设论域为非空集合 X,x 为 X 中的元素,对于任意的 $x \in X$ 有如下映射:$X \rightarrow [0,1]$, $x \rightarrow \mu_A(x) \in [0,1]$,则称由序对 $A = \{(x, \mu_A(x))\}$ 组成的集合为 X 上的模糊集合,称 $\mu_A(x)$ 为 x 对 A 的隶属函数,对于某个具体的 x 而言,

收稿日期: 2009-06-12; **修回日期**: 2009-08-18 **基金项目**: 国家"863"计划资助项目(2009AA01Z403)
作者简介:李伟(1980-),男,山东淄博人,博士研究生,主要研究方向为信息安全(7imei@163.com);范明钰(1962-),女,教授,博导,博士,主要研究方向为信息安全.

称 $\mu_A(x)$ 为 x 对 A 的隶属度。

信任关系通常由语言变量来描述,语言变量是以自然语言或人工语言中的字或句为取值域的变量,其取值不是数值,语言变量可以表示那些本身具有模糊性,十分复杂或定义很不完善,无法用通常精确方式来描述的概念。

根据模糊集合理论,可以用元组(L, $S(L)$, U_L, G_L, M_L)来表示语言变量[1]。其中 L 是变量名称,U_L 是语言变量的论域,$S(L)$是变量的值的集合,G_L 是语法规则,用于产生变量值的名称,M_L 是语义规则,用于产生隶属度函数。

例如,定义模糊语言变量信任一词,用符号 T 来表示,信任的程度用不同的信任等级来描述,分别为不信任、有点信任、信任、非常信任、完全信任五个等级,分别用数字 1 ~5 来表示,那么这里论域 U_T = {1,2,3,4,5},语言值集合 $S(T)$ = {不信任、有点信任、信任、非常信任、完全信任},语法规则 G_T 是将表示程度的修饰词语模糊语言变量信任连接起来的规则,语义规则 M_T 表示各语言值代表的模糊集合的隶属度函数。

3　模糊认证路径和信任级别的确定

在这种认证关系中,两个实体之间首先计算信任值,可以用一个 0 ~1 的数值来表示。其中 0 表示完全不信任,1 表示完全信任,而(0 ,1)之间的数值表示介于完全不信任和完全信任之间,数值越大表示信任的程度越高。

根据隶属度函数的规则,信任值将进一步转换成对各个信任级别的信任向量 V = {v_1, v_2, v_3, v_4, v_5}。其中 v_i(i = 1, 2, 3, 4, 5)表示根据隶属度函数计算出的信任值对应的各个信任级别的隶属度,对于极端情况,当信任值等于 0 时,则 V = {1, 0, 0, 0, 0 },当信任值等于 1 时 V = {0, 0, 0, 0, 1 },对于介于 0 ~1 的信任值则 V 根据具体的隶属度函数来计算。

网络中间实体之间信任的传递是基于信任值的,当信任值到达终端实体时再根据信任值确定信任向量,最终计算出信任等级。因此,本文将首先讨论信任值的传递。

在网络通信中信息的重要程度也有差别,对于重要信息一般要求发送者的信任值要大,这也是跟日常生活相符的。

有了上述的信任关系之后,要解决的问题是网络中任意两个实体信任值的计算问题,为此需要根据不同的网络结构来研究相关的算法。

3.1　单一路径信任值的计算

这是最简单的一种情况,在这里任意两个实体之间只有一条可达路径,实际上就是树状结构的 PKI 体系。假设任意两个实体 A 和 B,它们都跟 CA 直接相连。其中 A 与 CA 通过路径 R_1 相连,B 与 CA 通过路径 R_2 相连,用 μ_R(B, A)来表示 B 对 A 的信任程度,下标 R 代表 B 到 A 的路径,在这里路径是惟一的。设 CA 对 A 的信任程度为 μ_{R1}(CA, A),B 对 CA 的信任程度为 μ_{R2}(B,CA),则 B 对 A 的信任程度可以通过如下公式进行计算:

$$\mu_R(B,A) = \mu_{R2}(B,CA) \wedge \mu_{R1}(CA, A) \tag{1}$$

其中:∧为模糊数学中的合取运算,表示两者中取较小的数值。

如果 A 和 B 通过多层 CA 连接则计算方法与上述相似,即将连接 B 与 A 的各段路径的信任值进行合取运算。各个 CA 之间的信任值可以从他们相互签发的前向证书和后向证书所组成的证书链中获取,这可以通过在证书的扩展选项中添加信任值一项来实现。一般来说信任关系并不满足自反性,即 μ_R(B, A) = μ_R(A,B)不一定成立。

3.2　网状结构信任值的计算

在网状结构中,任意两个实体之间的连接路径不惟一,这给信任值的计算带来了一定的困难,假设实体 A 与 B 之间的连接路径有 p 条,分别用 L_1, L_2, …, L_p 来表示。一般来说 A 与 B 之间的信任值计算有两种方式,一种是基于最大信任的计算,计算公式如下:

$$\mu_R(B,A) = \bigvee_{i=1}^{p} \mu_{Li}(B , A) \tag{2}$$

另外一种是基于最小信任的计算,计算公式如下:

$$\mu_R(B,A) = \bigwedge_{i=1}^{p} \mu_{Li}(B , A) \tag{3}$$

其中:μ_{Li}(B , A)是路径 L_i 的信任值,在本文中采用式(2)进行计算。

理论上来说,可通过找出 A 与 B 间的所有路径,然后按照式(2)计算出两者之间的信任值,这在小规模的网络中是可行的,但是在中等或大规模的网络中计算量非常大,所以在现实中必须找到可行的信任值计算方法。可以通过计算模糊图生成树的思想来解决这一问题。为此,首先给出如下定理:

定理 1　设 G = (V , R)是 PKI 体系结构所组成的网络。其中 V 代表实体节点,R 代表节点之间的连接,对于以某一实体为根节点的所有生成树 T_c,如果存在生成树 T 使得 $\sum_{e\in E(T_c)} \mu_R(e) \leqslant \sum_{e\in E(T)} \mu_R(e)$,那么树 T 就是这一实体的信任树。其中 e 表示树中这一实体与其他实体相连接的路径或中间路径。这一实体对其他外部任何网络实体的信任值可以通过信任树中两者之间的惟一路径计算。

证明　设对于任意 $e' \in E(T)$,从 T 中移除 e'后得到 T_1 和 T_2,则 $\mu_R(e')$ = max ($\mu_R(e)$)。其中 $e \in E^*(e')$,$E^*(e')$是 T_1 和 T_2 间的所有连接路径,否则设存在另一路径 e^* 使得 $\mu_R(e^*)$ = max ($\mu_R(e)$),用 e^* 替换 e'后可得到另一树 T^* 但是 $\sum_{e\in E(T)} \mu_R(e) \leqslant \sum_{e\in E(T^*)} \mu_R(e)$,这与 T 的定义矛盾。假设 R 是 T 中连接 A 与 B 的惟一路径,μ_R(A,B) = $\mu_R(e)$,则从 T 中移除 e 后得到 T_1 和 T_2,假设 A ∈ $V(T_1)$,B ∈ $V(T_2)$,则有以上知 $\mu_R(e)$是 T_1 和 T_2间所有连接路径中信任值的最大值。证毕。

由于模糊信任关系一般不满足自反性,不同实体的信任树有可能不同。在实际应用中信任树是由网络中的实体来自己计算的,信任树与模糊图论中的最大树相对应。在模糊图论中有相应的算法[7]。网络中的节点只需要计算它对相邻节点的信任值即可。

3.3　不同认证域的信任值计算

实际应用中经常遇到不同认证域中实体的通信问题,这时可以通过域间信任传递的方式来解决。假设有两个认证域,它们的信任锚分别是 CA_1 和 CA_2,CA_1 和 CA_2 的网络结构可以是任何形式的,假设 A 和 B 分别是属于 CA_1 和 CA_2 网络的实体,那么 A 对 B 的信任值可以如下计算:a)根据 A 到 CA_1 的证书链计算出 A 对 CA_1 的信任值;b)根据 CA_1 和 CA_2 的交叉证书计算出 CA_1 对 CA_2 的信任值;c)根据 CA_2 的认证树得到 CA_2 对 B 的信任值。

根据以上步骤得到的数据可以计算出 A 对 B 的信任值。

3.4　信任级别的计算

首先定义五个级别对应的信任向量:

$$T_1 = M_T(\text{不信任}) = (1,0,0,0,0)$$
$$T_2 = M_T(\text{有点信任}) = (0,1,0,0,0)$$
$$T_3 = M_T(\text{信任}) = (0,0,1,0,0)$$
$$T_4 = M_T(\text{非常信任}) = (0,0,0,1,0)$$
$$T_5 = M_T(\text{完全信任}) = (0,0,0,0,1)$$

计算出信任值后,将根据具体的隶属度函数计算出信任值对应的信任向量 $V = \{v_1, v_2, v_3, v_4, v_5\}$。其中 $v_i (i = 1, 2, 3, 4, 5)$,然后信任级别的确定可通过如下方式之一来计算:

a)基于格贴近度的计算方式。当得到信任向量 V 之后,计算它与各个级别的贴近度 $\sigma(V, T_i) = (V \circ T_i) \wedge (1 - V \ 7 \ T_i)$,这里 $\circ$和7 分别表示内积和外积,然后取最大值即可得出相应的信任级别。

b)基于去模糊化处理。当得到信任向量 $V = \{v_1, v_2, v_3, v_4, v_5\}$。其中 $v_i (i = 1, 2, 3, 4, 5)$之后,根据去模糊化函数 $DF(V) = \sum_{i=1}^{5} v_i m_i$。其中 v_i 是 V 中的第 i 个元素,m_i 表示第 i 个位置,这样便得出一个介于 1 ~ 5 的数值,然后根据最邻近原则确定信任级别。

4 模糊认证过程

有了认证路径的计算方法后,就可以此为基础对基本 PKI 认证过程进行扩展。假设网络中的通信实体 A 要向 B 发送消息 m,那么他们的通信过程如下:$A \rightarrow B \{M, Sig_A(M), PUB_A, Cer(A)\}$。其中 $Sig_A(M)$是 A 利用自己的私钥对消息 M 的签名,PUB_A 是 A 的公钥,Cer(A)是为 A 的证书。当 B 接收到上述消息之后,首先使用 CA 公钥来验证 Cer(A)的合法性,再通过 PUB_A 来验证签名 $Sig_A(M)$来决定消息的真实性,然后 B 根据自己的信任树来计算对 A 的信任值 $\mu_R(B, A)$,根据信任值来决定消息的信任级别。一般来说对于重要消息要求的信任值要相对较大,从而信任级别要相对较高。

5 结束语

本文中根据模糊逻辑对基于证书的 PKI 认证方式进行了扩展,以模糊图论为基础对认证路径的构造以及信任值的传递计算规则进行了研究,并根据计算出来的信任值给出了一种直观的信任推理机制来确定信任级别,为网络认证的研究提供了一条新的思路。

参考文献:

[1] 唐文,胡建斌,陈钟. 基于模糊逻辑的主观信任管理模型研究[J]. 计算机研究与发展,2005,42(10):1654-1659.

[2] JASANG A. A logic for uncertain probabilities [J]. International Journal of Uncertainty Fuzziness, Fuzziness and Knowledge-based Systems, 2001,9(3):279-311.

[3] BLAZE M, FEIGENBAUM J, KEROMYTIS A D. Trust management for public-key infrastructure [C]//Proc of Cambridge Security Protocol International Workshop. Berlin: Springer-Verlag,1998: 59-63.

[4] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks [C]// Proc of the 3rd European Symposium on Research in Computer Security. London:Springer-Verlag,1994: 3-18.

[5] 张仕斌,何大可,遠藤誉. 模糊自主信任建立策略的研究[J]. 电子与信息学报,2006,28(8):1492-1496.

[6] 谢冬青,冷键. PKI 原理与技术[M]. 北京:清华大学出版社,2004:79-80.

[7] 彭祖赠,孙韫玉. 模糊数学及其应用[M]. 武汉:武汉大学出版社,2004:182-188.

(上接第 1018 页)须嵌入溢出定位图、不适合彩色图像等缺点,提出一种基于色彩分量间预测误差差值扩展的彩色图像可逆数据隐藏算法。该算法将差值扩展量分散到两个色彩分量中,减少了对图像的修改,从而提高含密图像质量。信息提取不需要原始图像,提取端不需要溢出定位图即可提取数据并恢复原始图像,算法实现和运算效率都具有一定的优势。辅助信息的嵌入位置由密钥决定,隐藏数据相对安全,信息检测简单、高效,避免在不含隐藏数据的图像中提取信息。实验表明,该算法在不影响嵌入容量和图像质量的基础上,提高了嵌入、检测和提取的效率,有利于批量嵌入。算法的不足之处在于,当Ⅲ类差值比较分散时,嵌入容量受到限制,下一步的工作重点是在消除定位图的前提下提高嵌入容量。

参考文献:

[1] TIAN Jun. Reversible data embedding using a difference expansion [J]. IEEE Trans on Circuits and Systems for Video Technology,2003,13(8):890-896.

[2] THODI D M, RODRIGUEZ J J. Expansion embedding techniques for reversible watermarking [J]. IEEE Trans on Image Processing, 2007,16(3):721-730.

[3] ALATTER A M. Reversible watermark using the difference expansion of a generalized integer transform [J]. IEEE Trans on Image Processing,2004,32(8):1147-1156.

[4] 陈开英,胡永健,李健伟. 利用差值扩展进行可逆数据隐藏的新算法[J]. 计算机应用,2008,28(2):455-459.

[5] 邓世文,刘焕平,叶宏宇. 基于 Laplacian 残差扩展的可逆嵌入算法[J]. 计算机工程与应用,2008,44(3):110-113.

[6] 彭德云,王嘉祯. 基于错误控制编码的差值扩展可逆数字水印[J]. 计算机工程,2007,33(21):18-20.

[7] COLTUC D, CHASSER J M. Very fast watermarking by reversible contrast mapping[J]. IEEE Signal Processing Letters,2007,14(4): 255-258.

[8] LIN C, YANG S, HSUEH N. Lossless data hiding based on difference expansion without a location map [C]//Proc of Congress on Image and Signal Processing. 2008:8-12.

[9] 周璐,胡永健,曾华飞. 用于矢量数字地图的可逆数据隐藏算法[J]. 计算机应用,2009,29(4):990-993.

[10] WU Dan, WANG Guo-zhao, GAO Xiao-liang. Reversible watermarking of SVG graphics[C]//Proc of International Conference on Communications and Mobile Computing. 2009:385-390.

[11] HU Yong-jian, LEE H, LI Jian-wei. DE-based reversible data hiding with improved overflow location map [J]. IEEE Trans on Circuits and Systems for Video Technology,2009,19(2):250-260.

[12] CHRYSOCHOS E, VARSAKI E E, FOTOPOULOS V, *et al*. High capacity reversible data hiding using overlapping difference expansion [C]//Proc of Workshop on Image Analysis for Multimedia Interactive Services. 2009 :121-124.

[13] 祝玉新,孙星明,杨恒伏. 基于 Haar 小波的彩色图像可逆水印算法[J]. 计算机应用研究,2007,24(6):165-169.

[14] 杨边,陆哲明,徐殿国,等. 基于邻近像素的低复杂度预测矢量量化图像压缩编码算法[J]. 电子学报,2003,31(5):707-710.

[15] 曹文伦,彭国华,秦洪元,等. 利用色彩分量相关性的彩色图像分形编码方法[J]. 计算机工程与应用,2004,40(22):51-55.