doi:10.3969/j.issn.1000-436x.2013.03.024

基于三维球体模型的 XML 通信协议安全评估方法

杨宏宇，于巾博，谢丽霞
（中国民航大学 计算机科学与技术学院，天津 300300）

摘 要：针对 XML 通信协议的安全评估问题，提出了一种基于三维球体模型的协议安全评估方法。首先利用评估指标在球体外壳层的坐落位置构建 XML 通信协议的三维安全评估指标体系，以该坐标系投影面积为度量标准，运用层次分析法(AHP, analytic hierarchy process)、球体半径以及开合角度获取一、二级评估指标的权值。从 XML 协议的内容、通信载荷、安全隐患 3 个层面计算 XML 通信协议各安全分量的量化评估值，通过量化计算和综合分析得到 XML 通信协议的安全性评估结果。仿真结果表明该方法能有效地评估协议的安全性并可满足对 XML 通信协议的安全性评估需要。

关键词：XML；协议；三维球体模型；层次分析法；安全评估
中图分类号：TP393.08 **文献标识码：**A **文章编号：**1000-436X(2013)03-0183-09

Three-dimensional spherical model based XML communication protocols security evaluation method

YANG Hong-yu, YU Jin-bo, XIE Li-xia
(School of Computer Science and Technology, Civil Avia ion University of China, Tianjin 300300, China)

Abstract: Aiming at the problems of security assessment in XML communication protocols, a novel three-dimensional spherical model based protocol security evaluation method was proposed. Firstly, a three-dimensional security evaluation index system was constructed through positions of indexes on the spherical shell. Secondly, by using the coordinate's projection area as a measure criterion, evaluation indexes' weights of the first level and the second level were obtained with the analytic hierarchy process (AHP), the sphere and the sector angle. Thirdly, security components values of XML communication protocol were calculated in the aspects of XML's content, communication load and security vulnerability. Finally, the security evaluation result of XML communication protocol was achieved through quantization calculation and further comprehensive analysis. Experimental results show that this method is competent for the protocol security evaluation and meets security evaluating requirem L communication protocols effectively.

Key words: XML; protocol; three-dimensional spherical model; AHP; security evaluation

1 引言

XML 作为数据表示和信息交换的通用标准格式，在 Web 服务协议栈（SOAP、WSDL、UDDI 等）及其他通信协议中广泛应用，这类协议使用约定结构的 XML 数据文件完成通信双方的信息交换，具有易扩展、跨平台、异构通信等特性。由于基于 XML 的通信协议在网络通信中的基础作用十分突出，一

收稿日期：2012-05-24；修回日期：2012-10-11
基金项目：国家自然科学基金资助项目（60776807, 61179045）；国家高技术研究发展计划（“863”计划）基金资助项目（2006AA12A205）；天津市科技计划重点基金资助项目（09JCZDJC16800）；中国民航科技基金资助项目（MHRD201009，MHRD201205）；中央高校基本科研业务费专项基金资助项目（ZXH2009A006）
Foundation Items: The National Natural Science Foundation of China (6077 07, 61179045); The National High Technology Research and Development Program of China (863 Program) (2006AA12A205); The Key Project of Science and Technology Support Program of Tianjin (09JCZDJC16800); The Science & Technology Project of CAAC (MHRD201009, MHRD201205); The Central University Basic Science Research Program(ZXH2009A006)

旦协议中的漏洞被利用，将直接影响Web服务应用的安全性。因此，研究XML通信协议的安全评估方法已成为信息安全研究领域的一个热点问题。

目前，国内外已陆续开展针对XML通信协议的安全性评估研究。文献[1]设计了一种威胁模型STRIDE（spoofing, tampering, repudiation, information disclosure elevation），从诈骗、篡改、否认、信息泄露、拒绝服务和权限提升6个方面获取Web协议消息的安全风险值，为查找Web服务安全漏洞提供了有价值的参考依据，但该方法不能评估由于组件的交互作用而导致的关联性威胁，也缺少对协议整体的综合评估。文献[2]提出了一种面向服务的简单对象访问协议(SOAP, simple object access procotol)消息交互的安全机制，从加密、签名、服务时间等角度对SOAP协议进行安全评估。该方法可实现SOAP协议消息的完整性和机密性，但该机制评估对象单一，不适用于其他的XML通信协议。文献[3]针对Web服务协议消息安全措施选择问题，从用户非对称密钥、安全证书、安全令牌等7项技术进行实验评估，为Web服务安全措施的选择提供依据。但该方法未建立完整的安全指标评估体系，缺乏对Web服务协议的定性分析。文献[4]使用SOAP扩展对Web服务进行压缩和记录日志，并将XML签名和加密技术规范融入到SOAP协议中，优化了Web服务的传输效率，但研究重点仅从完整性、不可否认性和身份验证角度对SOAP协议进行安全扩展。文献[5]主要针对XML通信协议中的UDDI协议存在的安全问题提供身份认证、访问控制、XML签名等多项安全保障措施和负载，该方法仅提高了UDDI注册库及数据的访问和传输的安全性能，缺乏有效的安全评估，不能对协议漏洞引起的威胁进行主动防御。文献[6]依据现有PKI的XML安全技术和验证机制，对SAML协议的机密性和完整性进行评估，但评估的指标和性能较低。

从上述研究可以看出，在目前针对XML通信协议的安全性研究中，大多局限于协议某一层面的安全评估，主要关注XML通信协议的安全实现机制，并未从综合评估角度研究基于XML通信协议的安全性。本文针对XML通信协议的安全性评估问题，提出了一种基于三维球体模型的安全评估方法，设计了XML通信协议的安全评估指标三维坐标系，采用球体各坐标投影面积作为评估指标的权值和安全分量指标取值的度量标准，有效地解决了指标重合问题，弥补了国内外在XML通信协议的相关评估指标体系和评估方法上的不足。

2 基于三维球体模型的安全评估指标体系

2.1 模型层次结构

前苏联数学家马库雪维奇把人脑储存的信息分为核与壳2类，提出信息构建的球体模式[7]，本文将该思想引入到协议安全性评估的应用之中，提出XML通信协议的三维球体模型。在该球体模型中，根据协议评估价值和发展成熟度，可将球体划分为一定逻辑关系组成的层次化结构。从内向外依次为网络接口层、网络层、传输层及应用层协议（如图1所示）。

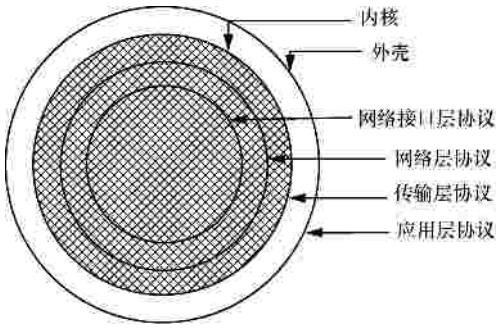


图1 三维球体模型层次结构

2.2 评估指标体系

XML通信协议隶属应用层，因此本文借助球体模型的外壳层构建XML通信协议的安全评估指标体系。首先，设计了针对XML通信协议安全性评估的一、二级评估指标——三维坐标系，设定一、二级评估指标的坐落面（如图2所示）。该三维坐标系由xOy、xOz和yOz 3个平面划分为8个象限，设XML通信协议的安全性总目标为A，而后从XML协议内容、通信载荷、安全隐患3个面确定一级评估指标B_i、二级评估指标C_{ij}及其坐落面。

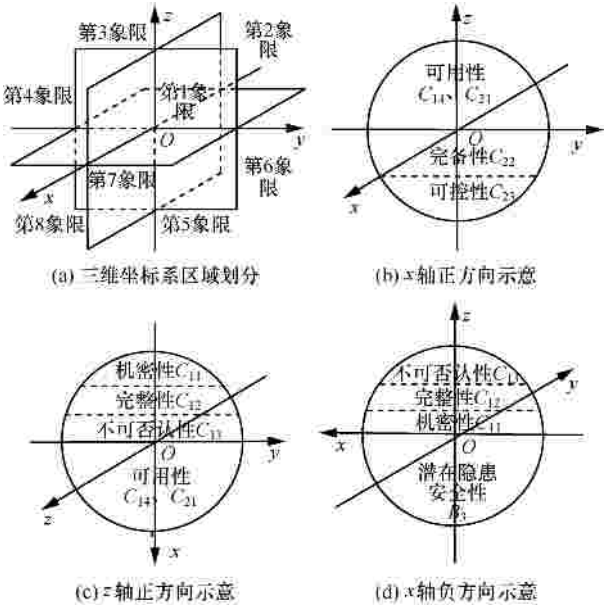
1) XML协议内容的安全性B_1。评估指标B_1位于第1、2、3、4象限，按XML内容要素划分为机密性C_{11}、完整性C_{12}、不可否认性C_{13}和可用性C_{14}。

2) 通信载荷的安全性B_2。评估指标B_2位于第1、4、5、8象限，按语义三要素划分为可用性C_{21}、完备性C_{22}和可控性C_{23}。

3) 安全隐患的安全性B_3。评估指标B_3位于第6、7象限，按4种基本攻击类型划分为截获C_{31}、篡改C_{32}、伪造C_{33}和中断C_{34}。

需要说明的是，为加强对某方面的重点调查和

评价，有时评估指标之间会出现一定程度的重合[8]。三维球体模型与一般评估模型的区别在于解决评估指标的重复问题，去除冗余值，从而保障了评估结果的合理性。



(a) 三维坐标系区域划分　(b) x轴正方向示意　(c) z轴正方向示意　(d) x轴负方向示意

图 2　一、二级评估指标坐落面设定

2.3　评估指标权值的计算

依据所构建的安全评估指标体系，首先采用层次分析法[9]对一、二级评估指标的权值进行计算，根据球体模型的特点，以球体 xOz 坐标平面的投影面积分配评估指标的权值。利用球体半径以及扇面的开合角度对一、二级评估指标权重进行直观表示，保证了安全评估的全面性。评估指标的权值计算过程设计如下。

步骤 1　一、二级评估指标权值计算

1) 构造一级评估指标 B_i 的判断矩阵 $\boldsymbol{P}_0$，以及隶属于 XML 内容安全性、通信载荷安全性和隐患安全性的二级评估指标 C_{ij} 的判断矩阵，分别记为 $\boldsymbol{P}_1$、$\boldsymbol{P}_2$、$\boldsymbol{P}_3$。

$$\boldsymbol{P}_0=\begin{bmatrix}1 & 3 & 5\\ 1/3 & 1 & 4\\ 1/5 & 1/4 & 1\end{bmatrix}$$

$$\boldsymbol{P}_1=\begin{bmatrix}1 & 1 & 3 & 1\\ 1 & 1 & 3 & 1\\ 1/3 & 1/3 & 1 & 1/3\\ 1 & 1 & 3 & 1\end{bmatrix}$$

$$\boldsymbol{P}_2=\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}$$

$$\boldsymbol{P}_3=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\end{bmatrix}$$

2) 采用方根法计算权向量，设一级评估指标权向量 $W_0=(W_1,W_2,W_3)^{\mathrm{T}}$，二级评估指标权向量 $W_1=(W_{21},W_{22},W_{13},W_{14})^{\mathrm{T}}$、$W_2=(W_{21},W_{22},W_{23})^{\mathrm{T}}$、$W_3=(W_{31},W_{32},W_{33},W_{34})^{\mathrm{T}}$，计算公式为

$$W_i=m_i/\sum_{j=1}^{n}m_j \tag{1}$$

其中，m_i 为判断矩阵各行元素乘积的 n 次方根，经一致检验，各矩阵的相对一致性指标均小于 0.10，故判断结果合理。

3) 评估指标的权值分配

采用坐标 xOz 平面上的投影面积作为评估指标的权值，设三维球体模型初始半径 r_0 为 1，总面积 S_0 为 p。一、二级评估指标的权值集合即投影面积集合为

$$S_i=S_iW_i \tag{2}$$

步骤 2　重合指标的处理

在实际评估中，评估指标需要从不同角度相互弥补和验证，因此不可避免地会发生重合。为保障评估的合理性，依据基本不等式原理，$S_{14}+S_{21}\le 2\sqrt{S_{14}S_{21}}$，以缩减的方式去除重合指标 C_{14} 和 C_{21} 的冗余值。

步骤 3　计算半径数据

重合指标处理前，球体半径 r_i 可通过下式计算。

$$S_1=\frac{1}{2}\pi r_1^2,\quad S_2=\frac{1}{2}\pi r_2^2,\quad S_3=\frac{1}{4}\pi r_3^2 \tag{3}$$

重合指标处理后，对指标坐落区域进行重新划分。其中，B_1 的非重合指标 C_{11}、C_{12}、C_{13} 置于第 2、3 象限，B_1 与 B_2 的重合指标 C_{14}、C_{21} 置于第 1、4 象限，B_2 的非重合指标 C_{22}、C_{23} 置于第 5、8 象限，潜在隐患安全性 B_3 仍位于第 6、7 象限，重新计算半径数据 R'，公式如下。

$$S_{11}+S_{12}+S_{13}=\frac{1}{4}\pi r_1'^2,\quad 2\sqrt{S_{14}S_{21}}=\frac{1}{4}\pi r_2'^2,$$

$$S_{22}+S_{23}=\frac{1}{4}\pi r_3'^2,\quad S_4=\frac{1}{4}\pi r_4'^2 \tag{4}$$

半径数据直观地反映了一级评估指标权重，从

所绘制的 XML 协议的三维球体模型 Y 轴正方向视图及更新视图（如图 3 所示）可以看出，球体评估模型所带来的优势之一就是能有效地解决评估指标重复的问题。

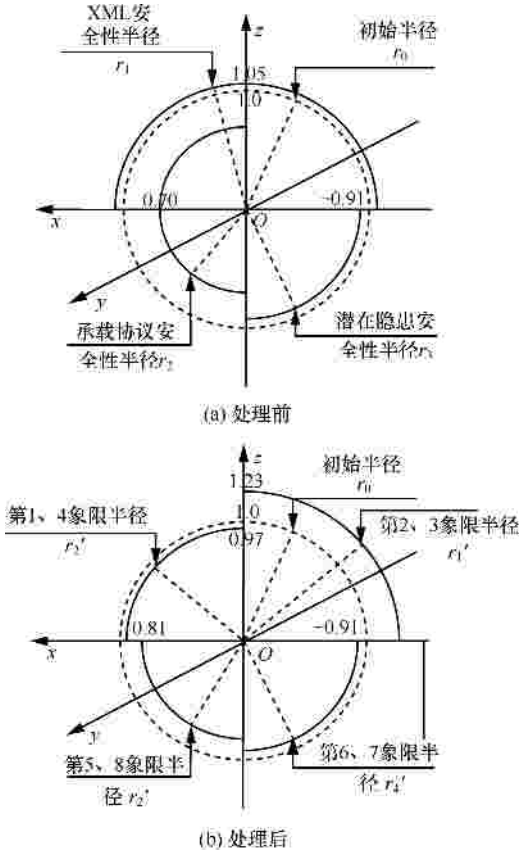


图 3 y 轴正方向半径数据示意

步骤 4 计算上下开合角度

开合角度是指在三维坐标系中以球心为原点发出的射线沿 xOz 平面的上下开合角，根据 $a = S_{扇}/S_{圆} \times 360^{o}$，可求得各二级评估指标开合角度，并据此绘制球体模型 y 轴正方向上下开合角度示意（如图 4 所示）。可以看出，开合角度能够直观地反映二级评估指标的权重。

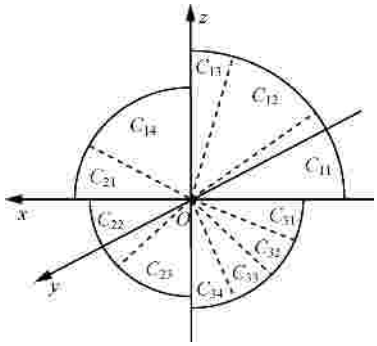


图 4 y 轴正方向上下开合角示意

3 安全评估

在 XML 协议的三维球体模型中，基于 xOz 坐标平面的投影用于评估指标的权值度量，其他各坐标平面中的投影用于评估指标取值度量。在此基础上，本文提出了一种 XML 通信协议的安全性分量评估方法，通过对第二、三级评估指标的定量计算和分析获得安全评估量化值。

3.1 基于 xOy 坐标的 XML 协议内容安全分量评估

首先，建立安全评估指标集 $B_1(C_{11},C_{12},C_{13},C_{14})$ 的 XML 内容三级安全分量评估指标，如表 1 所示。

表 1 面向 XML 协议内容的安全分量评估指标

安全等级	评估指标
二级	机密性 C_{11} 完整性 C_{12} 不可否认性 C_{13} 可用性 C_{14}
三级	加密强度 D_{111}，信息重要度 D_{112} 公钥设施健壮性 D_{121}，密钥保管力度 D_{122} 行为不可否认 D_{131}，时间不可否认 D_{132} 抵御拒绝服务攻击能力 D_{141}，灾难恢复的能力 D_{142}

根据三级评估指标各自的特点，自底向上设计二级评估指标评估函数。4 个内容安全分量的二级评估指标计算式为

$$V_{11} = Value_{11}(D_{111},D_{112}) = \mathrm{MIN}\left(\frac{V_{111}}{V_{112}},1\right)$$

$$V_{12} = Value_{12}(D_{121},D_{122}) = 1 - P_{12}P_{21} = \mathrm{e}^{-l} = \mathrm{e}^{-(1-V_{121})(1-V_{122})}$$

$$V_{13} = Value_{13}(D_{131},D_{132}) = V_{131} + V_{132}$$

$$V_{14} = Value_{14}(D_{141},D_{142}) = \mathrm{lb}[(2^{V_{141}} + 2^{V_{142}})/2] \tag{5}$$

在式（5）中，机密性 V_{11} 反映加密强度 D_{111} 与信息重要度 D_{112} 的博弈度量，其中，

$$V_{111} = \int_0^{t_{safe}/t_{total}} \left(\frac{key\_bits}{40} \cdot \frac{1}{key\_times}\right)\mathrm{d}t \tag{6}$$

通过密钥位数 key_bits、密钥重复利用次数 key_times 以及密钥保密性 t_{safe} 3 方面数据获取；V_{112} 按信息泄露的危害程度划分为一般(0~0.3)、严重（0.3~0.8）和特别严重（0.8~1）。

在式（5）中，完整性 V_{12} 采用以公钥算法为基础的数字签名技术，其中，$P_{12}P_{21}$ 表示完整性发生时通信链路转换的概率；取值 V_{121} 按设施保护等级划分为一级(0~0.2)、二级(0.2~0.4)、三级(0.4~0.6)、

四级(0.6~0.8)和五级(0.8~1)；V_{122} 依据实际防护手段划分为强(0.8~1)，中(0.4~0.8)和弱(0~0.4)。

在式(5)中，不可否认性 V_{13} 以是否使用某项技术 *Tech* 作为 V_{131}、V_{132} 的取值依据，其中，

$$V_{131}=have_{131}(x)=\begin{cases}0.6, & x\in Tech_{131}\\ 0, & \text{其他}\end{cases} \tag{7}$$

$$V_{132}=have_{132}(x)=\begin{cases}0.4, & x\in Tech_{132}\\ 0, & \text{其他}\end{cases} \tag{8}$$

在式(5)中，可用性评估 V_{14} 以 XML 部分抵御拒绝服务攻击作为主要考量因素。根据文献[10]对 XML 拒绝服务攻击的描述，将 XML 攻击类型划分为直接 XML 解析器攻击、XML 验证攻击和 XML 文件引用攻击，由此可设计评估指标 D_{141}、D_{142} 的评分表，分别按 XML 部分抵御拒绝服务攻击能力和灾难恢复能力划分为强(0.8~1)、较强(0.6~0.8)、中等(0.4~0.6)、较弱(0.2~0.4)和弱(0~0.2) 5 类评估值。

3.2　基于 *yOz* 坐标投影的通信载荷安全分量评估

首先，在安全评估指标集 $B_2(C_{21},C_{22},C_{23})$的基础上建立通信载荷安全三级安全评估指标，如表 2 所示。

表 2　面向通信载荷的安全分量评估指标

安全等级	评估指标
二级	可用性 C_{21} 完备性 C_{22} 可控性 C_{23}
三级	抵御拒绝服务攻击的能力 D_{211}，灾难恢复的能力 D_{212} 定界字符可去除性 D_{221}，定界字符可注入性 D_{222} 交互过程的原子性 D_{231}，交互过程的隔离性 D_{232}

根据协议三要素语义、语法和时序的特点，建立通信载荷安全分量的二级评估指标函数。3 个通信载荷的安全分量评估指标公式为

$$\begin{aligned}V_{21}&=Value_{21}(D_{211},D_{212})=\mathrm{lb}[(2^{V_{211}}+2^{V_{212}})/2]\\ V_{22}&=Value_{22}(D_{221},D_{222})=V_{221}+V_{222}\\ V_{23}&=Value_{23}(D_{231},D_{232})=\min(V_{231},V_{232})\end{aligned} \tag{9}$$

在式(9)中，可用性 V_{21} 函数以通信载荷部分的抵御拒绝服务攻击能力为主要考量因素，其中，

$$V_{211}=relation(x)=\frac{1}{\sum_{i=1}^{field\_num}(x\cdot vul\_num_i)} \tag{10}$$

其中，x 表示关联度值，$field\_num$ 为协议首部字段的个数，vul_num_i 为协议首部第 i 字段已发现相关漏洞的个数；取值 V_{212} 复用 D_{142} 设定的评分规则。

在式(9)中，完备性 V_{22} 面临的安全威胁主要是对定界字符的恶意利用，其中，

$$V_{221}=\frac{1}{2+deletion\_num} \tag{11}$$

$$V_{222}=\frac{1}{2+injection\_num} \tag{12}$$

式(11)和式(12)中，参数 2 代表均分操作，$deletion\_num$ 为去除相应定界字符后对通信造成危害性影响的首部字段数目，$injection\_num$ 为注入相应定界字符后对通信造成危害性影响的首部字段数目。

在式(9)中，可控性 V_{23} 评估以数据库事务的弱化属性集为参照，其中，

$$V_{231}=\frac{1}{sequence\_num} \tag{13}$$

式(13)中的 $sequece\_num$ 为完成交互事件所需交互次数，并且

$$V_{232}=\min\left(\frac{identifier\_bits}{32}\cdot coefficient,1\right) \tag{14}$$

其中，$coefficient$ 代表标识生成的随机度，具体取值为优(0.8~1)、良(0.5~0.8)或一般(0~0.5)。可知，V_{232} 由协议数据标识字段的位数 $identifier\_bits$ 决定。

3.3　基于 *yOz* 坐标负投影的安全隐患分量评估

首先，建立安全评估指标集 $B_3(C_{31},C_{32},C_{33},C_{34})$ 的安全隐患三级安全评估指标（如表 3 所示）。

表 3 中的二级指标截获 C_{31}、篡改 C_{32}、伪造 C_{33} 和中断 C_{34} 具有相同的三级评估指标集。

表 3　面向安全隐患的安全分量评估指标

安全等级	评估指标
二级	截获 C_{31} 篡改 C_{32} 伪造 C_{33} 中断 C_{34}
三级	可发现性 D_{311}，可发现性 D_{321}，可发现性 D_{331}，可发现性 D_{341} 可重现性 D_{312}，可重现性 D_{322}，可重现性 D_{332}，可重现性 D_{342} 可利用性 D_{313}，可利用性 D_{323} 可利用性 D_{333}，可利用性 D_{343}

本文采用模糊论评估方法[11]，对 XML 通信协议的各安全分量进行评估，所设计的评估过程如下。

1) 设定评估指标因素集 $U=[u_1,u_2,u_3]=$[可发现性，可重现性，可利用性]；

2) 设定评语集 $L=[l_1,l_2,l_3,l_4,l_5]=$[低，较低，一般，较高，高]；

3) 确定评估指标权重，构造三级评估指标判断矩阵为

$$\boldsymbol{P}=\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}$$

由此计算权重向量 $\boldsymbol{A}=[a_1,a_2,a_3]$。

4) 根据各个元素在评语集中的隶属关系，建立隶属函数，确定模糊评价向量 $\boldsymbol{R}$ 及模糊综合评估向量 $\boldsymbol{B}$。

$$\boldsymbol{B}=\boldsymbol{A}\cdot\boldsymbol{R}=[a_1,a_2,a_3]\cdot\begin{bmatrix}r_{11} & r_{12} & r_{13} & r_{14} & r_{15}\\ r_{21} & r_{22} & r_{23} & r_{24} & r_{25}\\ r_{31} & r_{32} & r_{33} & r_{34} & r_{35}\end{bmatrix} \quad (15)$$

5) 根据加权平均法，计算得出最终的安全分量综合评价结果。

3.4 综合评估

基于以上内容，结合三维球体模型在 xOz 平面上的投影面积（作为评估指标的权值）和以三级评估指标为基础计算得到的分量评估值（作为评估指标的取值）计算安全性综合评估结果。一、二级安全评估指标的安全分量评估结果如表 4 所示。

表 4 综合评估结果计算

安全等级	指标 B_1 评估值	指标 B_2 评估值	指标 B_3 评估值
一级	$Q_1=V_1\cdot S_1'^{\mathrm{T}}$ $V_1=(V_{11},V_{12},V_{13},V_{14})$ $S_1'=(S_{11}',S_{12}',S_{13}',S_{14}')$	$Q_2=V_2\cdot S_2'^{\mathrm{T}}$ $V_2=(V_{21},V_{22},V_{23})$ $S_2'=(S_{21}',S_{22}',S_{23}')$	$Q_3=V_3\cdot S_3'^{\mathrm{T}}$ $V_3=(V_{31},V_{32},V_{33},V_{34})$ $S_3'=(S_{31}',S_{32}',S_{33}',S_{34}')$
二级	$Q_{11}=V_{11}*S_{11}'$, $S_{11}'=0.169\ 8p$ $Q_{12}=V_{12}*S_{12}'$, $S_{12}'=0.169\ 8p$ $Q_{13}=V_{13}*S_{13}'$, $S_{13}'=0.039\ 2p$ $`Q_{14}=V_{14}*S_{14}'$, $S_{14}'=0.159\ 0p$	$Q_{21}=V_{21}*S_{21}'$, $S_{21}'=0.076\ 4p$ $Q_{22}=V_{22}*S_{22}'$, $S_{22}'=0.081\ 6p$ $Q_{23}=V_{23}*S_{23}'$, $S_{23}'=0.081\ 6p$	$Q_{31}=V_{31}*S_{31}'$, $S_{31}'=0.051\ 6p$ $Q_{32}=V_{32}*S_{32}'$, $S_{32}'=0.051\ 6p$ $Q_{33}=V_{33}*S_{33}'$, $S_{33}'=0.051\ 6p$ $Q_{34}=V_{34}*S_{34}'$, $S_{34}'=0.051\ 6p$

其中，一级评估指标 C_i 的取值用 V_i 表示，二级评估指标 C_{ij} 取值用 V_{ij} 表示，且 V_{ij} 由所属评估函数计算所得，并且规定 $V_{ij}\in[0,1]$，可知评估结果 Q 的取值区间为 $Q\in[0,\mathrm{p}]$。

最后，将最终评估结果 Q 的取值范围划分为 7 个区间，定义各区间的安全性评价，如表 5 所示。

表 5 综合评估结果评价

最终评估结果	Q 取值范围
低	0~0.3p
较低	0.3~0.5p
中下	0.5~0.6p
中平	0.6~0.7p
中上	0.7~0.8p
较高	0.8~0.9p
高	0.9~p

4 实验与分析

为了对基于三维球体模型评估方法的适用性和有效性进行验证和比较，本文设计了 2 组实验，采用基于三维球体模型的评估方法分别对 SOAP 协议和 SAML 协议进行安全性评估。

4.1 典型协议的安全性评估实验

4.1.1 基于 XML 的 SOAP 协议安全性评估

本实验的评估对象为安全电子银行仿真系统[12]。该系统由 apache jakarta tomcat、apache axis、apache XML security 等组件构成并部署在真实网络环境中，能完成电子银行的余额查询、资金转账等主要功能。系统 Web 架构如图 5 所示。

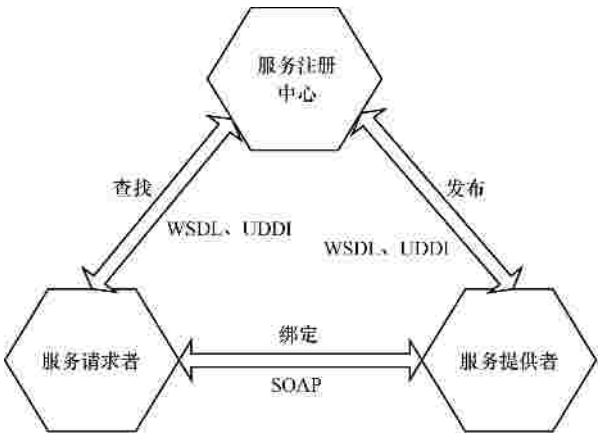


图 5 安全电子银行仿真系统 Web 服务架构

首先，利用 Soap Monitor 分组抓捕工具截取 SOAP 协议数据分组[13,14]，然后参照协议数据、设计文档，采用第 3 节所描述的量化算法计算 SOAP 协议的安全性指标。仿真实验数据及计算结果如表 6 所示。

根据安全评估指标和一、二级安全评估指标的安全分量评估结果（如表 4 所示），可得到该电子

银行系统的综合评估结果为 $\boldsymbol{Q}=\boldsymbol{V}\cdot\boldsymbol{S}'^{\mathrm{T}}=0.712\ 1\mathrm{p}$，根据综合评估结果的评价分区，如表 5 所示，可得 SOAP 协议的安全性为“中上”。

从表 6 可知，在该仿真系统协议评估中，XML 部分的不可否认性指标值点最低，可通过加入数字时间戳技术增强不可否认性指标的安全性。类似地，对于其他较低的安全指标点，可通过相关安全技术提高其安全性。

表 6　评估指标取值结果汇总

评估指标	取值
V_{11}	1
V_{12}	0.923 1
V_{13}	0.6
V_{14}	0.703 5
V_{21}	0.551 1
V_{22}	0.583 3
V_{23}	0.5
V_{31}	0.48
V_{32}	0.72
V_{33}	0.58
V_{34}	0.54

4.1.2　基于 XML 的 SAML 协议安全性评估

由于 SAML 只提出了一个标准的、用于交换认证和授权信息的、基于 XML 的架构，并没有提出如何确保这些信息安全的机制，所以 SAML 协议也面临安全问题。

该实验以一个经典的基于 SAML 的单点登录系统（SSSO, SAML-based single sign on）为评估对象。在该系统中，服务请求方（SP, service provider）通过向身份认证服务器（IDP, identity provider）发送 SAML 请求，由 IDP 返回 SAML 响应来获得认证信息。其 SAML 协议断言获取流程如图 6 所示。

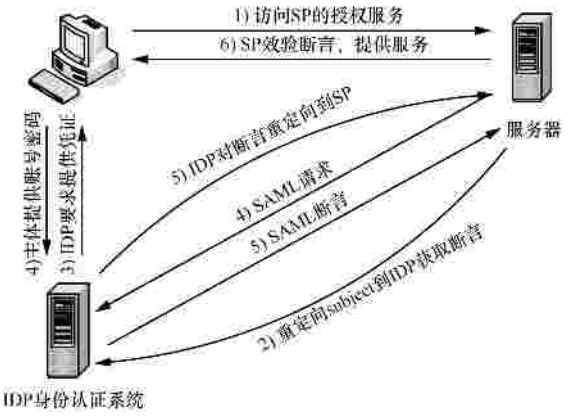


图 6　SAML 协议断言获取流程

首先，使用 apache group 发布的小程序 TCP tunnel/ monitor 截获该系统运行过程中站点之间传输的 SOAP 消息，提取 SAML 请求数据后对其进行安全评估，仿真实验数据及计算结果如表 7 所示。

表 7　SAML 评估指标取值结果汇总

评估指标	取值
V_{11}	0.56
V_{12}	0.860 7
V_{13}	0.6
V_{14}	0.603 3
V_{21}	0.435 4
V_{22}	0.666 7
V_{23}	0.6
V_{31}	0.42
V_{32}	0.53
V_{33}	0.64
V_{34}	0.49

通过式（16）计算，可得该单点登录系统的评估结果为 $\boldsymbol{Q}=\boldsymbol{V}\cdot\boldsymbol{S}'^{\mathrm{T}}=0.604\ 6\mathrm{p}$，该系统所使用的 SAML 协议的安全性为“中下”。

从表 7 可知，在 SSSO 系统中，SAML 协议的机密性和安全漏洞分量指标值较低，易被攻击者截获和篡改。可以通过采用符合 WS-Security 规范的 XML 数字签名和 XML 加密技术来满足数据机密性和对消息发送方验证的需求，通过添加自定义的标识元素（时间戳、随机数等）防止恶意用户截获等方法提高 SAML 协议的安全性。

由于在 XML 通信协议的安全性问题的研究中尚无统一的安全评估标准，因此邀请了十位业内专家依据经验对 SOAP 协议、SAML 协议进行综合评判。评判结果如表 8 所示，通过比较可知，基于三维球体模型的安全性综合评估方法所得出的评价结果与多数专家的评判结果是一致的。

表 8　专家经验评判结果

协议	专家									
	1	2	3	4	5	6	7	8	9	10
SOAP	中上	中上	中平	中上	中上	中上	中平	中上	较高	中上
SAML	中平	中下	中下	中平	中下	中下	中下	中上	中下	中下

4.2　对比评估实验

为了进一步验证基于三维球体模型的评估方

法的有效性，采用可靠性模型评估方法[15]、STRIDE 模型评估方法[1]、信息熵评估方法[16]对 SOAP 协议和 SAML 协议进行安全性评估的对比实验。

采用文献[15]的可靠性模型评估，对 4.1 节的 2 个仿真系统的 XML 通信协议进行攻击测试，通过计算每个攻击的可能性权值、后果权值、抵御难度权值获取各攻击的危险度量，通过综合计算得到协议内容层面的安全度量值，评估结果如表 9 所示。

表 9 可靠性模型评估指标值

协议	可靠性	机密性	完整性
SOAP	0.165 8	0.451 5	0.392 0
SAML	0.103 5	0.096 0	0.352 4

采用文献[1]的 STRIDE 威胁模型，获取 4.1 节 2 个仿真系统的 XML 通信协议的抗假冒能力、抗篡改能力、抗否认能力、抗信息泄露能力、抗拒绝服务能力、抗提升特权能力 6 个属性的风险值及协议漏洞层面的安全度，评估结果如表 10 所示。

表 10 STRIDE 模型评估指标值

协议	抗假冒	抗篡改	抗否认	抗泄露	抗拒绝服务	抗提升特权	总安全度
SOAP	0.14	0.22	0.23	0.22	0.25	0.16	0.78 (中上)
SAML	0.12	0.39	0.32	0.35	0.28	0.14	0.69 (中下)

采用文献[16]的多属性决策理论，将 4.1 节 2 个仿真系统的 XML 通信协议的安全属性值组成决策矩阵，利用信息熵的方法计算各属性的客观权重，最后以风险值的形式给出其安全程度，评估结果如表 11 所示。

表 11 信息熵评估指标值

协议	认证	机密性	完整性	可用性	授权	审计	不可否认
SOAP	0.156 8	0.172 0	0.102 5	0.120 0	0.075 0	0.135 5	0.095 8
SAML	0.126 9	0.062 4	0.093 3	0.084 5	0.060 0	0.142 0	0.075 0

通过评估对比实验可以得出以下结论。

1) 基于三维球体模型的评估方法与 STRIDE 威胁模型得到的评估结果一致，均符合多数专家的评判，因此，可以有效地评估 XML 通信协议。

2) 可靠性模型评估、STRIDE 威胁模型虽然都能对协议的安全性进行建模与分析，但都局限于某个维度，而基于三维球体模型的评估方法的评估角度相对全面，并在分量评估的基础上能进行安全性的综合评判。

3) 信息熵评估方法中的各安全属性都是简单模糊化值，并没用对安全属性进行量化，而本文的综合评估方法量化到三级指标，为 XML 通信协议评估提供了更准确的数据。

4) 基于三维球体模型的评估方法在指标体系建立、重合指标处理及评估结果的直观反映等具有更大的优势，使得其对 XML 通信协议的安全评估更具客观性。

5 结束语

本文结合 XML 通信协议特点，提出了一种面向 XML 通信协议的三维球体模型，提出基于三维球体模型的协议安全性综合评估方法。通过对 SOAP 协议、SAML 协议的安全评估实验和 3 种评估方法的评估对比实验，验证了本文提出的安全评估方法对 XML 通信协议的适用性和有效性。

未来研究工作的重点是进一步实现 XML 通信协议评估的自动化，包括协议数据的自动采集、评估指标数据的自动识别等内容。

参考文献：

[1] LI J, CHEN H, DENG F, *et al*. A security evaluation method based on threat classification for Web service[J]. Journal of Software, 2011, 6(4): 595-603.

[2] 程睿. 基于 SOA 的 SOAP 消息交互安全机制的研究与实现[D]. 西安: 西安电子科技大学, 2008.
CHENG R. Research and Implementation on Security Mechanism of SOAP Message Exchange Based on SOA[D]. Xian: Xidian University, 2008.

[3] ALROUH B, GHINEA G. A performance evaluation of security mechanisms for Web services[A]. Proc of the 2009 Fifth International Conference on Information Assurance and Security[C]. Piscataway, USA, 2009. 715-718.

[4] 孙丁丁. 通过SOAP扩展优化Web服务性能的研究[D]. 乌鲁木齐: 新疆大学, 2007.
SUN D D. Research on Optimizing Web Service via SOAP Extension[D]. Urumqi:Xinjiang University, 2007.

[5] 陈晓苏, 周晴, 肖道举. Web 服务中 UDDI 安全机制研究[J].华中科技大学学报,2005,30(8):58-60.
CHEN X S, ZHOU Q, XIAO D J. Study of security mechanisms of UDDI in Web service[J]. Journal of Huazhong University of Science and Technology(Nature Science),2005,30(8):58-60.

[6] 尹星. 基于 SAML 的单点登录模型及其安全的研究与实现[D]. 镇江: 江苏大学,2005.
YIN X. Research and Implementation of SAML-Based SSO Model and it's Security [D]. Zhenjiang: Jiangsu University, 2005.

[7] 宓洽群.大学教学原理[M]. 上海: 上海交通大学出版社, 1989.

97-100.
MI Q Q. University Teaching Principles[M]. Shanghai: Shanghai Jiaotong University Press, 1989. 97-100.
[8] 徐耀玲, 唐五湘, 吴秉坚. 科技评估指标体系设计的原则及其应用研究[J]. 中国软科学, 2010, 30(2):48-51.
XU Y L, TANG W X, WU B J. Design principle and application of S&T evaluation index system[J]. China Soft Science, 2010, 30(2):48-51.
[9] 杨宏宇, 谢丽霞, 朱丹. 漏洞严重性的灰色层次分析评估模型[J]. 电子科技大学学报, 2010, 39(5):778-782.
YANG H Y, XIE L X, ZHU D. A vulnerability severity grey hierarchy analytic evaluation model[J]. Journal of University of Electronic Science and Technology of China, 2010, 39(5):778-782.
[10] PANG J, PENG X. Trustworthy Web service security risk assessment research[A]. Proc of the 2009 International Forum on Information Technology and Applications[C]. Piscataway, USA, 2009. 417-420.
[11] 周晓洁.基于模糊综合评价法的船舶热源系统优选研究[D]. 上海: 上海交通大学, 2010.
ZHOU X J. Study on The Selection of Marine Heat Source System Based on Fuzzy Comprehensive Evaluation Method[D]. Shanghai: Shanghai Jiaotong University, 2010.
[12] 加尔布雷斯. Web 服务安全性高级编程[M]. 北京: 清华大学出版社, 2003. 400-444.
GALBRAITH B. Professional Web Services Security[M]. Beijing: Tsinghua University Press, 2003.400-444.
[13] FLY R. Detecting fraud on websites[J]. IEEE Security & Privacy, 2011, 9(6):80-85.
[14] ANTUNES N, VIEIRA M. Defending against Web application vulnerabilities[J]. IEEE Computer, 2012, 45(2):66-72.
[15] 陈伟琳. 协议安全测试理伦和方法的研究[D]. 北京: 中国科学技术大学, 2008.
CHEN W L. Research on Testing Theory and Methods of Protocol Security[D]. Beijing: University of Science and Technology of China, 2008.
[16] 赵德明. 多维度 Web 服务安全性评估[D]. 北京: 中国石油大学, 2011.
ZHAO D M. Multiple Dimension Security Assessment of Web Service[D]. Beijing: China University of Petroleum, 2011.

作者简介：

杨宏宇（1969-），男，吉林长春人，中国民航大学教授、博士生导师，主要研究方向为网络信息安全。

于巾博（1987-），女，内蒙古赤峰人，中国民航大学硕士生，主要研究方向为网络信息安全。

谢丽霞（1974-），女，重庆人，中国民航大学副教授、硕士生导师，主要研究方向为网络信息安全。

（上接第 182 页）

[6] KOIKE-AKINO T, MOLISCH A F, DUAN C J, *et al*. Capacity, MSE and secrecy analysis of linear block precoding for distributed antenna systems in multi-user frequency selective fading channels[J]. IEEE Trans on Communications, 2011, 59(3):888-900.
[7] STEGER C B. Wireless Downlink Schemes in a Class of Frequency Selective Channels with Uncertain Channel State Information[D]. Houston: Rice University, 2004.
[8] SU B. Blind Channel Estimation Using Redundant Precoding: New Algorithms, Analysis and Theory[D]. California: Institute of Technology Pasadena, 2008.
[9] ZHAO W X, FANG F. A diverse proof of OFDM channel estimation comparing CP-sequences and training-sequences methods under LS frame[A]. Proc of Information Theory and Artificial Intelligence Computing[C]. IEEE Press, 2011.
[10] GÜREL I, Channel Estimation for OFDM Systems[D]. Middle East Technical University, 2005.

作者简介：

赵旺兴（1986-），男，湖南邵东人，电子科技大学硕士生，主要研究方向为 OFDM 系统传输优化的信号处理。

万群（1971-），男，江西南昌人，电子科技大学教授、博士生导师，主要研究方向为阵列信号处理、无线定位及波束形成信号处理。

陈章鑫（1979-），男，四川乐山人，电子科技大学副教授，主要研究方向为无源定位理论和算法、传感器网络节点定位和分布式系统。