Research on the Security of Web Services Model Based on P2P

Abstract

With the rapid development of Web Services and P2P, the combination of the two distributed computing technologies is available. Through analyzing and researching, a new distributed computing model of Web Services based on P2P is presented. Further more, a method integrated with Digital signature, MAC, XML encryption is provided to improve security of the model, based on analyzing.

Key Words: Web Services; Peer-2-Peer; Digital signature; JXTA

1 Introduction

Web Services and P2P technology are focus of research presently. Appearance of Web Services comes from requirement of realizing RPC through internet, and a new Service-oriented Architecture is presented through combining component-oriented method and predominance of web technology[1]. In essence, Web Services is still a centralized model[2].P2P is also a new technology of network calculation, and this kind of technology is not through relaying equipment but straight to exchange data or service among different PC users. Each user may connect directly the computer of other users to exchange files, and does not connect to server to browse and down. Because Intermediate link is eliminated, P2P technology makes communication of network become easier and more direct. P2P which changes Internet present state of taking big website as the center returns to "non-centre ", and furthermore, returns power to users[3]. Compared with traditional C/S model, because of utilizing effectively a large number of information resources left unused in the network, memory space , processor cycle ,etc., it avoided the bottleneck question that the server brings. Besides helping the performance of optimizing, P2P mode can also be used for dispelling the danger of the overall situation of influence because of some single troubles. If P2P mode is adopted by enterprises, The distributed service between clients is utilized to replace the some data centre functions with expensive expenses, and the data search and backup can run on the client.

Web services and P2P are in developing in earlier stage at present. As the competition between Web service provider is aggravated, The whole structure of Web serve is still in changing constantly. If disperse system and centralized system are integrated, fully using the cooperation relation existing between Web serves and P2P, raising Web serve flexibility of network[4] through discretization technology of P2P, distributed calculating based on Web services is more stalwart , high-efficient and has better more interoperability. It is very importantly meaningful for distributed technology, Web service and P2P development.

2 New calculation model of web services based on P2P

One main question of P2P is locating P2P serves as well as understanding the first floor correspondence agreement. The general P2P way searches the suitable P2P application procedure on Internet and installs and customizes application procedure. In integrated environment, customer API is used frequently or the tool bag provides seals, that is, this can hide the application procedure agreement detail and make it easy. Web services have provided the UDDI registration service for the localization application

procedure. In addition, it also provided the transmission and the binding agreement that is distinguished by the server. In a word, Web services technology may solve many frequently asked questions in designing, establishing and disposing P2P application procedure. Using XML, SOAP, WSDL, HTTP and UDDI jointly make P2P application based on web services be even more standard, be easier to visited, understand and integrate.

However, all of technique related web services at present and main realization of Web services all rely on the traditional client-server correspondence model. One example of using client-server correspondence model in the Web service application procedure is SOAP agreement based on HTTP above the agreement foundation. Because UDDI is one kind based on the OAP foundation above technology, in nature, UDDI has also used the client-server correspondence pattern. P2P application procedure distinguishes between the traditional client-server pattern, and it is one kind of distributed system. In order to make application system with distributed structure be able to provide the high grade service under the open style environment, reduce response time of Web service, enhance system robustness, realizing the Web service under the P2P environment is one kind of effective solution. After the research, a new calculation model of web services based on P2P is presented, as shown in Figure 1:under this model, each peer may act as the service provider, and may take the service request, reduce to the high end server dependence, fully use massive at ease resources, enhance the Web service efficiency. The concrete process is: Service provider node(peer) may issues its service to UDDI, and service request node(peer) retrieves the related information of service which need through UDDI. After retrieves to the service which needs, sends out the request through the JXTA pipeline to the service provider, Meanwhile, the tenderer of service also returns the corresponding information for the request through the JXTA pipeline. Its core is to connect the service request with the service provider through the pipeline, namely, they do not contact through the tradition SOAP protocol based on HTTP above, but are carried on the relation through SOAP agreement based on P2P foundation above. See Figure 2.

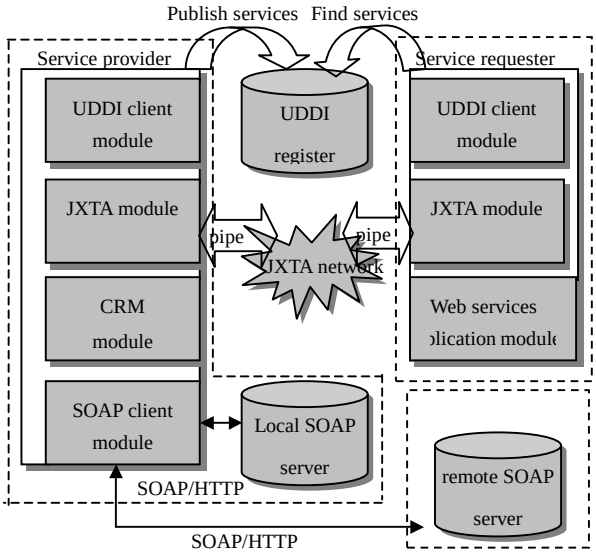

Figure 1. Web services model in P2P.

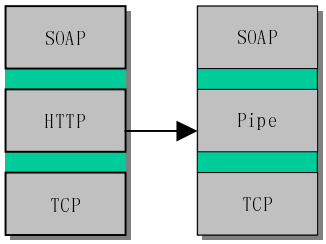

Figure 2.improved SOAP protocol

3 Security of calculation model of web services based on P2P

3.1 Security of P2P/JXTA

In the traditional significance, the secure definition is: the protection information, the system and the service exempts the malicious infringement, the misoperation and the calamity event destruction. Generally

speaking, the network security has five basic safe requests: confidentiality, user, the entity or the process that has not passed through the authorization is unable to steal the information. Authorization, the authorization is determined to permit users what they can do, and give the different type user the different privilege. The integrity, guarantees that users who have not passed through the authorization are not able to change or the deletion information, thus the information cannot intend or have no intention to destroy in the transmission process, maintains the integrity, the unification of information. The primitive proof, the indication to users of the information or the data transmission. Non-repudiation, guarantees which users of information transmission cannot deny or the denial to transmit the information. The final three safe requests are each other correlations, difference of the data integrity and the primitive proof is that users cannot guarantee the information is not duplicated transmitted though the data is complete. The encryption key is appropriate for the primitive proof in authentication, but it is not suitable in "prevented denies".

JXTA has drawn up group of agreements for construction of the P2P network. JXTA is mainly composed by six agreements that are specially designed for specific, distributed, the coordinated network computation. Using these agreements, peers may cooperate mutually to establish the self-organization, the self-control coordinated group, and don’t care about position where they locate in the network, And needn’t to management structure of concentration. The JXTA platform provides the security feature as follows: Secure Transport layer, TLS, namely, Secure Sockets Layer, SSL; Peer certificates; Personal security environment.

3.2 Security of web services

At present, security socket layer (SSL) and actual Transport layer Security (TLS) are used for the application procedure of web services to provide the security of transmission rank. SSL/TLS has provided several secure function, including authentication, data integrity and data confidentiality. If SSL/TLS based on HTTP is used, the entire strip news can be encrypted. In the first destination, the entire strip news is deciphered, which there is a threat of sniffer before it which is again completely encrypted transmits to the next node. Obviously the SSL encryption based on HTTP exists merely in the transmission process, it is not lasting. Namely, SSL/TLS only can provide safe conversation of the transmission level/Network level, but cannot provide the safety mechanism of the application layer. For example, A node send the information to C node, but they must pass through B node, the information is transmitted with SSL/TLS between A and B, B and C, therefore it is safe between A and B, B and C, but security of the information cannot be guaranteed in B node.

3.3 Security of new model

In the new model, mainly using the SOAP security safeguards the web services security. Realization of SOAP security solution is based on three W3C XML standard: XML Digital Signature, XML encryption, and XML Key Management Services. The SOAP level security is above the transmission level and the application layer, expand the SOAP level security, apply five basic requests of security to the entire SOAP information, including SOAP head as well as SOAP body. At the same time, the more security measure also may unify the SOAP level security and the transmission level as well as the application procedure solves. Both receive leg and transmit leg can be confirmed by the identification authentication. One kind is identification authentication of the news founder, it is called the news identification authentication, the other kind is status

confirmation receive leg and transmit leg, it is called transmit leg/receive leg identification authentication. Usually, the news identification authentication is realized through the news which attaches a digital signature or message authentication code in transmission process. The news identification authentication is unable to guarantee who has transmitted this news, which needs to pay attention. Identification authentication of transmit leg and the receiving end can guarantee who they are. In other words, transmit leg can confirm status of news receiving end, and the receiving end can confirm status of news transmit leg. But this confirmation is unable to guarantee who founded this news. The news identification authentication technology makes use of two general technologies: Message Authentication Code and digital signature. Besides above two

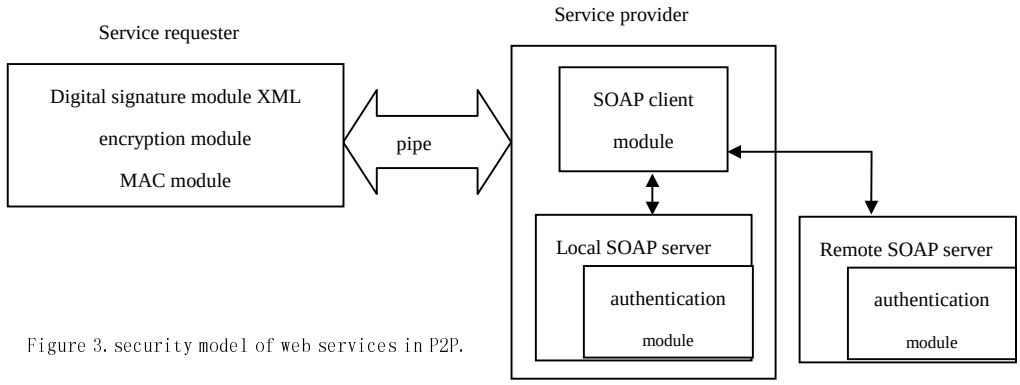

Figure 3. security model of web services in P2P.

secure request, non-repudiation is also a quite important request in the Web service application. Non-repudiation guarantee malicious transmit let is unable to deny fact that he has founded and transmitted this specific news. That is, non-repudiation guarantee that transmit leg of the news and the news founder was the identical person.

Moreover, the entire XML documents may encrypted, then safely transmit it to one or many receiving ends. That is SSL or the TLS common function. It makes one be even more interesting that different part of the identical documents may carry out different processing. The XML signature may define a series of XML element that may inlay or attach to any XML documents. Thus, the addressee can confirm whether the receiving news and the transmitting news is the same.

WS-Security criterion can solve security problem about authentication, authorization, confidentiality, integrity, non-repudiation, and so on, and it provides the solid foundation for the application of web services. WS-security unified XML Signature and XML the Encryption standard, through inserting the security information in SOAP head (digital signature, the X.509 certificate),and guarantee the integrity and the secrecy of SOAP message.

Through above analyzing and researching, in order to guarantee security of Web services in P2P environment, a security model is presented. See Figure 3.

The service request has the SOAP information through using the encryption module. And then, he carries out digital signature, encryption, and so on for partialness and entireness of the requesting information. At last, he places the result in SOAP head. SOAP information that has been processed is transmitted to service provider through pipelining. The service provider, which attaches SOAP information that received to HTTP head through SOAP client module, transmits request to local or the long-distance SOAP server. SOAP engine firstly intercepts head information that passes on, and then

carries out the confirmation with the confirmation module.

4 Conclusion

A new distributed computing model of Web Services based on P2P is presented this paper. Under this model, we has conducted the more detailed analysis and research to its security, and proposed and realized web services security based on the P2P through digital signature, MAC, XML encryption enhanced, and so on. The practice proves that this method is feasible. But we discover in the work that the client side cannot automatically found the SOAP news and transmit the SOAP news, but through the hard code or programs, which increased the client side work load and complexity. We hope this will be solved in the next step of work.

References

[1] Shi Jing, Ding Changming, Zhao Zeyu, Xue Xiangyang. Web Overview of Web Services Composition Research [J]. Computer Science, 2004, 31(6): 54-58.

[2] Yue Kun, Wang Xiaoling, Zhou Aoying. Underlying Techniques for Web Services: A Survey[J].Journal of Software,2004、15(3):428-442.

[3] Robert Flenner, Michael Abbott, etc. Java P2P Unleashed[M]. Beijing：Post & Telecom Press，2003.

[4] Quan Z. Sheng, Boualem Benatallah. SELF-SERV:A Platform for Rapid Composition of Web Services in a Peer-to-Peer Environment[C].Proceedings of the 28th VLDB Conference, Hong Kong, China, 2002: 1-8.