# 원격 의료지원 서비스 환경의 공격 기법과 대응 방안

허윤아, 홍근목, 이근호
백석대학교 정보통신학부
e-mail: yj72722@bu.ac.kr, mok0524@naver.com, root1004@bu.ac.kr

# Attacks and Countermeasures of Telemedicine Support Services Environment

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

요 약

U-Healthcare는 언제 어디서나 환자의 생체 건강을 관리하고 유지할 수 있도록 하는 정보통신기술이다. U-Healthcare통신은 대부분 무선통신을 사용하여 검진 결과나 위급 시에 감지된 환자의 정보를 병원 서버로 전송한다. 이 때 U-Healthcare기기나 병원 서버에 악의적인 행위자가 DDoS공격을 하면 환자의 정보는 병원서버까지 전송되지 못해 병원의 도움을 받을 수 없는 상황이 발생된다. 이에 대응하기 위하여 본 논문은 U-Healthcare 통신 공격 패턴과 시나리오를 빅데이터로 구축한다. 그 후 악의적인 사용자가 U-Healthcare기기나 서버를 공격하면 DB와 연동하여 일치된 공격을 막을 수 있다. 앞으로 원격 의료 서비스에서 나타날 수 있는 보안 위협을 알아보고, 빅데이터를 활용하여 보안 위협에 대응할 수 있는 방법을 제안한다.

## 1. 서론

U-Healthcare는 환자의 생체신호 및 건강회복 및 유지 등 관리하기 위해 언제 어디서나 이용할 수 있는 정보통신 기술이다. U-Healthcare 서비스는 사회 경제적으로 의료비 절감과 시간 절약 등 가장 효과적인 대안으로써 많은 국가에서 추진하고 있다.

U-Healthcare 통신으로는 무선통신과 유선통신이 있다. 무선은 ZigBee, Bluetooth, Wireless USB, WiFi, RFID 등이 있고, 유선은 Serial, USB 등이 있다. 유선 통신 기술은 공격에 안전하지만 무선 통신 기술에서는 보안의 한계가 있다. U-Healthcare기기에서 무선통신을 통해 DDoS 공격을 당하게 된다면 환자 정보를 얻을 수도 있지만 환자가 위급 시에는 감지된 환자의 상태가 병원의 서버에 전송이 되지 않는 위험한 경우가 발생될 수 있다. 이처럼 원격 의료에서 보안을 대처하지 않으면 나타날 수 있는 위협에 대한 대응 방안이 필요하다.

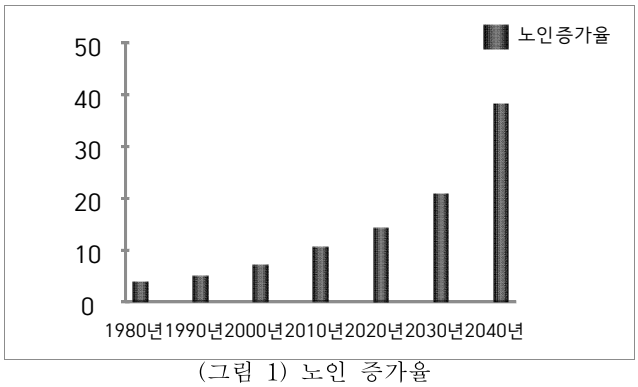
대응하기 위해 시스템을 공격하는 여러 기법과 그에 대한 대응 방안을 빅데이터에 저장한다. 저장된 빅데이터는 U-Healthcare기기와 접목하여 보안장비 및 보안솔루션으로부터 수집 된 다양한 로그를 분석하고 보안시나리오 기반 상시 모니터링을 통하여 보안사고 방지 및 침해에 대응한다.

## 2. 관련연구

### 2.1 U-Healthcare

U-Healthcare는 언제 어디서나 이용할 수 있도록 정보통신기술을 기반으로 사용하는 보건의료서비스이다.

현대에 들어서면서 의학이 발달하고 생활수준이 높아지면서 사망률이 현저하게 줄었다. 또 매년 출산율은 감소하고 사망률은 떨어지면서 인간의 평균수명이 높아지고 있다. 그림 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.




(그림 1) 노인 증가율

이렇게 고령화 사회가 진행되면서 의료 시장은 자연스럽게 커질 것이고 노인들은 좀 더 편하게 진료 받기를 원하게 될 것이다.

U-Healthcare시장은 크게 만성 질환자 대상의 치료 중

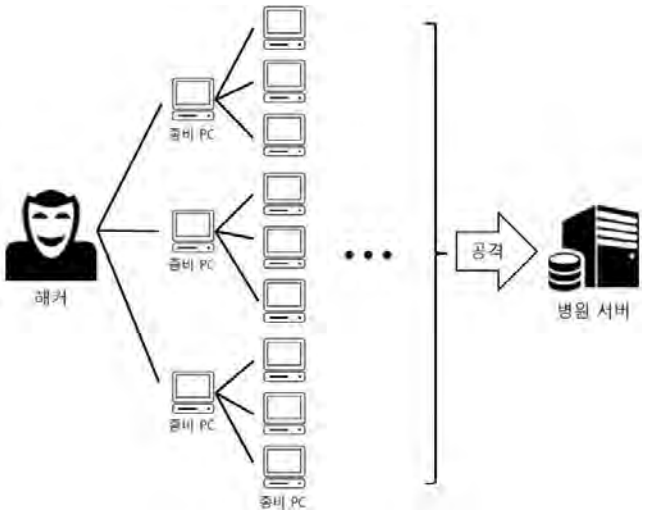
심 서비스 U-Medical, 고령자 대상의 U-Silver, 건강관리 서비스인 U-Wellness로 분류된다. 한국보건산업진흥원에 따르면 U-Healthcare 세계시장은 '09년 기준 1,431억불 규모로서 매년 15%이상 지속성장할 것을 전망하였으며, 분야별 평균성장률은 U-Silver(9.7%), U-Medical(15.0%), U-Wellness(17.9%)으로 나타났다. 특히 U-Wellness 시장은 법적 제약이 적어, 기존 체육시절을 증가하는 체육활동 관심 층과 연계시킬 경우 급속 성장 가능할 것으로 전망되었다[1].

### 2.2 빅데이터

빅데이터는 기존의 데이터 수집, 저장, 관리, 분석 역량을 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[2].

## 3. 보안위협

U-Healthcare은 무선 통신 기술에서는 보안의 한계가 있다. U-Healthcare기기 무선통신을 통해 전송되는 데이터를 DDoS 공격을 당하게 되면 위급한 환자의 정보가 병원 서버에 전송이 되지 않는 위험한 경우가 발생될 수 있다.




(그림 2) DDoS 공격 시나리오

그림2를 보면 수많은 좀비 PC가 한꺼번에 서버를 공격하게 된다면 공격대상인 서버나 U-Healthcare 기기는 다운이 될 것이다. 예를 들어 총 좀비 PC는 10000대라 하고 한 좀비 PC당 3개의 패킷을 보낸다 할 때 서버에 공격되는 패킷은 30000개가 되어 서버가 다운이 된다. 서버가 다운이 되면 위급 시 보내지는 패킷을 받을 수 없기 때문에 환자의 상태가 위험해진다. 이렇게 발생한 DDoS 공격 분석을 빅데이터를 이용하여 보안 위협을 줄인다.

이처럼 원격 의료에서 보안을 강화하지 않으면 나타날 수 있는 위협과 바이러스로 인한 진단오류발생으로 생명의 위협까지 느낄 수 있다. 그리고 RFID를 통해 과도한 개인정보 수집으로 프라이버시 침해 가능성 증가, 보안특성 의료정보에 대한 비밀성 위협, 의료정보에 대해 인가되지 않은 사람의 접근으로 개인 의료정보가 폭로되거나 조작될 수 있으며 내부자에 의한 개인 의료정보 유출사고가 일어날 수 있다[3].

## 4. 대응방안

지금까지 발생한 DDoS 공격을 빅데이터로 분석하여 원격 의료 서비스의 위협적인 보안에 대해 효율적으로 대응하기 위해 제안하고자 한다.


(그림 3) 빅데이터를 통한 DDoS 탐지

그림 3은 DDoS 공격 중이라고 가정한다. U-Healthcare 기기는 병원서버에 인가된 대상이로 지정해 놓는다. 근데 비인가 된 좀비 PC들의 패킷들이 병원서버로 들어왔다. 여기에 임계 기준(최대 허용값)을 20%로 잡는다면 모든 패킷 80%는 차단을 하고 20%는 허용을 한다. 즉 병원서버에 5번 연결 중 4번은 서버가 다운되었다고 뜰 것이고, 5번 연결해서 1번은 정상 통신이 된다.

또 다른 방법은 5초에 패킷이 3개 이상 들어올 시 공격 IP주소를 임시로 차단하는 방법도 있다.

원활한 원격 의료 서비스를 보안하기 위해 보안에 취약한 공격 패턴이나 시나리오에 대한 대응 기술을 수집하여 로그를 분석한다. 수집한 방대한 로그들은 데이터베이스에 저장한 후 하둡 분산시스템과 맵리듀스를 통해 하둡에 적재한다. 그 후 별도로 공격 시나리오가 적재된 데이터베이스와 비교하여 일치하면 데이터베이스에 저장된 대응 방안으로 자료와 원격 서비스를 보호한다.

## 5. 결론

U-Healthcare의 사용은 점점 보편화가 되어가고 있다. 원격으로 의료 서비스를 받아 시간과 돈을 절약해서 효율적로 건강관리를 받을 수 있는 편리한 장점이 있지만 U-Healthcare는 U-Healthcare 기기와 병원서버간의 데이터 전송을 통해 진료 서비스를 받는다. 악의적인 사용자가 U-Healthcare기기나 병원서버에 공격을 가하게 된다면 위급한 환자의 데이터를 받지 못하는 위험이 발생하게 되는 보안의 취약점이 있다. 또 네트워크에서 중요시 여기는 무결성, 기밀성, 가용성을 지켜야 한다는 것을 깨달았고, 이것을 지키기 위해서 다양한 기기들에 대한 보안 리스크 시나리오, 패턴 등 정보를 저장하기엔 방대하다는 점을 알았다. 그래서 무수한 공격을 대응하기 위해 빅데이터를 사용하고 분산처리를 통해 분석함으로써 빠르고 능동적으로 대처할 수 있도록 할 것이다. 본 논문에서는 빅데이터를 통해 원격 의료 서비스에 대한 보안 취약점을 진단하고 해결하기 위해 대응방안을 제안한다.

## 감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348)

## 참고문헌

[1] 배장은, 김승인, “여가만족도 향상을 위한 가상현실 게임과 u-Healthcare 기반의 피트니스 제안”, 한국연구제단, Vol. 15, No.1

[2] 이재성, 홍성찬, “기업의 빅데이터 적용방안 연구 -A사, Y사 빅데이터 시스템 적용사례에 대한 학술자료“, p.103-111

[3] 노시춘, 최진탁. “U-Healthcare의료정보 시스템 네트워크 보안프레임 워크 설계방법”, 융복합지식확회논문지, Vol.1, No1, p.31-37