PANDA[1]와 VNC에 기반한 U-Kiosk 구현

석현철○ 박기웅 임상석 박규호
한국과학기술원 전자전산학과 컴퓨터공학연구실
{hcseok○, woongbak, sslim}@core.kaist.ac.kr, kpark@ee.kaist.ac.kr

Implementation of U-Kiosk based on PANDA and VNC

Hyunchul Seok○ Ki-Woong Park, Sang Seok Lim, Kyu Ho Park
Computer Engineering Research Laboratory
Department of Electrical Engineering and Computer Science
Korea Advanced Institute of Science and Technology

요 약

휴대용 단말기의 보급과 인터넷 및 무선 네트워크의 발달로 사용자들이 사용하는 개별 장치들이 보편화되어 있으며, 이들을 서로 유기적으로 엮은 서비스가 등장하고 있다. 본 논문에서는 이러한 서비스의 한 종류로 U-Kiosk의 개념을 소개한다. U-Kiosk는 Kiosk 단말장치나 공용 PC를 사용자 개인의 PC처럼 사용할 수 있도록 하는 서비스로서 유무선 네트워크를 이용하여 개인의 모바일 장치나 개인 PC로 접속을 하여 이들의 리소스를 직접 제어할 수 있는 기능을 제공한다. 이것을 실현하기 위한 방안으로 본 논문에서는 공용 PC에서 개인 PC의 바탕화면 설정을 포함해 모든 자원을 직접 사용할 수 있도록 하는 부분을 구현하고 설명을 하였으며, 인증 과정에서 사용자의 개입을 최소한으로 줄이는 방법에 대해서 소개한다. 이를 위하여 초소형 보안 단말기인 PANDA를 사용하였으며, Zigbee 통신을 사용하여 사용자의 위치정보를 파악하여 자동으로 인증을 하도록 하는 Transient Authentication의 개념을 도입하였다. 두 컴퓨터 간의 원격 접속을 위해서는 VNC를 이용하여 구현하였으며, 사용자가 공용 PC로부터 일정 거리 안에 있을 경우, 자동으로 원격 접속이 이루어지고, 공용 PC로부터 멀어질 경우 자동으로 접속이 종료되도록 구현하였다. 이를 기반으로 제안하는 U-Kiosk의 개념에 맞는 테스트 베드를 구축 하였다. 이는 UFC Project[2]의 일부로서 차후 완벽한 인증 인프라를 구축하여 보다 안정적이고 사용하기 편리한 U-Kiosk의 구현에 초석이 될 것이다.

1. 서 론

컴퓨팅 기술의 발달로 휴대용 모바일 장치들이 보편화됨에 따라, 집에서 PC를 통해 작업을 하던 단계를 지나 어디에서나 개인 장치를 가지고 업무를 보거나 간단한 이메일을 확인하는 작업을 수행할 수 있다. 기존 컴퓨팅 환경에서 유비쿼터스 컴퓨팅 환경으로 진화함에 따라, 각 장치들은 자신들이 원래 가진 기능만을 제공하던 단계를 지나 발달된 네트워킹을 통하여 서로 동적으로 관련을 맺고 보완적으로 일을 수행해 나가고 있다. 일반적으로 모바일 장치들은 그 크기와 무게의 제한으로 인해 상대적으로 제한된 입출력 장치를 가지거나, 데이터를 저장하는 공간에 한계를 지니는 것이 특징이다. 이러한 단점을 보완하기 위해서 a Collaborative Web Browsing[9] 등과 같은 연구가 수행이 되었다.

이 연구의 경우에는 여러 휴대용 단말 장치를 모아서 공용으로 서비스를 받는 방법에 관해서 연구되었는데, 개인 각자에 맞는 개별 서비스를 제공하는 측면에는 한계를 지니는 단점을 가지고 있다. 이를 개선하여 사용하는 방안으로 개인 장치간의 연결, 또는 공용 장치와 개인 장치간의 연결을 통한 서비스를 생각해 볼 수 있다. 예를 들어, 개인 모바일 장치를 다른 컴퓨터를 통해서 직접 제어가 가능하다면, PC의 익숙한 환경과 자신의 개인 장치에서의 작업 수행이란 측면에서 사용자의 편리성을 더욱 도모할 수 있을 것이다. PDA의 경우에는 입력 장치에 제한을 가지고 있는 반면, 키보드와 마우스 등을 갖춘 일반적인 PC를 통해서 개인의 모바일 장치의 자원을 사용하는 경우, 간단한 문서 작업을 하는 동안에는 익숙한 PC 환경에서 작업 수행이 가능하며, 작성한 자료는 모두 PDA에 존재하게 된다. 후에 PC에서 작업을 마치면, PDA에서 계속해서 같은 문서 작업을 이어서 수행하거나, 이동 후 다른 PC를 통해서 연속적으로 작업을 처리할 수 있는 기능을 제공을 할 수가 있게 된다.

본 논문에서는 이러한 기능을 제공해 줄 수 있는 방법으로 U-Kiosk를 소개한다. 네트워크를 통한 개인의 장비에 직접 접속하는 것을 포함하고 있으므로, 이를 구현하기 위해서는 우선 자신의 장비에 접속을 안전하게 하기 위한 선결과제로 강력한 인증을 통한 보안이 구축이 되어야 할 것이며, 반복적인 인증 절차에서 사용자의 개입을 줄이는 것도 중요한 일이 될 것이다.

* 본 연구보고서는 정보통신연구진흥원에서 지원하고 있는 차세대PC연구사업의 연구 결과입니다.

1) Personal Authentication Network Device Architecture. 초소형 보안 단말기. Core Lab

2) A Ubiquitous Fashionable Computer project

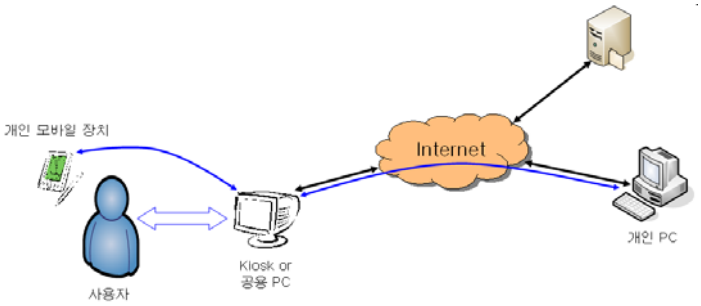

그림 1: U-Kiosk 개념 구조

2. U-Kiosk의 개념

우리가 제안하는 U-Kiosk는 Kiosk 장치와 같이 각 건물에 배치된 단말 장치나 정보 검색용 PC 등을 사용하여 개인의 PC나 모바일 장치에 접속하여 마치 자신의 PC처럼 사용하는 것을 가능하게 하는 것을 의미한다. 유비쿼터스 컴퓨팅 환경에 걸맞게 대부분의 주요 건물에서는 그 건물을 소개하는 Kiosk 장치나 네트워크에 연결된 PC 등이 구비된 경우가 대부분이다. 이러한 장비들을 통하여 개인 장치들에 접속을 하여 개인 장치들을 직접 사용하도록 하는 것이다. 그림 1은 본 논문에서 제안하는 U-Kiosk의 개념을 나타낸다. 사용자가 단말기 (Kiosk, 공용 PC)로 접근할 경우, 인증을 거쳐서 사용자의 개인 장치로 연결을 시도한다. 단말 장치에 해당하는 Kiosk나 공용 PC는 LAN이나 블루투스, Zigbee 등의 네트워크에 연결된 것을 전제로 한다. 따라서 단말기가 인터넷과 연결이 된 경우나 wireless 통신이 가능한 경우, LAN을 통하여 사용자 개인의 PC로 연결을 하여 마치 자신의 개인 PC인 것처럼 Kiosk 장치를 사용하거나, wireless 통신을 통하여 사용자가 지니고 있는 모바일 장치로 연결을 하여 공용 PC를 자신의 개인 모바일 장치로 사용을 하는 것이다.

인증의 경우에는 보안을 위하여 반드시 필요하지만, 사용자에게 부담을 가중시킬 수 있으므로, 부담을 최소화하고 보안 수준을 높일 수 있도록 Transient Authentication[6]을 가능하게 할 수 있는 인증용 장치를 몸에 지니는 것을 전제로 한다. 이러한 구조에서 사용자는 인증을 하는 과정에서 자신의 개입을 최소화할 수 있으며, 네트워크를 통해 개인 PC나 개인 모바일 장치로 연결을 할 수 있다.

U-Kiosk를 구현하기 위해서는 3가지 중요한 요구 사항이 있다.

1) 사용자를 인증할 수 있는 보안 인프라가 구축이 되어야 한다. 이것을 통하여 악의의 사용자가 Kiosk나 공용 PC를 사용하는 것을 막고, 사용자 개인의 장비에 불특정 사용자가 접속하는 것을 막을 수 있어야 한다.
2) 단말 장치를 통해서 접속하는 시간이 짧아야 하며, 접속 시에 사용자의 개입이 적어야 한다. 유비쿼터스 환경에서는 자리를 이동하며 수시로 접속을 하는 경우가 많다. 따라서 매번 오랜 시간을 기다리거나 사용자가 접속을 위해서 많은 일을 하게 하여서는 안된다.
3) 작업의 연속성이 보장되어야 한다. 작업을 하던 환경이 저장이 되어, 다시 접속할 시에 접속을 종료하던 시점부터 시작할 수 있어야 한다. 이는 개인 PC를 항상 소지하고 다니는 것과 같은 기능을 제공할 것이다.

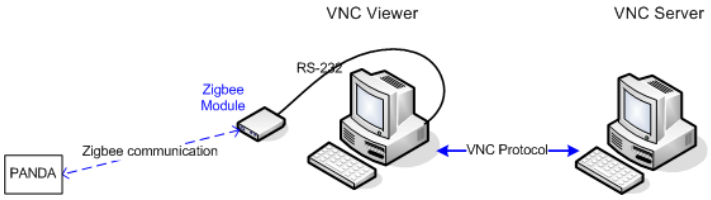

그림 2: Implementation 전체 구성도

위 3가지 요구사항을 만족한 구조로 구현을 할 경우 사용자에게 안정성과 기능성을 제공해 줄 수 있게 된다.

3. Implementation

본 논문에서는 앞에서 소개한 U-Kiosk의 구조에서 사용자가 공용 PC를 통해서 사용자 개인 PC에서 작업을 끊임없이 수행하는 것을 가능하도록 하고, 사용자의 개입을 최소한으로 줄이도록 하는 일에 중심을 두었다. U-Kiosk가 가져야 할 3가지 특징을 만족하기 위해서 사용한 하드웨어 및 소프트웨어를 설명하면 다음과 같다.

U-Kiosk를 구현하기 위해서 중요한 것은, 먼저 개인 사용자가 자신의 신분을 인증 받을 수 있어야 한다는 것이다. 우리는 이 장치로 PANDA[1]를 사용한다. 이 장치는 Kiosk에 장착된 Zigbee Sensor Module과 통신을 통해서 인증을 수행하는 기능을 가지고 있다.

공용 PC에서 사용자 개인 PC로의 원격 접속기능을 구현하기 위해서 VNC[3]를 사용하였다. Kiosk로 사용되는 장치는 VNC Viewer가 설치된 공용 PC를 사용하였으며, 개인 PC에는 VNC Server를 설치하여 Kiosk로부터 접속이 가능하도록 구성한다.

Zigbee Sensor Module과 Kiosk에 해당하는 공용 PC는 RS-232를 통해 연결을 하였다. 이것을 통하여 VNC Viewer는 Zigbee Sensor Module에서 보내는 명령을 받아서 처리하도록 하였다. 이런 명령에는 VNC Server로 접속을 맺거나 종료시키는 명령들로 구성이 된다. 그림 2는 구성할 U-Kiosk의 전체적인 구성을 보여준다.

3.1 PANDA [1]

유비쿼터스 컴퓨팅 환경에서는 수많은 장치들 간 유기적인 통신이 이루어진다. 이 과정에서 사용자가 알지

못하는 장치들과 통신이 이루어진다던가, 공격자에 의한 정보의 유출과 같은 피해를 당할 수도 있다. 따라서 모바일 장치들은 사용자가 정의한 장치들 간의 안전한 통신을 위해서 장치들 간의 인증을 하도록 하는 보안 인프라를 구축하는 것이 중요하다.

사용자의 인증을 위한 방법으로 패스워드나 토큰을 이용하거나, 스마트카드나 passive RFID 등을 사용하는 방식을 이용할 수 있다. 하지만 패스워드나 토큰의 경우 사용자의 개입이 항상 필요하게 되어, 수많은 인증 절차에 대해서 사용자의 부담을 가중시켜 사용 편리성을 떨어뜨린다. 게다가 스마트카드나 passive RFID 경우에도 기본적으로 사용성에 단점이 있는데, 사용자가 항상 장치로부터 제거해서 로그아웃을 해야 한다고 기억하고 있어야 하며, 실제로 제거해서 로그아웃을 해야만 한다는 것이다.[10]

사용자의 편리성 측면에서는 인증을 담당하는 장치가 wireless 통신이 가능하도록 하는 것은 보다 편리한 인증 방식을 제공할 수 있다. 단순히 사용자가 몸에 지닌 상태로 가까이 다가갈 경우 인증 절차가 실행이 되도록 수행할 수 있는 것이다. 예를 들어, Ensure Technologies 회사의 XyLoc system[4]은 블루투스를 이용한 개인 PC의 인증을 제공하는 모바일 모듈로서 사용자의 개입 없이 자동으로 인증을 통해 PC의 사용 권한을 줄 수 있는 기능을 제공한다.

따라서, 좀 더 사용자의 편의를 제공해 줄 수 있는 보안 장치를 개발하기 위하여 the Ubiquitous fashionable computer (UFC) project의 2차년도에 기존의 인증 방식을 보완하여 새로운 인증 장치인 PANDA (Personal Authentication Network Device Architecture)를 개발 하였다.

우리가 PANDA라고 명명한 이 장치의 경우 다음 3가지의 요구를 만족시키도록 개발이 되었다.

1) PKI 기반의 인증 protocol을 지원한다.
2) 무선 통신 모듈의 신호 범위내의 장치들 간의 ad-hoc 통신 채널을 형성할 수 있도록 한다.
3) location based authentication 능력을 제공할 수 있다.

따라서, PANDA를 가진 사용자가 인증 장치로 접근함에 따라 사용자의 부가적인 개입이 없이 인증을 할 수가 있으며, 사용자의 위치 정보를 바탕으로, 이동 경로를 예측하여 미리 인증을 준비함으로서 인증시간을 줄일 수 있는 서비스도 제공할 수 있게 된다.

하지만 이번 논문에서는 PANDA를 사용하여, 사용자의 VNC Server로 접속을 할 수 있는 방법을 소개하지만, PKI에 근거한 인증을 추가하지는 않았다. 거리에 따른 접근 정도를 확인하여 어느 정도 거리에 들어올 경우 PANDA 장치에 기록된 개인 PC 정보를 이용하여 자동적으로 로그인을 가능하도록 구현하였다.

3.2 Zigbee communication

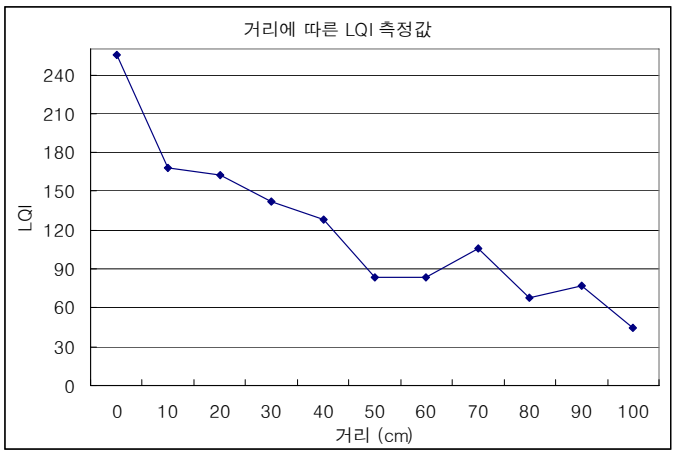

그림 3: 거리에 따른 LQI 측정값 (거리 cm)

사용자가 Kiosk나 공용 PC로의 접근성은 PANDA 모듈과 Zigbee Sensor 모듈 사이의 Zigbee communication을 형성하여 판단하도록 하였다. Zigbee 통신을 위해서 Chipcon 사의 CC2420 chip[5]을 사용한다. 그림 2에서 VNC Viewer에 연결된 Zigbee 모듈은 CC2420DB Development Board를 사용하여 연결하였으며, 사용자의 인증용 장치인 PANDA에는 CC2420s chip을 사용하여 서로 간에 Zigbee 통신이 가능하도록 구성하였다.

PANDA는 사용자 인증과 권한 설정 기능을 제공하여 Transient Authentication을 구현하기 위한 핵심 장치에 해당하지만, 본 논문에서는 단순히 공용 PC로의 접근 제어를 위한 장치로 사용하며, 사용자의 개인 PC (VNC Server)로 접근 가능한 IP 정보와 password 정보를 저장하여, Zigbee Sensor 모듈로부터 요청을 받을 경우, 해당 정보를 응답하도록 구성하였다.

Zigbee Sensor 모듈의 경우, PANDA의 접근을 확인하고, 접근할 사용자 개인 PC의 정보를 PANDA로부터 얻어와 공용 PC (VNC Viewer)로 그 정보를 전달하는 역할을 수행한다.

PANDA의 접근을 확인하기 위해서, 본 논문에서는 LQI (Link Quality Indicator) 값을 측정하여서 사용하였다. LQI의 값은 두 장치간의 거리가 멀어짐에 따라서 값이 떨어지게 된다. 어느 정도의 값을 기준으로 사용자의 접근 유무를 파악할 것인지를 결정하기 위해 거리에 따른 LQI 값을 측정하여, 그림 3에 나타내었다. 이 측정값은 각 거리에서 LQI의 값을 20번 측정하여 평균한 값을 그래프로 나타낸 것이다. 그래프에는 70cm에서 오히려 높은 수치를 보이는데, 여기에 영향을 받지 않도록, 이보다 높은 LQI 값을 결정한다. 따라서, 사용자의 존재유무는 범위 40 cm안에 들어와 있는 것으로 LQI 값이 120 이상에 대해서 처리하도록 하였다.

Zigbee Sensor 모듈에서 LQI Request Message를 주기적으로 보내도록 하였다. LQI Request Message를 보내는 시간 간격은, PANDA를 장비한 사용자의 접근을 파악하는 시간과 밀접한 연관이 있다. 따라서 가급적 주

기를 줄여서 polling을 자주하는 것이 빠른 시간에 사용자의 유무를 파악할 수 있다. 실험에서는 그 값은 0.3초로 설정을 하였다. 게다가 LQI 측정에서 같은 위치에서도 LQI의 값의 변동이 생기는 것을 확인했는데, 정의한 범의 내에 PANDA의 존재의 유무는 3번 정도의 연속적인 결과에 대해서 판단을 하여 순간적인 LQI 값의 변동에 대해서 잘못된 동작을 하지 않도록 한다.

3.3 VNC (Virtual Network Computing)

VNC는 RFB (Remote Frame Buffer) protocol을 사용하는 desktop sharing system이다.[2] VNC Server와 VNC Viewer (client)로 구성이 되며, VNC Client는 키보드와 마우스의 입력을 VNC Server로 전달하여, VNC Server의 제어를 가능하게 한다. VNC Server의 경우에는 자신의 디스플레이 화면의 변화를 맺어진 채널을 통해 VNC Viewer로 전송하여, VNC Viewer의 화면으로 보여주게 된다.

VNC는 open source로서 제공이 되고 있으며, platform에 독립적으로 동작을 하기 때문에 개발자는 자신의 환경에 맞게 최적화 할 수 있는 장점이 있다. 게다가 VNC Server의 화면에서 변화가 있는 부분만을 전송을 함으로서 네트워크의 트래픽을 감소시킬 수 있으며, 접속 후 VNC Server의 제어를 가져오는 시간이 짧아서, 원격 제어를 위해 접속을 할 경우 사용자가 편리하게 사용할 수 있다.

게다가 VNC의 채널을 종료한 후에, 다시 접속할 경우에도, VNC Server인 개인 PC의 작업 상태가 그대로 보여지게 되므로, 작업의 연속성이 보장된다. 따라서 이번 논문에서 원격 접속을 위한 솔루션으로 사용하였다.

3.4 VNC Viewer

VNC Viewer의 경우 VNC Server로 연결 후에 사용자의 개인 컴퓨팅 화면을 그대로 보여준다. 그리고 VNC Viewer에서의 키보드와 마우스의 입력을 전달하여, VNC Server의 컴퓨터에서 작업을 수행하도록 한다. 이를 위해 connection을 맺을 때, VNC Server의 주소 정보와 접속 password를 얻어야 한다. 이는 사용자가 직접 개입을 하는 부분이므로, 이를 수정하여 PANDA를 가진 사용자가 Zigbee Sensor 모듈에 다가감에 따라 자동으로 인증을 거쳐 VNC Server로 접속이 되도록 기능을 수정하였다.

구현은 VNC Viewer가 Serial port로부터 들어오는 Zigbee Sensor 모듈의 메시지를 받아서, 메시지 type에 맞는 동작을 수행하도록 구현하는 것이다. VNC Viewer의 경우에는 VNC Server로의 접속 채널을 맺는 것과 맺은 채널을 종료하는 두 가지 일을 하게 되므로 Zigbee Sensor 모듈에서 보내는 명령도 채널 형성과 채널 종료 명령으로 구성을 하였다. PANDA가 공용 PC 앞으로 왔을 때, Zigbee Sensor 모듈이 보낸 connection 명령으로 VNC Viewer는 VNC Server로 자동적으로 채널을 맺도록 수정하였다. 반대로 멀어질 경우 VNC Viewer는 disconnection 명령을 받게 되고, VNC Server와의 채널을 자동으로 종료하여 로그아웃이 되도록 수정하였다.

표 1: 각 장치에서 주고받는 메시지 형식

```
/* Command Define */
#define ZC_CMD_ZDO_MGMT_LQI_REQ              0x0A0F
#define ZC_CMD_ZDO_MGMT_LQI_RES              0x1A0F
#define ZC_CMD_ZDO_MGMT_VNC_CONN             0x0A1F
#define ZC_CMD_ZDO_MGMT_VNC_DISCONN          0x1A1F
#define ZC_CMD_ZDO_MGMT_INFO_REQ             0x0A2F
#define ZC_CMD_ZDO_MGMT_INFO_RES             0x1A2F

/* Header */
struct zc_frame_hdr {
        uint8_t     zh_sop;
        uint16_t    zh_cmd;
        uint16_t    zh_len;
        uint8_t     zh_fcs;
};

/* Message = Header + Payload (data) */
```

3.5 Protocol & Message

PANDA와 Zigbee Sensor 모듈 간, 그리고 Zigbee Sensor 모듈과 VNC Viewer 간의 통신 메시지의 형식을 정의 하고 주고받는 메시지의 순서를 정의하는 것이 필요하다.

구성한 U-Kiosk 모델에서 필요한 명령의 종류를 확인하면, 주기적으로 LQI를 판단하기 위해서 Zigbee Sensor 모듈에서 PANDA로 보내는 LQI Req 메시지와 응답인 LQI Res 메시지가 필요하다. 한편 개별 사용자의 VNC Server의 주소 정보와 password 정보를 얻어오기 위해서 이를 요구하는 메시지가 필요하며, 이를 INFO Req라고 정의하였다. 그리고 이 메시지의 응답으로 INFO Res를 정의한다. 마지막으로 VNC Viewer에 VNC Server로의 채널 연결과 채널 종료를 명령하기 위해서 VNC_CONN 명령과 VNC_DISCONN 명령으로 구성을 한다. 이상으로 총 6개의 명령을 정의를 하였으며, 전체적인 명령의 구성은 표 1과 같다.

메시지는 Header와 Payload로 구성을 하였으며, Header는 SOP와 명령의 종류, Payload의 길이, checksome으로 구성을 한다. Checksome은 명령의 종류와 Payload의 길이를 사용하여 계산하도록 하였다.

VNC Viewer의 자동 로그인 과정은 다음과 같다. Zigbee 모듈에서 LQI Req를 이용하여서 주기적으로 PANDA의 LQI 값을 확인을 한다. LQI 값이 120을 초과할 경우, PANDA로 VNC Server의 정보를 요구한다. 응답 메시지는 VNC Server의 주소 정보와 password 정보를 가진다. 이 응답 메세지로 받은 주소 정보와 password 정보를 VNC_CONN 메시지에 담아서 serial을 통해 VNC Viewer로 전달한다. VNC Viewer에서는 이 값

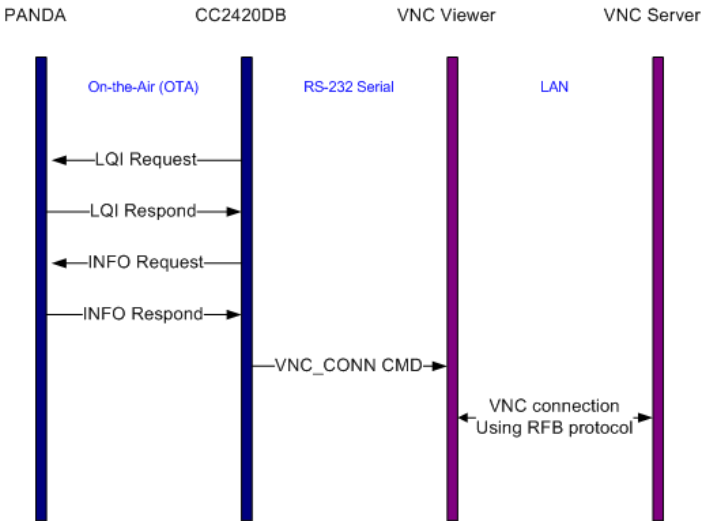

그림 4: U-Kiosk: connection 시 메시지 흐름

을 가지고, VNC Server로 자동으로 접속을 시도하여 채널을 형성한다. 이러한 과정을 그림 4에 나타내었다.

VNC Connection이 맺어지고 사용자가 공용 PC (VNC Viewer)에서 작업을 하는 동안에도 Zigbee Sensor 모듈에서는 계속적으로 LQI 값을 모니터링한다. 사용자가 공용 PC 앞에 있는 동안에는 LQI 값이 120 보다 큰 값이 측정이 되어 VNC Connection이 유지가 되지만, 사용자가 자리를 벗어나는 경우에, LQI의 값이 떨어지게 된다. 이 경우 Zigbee Sensor 모듈에서는 VNC Viewer로 채널을 종료하도록 VNC_DISCONN 명령을 내린다. 따라서 자리를 벗어나는 것으로 자동적으로 세션이 닫히도록 구성을 한다. 이 과정은 그림 5에서 확인할 수 있다.

4. Evaluation

사용자가 Kiosk나 공용 PC 앞으로 다가 섰을 때, 개인 PC의 화면을 확인하고 컨트롤 할 수 있게 되는데 까지 걸리는 시간을 최소화 할 수 있어야 한다. U-Kiosk 서비스가 사용자에게 편리함을 제공하기 위해서는, 사용자가 설정이 될 때까지 기다리는 시간에서 지루함을 느끼지 않아야 한다. 여기서는 이 논문에서 제안한 방법과

표 2: 원격 접속에 걸리는 시간

데스크 탑 PC, 100Mbps 랜, 동일한 네트웍 대역			
	U-Kiosk (Connection + Log-on)	원격 데스크 탑	
		Connection	Log-on
시간	1.83 초	0.98초	0.76 초

노트북, 11Mbps 무선랜, 다른 네트웍 대역			
	U-Kiosk (Connection + Log-on)	원격 데스크 탑	
		Connection	Log-on
시간	2.65 초	1.35 초	1.41 초

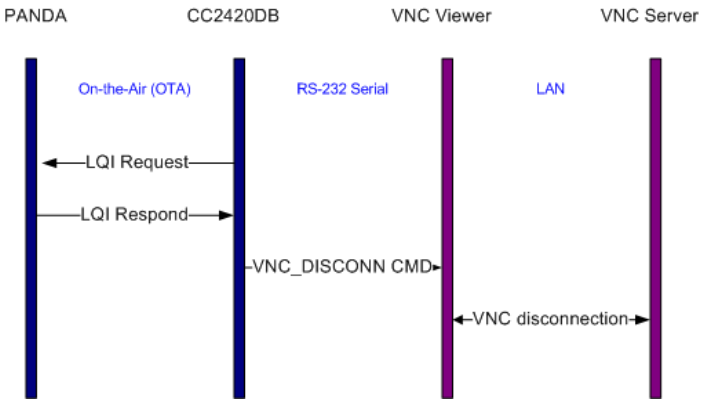

그림 5: U-Kiosk: disconnection 시 메시지 흐름

윈도우 시스템에서 제공하고 있는 원격 데스크 탑과의 원격 접속의 시간을 측정해 보았다. 그 결과를 표 2에 정리하였다.

VNC와 원격 데스크 탑은 공통적으로 접속하려는 개인 PC로 채널을 맺고 password를 이용하여 로그인을 하는 과정으로 이루어진다. VNC를 이용한 U-Kiosk에서는 자동으로 로그인 기능을 추가하면서 두 과정이 한번에 수행이 되고, 이 두 과정이 포함된 시간을 측정하였다. 따라서 이를 비교하기 위해서 원격 데스크 탑에서도 접속을 맺는 데 걸리는 시간과, Log-on 하는데 걸리는 시간으로 두 가지를 측정하여 기록하였다.

결과를 보면 100Mbps 랜에 같은 네트워크를 물린 경우에서는 원격 데스크 탑이 조금 더 빠른 결과를 보이지만, 네트워크 상황이 나빠질 경우에는, 11Mbps의 다른 네트워크에서의 결과와 같이, VNC를 이용한 것이 조금 더 이득을 보는 것을 확인할 수 있다.

구현된 U-Kiosk의 경우에 사용자의 접근과 정보 확인에 있어 1초 가량의 시간이 걸린다. 하지만 원격 데스크 탑의 경우에는 사용자가 직접 IP와 password를 입력하므로 이보다 긴 시간이 필요하다.

5. Future Work

Wireless zigbee 통신이 가능하도록 설계된 PANDA의 경우 기본적으로 강력한 인증을 통한 보안 기능을 제공하기 위한 장치이다. PANDA와 Zigbee Sensor 모듈간의 보안기능을 제공함으로서 안정적으로 공용 PC를 통해서 자신의 개인 PC나 모바일 장치로 접속을 할 수 있게 된다. 게다가 사용자가 따로 인증을 받기 위해서 부가적인 일을 하지 않아도 자동적으로 인증 절차가 수행이 되도록 하는 기능을 제공한다. 이는 Transient Authentication[6]을 기반으로 하여 사용자의 편리성을 도모할 수 있는 장점을 가진다.

본 논문에서는 보안적인 부분은 사용하지 않은 채, PANDA와 Zigbee Sensor 모듈 간의 거리에 초점을 두었다. 따라서 PANDA와 Zigbee Sensor 사이의 인증 시스템을 추가하여야 한다. 이를 위해서 Delegation

Server를 둔 인증 인프라[8]를 구축해 두었으며, 구현단계에 있다. 게다가 이를 도입할 경우 사용자의 인증에 필요한 시간이 0.343초로 줄어들어[8] 사용자의 대기 시간도 더욱 줄어들게 된다.

6. Conclusion

본 논문에서는 U-Kiosk의 개념을 소개하고, 이를 구현하는 한 가지 방법을 제시하였다. 인증을 위한 PANDA 장치와 VNC Open-source를 사용하여 공용 PC로부터 개인 PC로 접속이 가능한 구조이다. PANDA와 Zigbee Sensor 모듈로 사용자의 위치를 확인하여 자동적으로 개인 PC로 연결이 되도록 하였다. 개인 PC로 채널 연결 시 필요한 정보는 PANDA에 저장시켜 Zigbee Sensor 모듈과의 통신을 통하여 얻어와 사용한다.

사용자의 접근에 따라서 공용 PC로 부터 자신의 개인 PC를 사용할 수 있게 되는데 까지 걸리는 시간은 100Mbps에서 2.73 초 (0.9 초 + 1.83 초) 정도로서 충분히 사용자가 부담을 느끼지 않을 시간이 된다. 접속 후 몇 가지의 작업을 하고, 재접속을 하여 확인한 결과 작업의 연속성이 제공되는 것을 확인할 수 있다. 이것은 과거 일상생활과 컴퓨팅 활동이 분리되었던 것과는 달리, 오늘날 일상생활과 밀접한 관련을 맺고 있는 유비쿼터스 컴퓨팅 환경에서 자신의 업무나 작업을 어디에서나 연속적으로 할 수 있는 환경을 만들어 줄 수 있다는 점에서 의의를 가진다.

References

[1] Ki-Woong Park, Sang Seok Lim, Young-Woo Park, Kyu Ho Park, "PANDA: An Interoperable Mobile Security Card for Ubiquitous Services."

[2] http://en.wikipedia/org/wiki/Vnc

[3] Tristan Richardson, Quentin Stafford-Fraser, Kenneth R. Wood and Andy Hopper, "Virtual Network Computing." IEEE Internet Computing Volume 2, Number 1 January/February 1998

[4] Ensure Technologies, http://www.ensuretech.com/.

[5] Chipcon Products, http://www.chipcon.com/.

[6] Brian D. Noble, Mark D. Corner, "The Case for Transient Authentication," the 10th ACM SIGOPS European Workshop, Saint-Emilion, France, September, 2002.

[7] Mark D. Corner, "Transient Authentication for Mobile Devices," Doctoral Dissertation, University of Michigan.

[8] Ki-Woong Park, Sang-Seok Lim, Kyu-Ho Park, "A New PKI based Single Sign-On Protocol for a Diminutive Security Device, PANDA, in a Ubiquitous Security Environment," Core Lab. Technical report.

[9] Takuya Maekawa, Takahiro Hara, Shojiro Nishio, "A Collaborative Web Browsing System for Multiple Mobile Users," Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)

[10] Mark D. Corner, "Transient Authentication for Mobile Devices", A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the University of Michigan, 2003