XML-Based Digital Signature Accelerator in Open Mobile Grid Computing

Namje Park[1], Kiyoung Moon[1], Kyoil Chung[1],
Seungjoo Kim[2], and Dongho Won[2]

[1] Information Security Research Division, ETRI,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{namjepark, kymoon, kyoil}@etri.re.kr
[2] School of Information and Communication Engineering, Sungkyunkwan University,
300 Chunchun-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea
skim@ece.skku.ac.kr, dhwon@dosan.skku.ac.kr

Abstract. As Grid technology evolves it is becoming evident that the inclusion of mobile devices in a Grid environment will benefit both the Grid and mobile network communities. Many mobile devices, however, have limits on their computational resources that make it difficult to achieve this goal. The goal of this paper is to investigate how well the most limited wireless devices can make use of grid security services. This paper describes a novel security approach on fast mobile grid services based on current mobile web services platform environment using XML signcryption mechanism.

1 Introduction

Grid is the umbrella that covers many of today's distributed computing technologies. Grid technology attempts to support flexible, secure, coordinated information sharing among dynamic collections of individuals, institutions, and resources. This includes data sharing but also access to computers, software and devices required by computation and data-rich collaborative problem solving. So far the use of grid services has required a modern workstation, specialized software installed locally and expert intervention. In the future these requirements should diminish considerably. One reason is the emergence of grid portals as gateways to the Grid. Another reason is the 'web services' boom in the industry. The use of XML as a network protocol and an integration tool will ensure that future grid peer could be a simple wireless device [2, 3].

Mobile communications represent one potential new area where Grid technology may be applied. In parallel with the evolution of Grid computing, mobile communications technology has developed to the stage where wireless networks are now becoming commonplace in the home environment. The potential for new applications based around the convergence of mobile devices and Grid technology is now becoming apparent to both the research and business communities [2, 3].

Furthermore, open mobile grid service infrastructure will extend use of the grid technology or services up to business area using web services technology. Therefore differential resource access is a necessary operation for users to share their resources securely and willingly. Therefore, this paper describes a novel security approach on fast mobile grid services based on current mobile web services platform environment using XML signcryption mechanism.

H. Zhuge and G.C. Fox (Eds.): GCC 2005, LNCS 3795, pp. 323 – 333, 2005.

2 Emerging Technologies and Background

2.1 Open Mobile Grid Architecture and XML Protocols

The XML protocol-based Web Services interfaces were initially promising as a communication method between wireless devices and back-end servers. A prime candidate for wireless Grid applications is the new Open Grid Services Architecture (OGSA) model used in the Globus Toolkit 3 [10]. Wrapping the existing Grid middleware with XML interfaces holds the promise of providing a universal solution also to wireless devices. As it happens the XML multipurpose protocol stack can be reused over and over again, while the protocol implementation and payload can be described with Web Service Description Language (WSDL) in plain text. However given account to the limited memory constraints, Web Services technology is likely too heavy for first generation MIDP devices. The fact remains, that Web Service protocol implementations such as kSOAP weigh 41 kilobytes i.e. over 30 percent of standard application memory of low-end MIDP device whereas more lightweight protocols such as kXML-RPC requires only 24 kilobytes. The overhead of Simple Object Access Protocol message parsing in light J2ME-based wireless devices has also been studied and the results show 2-3 times slower response times compared to a proprietary protocol that communicates with a proxy client that utilizes Web Services on behalf of the wireless client. The upper scale of MIDP devices is quickly changing and highend mobile phones will provide as large memory footprints as 16Mb. Mobile Web Services is a future technology trend addressed by Microsoft, Open Mobile Alliance and the Parlay Group [11].

2.2 The Performance Problem of XML

XML-based messaging is at the heart of the current grid based on web services technology. XML's self-describing nature has significant advantages, but they come at the price of bandwidth and performance. XML-based messages are larger and require more processing than existing protocols such as RMI, RMI/IIOP or CORBA/IIOP: data is represented inefficiently, and binding requires more computation. For example, an RMI service can perform an order of magnitude faster than an equivalent web service-based grid. Use of HTTP as the transport for Web Services messages is not a significant factor when compared to the binding of XML to programmatic objects.

Increased bandwidth usage affects both wired and wireless networks. Often the latter, e.g. mobile telephone network, have bandwidth restrictions allotted for communication by a network device. In addition, larger messages increase the possibility of retransmission since the smaller the message, the less likely it will be corrupted when in the air. Increased processing requirements affects network devices communicating using both types of networks (wired and wireless). A server may not be able to handle the throughput the 'network' demands of it. Mobile phone battery life may be reduced as a device uses more memory, performs more processing and spends more time transmitting information. As the scale of Web Services usage increases, these problems are likely to be exacerbated.

Fast grid services attempts to solve these problems by defining binary-based messages that consume less bandwidth and are faster and require less memory to be processed. The price for this is loss of self-description. Fast grid service is not an attempt to replace XML-based messaging. It is designed to be an alternative that can be used when performance is an issue.

2.3 XML Signature Acceleration - XML Signcryption

XML signcryption structure and schema has been proposed. Shown below is the XML signcryption XML document.

```
<?xml version="1.0" encoding="UTF-8"?>
<XML_Signcryption>
<SignedInfo>
<CanonicalizationMethod Algorithm/>
 <SignatureMethod Algorithm/>
 <EncryptionMethod Algorithm/>
<Reference URI>
 <DigestMethod1 Algorithm/>
 <DigestMethod2 Algorithm/>
 <DigestValue/>
 </Reference>
 </SignedInfo>
 <SigncryptionValue> </SigncryptionValue>
<Rvalue> </RValue>
 <Svalue> </Svalue>
 </XML_Signcryption>
```

Fig. 1. Basic Architecture of Proposed XML Signcryption

The root element XML signcryption is the fundamental element of the XML documents. Within the root element are contained various other elements such as signed info and the Signcryptionvalue, Rvalue and Svalue [6, 7]. The SignedInfo element contains the information about the signcryption methodology used. It described about the implementation details about signcryption. Within the signed info element there are other elements such as CanonicalizationMethod Algorithm, SignatureMethod Algorithm, EncryptionMethod Algorithm and Reference URI. The CanonicalizationMethod indicates the method that is used for canonicalization. The canonical method allows the use of different characters in the XML document. For example, if there are white spaces in the xml document, these are removed because of the XML canonicalization method used.

The signatureMethod element indicates the signature element used in the signcryption process. EncryptionMethod is the encryption method that is used in the signcryption process. In our example, the algorithm used is DES. The element Reference indicates the link of the file that is being signcrypted. It contains the path of the file that is being signcrypted. The reference URI also contains the different Hashing algorithms that are being used in the signcryption process. In our implementation, we are using MD5 and SHA1.

As indicated in sections above, the result of signcryption are three values, namely c, r and s. these three values are required by the system to create the plain text from these messages. When signcryption is performed on a data, the output is a signcryption value. Signcryption requires different digest functions. The description of the hash functions and also the different parameters required for encryption. The encryption method that is used for signcryption is also shown in the XML document. This information is also shown in the canonicalization method is used to embed a document in another document. Using Xpath filtering, an appropriate file is opened so that the file is opened using the application specified.

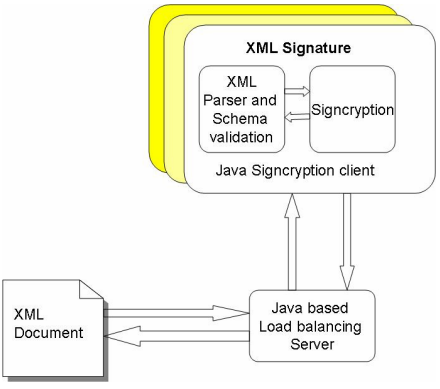

Fig. 2. Architecture for XML-based Signature Acceleration

Signcryption technique has two different variations. These variations are Shortened Digital Signature Standard 1 [6, 7] and Shortened Digital Signature Standard 2. Using JCE based crypto library, Signcryption will be programmed using verification to [6, 7, 9].

XML signcryption schema is shown above. The schema is required to validate the received XML message for its integrity. A part of the XML signcryption module is to create a technique where in badly formed XML documents need to be removed. Survey shows that a lot of attacks on XML servers are due to the fact that the XML documents created are not properly formed. The hardware-based solutions perform this additional task. The software-based module also needs to check the validity of the schema before the document is passed onto the next stages for verification.

The schema defines the various attributes and the elements that are required in a XML document. These attributes declare the feature of the XML document. The Id the element possesses and Multipurpose Internet Mail Extensions (MIME) so as to allow non-textual message to be passed can be incorporated into the XML document. The mode in which the signcryption has occurred, Type specifies a built-in data type.

```
<element name="XML_Signcryption" type="SigncryptionType"/>
  <complexType name="SigncryptionType">
   <sequence>
    <element ref="SignedInfo"/>
   <element ref="SignatuereMethod"/>
   <element ref="EncrptionMethod" />
   <element ref="Reference" minOccurs="0"/>
   </sequence>
      <attribute name="Id" type="ID" use="optional"/>
      <attribute name="MimeType" type="MIME" use="optional"/>
      <attribute name="Mode" type="MODE" use="required"/>
   <attribute name="Type" type="TYPE" use="required"/>
   <attribute name="Encoding" type="CODING" use="optional"/>
  </complexType>
 </element>
```

Fig. 3. XML-Signcryption Schema , root element

The XML signcryption schema and is being used with Java Crypto Extensions and SAX parser to create a XML signcryption module. As the signcryption algorithm is faster compared to other signature algorithms, because of its reduced computation, the system is faster. This system introduces faster processing and also provides an additional feature of encryption along with the signature. Hence, the XML signcryption not only performs the integrity of the XML document, but also performs the confidentiality of the system. This additional facility is provided to the system with faster execution time.

The proposed XML signcryption test environment, as shown in figure 6, an XML document is parsed and schema is validated using SAX parser. After the XML document is validated, the information is passed to signcryption module. The signcryption components can verify/generate the signature for an XML document.

3 The Mobile Grid Security Infrastructure

Web services can be used to provide mobile security solutions by standardizing and integrating leading security solutions using XML messaging. XML messaging is referred to as the leading choice for a wireless communication protocol and there are security protocols for mobile applications based upon it. Among them are the follows. SAML is a protocol to transport authentication and authorization information in an XML message. It could be used to provide single sign on web services. XML signatures define how to digitally sign part or all of an XML document to guarantee data integrity. The public key distributed with XML signatures can be wrapped in XKMS (XML Key Management Specification) formats. XML encryption allows applications to encrypt part or all of an XML document using references to pre-agreed symmetric keys. The WS-Security, endorsed by IBM and Microsoft, is a complete solution to provide security to web services. It is based on XML signatures, XML encryption, and an authentication and authorization scheme similar to SAML (Security Assertions Markup Language). When a mobile device client requests access to a back-end application, it sends authentication information to the issuing authority. The issuing authority can then send a positive or negative authentication assertion depending upon the credentials presented by the mobile device client. While the user still has a session with the mobile applications, the issuing authority can use the earlier reference to send an authentication assertion stating that the user was, in fact, authenticated by a particular method at a specific time. As mentioned earlier, location-based authentication can be done at regular time intervals, which means that the issuing authority gives out location-based assertions periodically as long as the user credentials make for a positive authentication.

CVM (Certificate Validation Module) in XKMS system perform path validation on a certificate chain according to the local policy and with local PKI (Public Key Infrastructure) facilities, such as certificate revocation (CRLs) or through an OCSP (Online Certificates Status Protocol). In the CVM, a number of protocols (OCSP, SCVP, and LDAP) are used for the service of certificate validation. For processing the XML client request, certificate validation service from OCSP, LDAP (Lightweight Directory Access Protocol), SCVP (Simple Certificate Validation Protocol)

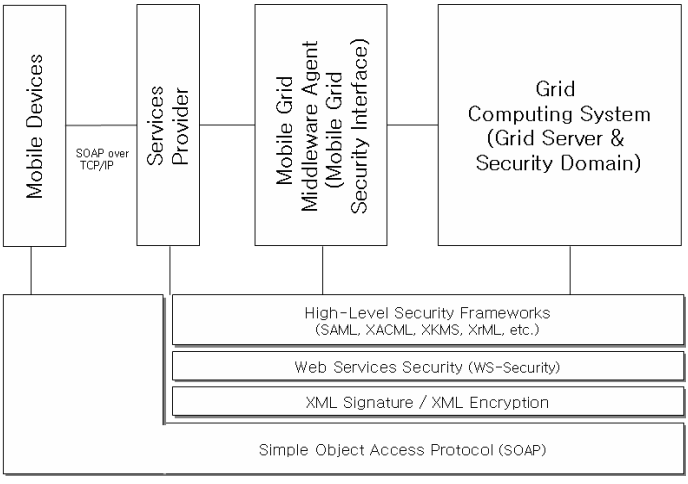

Fig. 4. Security Architecture for Open Mobile Grid Middleware

protocols in XKMS based on PKI are used. The XKMS client generates an 'XKMS Validate' request. This is essentially asking the XKMS server to go and find out the status of the server's certificate. The XKMS server receives this request and performs a series of validation tasks e.g. X.509 certificate path validation. Certificate status is determined. XKMS server replies to client application with status of the server's certificate and application acts accordingly. Using the OCSP protocol, the CVM obtained certificate status information from other OCSP responders or other CVMs. Using the LDAP protocol, the CVM fetched CRL (Certificate Revocation List) from the repository. And CA (Certificate Authority) database connection protocol (CVMP;CVM Protocol) is used for the purpose of that the server obtains real-time certificate status information from Cas [3, 4, 5]. The client uses OCSP and SCVP. With XKMS, all of these functions are performed by the XKMS server component [8, 10]. Thus, there is no need for LDAP, OCSP and other registration functionality in the client application itself.

4 Implementation Prototypes

In this architecture we are adopting a security-oriented approach currently conforming to the OGSA specification and using the Globus Toolkit 3 implementation. In the near future we plan to migrate to the newest WS specification and take advantage of the latest WSDL that will provide a lot of enhancements for Grid service development. Components of the grid security are XML security library, service components API, application program. Although message service component is intended to support XML applications, it can also be used in order environments where the same management and deployment benefits are achievable.

The figure for representing testbed system architecture of service component is as follows figure 5. We use testbed system of windows PC environment to simulate the

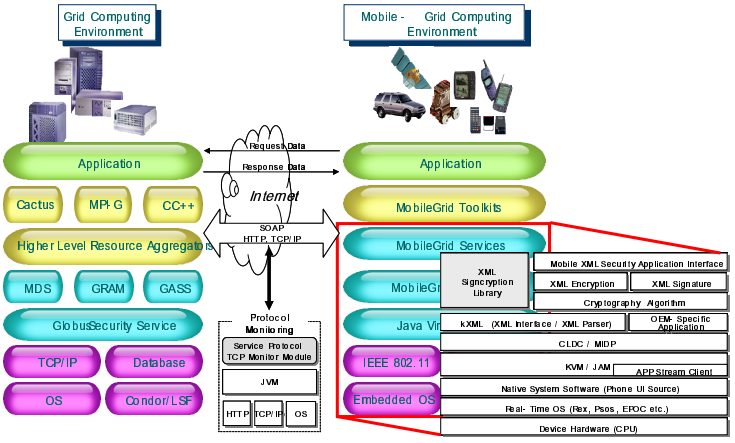

Fig. 5. XML Signcryption Component for Open Mobile Grid Services

processing of various service protocols. The protocols have been tested on pentium 3 and pentium 4 PCs. It has been tested on windows 2000 server, windows XP.

Java 2, Micro Edition (J2ME) is a set of technologies and specifications developed for small devices like smart cards, pagers, mobile phones, and set-top boxes. J2ME uses subset of Java 2, Standard Edition (J2SE) components, like smaller virtual machines and leaner APIs. J2ME has categorized wireless devices and their capabilities into profiles: MIDP (Mobile Information Device Profile), PDA and personal. MIDP and PDA profiles are targeted for handhelds and personal profile for networked consumer electronic and embedded devices. As the technology progresses in quantum leaps any strict categorization is under threat to become obsolete. It is already seen that J2ME personal profile are being used in high-end PDAs such as pocketPCs and mobile communicators. We will concentrate on the most limited category of wireless J2ME devices that use MIDP. Applications that these devices understand are Midlets. Typically maximum size of a Midlet varies from 30-50kbs and user can download four to six applications to his mobile phone. Midlet is a JAR-archive conforming to the Midlet content specification [2].

The server is composed server service component of mobile grid platform package. And the message format is based on Specification of W3C (World Wide Web Consortium). XML signcryption based technique that has been under study. Signcryption is a technique that provides both confidentiality and integrity by performing both the techniques of encryption and signature at reduced costs.

5 Simulative Network Performance Evaluation

As explained in section 2, the signcryption technique has been developed and tested against other signature systems. Table 1 below shows the time taken for the generating signcryption plotted against the number of iterations [12].

Table 1. Total time taken vs. number of iterations for both Signcryption and Unsigncryption

	Signcryption	Unsigncryption
Iterations	Ms	Ms
1	891	1672
10	1157	1906
100	3391	8125
200	6390	13890
300	8219	19109
400	10328	26078
500	12468	31437

Figure 6 shows the plotted information presented in the table 1. It can be seen that the time taken for verification of the signature takes a longer time than the generation of the signcryption value itself.

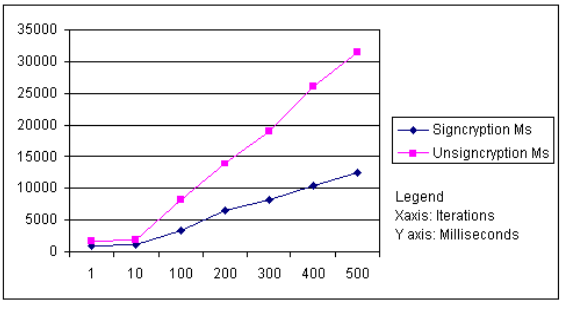

Fig. 6. Time taken plotted against number of iterations for Signcryption and Unsigncryption

Table 2 shows the time taken per iteration versus the number of iterations. Figure 7 shows in the information in a graphical form. It can be noticed that as the number of iterations increase the amount of time taken per iteration decreases significantly.

Table 2. Total time taken vs. Number of iterations for Signcryption and Unsigncryption

	Signcryption	Unsigncryption
Iterations	Ms/iteration	Ms/iteration
1	891	1672
10	115.7	190.6
100	33.91	81.25
200	31.95	69.45
300	27.40	63. 70
400	25.82	65.195
500	24.936	62.874

In the case of Unsigncryption the time taken per iteration is much more than the time taken for signcryption. The process provides both confidentiality and integrity at relatively lesser speed and lesser time as compared to other signature techniques.

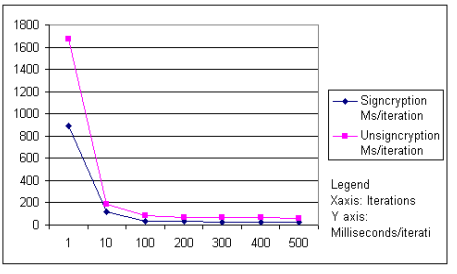

Fig. 7. Time taken plotted against number of iterations for Signcryption and Unsigncryption

5.1 Comparison Among the Signature Techniques

The different techniques discussed above has been tested and compared. The figure 8 shows the time taken per iteration for signature generation. It can be noticed that the time taken for signcryption decreases steadily as the number of iterations are increased. For one iteration, the time taken for signcryption is higher than other signature techniques. But as the number of iterations decrease, the performance of signcryption is comparable with the other techniques. But as the signcryption embodies both signature and encryption, signcryption would be recommended [12,13].

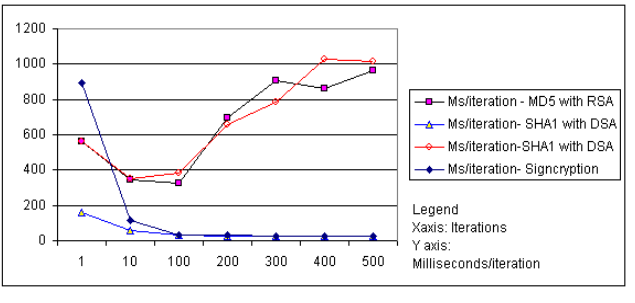

Fig. 8. Comparison between the algorithms for signature generation

It can be noted that the best performance in signature verification is performed by SHA1 with DSA. Figure 9 shows the comparison between the time taken per iteration versus number of iterations for signature verification for the signature algorithms discussed. It can be seen that the time taken for Unsigncryption is high for single iteration than compared to others. But as the time increases, the time taken for iteration decreases but is higher than the other techniques.

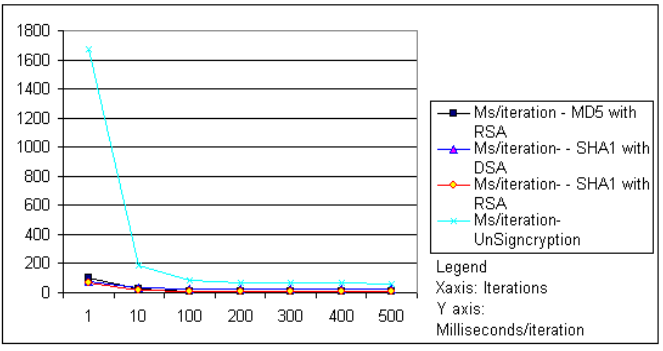

Fig. 9. Showing Comparison between the algorithms for signature verification

The time taken per iteration is not significantly lower in case of verification, but is significant in the case of signature generation except for signcryption. If the primary concern is integrity, then the ideal solution to use would be to use SHA1 with DSA. However if the concern is for both integrity and for confidentiality then signcryption would be an ideal solution to use. This can be demonstrated by figure 10.

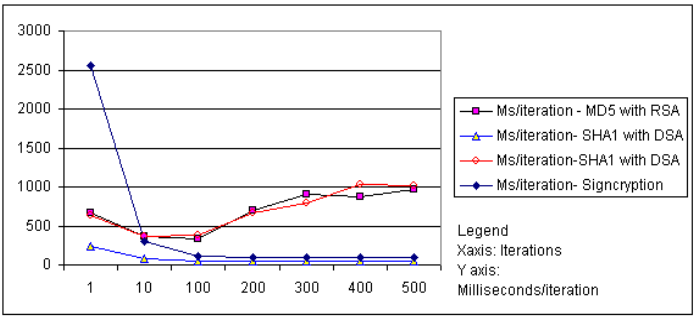

Fig. 10. Showing Comparison between the algorithms for both signature generation and verification

Figure 10 shows the time taken for single iteration of generation and verification plotted against the number of iterations. It can be seen from the graph that the time taken for SHA1 with DSA is the least. But it offers only integrity services. Signcryption offers both confidentiality and integrity and performs well when the numbers of iterations are used.

6 Conclusion and Further Works

Mobile grid services are so attractive that they can cover all walks of life. However, current grid is growing slower than expected. Many problems like accuracy, privacy, security, customer requirement have to be addressed. It should be understood that there is no single universal solution to grid. Signcryption technique allows simultaneous processing of encryption-decryption and Signature. It has been proved that the use

of signcryption decreases the processing time by 58%. Signcryption is being programmed using the field theory. Signcryption technique is very efficient as it uses only a single exponentiation for both encryption and signature.

We propose a novel security approach on fast mobile grid services based on current mobile web services platform environment using XML signcryption mechanism. Our approach can be a model for the future security system that offers security of open mobile grid security.

The further works are follows: the new problems may arise for introduction of secure mobility of grid services. These problems include protocol compatibility, security of mobile service and complexity of programming, etc. Our further works are to consummate protocol extension, implement the secure mobile agent's replant to Grid, and deeply research and implement secure mobile agent control mechanisms in grid environment.

Acknowledgement

The first author would like to thank Yuliang Zheng, Ph.D. of the University of North Carolina at Charlotte for his encouragement and assistance.

References

1. Mika Tuisku: Wireless Java-enabled MIDP Devices as peers in Grid Infrastructure. Helsinki Institute of Physics. CERN
2. Ye Wen: Mobile Grid Major Area Examination. University of California (2002)
3. E. Faldella and M.Prandini: A Novel Approach to On-Line Status Authentication of Public Key Certificates, in Proc. the 16th Annual Computer Security Applications Conference (2000)
4. Yuichi Nakamur, et. Al.: Toward the Integration of web services security on enterprise environments. IEEE SAINT '02 (2002)
5. Diana Berbecaru, Antonio Lioy: Towards Simplifying PKI Implementation, Client-Server based Validation of Public Key Certificates. IEEE ISSPIT (2002) 277-281
6. Joonsang Baek, et. Al.: Formal Proofs for the security of signcryption, PKC'02 (2002) 80 - 98
7. Y. Zheng: Digital signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption) , Advances in Cryptology -- Crypto'97. Lecture Notes in Computer Science, Vol. 1294. Springer-Verlag (1997) 165-179
8. Jang Hyun Baek, et. Al.: An Efficient Two-Step Paging Strategy Using Base Station Paging Agents in Mobile Communication Networks. ETRI Journal, Vol.26, No.5 (2004) 493-496
9. Proposed Fedral Information Proceeding standard for Digital Signature Standard(DSS), Fedral Register. Vol. 56. (1991)
10. I. Foster and C. Kesselman. Globus: A metacomputing infrastructure toolkit. International Journal of Supercomputer Applications, 11(2), 1997.
11. Miika Tuisku: Wireless Java-Enabled MIDP Devices as Peers in a Grid Infrastructure. Lecture Notes in Computer Science, Vol. 2970. Springer-Verlag (2004) 273-281
12. Seunghun Jin, et. Al.: Cluster-Based trust Evaluation Scheme in Ad hoc Network. ETRI Journal, Vol.27, No.4 (2005) 465-468
13. Yuliang Zheng, et. Al.: Research on Software-based XML Signature Acceleration. Project of ETRI, Vol. 1 (2004) 22-35