http://dx.doi.org/10.15207/JKCS.2015.6.4.243

U-Healthcare 기기에서 DRDoS공격 보안위협과 Big Data를 융합한 대응방안 연구

허윤아, 이근호
백석대학교 정보통신학부

A Study on Countermeasures of Convergence for Big Data and Security Threats to Attack DRDoS in U-Healthcare Device

Yun-A Hur, Keun-Ho Lee
Division of Information and Communication, Baekseok University

요 약 U-Healthcare는 언제, 어디서나 환자의 건강을 검사하고 관리하며 유지할 수 있도록 하는 의료와 IT가 융합된 서비스이다. U-Healthcare 서비스에서 이루어지는 통신은 검진한 분석 결과나 긴급 데이터를 무선 통신방식을 이용하여 병원 서버에 전송하는 방식이 활용되고 있다. 이 때 악의적인 접근을 수행하는 자(공격자)가 U-Healthcare기기나 BS(Base Station)에 DRDoS(Distributed Reflection DoS)공격을 하면 위급한 환자의 상황정보가 병원 서버까지 전송되지 않는 다양한 피해가 예상된다. 이를 대응하기 위해 DRDoS 공격 시나리오와 DRDoS에 대한 대응방안을 제안하고 대량의 패킷을 처리할 수 있는 빅데이터와 융합한다. 공격자가 U-Healthcare 기기나 BS(Base Station)를 공격 시 DB와 연동하여 일치하면 공격을 막는다. 본 논문은 원격의료 서비스인 U-Healthcare기기나 BS에서 나타날 수 있는 공격방법을 분석하고, 빅데이터를 활용하여 보안 위협에서의 대응방안을 제안한다.

• Key Words : U-Healthcare; BigData; IoT; M2M; Convergence

Abstract U-Healthcare is a convergence service with medical care and IT which enables to examine, manage and maintain the patient's health any time and any place. For communication conducted in U-Healthcare service, the transmission methods are used that patient's medical checkup analysis results or emergency data are transmitted to hospital server using wireless communication method. At this moment when the attacker who executes the malicious access makes DRDoS(Distributed Reflection DoS) attack to U-Healthcare devices or BS(Base Station), various damages occur that contextual information of urgent patients are not transmitted to hospital server. In order to deal with this problem, this study suggests DRDoS attack scenario and countermeasures against DRDoS and converges with Big Data which could process large amount of packets. When the attacker attacks U-Healthcare devices or BS(Base Station), DB is interconnected and the attack is prevented if it is coincident. This study analyzes the attack method that could occur in U-Healthcare devices or BS which are remote medical service and suggests countermeasures against the security threat using Big Data.

• Key Words : U-Healthcare; BigData; IoT; M2M; Convergence

*교신저자 : 이근호 (root1004@bu.ac.kr)
접수일 2015년 6월 15일 수정일 2015년 7월 8일 게재확정일 2015년 8월 20일

1. 서론

최근 정보통신 기술이 발전하면서 IoT 서비스들도 많이 발전하고 있다. 특히 의료기술에서도 네트워크를 이용한 원격으로 진료 서비스를 제공하는 대표적인 U-Healthcare 서비스 등 많은 발전이 이루어지고 있다[1].

U-Healthcare 서비스는 환자의 생체신호, 건강회복하거나 유지하며 관리하기 위해 언제 어디서나 이용할 수 있는 원격의료 서비스 기술이다[2]. U-Healthcare 서비스의 대상자는 대부분 사회에서 취약한 계층인 노인, 임산부, 질병에 걸린 환자, 아동을 목표로 하고 있다[3]. 또한 U-Healthcare의 장점은 사회 경제적으로 의료비 절감과 시간 절약할 수 있는 등 가장 효율적인 의료기술에서의 대안으로써 많은 국가에서 활용하여 확산되고 있다[4].

U-Healthcare는 무선 통신을 통해 서비스 하고 있다. 무선 통신의 종류로는 ZigBee, Bluetooth, Wireless USB, WiFi, RFID 등이 있다[5]. 무선 통신에 비해 유선 통신은 공격에 안전하기 때문에 무선 통신 기술에서 보안의 한계가 있다[6].

U-Healthcare 디바이스나 근거리 무선통신의 다리역할을 수행하는 Base Station이 고유 IP주소를 가지고 인터넷에 연결됨에 따라 원격으로 환자의 상태 정보의 패킷들을 보내게 된다[7]. U-Healthcare기기 또는 BS(Base Station)에 DRDoS 공격을 당하게 된다면 위급 시에 감지된 환자의 상태가 병원 서버에 전송이 되지 않는 위험한 경우가 발생될 수 있다[8].

이러한 시점에서 본문에서는 DRDoS 공격 기법을 분석하고 시나리오를 작성하여 DRDoS 공격이 가지는 패턴을 Big Data로 구축하여 공유하고 실시간 모니터링을 통해 대응하는 방안을 제안하고자 한다.

2. 관련연구

2.1 U-Healthcare

U-Healthcare는 소개된 지는 10여년이 지났지만 법적 제약하에 적절한 수익모델을 찾지 못해 산업이 아직 부상하지 못하고 있다. 그러나, 의료 산업 환경의 변화로 인해 향후 뚜렷한 성장 모멘텀을 갖게될 것으로 예상된다[7].

현대에 들어서면서 의학이 발달하고 생활수준이 높아지면서 사망률이 현저하게 줄었다. 또 매년 출산율은 감소하고 사망률은 떨어지면서 인간의 평균수명이 높아지고 있다. Fig. 1을 보면 65세 이상의 인구비율이 1960년에 3.3%였던 것이 2009년에는 10.7%로 증가했다. 이렇게 이어진다면 2026년의 노인 인구 비율은 20%이상 될 것이다.

이렇게 고령화 사회가 진행될수록 의료 시장은 자연스럽게 점점 더 커질 것이고 몸이 불편한 노인분들은 병원에 가서 직접 진찰받아 치료를 받아야하는 불편한 점을 개선하여 좀 더 편하게 진료 받기를 원하게 될 것이다[9].

IT기술과 인터넷이라는 정보통신망을 바탕으로 의료서비스분야에서도 편리함과 효율성을 장점을 갖고 있는 원격 의료 서비스인 U-Healthcare는 정보통신기술인 IoT(Internet of Things) 기술 중 하나이다[10]. U-Healthcare는 환자의 건강 상태를 언제 어디서나 U-Healthcare 기기(의료 기기)로 측정하여 현재의 상태를 병원으로 보내 검진을 받을 수 있도록 서비스하는 보건의료서비스이다. 현재 의료서비스는 의사중심으로 이루어져있다. 환자는 자신이 갖고 있는 질병에 대해 정확히 모르고 어떤 진료를 받고 있는지, 어떤 약을 처방받았는지 모르는 경우가 많다. 즉, 정보부족과 공간적, 시간적 제약으로 인해 의료기관을 선택하는 것도 제한되어 있다. U-Healthcare가 보편화되면 의사중심인 서비스가 환자(소비자) 중심의 서비스로 바뀌게 된다. 의료에 대한 정보와 검사 받을 시 어떤 치료를 받아야하는지 이 분야의 전문가가 누구인지 정보를 통해 알게 될 것이다. 즉, 환자의 선택과 자유가 주어진다[11].

U-Healthcare시장은 크게 만성질환 환자 대상의 치료중심 서비스 U-Medical, 고령자 대상의 U-Silver, 건강관리 서비스인 U-Wellness로 분류된다. 한국보건산업진흥원에 따르면 U-Healthcare 세계시장은 '09년 기준 1,431억불 규모로서 매년 15%이상 지속성장할 것을 전망하였으며, 분야별 평균성장률은 U-Silver(9.7%), U-Medical(15.0%), U-Wellness(17.9%)으로 나타났다. 특히 U-Wellness 시장은 법적 제약이 적어, 기존 체육시설을 증가하는 체육활동 관심 층과 연계시킬 경우 급속성장 가능할 것으로 전망되었다[12].

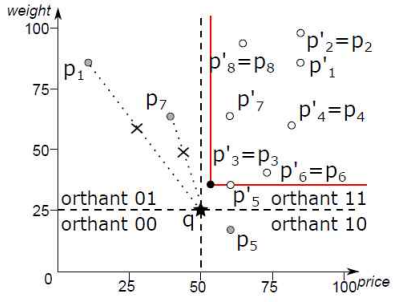
2.2 빅데이터

빅데이터는 기존의 데이터 수집, 저장, 관리, 분석 역

량을 넘어서는 대량의 데이터 세트를 의미하며 기존의 관계형 데이터와 비교하여 양, 속도, 다양성 및 복잡성에 있어서 그 차이를 볼 수 있다. 빅데이터의 정의는 다양하지만, 기업적인 측면에서 빅데이터를 기업의 효과적인 전략 도출에 필요한 상세하고 높은 빈도로 생성되는 다양한 종류의 정형 또는 비정형 데이터로 정의할 수 있다. 빅데이터를 특정 짓는 가장 큰 부분은 기존 기술로는 처리하기 어려운 정형 및 비정형 데이터가 다양한 형태로 혼재된 복잡도 높은 대용량 데이터를 신속하게 처리 가능하며 이를 기반으로 고급분석과 예측 등을 통한 새로운 차원의 서비스 창출이 가능하다는 점이다. 이렇듯 빅데이터는 방대한 규모(Volume)로 경제적 타당성으로 방대한 내용을 저장 가능하게 하고, 빠른 처리 속도(Velocity)는 고성능 분산병렬처리 기술을 보급, 다양한 형태(Variety)는 저장이 불가능했던 것들이 디지털 저장이 가능하게 되었다[13].

2.3 Dynamic skyline query

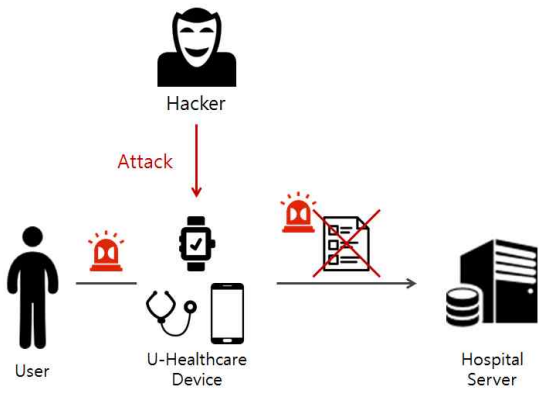
skyline은 n개의 속성에 대하여 더 이상 압도되지 않는 최적의 해를 찾는 쿼리를 말한다. 이는 다양한 어플리케이션의 의사결정에 활용되며, 최근 dynamic skyline 기법이 등장하여 특정 좌표를 기준으로 최적의 해를 찾는 것이 가능해졌다. [Fig. 1]은 dynamic skyline의 예를 나타내고 있다[14].



[Fig. 1] Dynamic skyline query

3. 공격 시나리오

U-Healthcare에서 사용하는 무선 통신 기술은 유선통신 기술보다 보안 위험에 노출되어 있다.

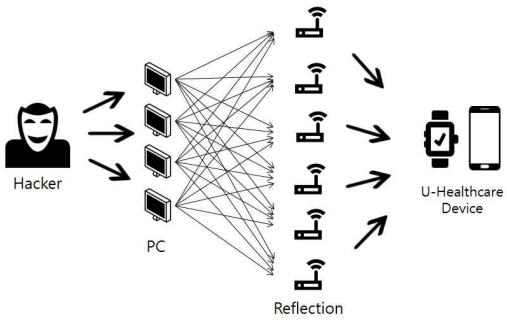


[Fig. 2] Attack Scenarios

평소에 사용자가 U-Healthcare기기를 통해 진찰을 받은 후 측정된 정보를 병원서버로 패킷을 전송하여 의사에게 전달한다. U-Healthcare는 이러한 원격 의료 시스템을 이용해 환자와 의사간의 피드백이 되도록 하는 시스템이다. 그런데 Fig. 2와 같이 심장질환 환자나 임산부, 노인, 아동 등 위급 시 측정된 정보를 병원 서버로 전달을 할 때 U-Healthcare기기 또는 BS(Base Station)에 DRDoS 공격을 당하게 되면 위급한 환자의 정보가 병원 서버에 전송이 되지 않는 위험한 경우가 발생될 수 있다.

이처럼 원격 의료에서 보안을 강화하지 않으면 나타날 수 있는 위협과 바이러스로 인한 진단오류발생으로 생명의 위협까지 느낄 수 있다[15]. 그래서 U-Healthcare 기기와 병원 서버 간의 원활한 통신을 위해 U-Healthcare 기기를 공격할 수 있는 시나리오인 DRDoS에 대해 분석하고 그에 대한 대응방안이 필요하다[16].

U-Healthcare 기기에서 위급한 환자의 정보를 측정하여 측정된 정보를 병원시스템에 보내게 되는데, 이때 U-Healthcare기기나 BS(Base Station)를 DRDoS 공격을 당하게 되면 임산부, 심장질환환자, 아동, 노인 등 위급한 환자의 상태 정보가 병원 서버에 전송이 되지 않는 위험한 경우가 발생 될 수 있다.



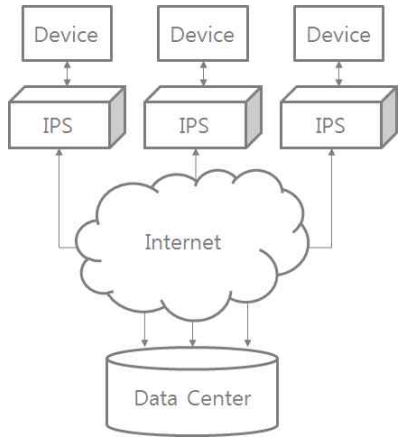
[Fig. 3] DRDoS Attack Scenarios

[Fig. 3]를 보면 수많은 좀비 PC가 반사체를 이용하여 한꺼번에 U-Healthcare기기나 BS(Base Station)를 공격하게 된다면 공격대상인 U-Healthcare기기나 BS(Base Station)는 다운이 될 것이다.

DRDoS는 TCP 연결할 때 쓰이는 3-way Handshaking 방식을 이용한 것으로 공격자(Hacker)는 출발지 IP를 병원 서버의 IP로 Spoofing하여 SYN패킷을 U-Healthcare기기나 BS으로 전송한다. SYN 패킷을 받은 U-Healthcare기기나 BS은 Spoofing된 병원 서버 IP로 SYN/ACK를 전송한다. U-Healthcare기기나 BS 입장에서는 실제로 패킷을 보낸 Spoofing된 병원 서버의 IP가 정말로 헤더에 쓰여 진 송신자가 맞는지 1회의 수신만으로 검증할 방법이 없다. 이를 이용하여 한 번 인증이 된 IP는 수많은 좀비 PC가 외부 공격자 타겟과 아무 상관없는 Router(Reflection)들을 통해 U-Healthcare기기나 BS에 공격하여 다운된다. 예를 들어 총 좀비 PC는 1000대라 하고 한 좀비 PC당 2개의 패킷을 보낸다 할 때 서버에 공격되는 패킷은 2000개가 되어 U-Healthcare기기나 BS가 다운이 된다. U-Healthcare기기나 BS가 다운이 되면 위급 시 보내지는 패킷을 받을 수 없기 때문에 환자의 상태가 위험해진다. 이렇게 발생한 DRDoS 공격 분석을 Big Data를 이용하여 보안 위협을 줄인다.

4. 대응방안

U-Healthcare 서비스를 대상으로 수행되는 DRDoS 공격에 대응하기 위하여 본 연구에서는 다수의 IPS가 공통 데이터 센터에서 탐지 규칙을 공유하는 구조와 효율적인 쿼리 기법을 제안한다. 데이터 센터에서 탐지 규칙을 저장할 시 빅데이터 처리에 최적화된 하둡 파일 시스템 형태로 구성하며 효율적인 쿼리를 구현하기 위하여 skyline 쿼리를 도입하였다.



[Fig. 4] Proposed system architecture

제안 시스템에서 [Fig. 4]와 같이 U-Healthcare 서비스 단말기 앞단에 IPS가 위치한다. IPS는 최소의 연산능력과 메모리로 설계되며 데이터 센터로 패킷의 패턴을 주기적으로 보내고 방어대상 호스트를 차단하는 역할을 수행한다. 그리고 데이터 센터는 패턴이 도착할 시 공격 유무를 확인하기 위한 쿼리를 구성하고 대규모 데이터를 활용하여 결과를 도출하게 된다. 처리의 결과가 공격일 경우 호스트 정보를 IPS로 보내고 IPS는 일정기간 동안 해당 호스트에서 보내지는 모든 패킷을 공격으로 간주하고 차단하게 된다[17].

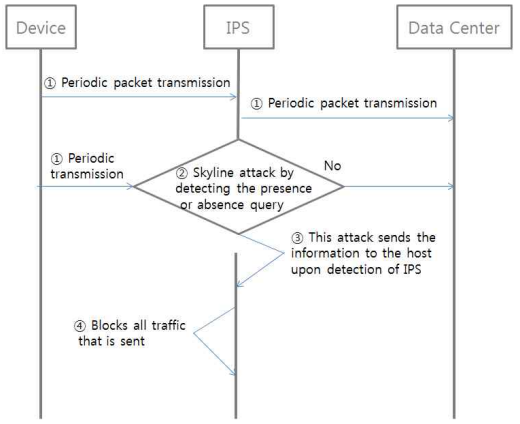
4.1 대규모 패턴 관리를 위한 분산 파일시스템

데이터 센터에서는 다수의 U-Healthcare 서비스 단말기에서 주기적으로 보내지는 패턴을 저장하게 된다. 그러므로 빅데이터 규모의 패턴을 효율적으로 저장하는 기법이 요구된다. 제안 시스템에서는 하둡 분산 파일시스템 형태로 구축하고 맵리듀스를 이용하여 신속한 쿼리 응답을 지원한다.

4.2 Skyline 쿼리를 이용한 공격탐지

주기적으로 보내지는 U-Healthcare 디바이스의 패턴은 대규모 분산 파일 시스템을 대상으로 Skyline 쿼리를 수행한다. 이러한 쿼리는 기존에 다양한 디바이스에서

보낸 대규모 패턴과 비교를 통해 결과를 도출한다. 기존에 저장된 패턴은 공격 유무를 나타내는 지표와 함께 저장되기 때문에 Dynamic skyline 기법을 이용하여 쿼리의 기준이 되는 패턴과 근사한 패턴들이 공격인지 여부에 따라 의사결정을 수행할 수 있다. 쿼리를 처리하는 과정은 [Fig. 5]와 같다.



[Fig. 5] Query Process

① 패킷 트래픽 패턴을 주기적으로 전송한다.
② Skyline 쿼리를 구성하고 처리하여 공격 유무를 탐지한다.
③ 공격이 탐지될 경우 호스트에 대한 정보를 IPS에 전송한다.
④ IPS는 방어대상 호스트를 테이블로 관리하여 전송되는 모든 트래픽을 차단한다.

위 시나리오를 통해 일정 패턴 감지에 대한 감지된 호스트를 테이블로 저장하고 관리하여 트래픽 패턴을 차단한다.

5. 결론

정보통신기술이 발전하면서 원격 의료 서비스인 U-Healthcare의 사용이 점점 보편화되어 가고 있다.

U-Healthcare의 주된 목표 대상은 노인, 심장질환 환자, 임산부, 아동과 같은 사회에 약한 계층을 위해 주로 서비스 되고 있다. U-Healthcare는 시간 절약과 공간의 제한이 없다는 면에서 여러 장점도 있지만 악의적인 사용자가 U-Healthcare의 기기나 BS를 DRDoS공격하게 되면 기기에 처리할 패킷들이 늘어 중단이 되게 된다. 이때 노인, 임산부, 아동, 질병에 걸린 환자 등 위급한 환자들의 상태 정보를 보내게 되면 병원서버까지 전송하지 못하는 경우가 발생되는 취약점이 있다.

본 논문은 이에 대응하기 위해 DRDoS 공격 시나리오와 패턴 등을 분석하였다. 그리고 공격 시나리오에 맞춰 IPS를 통해 데이터 센터로 오는 패킷의 패턴을 주기적으로 보내고 방어 대상 호스트를 차단하는 역할을 수행한다. 그리고 데이터 센터는 패턴이 도착할 시 공격 유무를 확인하기 위한 쿼리를 구성하고 대규모 데이터를 활용하여 결과를 도출하게되는 대응방안을 제시한다. 이러한 대응방안을 Big Data에 연결하여 BS를 상시 모니터링하며 무수한 공격을 분산처리를 통해 빠르게 분석하고 능동적으로 대처할 수 있도록 한다. 본 논문에서는 원격의료 서비스에 대한 보안 취약점을 진단하고 보안 사고에 대응한다.

ACKNOWLEDGMENT

이 논문은 2015학년도 백석대학교 대학연구비에 의하여 수행된 것임.

REFERENCES

[1] Byeongheon Jeon, Sangbum Han, "In a Mobile Environment, the Design and Implementation of Hospital Information System", The Conference of the KIPS, Vol. 38, No. 2, pp. 49-55, 2011.
[2] Keun-Ho Lee, “Analysis of Threats Factor in IT Convergence Security”, Journal of the Korea Convergence Society, Vol.. 1, No. 1, 2010.
[3] Chang-Gyu Kim, Mi-Ran Lim, "Development directions of voluntarism in University students", Journal of the Korea Convergence Society, Vol.. 2, No. 2, pp. 57-65, 2011.
[4] Han-Kyoul Kim, Kyoung-Sook Lee, Kwang-Hwan Kim, Yong-Ha Kim, "A Study on Determinats of Cancer Patients's Length of Hospital Stay on Medical Charges Pattern", Journal of the Korea Convergence Society, Vol.. 2, No. 4, pp. 53-58, 2011.

[5] Kyoung-nam Kim, Lee, Jae Moon, Sunghyuck Hong, MyounJae Lee, "Convergent Secure Wireless Sensor Network Routing Algorithm", Journal of the Korea Convergence Society, Vol.. 6, No. 1, pp. 65-70, 2015.

[6] Byung-Seok Yu, Sung-Hyun Yun, "The Design and Implementation of Messenger Authentication Protocol to Prevent Smart Phone Phishing", Journal of the Korea Convergence Society, Vol.. 2, No. 4, pp. 9-14, 2011.

[7] Seong-Gwon Yeo, Keun-Ho Lee, "Smart Phone and Vehicle Authentication Scheme with M2M Device", Journal of the Korea Convergence Society, Vol.. 2, No. 4, pp. 1-7, 2011.

[8] Chung-Geon Song, Keun-Ho Lee, "Design of Authentication System using Biometrics for U-Healthcare Environment in M2M", Journal of the Korea Convergence Society, Vol.. 3, No. 2, pp. 13-17, 2012.

[9] Mi-Kyoung Kim, Dahye Park, Okhee Ahn, "The Care Giving Burden of Primary Caregiver based on Nursing Needs of Long-term Care Insurance Grade", Journal of the Korea Convergence Society, Vol.. 5, No. 3, pp. 7-16, 2014.

[10] Keun-Ho Lee, "A Method of Defense and Security Threats in U-Healthcare Service", Journal of the Korea Convergence Society, Vol.. 3, No. 4, pp. 1-5, 2012.

[11] Kim Ok-nam, "Comming U-Healthcare", LG Business Insight, 2009.

[12] Cho, Kyoung-Lae, Kim, Sang-Yoon, Kim, Jung-Han, Oh, Am-Suk, Kim, Gwan-Hyung, Jean, Jae-Hwan, Kang, Sung-In, "u-Healthcare Monitoring System Design using by Smartphone based on Bluetooth Health Device Profile", The Korean Institute of Information and Commucation Engineering, Vol. 17, No. 6, 2013.

[13] Dong-Min Shin, Dong-Il Shin, Dong-Kyoo Shin, "Development of u-Health Care System for Dementia Patients", The Journal of Korea Information and Communications Society, Vol. 38, No. 12.

[14] S. B¨orzs¨onyi, D. Kossmann, and K. Stocker. The skyline operator. In IEEE ICDE, pages 421 - 430, 2001.

[15] Gyenongtaek Kim, Jaepuo Park, "A Design for Anonymous Authentication protocol for user information protection in U-HealthCare Environment", Soongsil University, 2014.

[16] Kyoung-lae Cho, Sang-yoon Kim, Jung-han Kim, Am-Suk Oh, Gwan-Hyung Kim, Jae-Hwan Jean, Sung-in Kang, "u-Healthcare Monitoring System Design using by Smartphone based on Bluetooth Health Device Profile", Korea Institute of Information and Communication Engineering, Vol. 17, No. 6, 2013.

[17] D. Papadias, Y. Tao, G. Fu, and B. Seeger. An optimal and progressive algorithm for skyline queries. In SIGMOD, pages 467 - 478, 2003.

저자소개

허 윤 아(Yun-A Hur) [학생회원]

・2012년 3월 ~ 현재 : 백석대학교 정보통신학부 학생

<관심분야> : M2M, U-Healthcare, 이동통신보안

이 근 호(Keun-Ho Lee) [종신회원]

・2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
・2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
・2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호