Efficient Authentication Framework in Ubiquitous Robotic Companion

Cheol-Joo Chae, Han-Jin Cho, Jae-Kwang Lee, *Member, KIMICS*

Abstract—The robotics industry, that is the major industry of the future and one of the new growth power, is actively studied around ETRI, that is the leading under state-run research institute of the advanced technique of U.S. and Japanese and knowledge economy part. And positive and negative and academic circles, the research institute, and the industrial circles communally pursue the intelligent service robot enterprise of a network-based called URC. This network-based intelligent robot does the RUPI2.0 platform and URC environment by the base. Therefore, a stability need to be enhanced in the through this near future when the research for the preexistence vulnerability analysis and security request is needed than the commercialized network-based intelligent robot in order to implement the network-based intelligent robot. Thus, in this paper, we propose the efficient authentication Framework which is suitable for the URC environment.

Index Terms— *URC, RUPI, Robot Security, Robot Authentication.*

I. INTRODUCTION

In the general home or the office environment, the intelligent service robot is the robot performing the inappropriate task that it fits for the given environment and it connects with the network system and interacts with the human. Actively the intelligent service robot reacts to the changing environment and is developed in the form providing the service adhering closely to the human unlike the industrial robot repeatedly executing the determined task. Recently, interest for network robot(u-Robot) which provide various services is rising. As the IT based intelligent service robot, the network robot is not restricted to the time, a place, and a situation and connects with the various sensor information within the ubiquitous environment and it deviates from the existing stand-alone type robot and interacts with the human actively it provides a service to a user. The URC (Ubiquitous Robotic Companion) can connect the network (URC network) to the existing robot terminal and provide the anytime and anywhere various services as the standard protocol (URC protocol) through a communication with the server (URC server). The URC network description can include the wire/wireless network design for the real time service for the service operation of URC and connectivity guranteed, and the embodiment technique and like that utilize the general network description. At this time, the security problem solution that can threaten the network robot is required as the necessary technology. Therefore, there is the necessity to we define the secrecy model at the network-based service robot environment[1].

In this paper, we analysis vulnerability in URC network-based and design efficient authentication framework in URC. In section 2, it introduces about the URC and RUPI. In section 3, we analyze about the security vulnerability which it can be generated in URC and RUPI. And in chapter 4, the efficient authentication framework is designed for the URC security and we describe about the result about the proposal framework in chapter 5.

Manuscript received November 13, 2008; revised February 15, 2009. Cheol-Joo Chae is with the Department of Computer Engineering, Hannam University, Dae-Jeon, Korea(e-mail:cjchae@hnu.kr). Han-Jin Cho is with the School of Computer Science, Information and Standard, Far East University, Korea(e-mail:hjcho@kdu.ac.kr). Jae-Kwang Lee is with the Department of Computer Engineering, Hannam University, Dae-Jeon, Korea(e-mail: jklee@hnu.kr)

II. URC AND RUPI

2.1 URC(Ubiquitous Robotic Companion)

URC needs "Software infrastructure" that can provide various service, "Hardware infrastructure" such as high-performance server for robot and "wire/wireless network infrastructure". Figure 1 shows example of URC configuration.

It can provide various service by connecting robot to network(URC network) and use standard protocol(URC protocol) and communicates with server(URC server).

Therefore, can overcome limitation of robot, and provide various services by cheap price. URC network technology includes wire/wireless network for URC real time service and connectivity guarantee. URC network technology can utilize current network technology. But guarantee of real time and security of robot are very important[2][3][4].

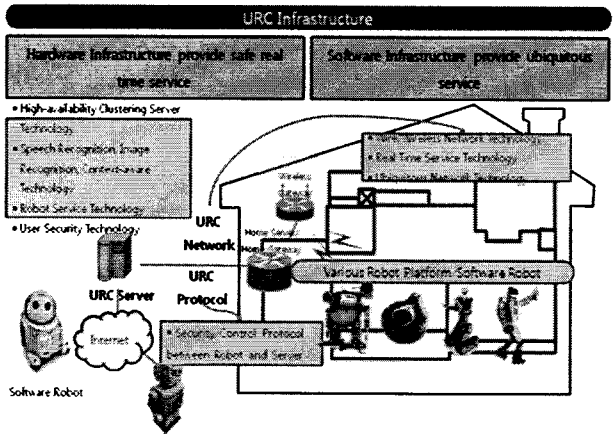

Fig. 1 Example of URC configuration

URC protocol is application protocol between URC server and URC client. URC client includes hardware robot as well as software robot or sensors in environment. URC protocol is doing based on TCP Socket and is consisted of Front End, URC Header, URC Profile Set etc. Front End is interface part to use URC protocol in URC server or URC client. Front End can become function instruction part and part that achieve function actually. URC Header is commonness message header. URC Profile Set includes URC client for specification function achievement and communication data set between robot[5]. URC access control system provides information dynamically using cognition user of robot. With this information, URC connection system composes necessary control logic in service utilization.

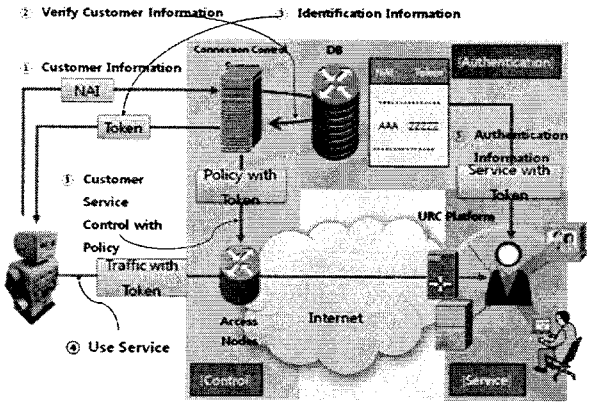

Fig. 2 URC access control system

As see in figure 2, user/robot acquires identification information through authentication process. It provides service using identification information and network-based service policy. Therefore, must be able to construct service system such as figure 3.

When first of robot operation or require IP assignment, access control platform acquire robot's device type and service information. And allocate IP by policy. When robot activates service, it must interwork with Bootstrap server to acquire informations(For example, URC location information, service server location information, robot's S/W version upgrade information). Robot requests authentication to access control system since initialization step. Access control system acquires location information, IP lease information and subscriber/service information from Profile DB for authentication. Then connect robot and server. Information that access control system acquires through this process are send to URC server and RAS(Remote Access System). This becomes base of each service.

2.2 RUPI(Robot Unified Platform Initiative)

The RUPI (Robot Unified Platform Initiative) refers to the robot software standard platform and all sorts standard having an inter-compatibility between the network robot software platform, an intercoperability between a communication and the various information appliances, and an inter-connectivity with the heterogeneous communication network.

The RUPI standard means the minimum requirement which the robot software has to follow the content of technique including the described thing, a component and interface, and etc. And the RUPI model of implementation means the embodiment subject which the RUPI standard immediately can immediately apply as the software module satisfying the RUPI standard.

The RUPI standard consists of the RUPI server, RUPI client, a communication and application component interface, the development tool, and etc. The RUPI client standard is the standard about the robot inside software. And the RUPI server standard manages RUPI client and is the standard about the server providing a service. We can look in the side that the RUPI standard together deals with the RUPI server software, for providing the various services through a network the network protocol, and the robot contents to be differed from the other technology of domestic and foreign. The robot aiming in RUPI is classified into the Thin-Client robot which it connects with the RUPI server to the when necessary and receives help and receives help in the normal times and it performs the independent function performs the most function. RUPI aims at the robot which is

various to the thin client (Thin-Client) robot of the low specification in the reach client (Rich-Client) robot of the high function.

This RUPI 2.0 is a complementary and reference implementation system development subject about a standard an accomplishing in 2009 figure 4 shows the conceptual structure of this kind of RUPI[6].

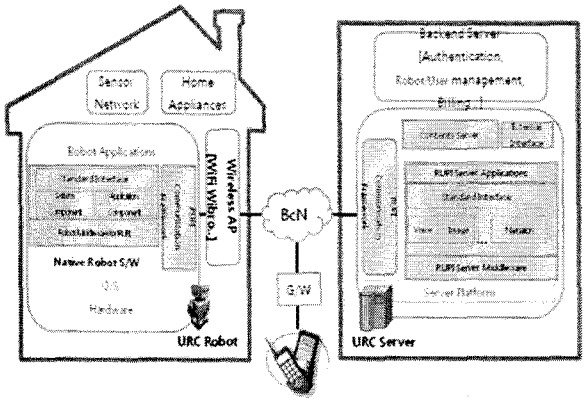

Fig. 3 RUPI conceptual structure

III. Vulnerabilities of URC and Security Requirement

3.1. Vulnerabilities of User/Robot Authentication

ID or passwords from the unprotected network or devices can be eavesdropped because URC clients and URC server operates the process of authentication. Eavesdropped Ids and passwords can be resent and used for authentication. In order to solve this eavesdropping problem, information of ids and passwords will rather be encrypted than be sent as simple statements. Another solution is to use one time password which uses new password for every authentication so as to lose the validity of retransmit by eavesdropping. However, there are some problems that encryption method is complex to manage keys which are used in encryption and a load happens. It also has a difficulty to generate one time password, store and manage.

3.2 Vulnerabilities of SSO(Single Sign-On)

SSO in technical means to share authentication information. How to share authentication information can be different according to the environment of server and application range, so how to apply SSO to existing web applications can be various too. That is why to develop by its own or to use SSO through outsourcing is usual. However, SSO solutions from its own developing process were produced without enough security, it has a problem that an attacker is able to log-in by a user's account by eavesdropping a SSO token transmitted through network by session snatch or snatching and repaying attack while a user moves another service that SSO is applied to. This vulnerability happens because it uses unreliable cookie (http cookie) for managing user's session. That is, a token means it is information which can be open to outside because it is transmitted by cookie. It should not be exposed in the network for perfect security, but it is easily exposed and managed due to reasons of cost and management. If repay attack is possible in the site that SSO is applied to, the attacker naturally has accessibility that easily accesses to other shared sites because of property of SSO that shares authentication information. This vulnerability is a serious fault because it exposes important information which a token includes to outside through the token[7].

3.3 Vulnerabilities of Protocol

As to the URC protocol, we use the application protocol of the TCP base so that a robot or URC clients of a network-based can communicate the URC server and communication. The URC robot is controlled through the interface defined in the URC protocol or the various service provided by the URC server is provided. Therefore, the URC protocol includes the weak point which TCP/IP has.

3.4 URC Security Requirement

There exists the security vulnerability to additionally has additionally to consider the wire / wireless network and protocol exist in the URC network. The vulnerability generated in an internet, and etc. is like that generated in the URC network to be complicated of the local network, it is needed to establish the preferentially synthetic security framework. And the security framework for the security infrastructure build-up at the URC on a network is thus needed. Table 1 shows security requirement in URC.

Table 1 Security Requirement in URC

Security Requirement	Description
Device Authentication	The authentication procedure about the device itself is needed in order to prevent the use of the device which it is not admitted.
User Authentication	In the URC, the user authentication function for the identification of the user using a device besides the device certification is certainly needed.
Authentication between device	For the smooth network robot service providing, the confidence for the resource sharing between the URC network elements has to be elementarily secured. Therefore, the cross certification is needed between a device.

Access control	According to the network robot service, the access privilege control function about the URC network resource is required. The kind of the network robot service which it can be offered as the network robot member is different. Moreover, the control range of the URC network element is different. Therefore, the access control is needed.

IV. Authentication Framework in URC

There exists a security vulnerability that should be considered additionally in the URC network among security vulnerabilities that happen in the exiting Internet because there are various wired/wireless networks and protocols together. That is, every URC server/client of URC network can be a target of various cyber attacks since it is connected to Internet. As there are a variety of information devices in URC network and sharing resources between devices, for the security, considerable requirements are to become more complicated and various. We can see the vulnerabilities that happen in the Internet happen in URC network again, therefore, comprehensive security framework should be stood first when it considers the complex of internet and a security framework is needed for security infra construction in URC network.

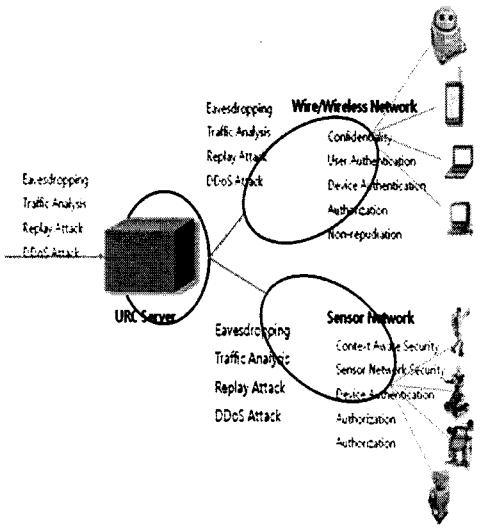

Fig. 4 URC security service structure

URC server is an equipment that plays a main roles of communication, control, and monitoring in the ubiquitous computing environment which composes URC network and controls a connection to the outside Internet. Various services including URC client control are provided through URC server, in order to provide continuous these various services and upgrades, to have a service framework which is extensible is a key point and a comprehensive security service structure is the same as figure 4.

4.1 User Authentication Module

User authentication and access control module is a basic authentication and access control module for URC client and URC server to remote control devices with user's ID and password after mutual authentication of every entity from URC client to URC server through previous mutual authentication module.

First, mobile host user connects to home gateway with one's ID and password. Home gateway checks whether the ID and password delivered to the user ID and password database exist or not. If they do not, the session ends. If they do, it goes to authorization module and it gets an authority for device control for the user based on RBAC policy.

Afterwards, instruction module deals instruction messages of authorized user, transmits them to middleware module for remote controls, and controls devices controled by various protocols (LnCP, UPnP, etc) with taken-back values.

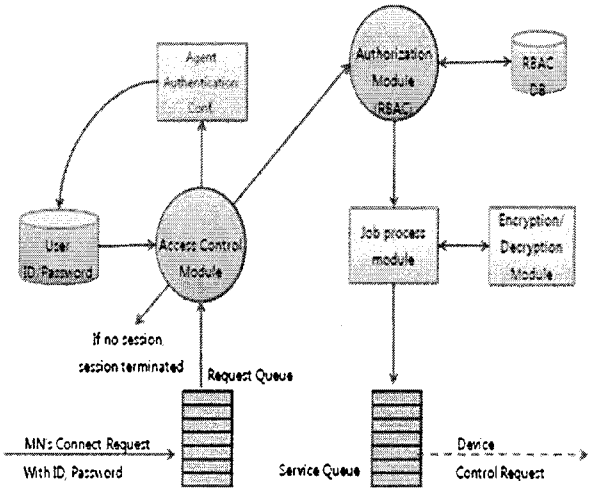

Fig. 5 User certificate and access control module

4.2 Device Authentication Module

So far device authentication is provided at the middleware level. Serial number certificate to confirm device validity is published by individual manufacturer itself, so in the future there should be a technical and political study of united issuance system and management system for device authentication information in order to provide various after-sales service for device or new services combined to device and user authentication function in ubiquitous

environment.

This study presumes that individual manufacturer issues certificates by following the standard and URC server enables to verify them according to the standard. It also presumes that a key and a certificate are issued to the device and the procedure is the same as figure 6.

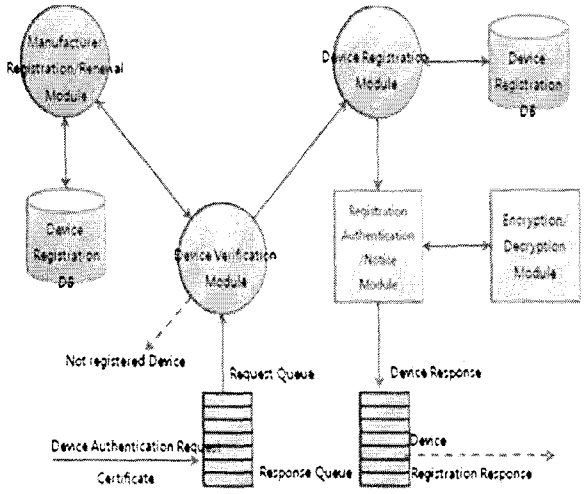

Fig. 6 Device certification and registration module

4.3 Authentication Framework

In the URC environment, the method proposed in this paper is the hybrid of the public key infrastructure authentication mechanism and minimum public key infrastructure authentication mechanism in order to authenticate the user/robot. The user/robot like that delivers the agent advertisement which the outside URC server sends to the URC server and the content that the URC server authenticates indirectly authenticates through a result. The user/robot sends the digital signature to the URC server. After approaching to the certificate authority and confirming the truth or not of the public key, the URC server proves the digital signature. Therefore, the URC server altogether can altogether authenticate the user/robot and outside URC server. Here, the digital signature of the user/robot provides the important non-repudiation about the location which a self registers and can control the URC network resources use with the management. In the case of the URC server, by the digital signature being sent to the outside URC server and being authenticated and generating MAC to the user/robot it is directly authenticated. The attestation about all apparatuses for concerning with the position registration procedure which is novel as this can be made.

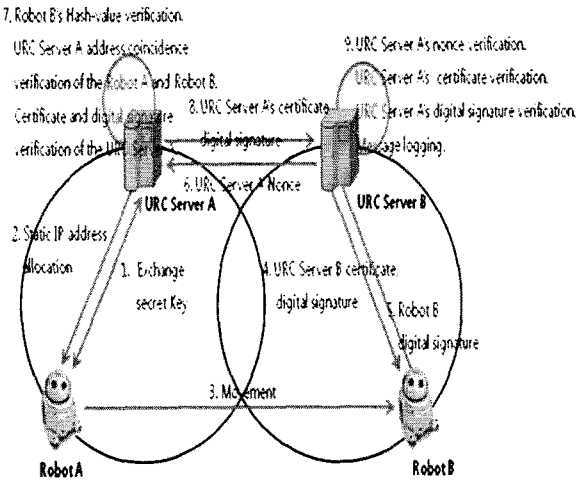

Fig. 7 Authentication framework in URC

V. Authentication Framework in URC

PDA was used in the authentication framework proposed in this paper as the URC robot. The Linux RedHat 9.0 was used as the URC server operating system. C / C++ Was used with the programming language for software development. As to the cryptographic library for an authentication, we used the OpenSSL 0.9.7. In the digital signature between a robot and the URC server, RSA and secure hash algorithm were used. The RSA 1,024 was used as the public key decoding/coding algorithm. And SAH-1 was used as the hash algorithms.

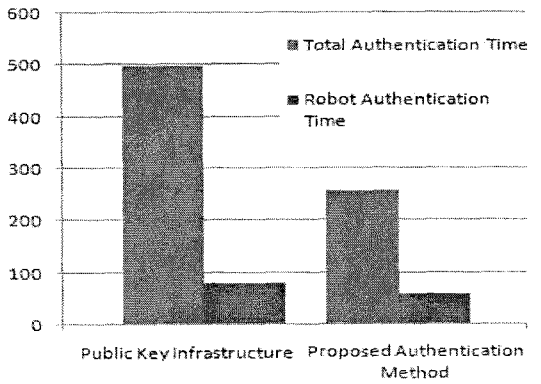

Fig. 8 Total registration and authentication time

Figure 8 shows the certification time at the authentication mechanism total time and robot. We can know in spite of the fact that the existing public key strengthens the security that use is difficult because it long takes time. In the case of the authentication framework proposed in this paper, the registration time was reduced in 60% in comparison with the public key system and a performance was

improved. And the digital signature for the non-repudiation service was added. Therefore, the authentication framework of this paper can provide the non-repudiation service and it doesn't reduce the effectiveness.

VI. CONCLUSIONS

In the world wide, the URC robot is actively studied. The URC security system is certainly needed in order to activate the IT based functionality service robot. In URC, by providing a function or the difficult service through a network to include in one piece robot an availability was improved. This research is gone through and it is expected as the in-depth research progress result about the security at the URC network robot environment and authentication problem in the future previously to prevent the security problem of a commercialization and the generalized network robot. The turning point when Korea can lead the network-based robot industry based on this with domestic and foreign will be able to become.

ACKNOWLEDGMENT

This paper has been supported by the 2008 Hannam University Research Fund.(2008A186)

REFERENCES

[1] Aekyung Moon, Minyoung Kim, Hyoungsun Kim, Kang-Woo Lee, Hyun Kim, "Development of CAMUS based Context-Awareness for Pervasive Home Environments", International Journal of Smart Home Vol 1, No. 1, January, 2007
[2] Brooks, R.A., "A robust layered control system for a mobile robot", IEEE Journal on Robotics and Automation, Vol.2, No.1, 1986
[3] H. Kim, Y. Cho, and S. Oh, "CAMUS: A Middleware Supporting Context-Ware Services for Network-Based Robots", IEEE Workshop on Advanced Robotics and Social Impacts, 2005
[4] Cho, Y.J. and Oh, S.R. "Fusion of IT and RT: URC(Ubiquitous Robotic Companion) program", JOURNAL ROBOTICS SOCIETY OF JAPAN, vol.23, no.5, pp22-25, 2005
[5] http://www.tta.or.kr
[6] http://www.rupi.or.kr
[7] Jan De Clercq, "single Sign-On Architectures" Proceedings of the International Conference on Infrastructure Security, pp. 40-58, 2002

Cheol-Joo Chae
Member KIMICS. Received B.S degree in Computer Engineering, Hannam University in 2004. Received M.S degree in Computer Engineering, Hannam University in 2006. Since 2006, he has been a Ph.D. Student in Computer Network Lab, Hannam University. The research areas of interest include Computer Security, Network Security, Ubiquitous Security.

Han-Jin Cho
Member KIMICS. Received Ph.D. degree in Hannam University, in 2002. In 2002, he joined the school of computer science, information and standard, Far East University, Korea. The research areas of interest include information security, network security, wireless communication.

Jae-Kwang Lee
Member KIMICS. Received Ph.D. degree in Kwang Woon University, in 1993. In 1993, he joined the department of Computer Engineering, Hannam University, Korea. His research interest is in the area of Network Security that includes Wireless network, Cryptograph, PKI, WPKI and Ubiquitous security.