Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 7 pp. 4884-4890, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.7.4884
ISSN 1975-4701 / eISSN 2288-4688

차세대 무선 네트워크 환경에서 메시지 보호를 위한 통신 시스템 설계

민소연[1*], 진병욱[2]
[1]서일대학교 정보통신과, [2]숭실대학교 컴퓨터학과

A Design Communication System for Message Protection in Next Generation Wireless Network Environment

So-Yeon Min[1*], Byung-Wook Jin[2]
[1]**Department of Information Communication, Seoil University**
[2]**Department of Computer Science, Soongsil University**

요 약 전 세계의 인구가 1인 평균 2대의 모바일 디바이스를 소지하는 시대가 다가오고 있으며 무선 네트워크 시장이 점차 확장되고 있다. 모바일 기기의 활용도가 높아짐에 따라서 와이파이(Wi-fi, Wireless Fidelity=Wireless LAN)가 선호하는 네트워크로 떠오르고 있다. 와이파이를 기반으로 공공기관, 의료, 교육러닝 및 콘텐츠, 제조, 리테일 등 다양한 영역에서 새로운 가치를 창출해가고 있으며, 글로벌 네트워크가 구축되어 복합적인 서비스를 제공하고 있다. 하지만 차세대 무선 네트워크 환경에서 무선 디바이스 식별자 취약, MAC 위조를 통한 네트워크 자원의 불법 이용, 무선 인증키 크래킹, 미허가 AP/디바이스에 대한 공격과 같은 취약점이 존재하고 있다. 또한 인증 고도화 및 안전한 고속 보안 접속과 같은 보안기술연구가 거의 진행되고 있지 않다. 그러므로 본 논문에서는 차세대 무선 네트워크 환경의 메시지 보호를 위한 디바이스 식별과 콘텐츠 분류 및 저장 프로토콜을 설계하여 안전한 통신 시스템을 설계한다. 제안한 프로토콜은 기존의 무선 네트워크 환경에서 발생하는 보안취약점에 관하여 안전성을 분석하였고 기존의 무선 네트워크 환경의 암호기법을 비교분석하여 보안성을 분석하였다. 기존의 암호시스템 WPA2-PSK보다는 대략 0.72배 느리지만, 보안성에서는 안전성을 강화되었다.

Abstract These days most of people possesses an average of one to two mobile devices in the world and a wireless network market is gradually expanding. Wi-Fi preference are increasing in accordance with the use growth of mobile devices. A number of areas such as public agencies, health care, education, learning, and content, manufacturing, retail create new values based on Wi-Fi , and the global network is built and provides complex services. However, There exist some attacks and vulnerabilities like wireless radio device identifier vulnerability, illegal use of network resources through the MAC forgery, wireless authentication key cracking, unauthorized AP / devices attack in the next generation radio network environment. In addition, advanced security technology research, such as authentication Advancement and high-speed secure connection is not nearly progress. Therefore, this paper designed a secure communication system for message protection in next-generation wireless network environments by device identification and, designing content classification and storage protocols. The proposed protocol analyzed safeties with respect to the occurring vulnerability and the securities by comparing and analyzing the existing password techniques in the existing wireless network environment. It is slower 0.72 times than existing cypher system, WPA2-PSK, but enforces the stability in security side.

Keywords : Next Wireless LAN, Message Protection, Security Threat, Wireless LAN Security

본 논문은 2015년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : So-Yeon Min(Seoil Univ.)
Tel: +82-2-490-7583 email: symin@seoil.ac.kr
Received June 29, 2015 Revised July 15, 2015
Accepted July 16, 2015 Published July 31, 2015

1. 서론

최근 사용자의 무선 디바이스 보급량과 무선 네트워크가 활용성이 증가됨에 따라 다양한 영역에서 새로움 부가가치를 창출해가고 있다. 2013년도 차세대 무선 네트워크 표준인 802.11ac가 승인됨에 따라 무선 네트워크의 시장이 활발해지고 있으며, 교육기관, 호텔, 제조, 기업 등에서 차세대 무선 네트워크를 도입하려는 움직임이 늘어나고 있다[1,3,7,10]. 특징으로는 다양한 무선 멀티미디어 서비스가 제공되며, 하나의 무선 단말기가 무선 LAN, 위성 및 무선 PAN을 액세스하여 기존의 유선 네트워크와 결합되어 복합적인 서비스를 제공하고 있다. 하지만 손쉬운 공격 도구를 이용하여 도청 및 네트워크 무력화에 대한 공격이 가능하다. 더 나아가 공공기관 뿐만 아니라 기업에서도 많이 활용되고 있어 사회, 국가적으로 큰 위협을 초래하고 있다. 또한 사용자 인식에서 무선 네트워크가 유선 네트워크에 비해 안전하지 않다는 의식이 있으며, 정부측면에서 무선 네트워크의 보안 지침 및 규지를 강화하고 있으나, 기술적 조치의 한계에서 사용성이 저하되고 있다[2,8].

그러므로 본 논문에서는 차세대 무선 네트워크 환경에서 안전한 통신을 위해 기존의 무선 네트워크상의 취약점과 발생할 수 있는 보안위협을 완화하기 위한 통신 시스템을 설계한다.

2. 관련연구

2.1 무선/모바일 시장 및 기술의 변화

스마트 디바이스 사용량의 증가로 2017년 스마트폰, 태블릿 기기, 노트북 등의 모바일 트래픽이 93% 처리될 것으로 전망하고 있다. 무선 네트워크 환경의 급속한 발전으로 인해 기업 및 공공기관에서 모바일 폭증 데이터의 우회 망으로 활용되는 추세이며 사용자 개개인의 무선 네트워크 환경이 기업형식으로 발전되고 나아가 공공부분으로 급속히 확대되고 있다. 하지만 무선보안 이슈가 모바일 전자정부, 스마트워크 사업 등 공공사업 추진의 최대 걸림돌로 등장하고 있다[5,6]. 정부는 '알기 쉬운 무선랜 보안 안내서'와 같은 해킹 및 정보보호를 방지하기 위한 수칙을 발표 했으나, 기술 및 보안정책의 부재로 한계점을 느끼고 있어 안전한 무선 네트워크 환경을 사용하기 위해 AP(Access Point)에 대한 보안, 인증 및 암호화 적용, 보안 정책의 실행, 무선 침입 방지 기법이 요구되고 있다[1].

2.2 무선 디바이스 식별을 위한 구조 및 요구사항

무선 디바이스 식별 관리기술의 구성도는 무선 디바이스 특징 정보를 수집하면서 디바이스를 식별하는 시스템과 무선 디바이스를 관리하고 제어하는 관리서버로 구성되어 있으며 다음과 같은 기능을 요구한다[2,3].

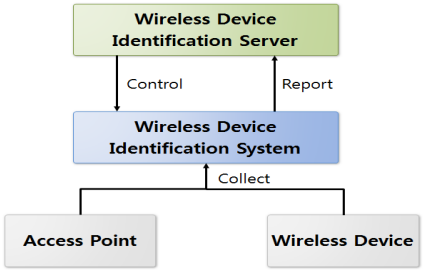

Fig. 1. Component of identification technology of wireless device

무선 디바이스 식별 기술은 시스템 인증 기능, 외부 인터페이스 기능, 무선 디바이스 식별 기능, 시스템 관리 기능, 사용자 인터페이스 기능이 있으며 기능의 요구사항은 Table 1과 같다[2,6,8].

Table 1. Requirements of identification technology of wireless device

Classification Function	Requirement
System Authentication Function	Authentication function for preventing be controlled by accessing the server illegally
External interface functions	After setting the identification signature function of the external interface for receiving transmit detection information attack
Wireless Device Identification	The ability to identify the wireless device that uses a fake identifier in the wireless network environment in real time
Systems management capabilities	Ability to manage the identification system of wireless device
User Interface Features	By controlling the identification system, the user interface function for outputting the detected information

2.3 무선 고속접속을 위한 보안 요구사항

2.2절에서 인증 및 데이터 보호와 같이 실질적인 보안 기능에서 요구사항을 정의하였으나, 2.3절에서는 무선접속을 위한 Provisioning, 식별 및 인증, 사용자의 데이터 보호, 감사 기록에 관하여 설명한다[2,4]. 우선 Provisioning은 IPR(Initial Provisioning functional Requirement)을 기반으로 인증 정보와 디바이스간의 신뢰관계를 확보해야한다. 식별 및 인증은 IAR(Identification and Authentication functional Requirement)을 기반으로 인증단계에서 소요되는 지연을 줄여야 하며, 무선랜 환경에서 사용자 데이터 보호를 위해서는 DPR(Data Protection functional Requirement)을 만족해야하고, 감사기록의 ARR(Audit Record functional Requirement)을 기반으로 보안위협이 발생 시 사후 추적이 가능해야한다[5,9,11,12].

3. 메시지 보호를 위한 권한 접근 시스템 설계

본 논문에 제안한 시스템은 사용자 디바이스, Wireless Access Server, Authority Server, Content Service Server로 구성된다. Wireless Access Server는 AP를 관리하는 접근서버로 악의적인 AP 검증하며, Authority Server는 사용자의 Device정보와 AP의 정보를 검증을 수행한다. 우선 사용자의 디바이스 인증을 수행 후 사용자의 데이터를 등급에 따라서 분류 및 저장을 한다. 사용자가 해당데이터에 접근을 할 때 제안한 통신 프로토콜을 수행한다.

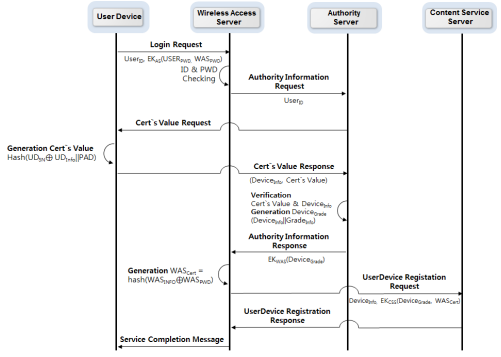

Fig. 2. Authority Authentication Process

3.1 사용자 디바이스 인증 프로토콜 설계

Fig. 2는 권한 인증 프로토콜을 설계를 제안한 부분으로 사용자 디바이스가 인증 과정을 수행 후 사용자 장비를 등록한다. 세부적인 절차는 아래의 서문과 같다.

1. 사용자는 ID, PWD와 Wireless Access Server의 PWD를 Wireless Access Server로 전송하여 로그인을 요청한다.
$$USER_{ID}, EK_{AS}(USER_{PWD}, WAS_{PWD})$$

2. Wireless Access Server는 ID와 PWD를 검사 후 Authority Server로 사용자의 ID의 정보를 요청메시지를 전송한다.

3. Authority Server는 사용자의 Device로 인증값을 요청메시지를 전송한다.

4. User Device는 인증값을 생성 후 Device의 정보와 함께 응답 메시지를 전송한다.
$$Cert\ Value = Hash(UD_{SN} \oplus UD_{\infty o} \| PAD)$$
$$(Device_{\infty o}, Cert\ Value) \quad (1)$$

5. Authority Server는 인증값과 디바이스 정보를 검증 후, Device Grade Value를 생성한다.
$$Device_{Grade} = (Device_{\infty o} \| Grade_{\infty o}) \quad (2)$$

6. 이후 WAS의 공개키로 암호화하여 Wireless Access Server로 Device Grade Value을 전송한다.

7. Wireless Access Server는 WAS 인증값을 생성 후 Device Grade를 공개키로 암호화하여 Content Service Server로 사용자 장비 등록 요청 메시지를 전송한다.
$$WAS_{Cert} = Hash(Was_{info} \oplus WAS_{PWD})$$
$$Device_{info}, EK_{Css}(Device_{grade}, Was_{Cert}) \quad (3)$$

8. Content Service Server는 등록 후 Wireless Access Server를 경유하여 User Device로 전송한다.

3.2 콘텐츠 분류 및 저장 프로토콜 설계

Fig. 3은 사용자의 콘텐츠를 저장 후 분류 및 저장을 수행하는 프로토콜로서 세부적인 절차는 다음과 같다.

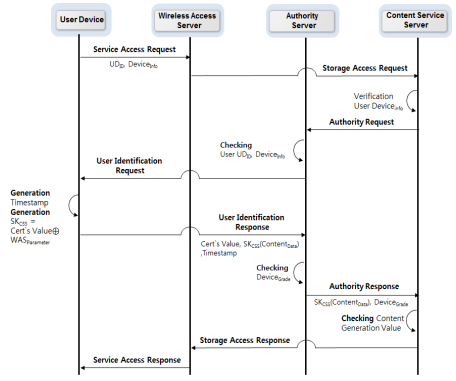

Fig. 3. Content Classification and Storage Process

1. 사용자는 Device를 사용하여 ID, Device의 정보를 Wireless Access Server로 서비스 접근 요청 메시지를 전송한다.

$$UD_{ID}, Device_{info} \quad (4)$$

2. Wireless Access Server는 Content Service Server로 스토리지 접근을 요청한다.

3. Content Service Server는 Authority Server 권한 요청 메시지를 전송한다.

4. 사용자 ID, 장비정보를 검사 후 사용자 신원 요청 메시지를 전송한다.

5. 세션키와 타임스탬프를 생성 후 Authority Server로 응답 메시지를 전송한다.

$$SK_{CSS} = Cert\ Value \oplus WAS_{Parameter} \quad (5)$$

6. Device Grade Value 검사 후 Content Data를 세션키로 암호화 하여 Content Server로 전송한다.

$$Cert\ Value, SK_{CSS}(Content_{Data}), TimeStamp \quad (6)$$

7. Content Server는 Content Data를 생성 후 Content Value를 생성한다.

8. 이후 Wireless Access Server를 경유하여 User Device로 서비스 접근 응답 메시지를 전송한다.

3.3 메시지 전송 프로토콜 설계

Fig. 4.는 메시지 통신 프로토콜을 설계한 부분으로 사용자 Device와 Wireless Access Server간의 Parameter를 교환 후 SSL을 설립하여 안전하게 메시지 통신 프로토콜을 설계하였다. 세부적인 절차는 다음과 같다.

1. User는 Wireless Access Server로 SSL & Content 요청 메시지를 전송한다.

2. Wireless Access Server와 Authority Server간의 파라미터를 교환 후 SSL 설립 응답 메시지를 사용자 Device로 전송한다.

3. 이후 Content Service Server로 콘텐츠 접근 요청 메시지를 요청한다.

4. 콘텐츠 검사와 Grade Value를 비교 후 WAS세션키를 생성한다.

$$SK_{WAS} = WAS_{Cert}, Device_{Grade} \| WAS_{Parameter} \quad (7)$$

5. 생성한 세션키를 사용하여 암호화 후 콘텐츠를 Wireless Access Server로 전송한다. 이후 SSL을 활용하여 콘텐츠를 전송한다.

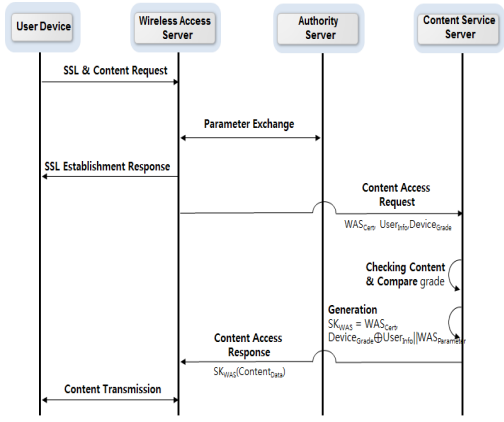

Fig. 4. Message Communication Protocol

4. 성능평가

4.1 안전성 분석권한

본 절에서는 방송통신전자진흥원의 차세대 무선랜 보안 기술동향 및 이슈의 무선랜 공격 기술을 참조하여 안전성을 분석하였다. 누구나 쉽게 무선 네트워크 환경으로 접속할 수 있는 특성을 이용하여 비 인가된 사용자가 사용할 수 있는 있는 공격으로는 도청 및 무선 스캐닝, MAC 프레임 기반 서비스 거부 공격, 인증 프레임 위조를 통한 서비스 거부 공격, 불법적인 내부망 연결 AP 또는 외부 AP 등이 있으며 안전성에 대한 강도를 검증한다.

(1) 도청 및 무선 스캐닝

암호화를 수행하지 않은 데이터를 송수신할 때 공격자는 데이터를 분석하여 다양한 정보를 유출 할 수 있는 공격을 말한다. 제안한 시스템에서는 사용자의 인증절차를 수행 후 데이터(콘텐츠)를 설계함으로써 안전하다.

(2) MAC 프레임 기반 서비스 거부 공격

무선 네트워크 환경의 MAC 프레임부분에 제어 및 관리 프레임을 탈취 후 위조하여 기기와 AP사이의 접속을 해제한다. 하지만 Authority Server에서 WAS_{Cert} , $Cert_{Value}$ 를 검증함으로써 MAC 프레임 서비스 거부 공격이 실패하게 된다.

(3) 인증 프레임 위조를 통한 서비스 거부 공격

인증 프로토콜 절차의 수식 (1), (3)과 콘텐츠 분류 및 저장 프로토콜의 (6)을 수행함으로서 인증 프로세스의 비정상 종료를 수행하는 서비스 거부 공격에 안전하다.

(4) 불법적인 내부망 연결 AP 또는 외부 AP

외부 공격자가 내부 망에 불법으로 접근하기 위해 설치하는 Rogue AP, 무선 단말로 편리한 내/외부 망에 접근하기 위해 Soft AP, 정상 AP로 동작시키기 위한 Mis-configured AP를 활용하여 기관내 내부 도메인으로 중요한 정보를 접근하는 방식이 있다. 제안한 시스템에서는 위의 언급된 접근방식을 보완하기 위해 $Content_{Data}$를 생성 후 SK_{WAS}를 활용하여 데이터를 안전하게 통신하도록 시스템을 설계하였다.

(5) 기타 공격

기존의 무선 네트워크 환경에서 AP와 단말기기간의 콘텐츠를 암복호화를 수행할 때 공통의 키를 사용한다. 하지만 본 논문에서 제안한 시스템에서는 사용자의 권한 등급과 콘텐츠를 분류하여 저장함으로써 콘텐츠 보호뿐만 아니라 유출방지가 가능하다.

4.2 보안성 비교분석

본 논문에서 제안한 시스템의 보안성을 분석하기 위해서 기존의 무선 네트워크 환경에서 사용되고 있는 시스템과 제안 시스템의 인증방식, 프로토콜 분석 방식, 데이터관리, 사용자 정보관리에 관하여 보안성을 평가하여, 비교분석 결과를 Table 2에 기술하였다.

Table 2. Proposed system and security comparative analysis of the authentication method of the existing system

	Existing System		Proposed System
	WPA	WPA2-PSK	
Key stream system	LFSR (Linear Feedback Shift Register)	Symmetric - key	Session Key
Authentication System	RC5	OTP	Authentication based on user and content information
Protocol Analysis System	Stream Cipher	Block Cipher	Block Cipher
Encryption System	TKIP	AES	Session key is generated based on the information
Data protection and classification	Protection only	Protection only	Enable
User Information Management	-	-	Enable

2.3절의 IPR(Initial Provisioning functional Requirement), IAR(Identification and Authentication functional Requirement), DPR(Data Protection functional Requirement), ARR(Audit Record functional Requirement)기반으로 보안성을 분석하였다. 또한 데이터 암호화 방식과 인증 수행 속도에 관하여 비교분석하였다. 제안프로토콜은 WPA보다 대략 1.16배 빠르고, 0.72배 느리게 나왔지만 WPA, WPA2-PSK는 단방향 인증이여서 보안위협부분에서 안전할 수 없으며, 비교분석의 내용을 Fig. 5에서 나타내었다.

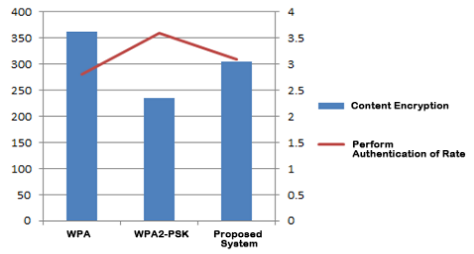

Fig. 5. Comparative analysis chart of the existing system and the proposed system

5. 결론

본 논문에서는 차세대 무선 네트워크 환경에서 사용자 인증과 콘텐츠 분류 및 저장 프로토콜을 설계하여 안전한 메시지 통신 시스템을 제안하였다. 제안하는 통신 시스템은 Wireless Access Server를 구성하여 사용자 디바이스와 AP의 정보를 검증하는 정보기반 인증기반 시스템을 설계하였으며, 콘텐츠는 사용자 등급 분류 및 저장 후 생성된 세션키로 콘텐츠를 암호화하여 메시지 보호방식을 설계하였다.

무선 디바이스 식별기술의 요구사항을 참조하여 도청 및 무선 스캐닝, MAC 프레임 기반 서비스 거부 공격, 인증 프레임 위조를 통한 서비스 거부 공격, 불법적인 내부망 연결 AP 또는 외부 AP 등과 같은 공격에 대하여 안전성을 분석하였으며, 기존의 무선 네트워크상에서 사용되고 있는 WPA, WPA2-PSK와 제안시스템에 관하여 키 스트림 방식, 인증 방식, 프로토콜 분석 방식, 암호화 방식, 데이터 보호 및 분류, 사용자정보 관리에 관하여 보안성을 비교 분석하였다.

향후 제안한 시스템을 적용하기 위해서는 사용자 정보, 무선 AP정보에 관한 보호가 필요하고, 내부자의 콘텐츠 유출에 관하여 감사기록에 관한 기능적 강화가 요구된다. 더 나아가 802.11ac규격을 활용되고 있는 다양한 영역에 접목에 관한 연구가 필요하다.

References

[1] TTA, "Security Requirements for WLAN Fast Link Set-up in Enterprise Environment", 2014. 12.

[2] TTA, "Functional Requirements for Wireless Device Identification in WLAN", 2013. 12.

[3] TTA, "Architecture and Interface for Wireless Device Identification in WLAN", 2014. 12.

[4] Sin-hyo Kim, "Next Wireless Lan Security Technology", 2013. 12.

[5] Kisa, "Security guide of easy-to-understand public wireless LAN", 2011. 12.

[6] KCA, "Wireless LAN security technology trends of the next generation and challenges", 2013.

[7] Joo-Hyung Son, Next-generation wireless LAN standard IEEE 802.11ax Standardization, Telecom Korean, 2014. 8. DOI: http://dx.doi.org/10.1109/QSHINE.2014.6928663

[8] IEEE 802.11: Standard for Information Technology Telecommunications and information exchange between systems－Local and metropolitan area network－Specific requirements－Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 2012. DOI: http://dx.doi.org/10.1109/IEEESTD.2012.6178212

[9] Kwansik Yoon, "A Mechanism for Controlling Accesses Dynamically in Smartwork Environment", VOL. 19 NO. 02 PP. 877~880, 2012. 11.

[10] Jae-Sung Park, Jae-Sang Cha, Chong-Hoon Lee, Heung-Mook Kim, Sung-Woong Choi, Ju-Phill Cho, Yong-Woon Park, Jin-Young Kim, "Phase Offset Estimation Based on Turbo Decoding in Digital Broadcasting System", *The Journal of The Institute of Webcasting, Internet Television and Telecommunication*, Vol. 9 No. 2, pp. 111~116, 2009.

[11] Young-Do Joo, "Analysis on Security Vulnerabilities of a Biometric-based User Authentication Scheme for Wireless Sensor Networks," *The Journal of The Institute of Webcasting, Internet Television and Telecommunication*, Vol. 14 No. 1, pp. 147~153, 2014.

[12] Gang-Seok Kim, Jee-Wan Huh, Wang-Cheol Song, "Zone based on Wireless Sensor Network Management Protocol for Smart Home," *The Journal of The Institute of Webcasting, Internet Television and Telecommunication*, Vol. 09 No. 5, pp. 65~71, 2009.

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 임베디드 시스템

진 병 욱(Byung-Wook Jin) **[정회원]**

- 2010년 2월 : 청운대학교 멀티미디어학과 (문학사)
- 2013년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과

<관심분야>
사물지능통신, USN, 네트워크 통신