U-Healthcare서비스의 보안 위협과 대응 방법

이근호
백석대학교 정보통신학부

A Method of Defense and Security Threats in U-Healthcare Service

Keun-Ho Lee
Division of Information Communication, Baekseok University

요 약 최근 IT기술의 발전에 따라 언제 어디서나 이용할 수 있는 U-Healthcare분야의 기술 개발이 빠르게 진행되고 있다. U-Healthcare 기술은 네트워크를 기반으로 하기 때문에 다양한 보안의 위협요소가 발생된다. 본 논문에서는 네트워크 공격 기반의 DOS/DDOS공격에 대한 위협을 알아보고, 기존 Detecting Early DOS/DDOS attacks through Packet Counting을 수정하여 U-Healthcare서비스 상황에 맞는 대응 기법을 제안한다.

• **주제어** : 융합, 유헬스케어, 보안, 방어, 위협

Abstract The fast-paced development in the field of U-Healthcare, which is available anytime and anywhere, is being underway in accordance with the development of IT technology. U-Healthcare technology has various security threats because it is based on network. The purpose of this paper is to examine the threats of DOS / DDOS attacks based on network attacks, and to propose the response technique that fit the situation of the U-Healthcare service by modifying the existing Detecting Early DOS / DDOS attacks through Packet Counting.

• **Key Words** : Convergence, U-Healthcare, Security, Defense, Threat

1. 서론

IT기반의 유비쿼터스 컴퓨팅 환경은 다른 기기와 장치간 융합, 정보의 개방성 및 공유성, 사용자 지향의 다양한 서비스 접근에 대한 확장성 등을 들 수 있다. 특히, 유비쿼터스 분야중 건강과 관련한 u-헬스케어는 윤택한 삶에 대한 사회적 욕구 증대와 IT기반 산업의 발전으로 인하여 의료 서비스 구축을 위한 정부의 전략적 정책과 많은 연구와 투자가 예상되고 있는 대표적인 서비스의 분야이다. u-헬스케어 서비스는 바이오 센서 및 스마트 의료 기기의 발달, 유무선 네트워크의 안정화, 의료 데이터의 교환 및 처리를 위한 표준 기술 등이 뒷받 침되면서 구체적인 서비스 실체화가 가속화되고 있다. u-헬스케어 서비스는 보다 정확하고 다양한 의료 서비스를 제공하기 위해 관련 기관 및 사용자간 의료 데이터의 교환과 공유를 필요로 한다. IT기술의 발전과 건강한 삶을 살기 위하여 스스로 관리하는 사람이 증가하면서 쉽게 언제 어디서나 이용할 수 있는 U-Healthcare분야가 급격하게 발전되어 가고 있다. 한국보건산업진흥원에 따르면 국내 U-Healthcare 시장 규모가 오는 2014년 약 3조 1000억원에 이를 것으로 추산했다. 이에 따라 지식경제부는 2009년부터 헬스케어 산업을 범정부 차원의 17개 신성장 동력에 포함시켰고 지난해부터 3년간 만성질환자 약 1만명을 대상으로 관리 시범사업인 스마트케어 프로젝트를

*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2012년 7월 16일 수정일 2012년 11월 15일 게재확정일 2012년 11월 25일

진행하고 있다. U-헬스케어 서비스는 타 유비쿼터스 컴퓨팅 기술 분야에 비해 다루어지는 정보 속성이 매우 민감하고 다양한 서비스 관계자 간 정보 공유가 빈번하게 이루어질 수 있다는 점에서 심각한 보안 위협이 존재한다. 의료정보가 불법적으로 노출 및 조작, 악용될 경우 개인 프라이버시 침해 및 안전하고 정확한 의료 서비스 위협 등을 초래할 수 있다. 이와 관련하여 최근 온라인상에서 개인 신상 정보 도용이나 매매 등으로 인해 피해 사례가 급증하고 있고 정부차원에서 이를 범죄 행위로 간주, 법적 제재 조치를 취한 사례는 프라이버시 보호의 중요성을 잘 나타내주는 예이다. 또한, 최근 미국에서 발생한 의료정보에 대한 해킹 및 악용 사례는 사회적으로 큰 반향을 일으켰을 뿐 아니라 의료정보보안에 대한 필요성을 사회적으로 재고시키는 계기가 되었다. 그러나 이러한 사회적 기여와 관련기술 개발에 비해 네트워크를 통해 사용자의 정보가 불법적으로 생성, 변경, 삭제되지 않도록 하는 보안 대응 방안 구축이 시급하다. 따라서 그에 따른 보안 위협을 빠르게 발견하고 대응할 수 있는 방안이 필요하다[1,2].

본 논문에서는 U-Healthcare서비스를 위한 네트워크인 WBAN(Wireless Body Area Network)의 보안위협을 시나리오를 제안하고 그에 따른 대응방안을 제안하고자 한다.

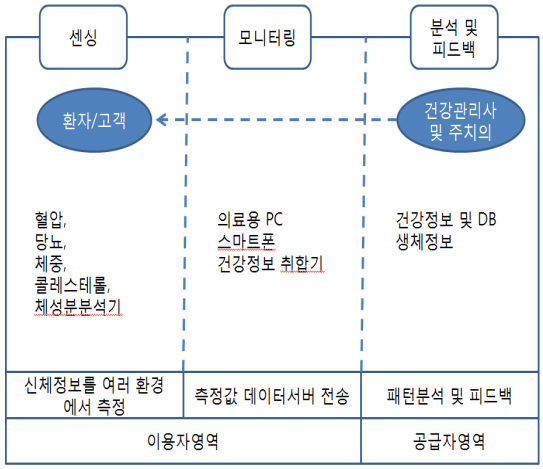
본 논문의 구성은 2장에서는 U-Healthcare 관련 연구로서 개념과 구성기술을 제시하고, 3장에서는 무선 신체영역 네트워크 환경에서의 U-Healthcare서비스의 보안위협을 분석하고 그에 따른 대응 방안을 제안한다.

2. 관련연구

2.1 U-Healhtcare

U-healthcare는 유비쿼터스 컴퓨팅기술을 보건의료에 접목한 것으로 “인체의 건강관련 정보를 시간과 공간의 제약 없이(Ubiquitous) 수집, 처리, 전달, 관리할 수 있게 해줌으로써 제공되는 원격지 의료 서비스”라고 정의한다. U-Healthcare가 완비된 이상적인 환경에서는 사용자들은 무자각 상태에서 자신의 건강상태를 실시간 하에 지속적으로 모니터링하고 가장 적절한 시점에 가장 적절한 조치를 취함으로써 자신의 건강상태를 최상으로 유지하는 것이 가능할 것으로 기대된다. 또한 이러한 이상적인 U-Healthcare 환경은 향후 도래할 노령화 사회 그리고 Well-Being을 추구하는 사회에서는 절실히 요청되는 환경이기도 하다[2,3].

Fig. 1은 U-healthcare 서비스에 대한 개념도 이다. Fig. 1에서 U-healthcare서비스는 센싱, 모니터링, 분석 및 피드백으로 구성된다. 센싱은 인체에서 발생하는 물리적, 화학적인 현상 변화를 감지하여 처리 가능한 전기적 신호로 변환하는 곳이며, 모니터링은 측정된 생체정보를 의미 있는 생체 신호 성분만을 선택하기 위한 필터링 처리와 의미 있는 정보로 만들기 위한 분석과정, 그리고 이를 시각화하기 위한 과정으로 구성된다. Fig. 1에서 분석은 단순히 현재 상태를 모니터링 할 뿐만 아니라, 장시간에 걸쳐 측정된 데이터로부터 건강상태, 생활패턴 등을 나타내는 새로운 건강자료를 분석하는 과정이고 피드백은 장시간에 걸쳐 파악된 건강 기지선이나 생활의 변화를 사용자의 행동변화, 경고등으로 사용자에게 제공하는 과정이다[4].



[Fig. 1] Concept of the U-healthcare Service

2.2 WBAN

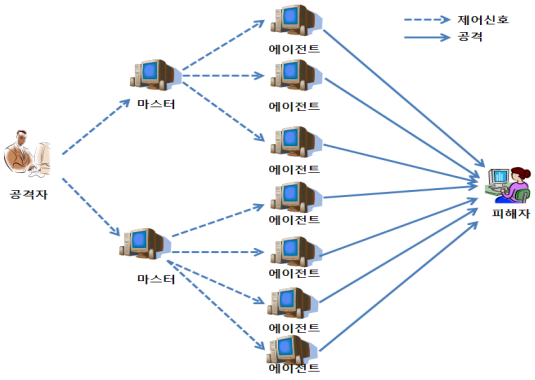
언제어디서나 인간 중심의 맞춤형 서비스를 제공받을 수 있는 유비쿼터스 환경을 구축하기 위해서 WBAN은 인간으로부터 정보를 수집하고, 인간에게 최적의 서비스를 제공하는 대표적인 응용기술이다. WBAN은 사람이 착용하는 옷이나 인체의 여러 디바이스 간을 연결하여 통신할 수 있는 새로운 유형의 무선 네트워크로써 인체를 중심으로 센서, 통신, 구동체 등의 다양한 기술이 복합적으로 적용된 IT-BT-NT의 기술 융합 및 융합 산업 활성화에 필수적인 요소로 각광 받고 있다.

현재 IEEE 802.15.6 TG BAN에서 주파수 분배, PHY/MAC및 응용 서비스 등을 중심으로 표준화가 활발히 진행되고 있다. WBAN은 3M 이내의 통신거리와 최대 10Mbps의 전송 속도를 요구하며, 가능한 주파수 대역으로 의료서비스 주파수인 MICKS(Medical Implant Communication Service), MEADS(Medical Data Service), WATS(Wireless Medical Telemetry Service) 등과 저 전력 주파수 인 ISM(Industrial, Scientific & Medical), UWB(Ultra Wide Band)대역이 고려되고 있다. 특히, WBAN은 사람의 생명에 직접적인 영향을 줄 수 있기 때문에 MEC, SAR등을 고려한 높인 신뢰성과 안전성이 요구되며, 이를 위한 토폴로지는 멀티홉을 지원하고, 암호화 및 인증 등의 보안 기술과 초저전력 네트워크 및 통신 기술이 요구된다[5,6].

3. U-Healthcare 보안위협

U-Helathcare 서비스에서의 다양한 기술적 보안 위협요소가 존재한다. 그중에서는 가장 중요한 기술적 보안 위협요소는 시스템간의 정보 공유를 통한 정보의 유출이 될 것이다. 정보의 유출시 민감한 개인정보의 유출로 인하여 개인의 프라이버시의 심각한 문제를 초래할 수 있다. 이러한 개인정보에 대한 민감한 정보의 유출이 가장 심각한 보안위협으로 대두되고 있다. 개인정보의 남용에 관한 '빅 브라더(big brother)' 문제와 같은 프라이버시 보호 의식이 확산되면서 u-헬스케어 분야에서도 최근, 데이터 보호 및 프라이버시 보호 문제를 중요 이슈로 간주, 법제도적, 기술적측면 등 다각적 차원에서 대응 방안을 강구하고 있다. 유무선 네트워크 기반 서비스에서 발생 가능한 보안상 취약점 및 공격이 u-헬스케어 환경에서도 유사하게 발생될 것이다. 따라서, 기반 네트워크 및 시스템에 대한 안전성, 신뢰성 보장 및 데이터 보호에 대한 보안 위협요소가 대두될 것이다. 대부분의 병원에서는 요청자의 단순 서비스 요청에 관한 로그만 남길 뿐, 데이터 습득 이후 활용, 폐기 등에 관한 의무사항 준수에 관련한 감사 체계가 부재한 상황이다. 이는 최근 심각한 보안 취약점으로 거론되고 있는 내부자에 의한 정보 유출의 위험성을 가중시킬 수 있다. 이러한 개인정보 유출과 기록에 대한 조작은 개인에게 상당히 치명적인 요소로 작용할 수 있다. 따라서, 신체영역관련 WBAN과 DDoS 공격에 대한 보안 위협요소를 통한 대응 방법을 제안한다.

무선네트워크 환경에서는 유선네트워크 환경에서보다 높은 보안 요구사항이 필요하다. 또한 개인의 의료정보를 취급하는 WBAN 상황에서는 보다 높은 보안 위협이 존재하기에 WBAN의 네크워크 상황에서 DDOS공격의 위협을 분석하고 이를 해결하기 위한 대응 방안에 대해 기술하고자 한다. DDOS공격은 TCP/IP 프로토콜의 보안 취약점을 이용하여 정상적인 서비스의 지연이나 시스템을 마비시키는 공격이다. 일반적인 DDOS 공격 구조를 Fig. 2에 나타내었다. DSoS공격에는 많은 다양한 공격기법이 존재하지만, 그중 Foolding공격, Connection 공격, Application 공격의 세분야의 공격에 대한 위협 시나리오를 도출하여 각 도출된 위협 대응을 위한 방법을 제안하였다[7,8,9,10].



[Fig. 2] Architecture of the DDOS Attacks

DDOS공격은 여러 가지로 구분되지만 본 논문에서는 Flooding, Connection, Application 3가지 공격을 기반으로 제안하고자 한다.

- Flooding 공격

Floodiong 공격은 정상 패킷과 동일한 패킷을 무작위로 전송하여 Target 시스템의 CPU, 메모리 등을 고갈 시키고 네트워크의 병목현상을 발생시켜 정상적인 서비스 제공을 방해하고 시스템의 과부하를 유발시키는 형태의 공격방법이다. 의료데이터 서버에 대한 공격의 시나리오가 가능하다. 특히, 센싱을 통한 임의적인 공격으로 인하여 의료데이터 서버가 정상적으로 작동하지 못하도록 공격이 가능하다.

- Connection 공격

Connection 기반 공격 중에 HTTP 공격의 경우에는

여러 대의 PC에게 동일하게 접속을 요청하여 서버의 HTTP처리 커넥션 용량을 초과시켜서 정상적인 HTTP 연결을 방해하는 형태의 공격이라고 할 수 있다. 마찬가지로 과다 TCP 커넥션 형태의 공격도 정상적인 TCP연결 가능 수치를 초과하는 연결을 시도하도록 하여 서버의 정상적인 연결 시도를 방해하는 형태의 공격이라고 할 수 있다. 센싱의 의료장비가 다양한 의료정보 서비스를 사용하는 것으로 가장하여 연결을 시도할 때 마다 각 세션의 정보가 생성이 되므로 많은 부하가 발생하여 네트워크의 서비스 제공을 마비시키는 기능이 가능하다.

- Application 공격

Application 기반 공격은 음성진료서비스를 위한 VoIP를 이용할 경우 SIP 단말의 등록을 위한 REGISTER패킷을 과도하게 요청하는 REGISTER storm 공격, 통화 시도를 과도하게 요청하는 INVITE공격, BYE공격 등이 있으며 기타 FTP공격, Email 스팸, DNS공격, DHCP 리퀘스트 공격, SQL공격, Netbios공격, RPC공격 등 각종 프로토콜의 취약점을 활용한 다양한 공격형태가 가능하다. 특히 센싱에서 사용하는 단말기의 애플리케이션의 취약점을 통한 서버에 대한 공격과 단말에 대한 정보를 스캐닝할 수 있는 공격이 존재한다.

4. U-Healthcare DDOS공격 대응방법

기존에 나와 있는 Detecting Early DOS/DDOS attacks through Packet Counting 알고리즘을 이용하여 U-Healthcare서비스 환경에서 일어날 수 있는 네트워크 공격에 대한 대응방법을 제시하고자 한다.

Detecting Early DOS/DDOS attacks through Packet Counting 알고리즘은 네트워크 패킷의 데이터를 볼 필요가 없으면서, 구현 복잡도를 최소화하고 오탐률을 줄이기 위해 적용 시스템의 특성에 맞게 자동 임계치를 설정하는 알고리즘이다. 이 알고리즘을 U-Healthcare 환경에 적합하도록 알고리즘을 수정하여 대응방법을 제안하였다.

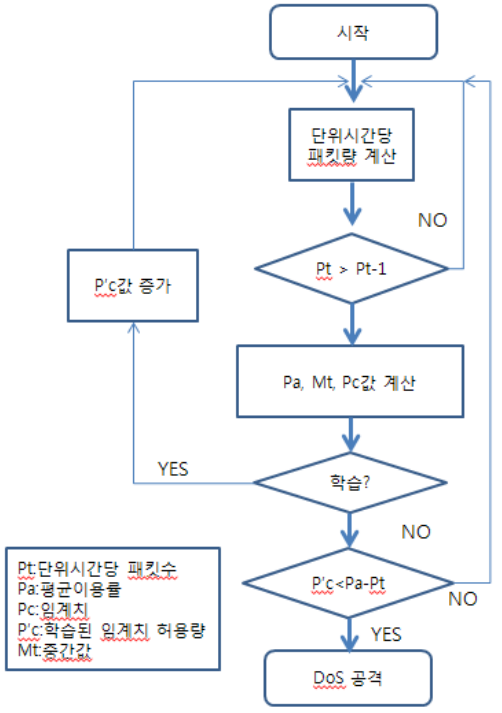
[식 1]

---

if {학습된 임계치 허용량 P'c <
[(특정포트의 평균 이용률 Pa) -
(특정포트의 단위 시간당 패킷수의 중간값 Mt)
]
},
Then Dos 공격 판정

이 알고리즘은 일정기간 학습을 거치는데 학습기간동안 시스템은 각각 임계치의 허용량을 점차적으로 증가시켜 학습을 거친 후 학습된 임계치 허용량을 바탕으로 [식 1]과 같이 DOS공격을 탐지하며, 사용자의 정상 트래픽에 대한 오탐율을 줄일 수 있다. 이러한 [식 1]은 다음과 같은 알고리즘으로 진행된다[11].

뿐만 아니라 지능형 공격에도 대응할 수 있기 때문에 U-Healthcare 장비에 이식할 경우 홈AP, 공용 AP환경에서의 다양한 공격도 효율적으로 대응 할 수 있다. U-Healthcare서비스 시장이 매년 확대 되고 있는 지금, 이러한 공격 대응 알고리즘을 이용하여 개인의 소중한 정보를 보호할 수 있을 것으로 기대 된다. 아울러 검출된 알고리즘을 기반으로 기본적인 Flooding공격과 Connection 공격, Application공격에 대응 방법으로서 단위시간당 패킷량의 계산을 통한 값을 비교하여 평균 이용율과 임계치의 특정값을 통하여 자체적인 학습이 진행이되어 패킷의 이용률이 늘어날 경우 이에 대한 사전탐지를 통해 센싱정보에 대한 서버에서의 안정성을 높일 수 있다.



[Fig. 3] Flowchart of the Attack Detection

4. 결론

본 논문에서는 IT기반의 빠른 기술의 발전에 따른 U-Healthcare 시스템에 대한 내용과 발생가능한 보안 위협요소를 도출하여 위험성이 예측이 되는 DDoS 공격에 대한 위협요소를 인체 영역 네트워크(WBAN)환경에서의 서비스의 보안 위협 및 Detecting Early DOS/DDOS attacks through Packet Counting 알고리즘을 이용한 대응 방안을 제안하였다. 이 공격 탐지 방법은 간단하고 오탐률이 적을 뿐만 아니라 지능형 공격에도 대응할 수 있기 때문에 U-Healthcare 장비에 이식할 경우 홈AP, 공용 AP환경에서의 다양한 공격도 효율적으로 대응 할 수 있다. U-Healthcare서비스 시장이 확대되고 규모가 커져가고 있는 상황에서 DDoS 공격을 예측할 수 있는 알고리즘을 제안하여 안정성을 높여 개인의 소중한 정보와 시스템의 안정성을 높일 수 있을 것으로 기대된다.

향후 연구로는 DDoS공격에 대한 U-Healthcare 시스템에서의 공격유형의 다양한 변화에 대한 서비스 시나리오를 통한 위협요소의 도출을 통한 대응할수 있는 기법의 연구를 통해 좀더 U-Healthcare의 시장 확대에 기여할 수 있는 네트워크 공격의 안전성 확보 기술이 요구되어 진다.

REFERENCES

[1] J.E. Song, S.H. Kim, M.A. Chung, K.I. Chung, “Security Issues and Its Technology Trends in u-Healthca”, Electronics and Telecommunications Trends, Vol. 22, No. 1, pp. 119-129, 2007.

[2] H.C. Kim, J..M. Kang, “Prospect and Trend of U-Healthcare Technology”, Communications of The Korea Information Science Society, Vol. 26, No. 1, pp. 38-45, 2008.

[3] Dongsoo Han, Sunjoon Park, Smita Kurkuri, “An Evolving Mobile E-Health Service Platform,” 1st International Conference on Design Science Research in Information Systems and Technology, 2006.

[4] Bong-Keun Lee, Yoon-Su Jeong, Sang-Ho Lee, “Design of Personal Information Security Model in U-Healthcare Service Environment” Journal of the Korea society of computer and information, Vol. 15, No. 1, pp. 189-200, 2011.

[5] Application Class Structure, IEEE802.15-15-08-0096-00-0006

[6] Frequency band consideration of SG-MBAN, IEEE 802.15-07-0640-10-0ban

[7] Sun Young Kim, “Algorithm Attack Detection using Statistics Scheme and Pattern Matching”, Chungbuk University Ph.D Paper, 2006.

[8] Eun-Hee Jeong, Byung-Kwan Lee, “A IPCW-IDS Design of DDoS attack detection scheme.” THE JOURNAL OF KOREA INFORMATION AND COMMUNICATIONS SOCIETY“, Vol. 35, No. 10, pp. 1443-1450, 2010.

[9]J Charzinski “TTP/TCP connection and flow characteristics” Performance Evaluation, pp. 149 - 162, 2000.

[10] H Sengar, D Wijesekera, H Wang, S Jajodia “”VoIP Intrusion Detection Through Interacting Protocol State Machines”” Dependable Systems and Networks, 2006.

[11] Tae-Won Kim, Jae-Il Jung, Joo-Young Lee, “DoS/DDoS attacks Detection Algorithm and System using Packet Counting”, Journal of the Korea Society for Simulation, Vol. 19, No. 4, pp. 151-159, 2010.

저자소개

이 근 호(Keun-Ho Lee) **[종신회원]**

- 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 전임강사
- 2010년 9월 ~ 현재 : 백석대학교 쿰인성개발원 팀장

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