Research on Security Evaluation of XML Communication Protocol

Lixia Xie
Civil Aviation University of China, College of Computer Science and Technology, 300300 Tianjin, China
Email: lxxie@126.com

Yanxin Yan
Civil Aviation University of China, College of Computer Science and Technology, 300300 Tianjin, China
Email: y.yyx@hotmail.com

Jiyong Zhang
Swiss Federal Institute of Technology in Lausanne, School of Computer and Communication Science, CH-1015 Lausanne, Switzerland
Email:jyzhang@epfl.ch

***Abstract*—According to the problem in communication protocol security assessments, a new protocol security comprehensive evaluation method based on the three-dimensional sphere model is presented. In this method, a three-dimensional security evaluation index system was built through positions of index on the external of spherical shell. Evaluation index weights of the top two levels were obtained through the analytic hierarchy process (AHP), with sphere radius and the retractable angles. Then, security components' values of communication content, communication load and security vulnerability of XML communication protocol were calculated. Finally, the security evaluation result of XML communication protocol was obtained through quantization calculation and comprehensive analysis method. The experimental results demonstrate that our method can meet the needs of communication protocol security evaluating effectively.**

***Index Terms*—security evaluation, protocol, sphere model, three-dimensional**

I. INTRODUCTION

As an important part of Web service protocol stack, XML communication protocol uses XML data file with conventional structures to complete the information exchange of both communication sides, and has the advantages of extend easily, multi-platform, heterogeneous communication and so on. This is the reason why XML communication protocol is widely used in recent years. Since the XML communication protocol plays an extraordinary role in network communication, once the vulnerability of the protocol is used, it can bring harmful result. Therefore the study on the security evaluation method of the XML communication protocol has become a hot issue in the information security field.

At present, studies on security evaluation of the XML communication protocol were conducted in succession both at home and abroad. Alrouh B and Ghinea G performed an experiment to evaluate the selection of Web services security measures from seven aspects as user asymmetric key, security certificate, security token and so on [1]. But their research only compared the performances of the protocol, and it did not perform the security evaluation of XML communication protocol. Tang K, Chen S and Levy D used Web service security strategy to evaluate the end-to-end security guarantee ability aiming at the evaluation of Web service security frame [2], but this research was short of qualitatively analysis on Web service protocol. Li J, Chen H and Deng F used STRIDE model to obtain the security risk values of Web protocol messages from six aspects as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege [3]. However, this method could not effectively evaluate the relevant threats caused by the interaction of components. Cheng R proposed a new message interaction security mechanism as simple object access protocol (SOAP) [4], and performed security evaluation to the protocol from the angles of encryption, signature, and service time and so on. However, this mechanism was not available for other XML communication protocols. Xu Y and Xie X proposed a method using Colored Petri Nets (CP-Nets) for the analysis of security protocols [5]. Specially, in this method, an intruder CP-Net model provided an open-ended base for the integration of multiple attack tactics. That is a viable approach to overcome the state space explosion problem.

Manuscript received December 15, 2012; revised January 1, 2013; accepted Jun 1, 2013.

Project number: National Science Foundation of China under Grant No. 60776807 and No. 61179045, the Key Project of Tianjin Science and Technology Support Program under Grant No. 09JCZDJC16800, the Science and Technology Project of CAAC under Grant No. MHRD201009 and No. MHRD201205.

Corresponding author: Lixia Xie (lxxie@126.com).

doi:10.4304/jsw.8.6.1428-1435

According to the security evaluation problem of XML protocol, we propose a security evaluation method based on three-dimensional sphere model. This paper designs a three-dimensional coordinate system for the security evaluation index of XML communication protocol, uses the coordinate projected area on the sphere as the weight of evaluation index and measure standard of security component index value, effectively solves the index coincident problem.

II. SECURITY EVALUATION INDEX SYSTEM

A. Hierarchical structure of the Model

А.И.Маркушевич, a mathematician of former Soviet Russia, divided the information stored in human brain into core information and shell information, proposed an information construction sphere model [6]. In this paper, the concept is introduced into the application of protocol security evaluation, and we propose a three-dimensional sphere model of XML communication protocol. In the sphere model, the sphere can be divided into gradational structures formed by certain logical relation according to protocol evaluation value and development maturity degree. To be specific, the sphere consists of a network interface layer, a network layer, a transmission layer and an application layer protocol from inside to outside (as shown in Fig. 1).

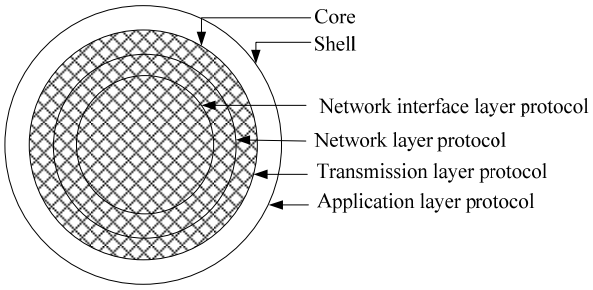


Figure 1. Hierarchical structure of three-dimensional sphere model.

B. Evaluation index System

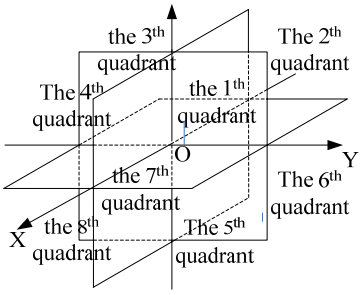
XML communication protocol belongs to the application layer. Therefore, this paper establishes the security evaluation index system of the XML communication protocol by means of the shell layer of the sphere model, designs a first and second levels evaluation index three-dimensional coordinate system according to the XML communication protocol security evaluation, and sets up a set-down surface of the first and second levels evaluation index as shown in Fig. 2. The three-dimensional coordinate system is divided into eight quadrants by three planes of XOY, XOZ and YOZ. The general goal of XML communication protocol security is supposed as A, then the first level evaluation index is B_i, the second level evaluation index is C_{ij} and the set-down surface thereof are determined from three aspects as communication content, communication load and security vulnerability.

(a) The security of communication content B_1: the evaluation index B_1 locates in 1st, 2nd, 3rd and 4th quadrants, and is divided into confidentiality C_{11}, integrity C_{12}, non-repudiation C_{13} and availability C_{14} according to communication content elements.

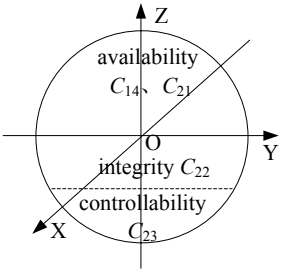
(b) The security of communication load B_2: the evaluation index B_2 locates in 1st, 4th, 5th and 8th quadrants, and is divided into availability C_{21}, integrity C_{22}, and controllability C_{23} according to three semantic elements.

(c) The security of security vulnerability B_3: the evaluation index B_3 locates in 6th and 7th quadrants, and is divided into interception C_{31}, interpolation C_{32}, falsification C_{33} and interruption C_{34} according to four basic attack types.

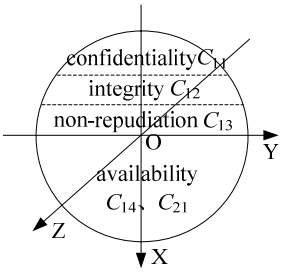
What needs to be explained is that sometimes there will be a certain degree of coincidence between the evaluation index in order to strengthen the key investigation and evaluation of some aspects [7]. The difference between the three-dimensional sphere model and general evaluation model is that the problem of coincident index is solved and the redundant value is deleted, with the result that the evaluation result is more reasonable.



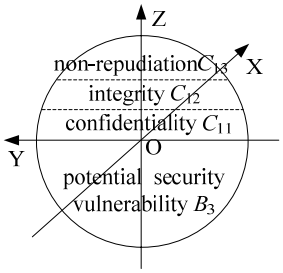
(a) Region division of three-dimensional coordinates.



(b) Positive direction View of X-axis.



(c) Positive direction view of Z-axis.



(d) Negative direction view of X-axis.

Figure 2. A set-down surface of the top two levels evaluation index.

C. Calculation of Evaluation Index Weight

On the basis of established security evaluation index system, the weight of each evaluation index is calculated by using sphere coordinate system projection method. According to the features of sphere model, the analytic hierarchy process method proposed in the paper [8] is used to calculate the weight of each evaluation index and delete the redundant value. The weights of first and second levels evaluation index are visually represented by sphere radius and retractable angle, so that the comprehensiveness of security evaluation is guaranteed. In the XML protocol three-dimensional sphere model, the projection area on XOZ coordinate plane is used to calculate the weight of the evaluation index. The calculation process of the weights of the evaluation index is as follows:

Step 1. Calculation of the weights of first and second levels evaluation index.

(a) Construct the judgment matrix P_0 of the first level evaluation index B_i, and the judgment matrixes P_1, P_2 and P_3 of the second level evaluation index C_{ij} belonged to XML security, communication load security and security vulnerability.

$$P_0=\begin{bmatrix} 1 & 3 & 5 \\ 1/3 & 1 & 4 \\ 1/5 & 1/4 & 1 \end{bmatrix} \quad P_1=\begin{bmatrix} 1 & 1 & 3 & 1 \\ 1 & 1 & 3 & 1 \\ 1/3 & 1/3 & 1 & 1/3 \\ 1 & 1 & 3 & 1 \end{bmatrix}$$

$$P_2=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad P_3=\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

(b) Calculate the weight vector by using square root method. The weight vector of the first level evaluation index is $W_0=(W_1, W_2, W_3)^T$; the weight vectors of the second level evaluation index are $W_1=(W_{21}, W_{22}, W_{13}, W_{14})^T$, $W_2=(W_{21}, W_{22}, W_{23})^T$, $W_3=(W_{31}, W_{32}, W_{33}, W_{34})^T$. The calculation equation is

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

where the m_i is n-th root of the product of elements in each row of the judgment matrix. The relative consistency index of the matrixes are all less than 0.10 according to consistency test, so the judgment result is reasonable.

(c) Weight allocation of evaluation index. The projection area on XOZ coordinate plane is taken as the weight of the evaluation index. The primary radius r_0 of the three-dimensional sphere model is 1, and the total area S_0 is π. The weight set of the first and second levels evaluation index, namely the projected area set, that is

$$S_i = S_i \times W_i \tag{2}$$

Step 2. Process of coincident index.

In the real evaluation process, the evaluation index need to compensate and validate each other from different angles, so the coincidence will occur inevitably. In order to guarantee the evaluation's reasonableness, according to the fundamental inequality principle $S_{14}+S_{21} \le 2\sqrt{S_{14}S_{21}}$, the redundant value of the coincident index C_{14} and C_{21} will be deleted by reduction method.

Step 3. Calculation of radius data.

The sphere radius can be calculated by the following equations before the process of coincident index:

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

As the coincident index are handled, the index set-down area are re-divided, which the non-coincident index C_{11}, C_{12} and C_{13} of B_1 are arranged in the 2nd and 3rd quadrants, the non-coincident index C_{22} and C_{23} of B_2 are arranged in the 5th and 8th quadrants, and the potential vulnerability security B_3 is still arranged in the 6th and 7th quadrants. The radius R' is re-calculated by (4):

$$S_{11}+S_{12}+S_{13}=\frac{1}{4}\pi r_1'^2,\ 2\sqrt{S_{14}S_{21}}=\frac{1}{4}\pi r_2'^2,$$
$$S_{22}+S_{23}=\frac{1}{4}\pi r_3'^2,\ S_4=\frac{1}{4}\pi r_4'^2 \tag{4}$$

The radius visually reflects the weights of first level evaluation index. From the positive direction view of Y-axis of XML protocol three-dimensional sphere model and the updated view (as shown in Fig. 3), it can be seen from the Fig. 3 that one of the advantages of the sphere evaluation model is that it can solve the problem of coincident index effectively.

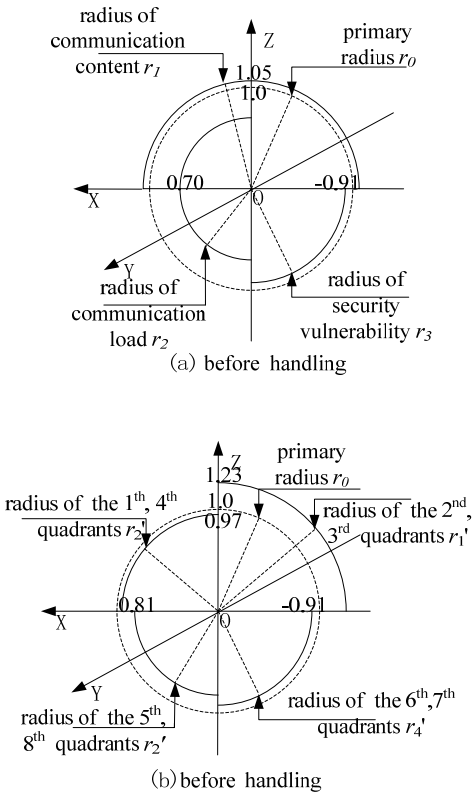


Figure 3. Radial view of Y-axis positive direction.

Step 4. Calculation of the up and down retractable angle.

The retractable angle, which reflects the second level evaluation index, refers to the up and down retractable angle of the ray sending from sphere center of the three-dimensional coordinate system along the XOZ plane. The retractable angle of the second level evaluation index can be calculated by (5) based on the positive direction view of Y-axis of the sphere model (as shown in Fig. 4).

$$\alpha = S_{Sector} / S_{Circle} \bullet 360^{\circ} \tag{5}$$

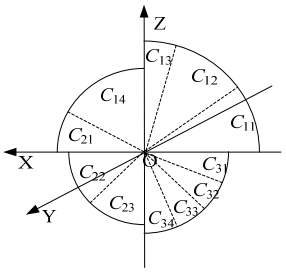


Figure 4. Retractable angle view of Y-axis positive direction.

III. SECURITY EVALUATION

In the XML protocol three-dimensional sphere model, the projection based on the XOZ coordinate plane is used to define the weights of evaluation index, and the projections on the other coordinate planes are used to define the value range of evaluation index. Based on this, this paper proposes an XML communication protocol security evaluation method which obtains a security evaluation quantized value through quantitative calculation of the second and third level evaluation index.

A. Evaluation of Content security Component

In the first place, three levels security evaluation index of communication content security are established on the basis of security evaluation index set B_1 (C_{11}, C_{12}, C_{13}, C_{14}) (as shown in Table Ⅰ).

TABLE I.

SECURITY COMPONENT EVALUATION INDEX OF COMMUNICATION CONTENT

2nd level	Confidentiality C_{11}	Integrity C_{12}	Non-repudiation C_{13}	Availability C_{14}
3rd level	Encryption intensity D_{111}	Public key facility robustness D_{121}	Behavior non-repudiation D_{131}	Denial service attack resistant ability D_{141}
	Information importance degree D_{112}	Key keeping strength D_{122}	Time non-repudiation D_{132}	Disaster recovery ability D_{142}

According to the features of the third level evaluation index, the evaluation functions of the second level evaluation index are designed from bottom to top. The second level evaluation index of the four content security components are calculated by the following equations

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

$$\begin{aligned} V_{12} &= Value_{12}(D_{121}, D_{122}) \\ &= 1 - P_{12}P_{21} = e^{-\lambda} \\ &= e^{-(1-V_{121})\cdot(1-V_{122})} \end{aligned} \ , \tag{6}$$

$$\begin{aligned} V_{13} &= Value_{13}(D_{131}, D_{132}) \\ &= V_{131} + V_{132} \\ V_{14} &= Value_{14}(D_{141}, D_{142}) \\ &= \log_2[(2^{V_{141}} + 2^{V_{142}})/2] \end{aligned}$$

In (6), the confidentiality V_{11} reflects the gaming measurement of encryption intensity D_{111} and information importance degree D_{112}, then

$$V_{111} = \int_0^{t_{safe}/t_{total}} (\frac{key\_bits}{40} \times \frac{1}{key\_times})dt \tag{7}$$

where V_{111} is obtained through the data of *key_bit*, *key_times* and *tsafe*; V_{112} is divided into common (0-0.3), serious (0.3-0.8) and specially serious (0.8-1) according to the degree of information leak hazards.

In (6), the integrity V_{12} is calculated by using the digital signature technology based on public key algorithm, in which P_{12} and P_{21} represent the transition probabilities of communication links when integrity occurs; V_{121} is divided into first level (0-0.2), second level (0.2-0.4), third level (0.4-0.6), fourth level (0.6-0.8), and fifth level (0.8-1) according to protection grade of facility; V_{122} is divided into strong (0.8-1), medium (0.4-0.8), and weak (0-0.4) according to practical protection means.

In (5), whether non-repudiation V_{13} uses a certain Tech or not is taken as the value basis of V_{131} and V_{132}, where

$$V_{131} = have_{131}(x) = \begin{cases} 0.6 & x \in Tech_{131} \\ 0 & Otherwise \end{cases} \tag{8}$$

$$V_{132} = have_{132}(x) = \begin{cases} 0.4 & x \in Tech_{132} \\ 0 & Otherwise \end{cases} \tag{9}$$

In (6), availability evaluation V_{14} takes the ability of resistant against denial of service attack of XML part as major consideration factor.

With reference to the description in paper [9] about denial of service attack of XML, the evaluation index D_{141} and D_{142} are divided into strong (0.8-1), comparatively strong (0.6-0.8), medium (0.4-0.6), comparatively weak (0.2-0.4), and weak (0-0.2) according to the ability of resistant against denial of service attack and disaster recovery ability.

B. Evaluation of Load Security Component

First of all, three levels security evaluation index of communication load security are established on the basis of security evaluation index set B_2 (C_{21}, C_{22}, C_{23}) (as shown in Table Ⅱ).

TABLE II.

SECURITY COMPONENT EVALUATION INDEX OF COMMUNICATION LOAD

2nd level	Availability C_{21}	Categoricalness C_{22}	Controllability C_{23}
3rd level	Denial service attack resistant ability D_{211}	Delimiter character removability D_{221}	Atomicity in interaction process D_{231}
	Disaster recovery ability D_{212}	Delimiter character injectivity D_{222}	Isolation in interaction process D_{232}

The second level evaluation index functions of the communication load security component are established according to the features of the three protocol element as semanteme, grammar and time sequence. Three security component evaluation index of the communication load are calculated by the following equations:

$$\begin{aligned} V_{21} &= Value_{21}(D_{211}, D_{212}) \\ &= \log_2[(2^{V_{211}} + 2^{V_{212}})/2]' \\ V_{22} &= Value_{22}(D_{221}, D_{222}) \\ &= V_{221} + V_{222} \\ V_{23} &= Value_{23}(D_{231}, D_{232}) \\ &= MIN(V_{231}, V_{232}) \end{aligned} \tag{10}$$

In (10), availability V_{21} takes the ability of resistant against denial of service attack of communication load part as major consideration factor, where

$$V_{211} = relation(x) = \frac{1}{\sum_{i=1}^{field\_num} (x \cdot vul\_num_i)} \tag{11}$$

The x is the degree of association, the *field_num* is the field number of protocol header, the vul_num_i is the number of vulnerabilities that have been found in the i-th field of the protocol header, and the V_{212} reuses the grade rule set by D_{142} to estimating.

In (11), the security threat that categoricalness V_{22} faces is mainly the malicious utilization of the delimiter character, where

$$V_{221} = \frac{1}{2 + deletion\_num} \tag{12}$$

$$V_{222} = \frac{1}{2 + injection\_num} \tag{13}$$

In (12) and (13), the parameter 2 represents equipartition operation, the *deletion_num* represents the

number of the header field which will bring harmful influence to communication after relevant delimiter character is deleted, and the *injection_num* represents the number of the header field which will bring harmful influence to communication after relevant delimiter character is injected.

In (10), the evaluation of the controllability V_{23} takes the softening attribute set of data base affaire as reference, where

$$V_{231} = \frac{1}{sequence\_num} \tag{14}$$

The *sequence_num* in (14) is the interaction number required for completing interaction event, and

$$V_{232} = MIN(\frac{identifier\_bits}{32} \cdot coefficient, 1) \tag{15}$$

In (15), the *coefficient* represents the randomness degree to generate ID, and the specific value category is excellent (0.8-1), good (0.5-0.8), and common (0-0.5). V_{232} is determined by the bit number (*identifier_bits*) of protocol data ID field.

C. Evaluation of Security Vulnerability Component

First of all, three levels security evaluation index of security vulnerability are established on the basis of security evaluation index set B_3 (C_{31}, C_{32}, C_{33}, C_{34}) (as shown in Table Ⅲ).

The second level index interception C_{31}, interpolation C_{32}, falsification C_{33} and interruption C_{34} in Table Ⅲ have identical third level evaluation index set.

TABLE III.

SECURITY COMPONENT EVALUATION INDEX OF SECURITY VULNERABILITY

2nd level	Interception C_{31}	Interpolation C_{32}	Falsification C_{33}	Interruption C_{34}
3rd level	Detectability D_{311} Reproducibility D_{312} Availability D_{313}	Detectability D_{321} Reproducibility D_{322} Availability D_{323}	Detectability D_{331} Reproducibility D_{332} Availability D_{333}	Detectability D_{341} Reproducibility D_{342} Availability D_{343}

This paper uses the evaluation method based on fuzzy theory [10] to evaluate each security component of XML protocol. The designed evaluation process is as follows:

Step 1. Set evaluation index factor set U= [u_1, u_2, u_3] = [detectability, reproducibility, availability];

Step 2. Set comment set L=[l_1,l_2,l_3,l_4,l_5] =[low, comparatively low, common, comparatively high, high];

Step 3. Determine the weights of evaluation index, and construct a third level evaluation index judgment matrix as

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

which is used to calculate weight vector A=[a_1,a_2, a_3].

Step 4. Establish membership function according to the membership of each element in the comment set, and determine fuzzy evaluation vector R and fuzzy integrated evaluation vector B:

$$B = A \cdot R = [a_1, a_2, a_3] \cdot \begin{bmatrix} r_{11} & r_{12} & r_{13} & r_{14} & r_{15} \\ r_{21} & r_{22} & r_{23} & r_{24} & r_{25} \\ r_{31} & r_{32} & r_{33} & r_{34} & r_{35} \end{bmatrix} \tag{16}$$

Step5. Calculate the final security component integrated evaluation result according to weighted average method.

D. Integrated Evaluation

On the basis of above mentioned contents, the security integrated evaluation result is calculated with reference to the projected area of the three-dimensional sphere model on XOZ plane (as the weight of evaluation index) and the component evaluation value obtained through calculation on the basis of the three levels evaluation index (as the value of evaluation index). The security component evaluation results of the first and second levels security evaluation index are shown in Table Ⅳ.

TABLE IV.

INTEGRATED EVALUATION RESULT

1st level	2nd level
Index B_1 evaluation value Q_1=V_1*$S_1'^T$ V_1=(V_{11},V_{12},V_{13}, V_{14}) S_1'=(S_{11}', S_{12}', S_{13}', S_{14}')	Q_{11}=V_{11}*S_{11}', S_{11}'=0.1698π
	Q_{12}=V_{12}*S_{12}', S_{12}'=0.1698π
	Q_{13}=V_{13}*S_{13}', S_{13}'=0.0392π
	Q_{14}=V_{14}*S_{14}', S_{14}'=0.1590π
Index B2 evaluation value Q_2=V_2*$S_2'^T$ V_2=(V_{21},V_{22},V_{23}) S_2'=(S_{21}', S_{22}', S_{23}')	Q_{21}=V_{21}*S_{21}', S_{21}'=0.0764π
	Q_{22}=V_{22}*S_{22}', S_{22}'=0.0816π
	Q_{23}=V_{23}*S_{23}', S_{23}'=0.0816π

Index B_3 evaluation value $Q_3=V_3*S_3'^T$ $V_3=(V_{31},V_{32},V_{33},V_{34})$ $S_3'=(S_{31}', S_{32}', S_{33}', S_{34}')$	$Q_{31}=V_{31}*S_{31}'$, $S_{31}'=0.0516\pi$
	$Q_{32}=V_{32}*S_{32}'$, $S_{32}'=0.0516\pi$
	$Q_{33}=V_{33}*S_{33}'$, $S_{33}'=0.0516\pi$
	$Q_{34}=V_{34}*S_{34}'$, $S_{34}'=0.0516\pi$

With the value of the first level evaluation index C_i is represented by V_i, the value of the second level evaluation index C_{ij} is represented by V_{ij}, V_{ij} is obtained by its affiliated evaluation function. It is stipulated that $V_{ij}\in[0,1]$, so the value interval of the evaluation result Q is $Q\in[0,\pi]$.

In the end, the value range of the final evaluation result Q is divided into seven intervals, and the security evaluation of each interval is defined as follows.

IV. Case Study

In order to verify the feasibility and validity of the model and method proposed in this paper for the security evaluation of XML communication protocol, the security electronic bank simulation system designed in the paper [11] was used as evaluation material, and the web service structure is shown in Fig. 5.

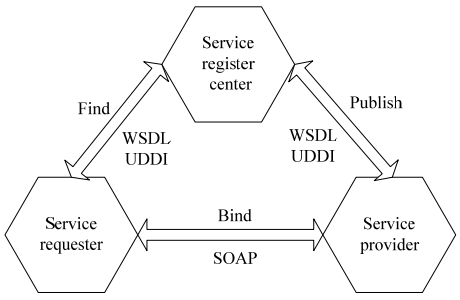


Figure 5. Web service structure.

In the experiment, the XML communication protocol-SOAP protocol applied in the electronic bank system was analyzed, the function *SoapMonitor* was used to intercept Soap protocol data package, and the security of the Soap protocol was analyzed and evaluated with reference to protocol data, designing document and the quantitative algorithm which have been described in section three of this paper. The simulation experiment data and calculation result are shown in Table Ⅵ.

Through Table Ⅳ and Table Ⅴ, the integrated evaluation result of the electronic bank system was calculated as $Q=V*S'T=0.7121\pi$, and the security grade of the SOAP protocol used in this system was medium high

TABLE V.

FINAL INTEGRATED EVALUATION RESULT

Low	Comparatively low	Medium low	Medium	Medium high	Comparatively high	High
0~0.3π	0.3~0.5π	0.5~0.6π	0.6~0.7π	0.7~0.8π	0.8~0.9π	0.9~π

It can be seen from Table Ⅵ that in this simulation system, the values of non-repudiation index of XML part are the lowest, so the security of the non-repudiation index can be enhanced by using digital timestamp adding technology, the values of component evaluation index of communication load part are comparatively low, it is suggested that comprehensive remedial measures should be taken to solve this problem. In the end, preventive measures should be taken to deal with the possibly occurred security threats with reference to one or several index for which the values of potential vulnerability are the lowest. In order to verify the feasibility of the evaluation model and method proposed in this paper, ten experts were invited to perform integrative judgment to this protocol according to their experiences, and the result is shown in Table Ⅶ.

TABLE VI.

EVALUATION INDEX CALCULATION RESULT

V_{11}	V_{12}	V_{13}	V_{14}	V_{21}	V_{22}
1	0.9231	0.6	0.7035	0.5511	0.5833
V_{23}	V_{31}	V_{32}	V_{33}	V_{34}	
0.5	0.48	0.72	0.58	0.54	

The comparison shows that the result obtained by the security integrated evaluation method based on the three-dimensional sphere model is consistently with the judgment result of at least half of above experts. Therefore, it can be regarded that the security integrated evaluation method can more effectively and objectively reflect the security state of XML communication protocol.

V. Conclusions

Combined with the features of the XML communication protocol, this paper proposes a three-dimensional sphere model for XML communication protocol, proposes a protocol security integrated evaluation method based on the three-dimensional sphere model and a security component evaluation method based on coordinate system projection. A simulation experiment is carried out to verify the feasibility and validity of the security evaluation method proposed in this paper for the XML communication protocol.

The future work in this field should be conducted in the filed including automatic XML communication protocol evaluation, automatic protocol data acquisition, automatic evaluation index data identification and so on.

TABLE VII.

EXPERT EXPERIENCE JUDGMENT RESULT

Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
Medium high	Medium high	Medium	Medium high	Medium high
Expert 6	Expert 7	Expert 8	Expert 9	Expert 10
Medium high	Medium	Medium high	Comparatively high	Medium high

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of this paper. This work was supported in part by National Natural Science Foundation of China under Grant No. 60776807 and 61179045, the Key Project of High Technology Program under Grant No. 2006AA12A106, the Key Project of Tianjin Science & Technology Support Program under Grant No. 09JCZDJC16800, the CAAC Science & Technology Project under Grant No. MHRD201009 and MHRD201205, the Central University Basic Science Research Foundation of CAUC under Grant No. ZXH2009A006.

REFERENCES

[1] Alrouh B, Ghinea G. "A performance evaluation of security mechanisms for web services", *Proceedings of the 2009 Fifth International Conference on Information Assurance and Security. Piscataway*, NJ: IEEE Computer Society, pp. 715-718, 2009.

[2] Tang K, Chen S, Levy D. "A performance evaluation of web services security", *Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference*, Piscataway, NJ: IEEE Computer Society, pp. 67-78, 2006.

[3] Li J, Chen H, Deng F. "A security evaluation method based on threat classification for web service", J*ournal of Software*, vol.6, no.4, pp. 595-603, 2011.

[4] Cheng R. *Research and Implementation of Security Mechanism of SOAP Message Exchange Based on SOA*, Xian Electronics Science and Technology University, 2008.

[5] Xu Y, Xie X, "Modeling and analysis of security protocols using colored Petri Nets", *Journal of Computers*, vol.6, no.1, pp. 19-27, 2011.

[6] Mi Q. *University teaching principle*, Shanghai: Shanghai Jiao Tong University Press, pp.97-100, 1989.

[7] Xu Y, Tang W, Wu B. "Design principle and application of S&T evaluation index system", *Soft Science in China*, vol.30, no.2, pp. 48-51, 2010.

[8] Yang H, Xie L, Zhu D. "A vulnerability severity grey hierarchy analytic evaluation model ", *Journal of University of Electronic Science and Technology of China*, vol.39, no.5, pp. 778-782, 2010.

[9] Pang J, Peng X. "Trustworthy web service security risk assessment research", *Proceedings of the 2009 International Forum on Information Technology and Applications*. Piscataway, NJ: IEEE Computer society, pp. 417-420, 2009.

[10] Zhou X. *Study on the Selection of Marine Heat Source System Based on Fuzzy Comprehensive Evaluation Method*, Shanghai Jiao Tong University, 2010.

[11] Ben G, *Professional Web Services Security*, Beijing: Tsinghua University Press, 2008, pp. 400-444.

Lixia Xie was born in Chongqing, China in April 1974. She received the B.S. degree in Electronic Information Engineering from Harbin Engineering University, in Harbin China, in 1996. She received the M.S. degree in Software Engineering from Nankai University, Tianjin China, in 2003. Since 1996, Ms. Xie has been with the School of Computer Science at Civil Aviation University of China, where she is currently an Associate Professor. Associate Professor Xie's current major fields of study include network security and information security, network intrusion detection, cloud computation environment security and security service, intelligent information system.

Yanxin Yan was born in Shanxi, China on November 1988.She received the B.S. degree in Computer Science and Technology from Binhai College, Nankai University, Tianjin China, in 2011. She is currently completing a Master of Science degree in Computer Science in Civil Aviation University of China. Ms. Yan's current major fields of study include network security and information security, network intrusion detection, cloud computation environment security and security service, intelligent information system.

Jiyong Zhang was born in Hubei, China in 1978. He received his B.S. degree in 1999, and his M.S. degree in 2001, both majored in computer science, from Tsinghua University, in Beijing China. He obtained his PhD degree in Computer Science from School of Computer and Communication Sciences, Swiss Federal Institute of Technology in Lausanne (EPFL) in April 2008. Dr. Zhang has been with the School of Computer and Communication Sciences at EPFL since 2008, where he is currently a Senior Researcher. Dr. Zhang's current research interests are human computer interaction, especially intelligent user interface, recommender systems, online product search, automated decision making, e-commerce technologies, etc.