센서간의 인증을 이용한 홈 네트워크 서비스 구현

*김성두, 이기영, 설정환
인천대학교 정보통신공학과
e-mail : sungdu0726@naver.com, kylee@incheon.ac.kr, aknari@naver.com

HomeNetwork service design using sensor's authentication

*Seong-Du Kim, Ki-Young Lee, Jeong-Hwan Seol
School of Information and Telecommunication Engineering
University of Incheon

요 약

본 논문에서는 유비쿼터스 사회로의 출발점인 '홈 네트워크'를 구축하는데 있어서 가장 기본이 되는 홈 서버와 센서간의 인증을 구현하는데 목적을 두었다. 홈 서버와 센서간에 통신을 할 때 해쉬함수 중 MD5를 통해 그룹키를 생성하고 그룹키를 조도센서에 적용하여 서버와 센서간의 인증이 이뤄지는 것을 확인하였다.

I. 서론

유비쿼터스(Ubiquitous) 컴퓨팅 환경은 사용자가 언제 어디서나 컴퓨터를 사용하고 있다는 의식없이 컴퓨터를 이용할 수 있도록 네트워크를 통해 상호 연결된 수 많은 컴퓨터를 사용자가 원하는 대로 쉽게 이용할 수 있는 컴퓨팅 환경을 말하며 더 나아가서는 사용자가 원하는 컴퓨팅을 컴퓨터가 스스로 알아서 제공하는 스마트 환경을 지향한다. 이러한 유비쿼터스 사회로의 출발점을 '홈 네트워크(Home Network)'로 생각 수 있다. 홈 네크워크를 통해 개인의 Life Style을 풍요롭게 하는 다양한 홈 디지털서비스를 누구나 원하는 기기로 시간과 장소에 구애 받지 낳고 제공받을 수 있게 된다. 이러한 풍요로움을 제공하는 홈 네트워크를 구축하기 위해서 고려해야 할 사항이 몇 가지 있다.

본 논문에서는 홈 네트워크 구축시 고려해야 할 사항중 홈 서버와 각각의 센서들 사이의 인증방법을 제안하고 제안된 방법을 구현을 통해서 서버와 센서들간의 인증이 되는 것을 보여주겠다.

본 논문은 산업자원부,한국산업기술평가원 지정 인천 대학교멀티미디어 연구센터의 지원에 의한 것입니다.

II. 본론

2. 홈 서버와(Home server)와 센서간의 인증

유비쿼터스 컴퓨팅 환경은 편리한 생활을 추구할 수 있도록 하는 순 기능이 있다. 그러나 컴퓨터, 센서(총칭 디바이스)들의 악의적인 서비스 거부 공격을 받았을 경우에는 우리의 일상생활에 치명적인 악영향을 미치는 역기능을 초래할 수 있다. 홈 네트워크 구성을 간략하게 생각해보면 각 가정(Home)마다 서버를 갖게 되고 센서 또는 센서가 부착된 각각의 디바이스들의 집합으로 생각할 수 있다. 홈 네트워크 환경에서 다양한 디바이스들로부터 안전하게 서비스를 받기 위해 가

장 기본적이면서도 필수적인 요소가 서버와 센서들 간의 인증이다. 인증 하는 방법으로는 각 가정(Home)을 같은 그룹범위로 생각하고 각 가정(Home)마다 고유한 그룹키를 사용하여 통신 하도록 한다. 즉, 같은 그룹안에서의 서버와 센서들은 같은 그룹키를 통해 통신을 하게 된다. 즉, 그룹키가 다르다면 통신자체가 불가능하게 되는 것이다. 그룹키를 이용한 인증방법을 통해 디바이스의 오작동 및 악의적인 공격에 대처 할 수 있을 것이다.

Ⅲ. 구현

홈 네트워크가 무선네트워크 환경에서 이뤄지기 때문에 보안에 매우 취약하다. 그래서 단순한 그룹키를 사용하는 것이 아니라 해쉬함수 중 MD5라는 알고리즘을 사용해서 그룹키를 생성하였다.

인증이 이루어졌다는 것을 보여주기 위해서 조도감지 센서를 이용했다. 그룹키를 사용하지 않았을 경우 모든 센서들이 감지한 데이터를 서버가 수신할 수 있다. 그러나 그룹키를 사용했을 경우 같은 그룹키를 가진 서버와 센서들만이 통신을 할 수 있다.

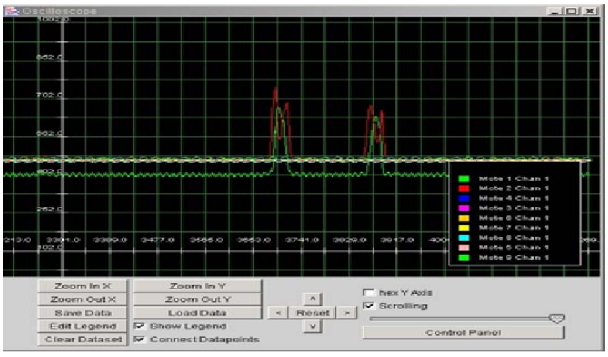

그림 1. 그룹키가 사용되지 않은 경우

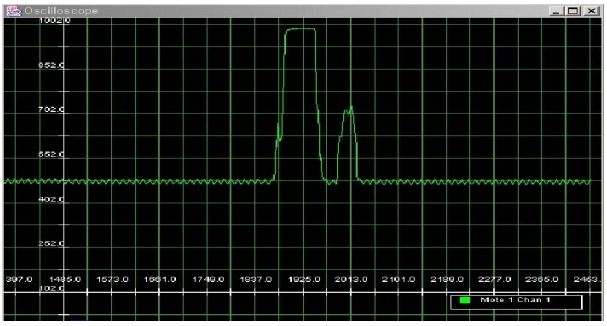

그림 2. 그룹키가 사용 된 경우

Ⅳ. 결론 및 향후 연구 방향

실험 결과를 통해 서버와 센서간의 인증이 이뤄지는 것을 확인 할 수 있었다. 본 논문에서는 홈 네트워크가 이루어지는 무선네트워크 환경에서 일어날 수 있는 여러 가지 악의적인 공격을 배제하고 가장 기본적인 인증방법을 구현하는데 목적을 두었다. 그러나 악의적인 공격을 통해 그룹키를 알아 낼 수 있다. 그래서 안전한 홈네트워크 환경을 위해 앞으로는 센서에서 작동 할 수 있는 암호알고리즘을 적용하는 연구도 계속 진행 되어야 할 것이다.

참고문헌

[1] 이덕규 외, “유비쿼터스 컴퓨팅 환경에서 속성인증서를 이용한 단일/멀티 도메인 인증”, 정보과학회 논문지, 제 32권 제 3호

[2] 한국전산원, “유비쿼터스 컴퓨팅환경에서 보안 및 인증 서비스 방향 연구”, 보안/인증기술 이슈 04-인증-01-2004.10

[3] 박용범, “ 홈네트워크 인증 현황”, TTA Journal No.99

[4] 강명희 외, “유비쿼터스 컴퓨팅 환경을 위한 익명성을 보장하는 사용자 인증 및 접근제어 모델”, 2005년 7월전자공학회 논문제 제 42권 CI 제 4호

[5] 조영복 외, “유비쿼터스 네트워크에서의 상호 인증 프로토콜”, 2004년 한국정보과학회 가을 학술발표 논문집 Vol.31, No.2