Journal of the Korea Academia-Industrial cooperation Society
Vol. 12, No. 7 pp. 3191-3196, 2011

DOI : 10.5762/KAIS.2011.12.7.3191

스마트 홈의 위험수준별 침입 트래픽 분석을 사용한 침입대응 기법에 대한 연구

강연이[1*], 김황래[1]
[1]공주대학교 컴퓨터공학부

A Study on Intrusion Detection Techniques using Risk Level Analysis of Smart Home's Intrusion Traffic

Yeon-i Kang[1*] and Hwang-Rae Kim[1]
[1]**Division of Computer Engineering, Kongju National University**

요 약 스마트 홈 시스템은 주거 생활의 편리함을 위해 새롭게 신축되는 건물에 대부분 설치되고 있다. 그러나, 스마트 홈 시스템이 보편화되고, 확산 속도가 빨라짐에 따라 해커들의 홈 네트워크 시스템 공격이 증가할 것으로 예상된다. 본 논문에서는, 스마트 홈의 위험수준별 침입 대응을 하기 위해 유선 네트워크와 무선 네트워크에서 발생한 침입 사례와 공격이 발생할 수 있는 가상 상황을 시나리오로 만들어 데이터베이스로 구축하였다. 이것을 기반으로 보안에 취약한 스마트 홈 사용자들에게 실시간으로 불법 침입 트래픽을 찾아내 침입 사실을 알려주고 공격을 차단하는 침입대응 알고리즘을 설계하였다.

Abstract Smart home system are being installed in the most new construction of building for the convenience of living life. As smart home systems are becoming more common and their diffusion rates are faster, hacker's attack for the smart home system will be increased. In this paper, Risk level of smart home's to do respond to intrusion that occurred from the wired network and wireless network intrusion cases and attacks can occur in a virtual situation created scenarios to build a database. This is based on the smart home users vulnerable to security to know finding illegal intrusion traffic in real-time and attack prevent was designed the intrusion detection algorithm.

Key Words : Smart home system, Attack, Intrusion, Traffic

1. 서 론

스마트 홈은 관리실에서 가정의 스마트 홈까지는 유선으로 연결되어 제어되고, 가정에서는 댁내에 설치된 홈 게이트웨이와 외부에서 모바일을 통해 제어가 무선으로 이루어진다고 볼 수 있다. 유선 네트워크에서도 많은 피해를 발생시키는 해킹 공격이 빈번하게 발생하는 상태인데, 무선 네트워크가 결합되어 제어하는 홈 네트워크는 유선 네트워크에서 내재된 모든 위협과 무선 네트워크에서 발생할 수 있는 해킹 위협까지 가중되었다고 볼 수 있다.

유선 네트워크로 내부 서버 시스템에 침입하게 되면 통과하는 경로 지점마다 방문한 사람의 로그가 기록되고 있지만 무선 네트워크의 접근은 방화벽, IDS, IPS, 웹 필터 등 보안 솔루션들을 우회하여 홈 네트워크에 설치된 가전제품에 직접 접근하여 공격할 수 있다.

기존 논문에서는 관리 서버를 관리하는 관리실에서 스마트 홈에 접근하는 위험 트래픽을 분석하여 위험한 공격이 발생한 상황을 사용자의 모바일로 통보해주고 차단 작업을 관리실에서 통합관리 하도록 되어 있었다[4].

*교신저자 : 강연이(kyl7249@nate.com)
접수일 11년 05월 06일 수정일 (1차 11년 06월 15일, 2차 11년 07월 06일) 게재확정일 11년 07월 07일

이렇게 관리실에서 총괄하여 관리하게 되면 총괄 관리에 대한 정밀한 관리가 이루어질 수 없을 수도 있고, 요즘 빈번히 발생하는 DDoS 공격으로 관리실의 서버와 스마트 홈에 설치된 가전제품들의 위험 트래픽 분석 및 통보가 어렵게 되는 상황이 발생할 수 있다.

본 논문에서는 가정에 있는 스마트 홈에 위험 트래픽인지 정상적인 트래픽인지 판별하도록 하는 프로그램을 내장시켜서 위험 트래픽이 접근하고 있는 상황을 스마트 홈에 게이트웨이로 보여주고 모바일로 통보해주므로 보안 지식이 없는 일반 사용자들도 실시간으로 발생하는 위협에 대한 조치를 취할 수 있도록 하고, 정밀한 분석은 관리실의 관리 서버가 수행하도록 하는 이중적인 보안 대책으로 보안 점검할 수 있는 알고리즘을 제안하였다 [1,2,4].

본 논문의 구성은 다음과 같다.

2장은 유선·무선 네트워크 침입 경로 분석 및 알고리즘을 구성을 위해 스마트 홈에 설치된 가전제품들을 위험수준별로 분류하는 작업과 보안점검 알고리즘의 구성에 대하여 기술하였다.

3장은 스마트 홈의 위험수준별 침입 트래픽 분석을 통한 침입대응 방안에 대한 알고리즘을 설계하였고, 스마트 홈에 설치된 가전제품들을 노드로 배치하고 AP를 접근하는 비정상적인 트래픽 수를 누적하여 해킹 감지 결과로 평가하였다.

4장에서는 결론 및 향후 연구방향을 기술한다.

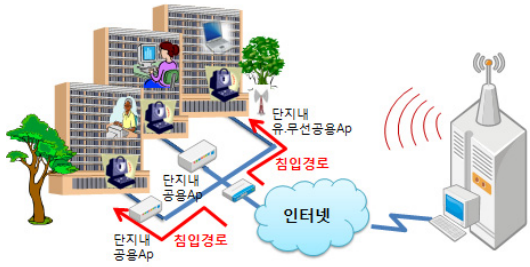
2. 관련 연구

2.1 유선·무선 네트워크 침입 경로 분석

유선 네트워크망은 가정으로 설치된 전용선을 컴퓨터에 연결하여 사용하는 경우가 가장 일반적인 네트워크 사용통로로 유선으로 접근하는 접근자만 관리하면 되었다. 아파트나 빌딩 같은 경우는 단지내에 들어오는 인터넷 공용AP에 연결하여 사용하기 때문에 관리할 곳은 한 개의 경로만 관리하기만 하면 되었다. 가전제품에 연결된 상태가 아니기 때문에 네트워크에 DDoS 공격 같은 것을 받아도 개인용 컴퓨터에 미치는 영향은 인터넷 접근만 불가능할 뿐 그렇게 크게 타격을 받지 않는다.

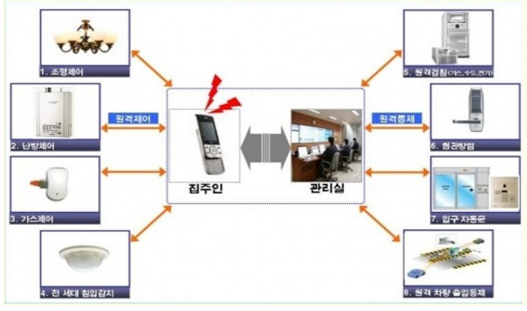
요즘 개인이 사용하는 인터넷망도 유선·무선이 결합되어 가정내에서도 무선인터넷 공유기 지원 AP(Access Point)를 사용하기 때문에 가정에 사용하는 컴퓨터에도 무선 접속을 활용하여 인터넷망을 사용하고 있다. 유선 접속에 무선 접속까지 결합되었기 때문에 유선 침입 경로외에 무선 침입 경로까지 공격으로부터 대비해야 하는 문제가 가중되었다.

가전제품에 연결되지 않고 단지 컴퓨터에만 네트워크망을 연결해서 사용하기 때문에 PC에만 침입을 방지할 수 있는 방화벽을 설치한다면 개인적인 피해가 그렇게 크게 작용하지 않고 있다는 것이다.



[그림 1] 아파트 단지내 유·무선 네트워크 구성도
[Fig. 1] Apartment wired·wireless network configuration

유선 네트워크의 해킹경로는 컴퓨터에 연결된 전용선이 전부였으나 요즘은 무선망까지 추가되어 그림 1에서 보는 것처럼 무선으로 침입할 수 있는 경로까지 생각을 해야 한다. 스마트 홈이 설치되지 않았을 때는 개인용 컴퓨터에 보안설정만 하면 보안이 유지되었다[2,3].



[그림 2] 스마트 홈 구성도
[Fig. 2] smart home configuration

스마트 홈이 점차 활성화되고 있는 현시점에서 댁내망은 PC뿐만 아니라 홈오토메이션, 가정에 모든 가전제품(홈시어터, 냉장고, 세탁기 등), 냉·난방 온도조절 및 ON/OFF 제어기, 가스제어시스템(감지/제어/차타기 등), 도어락 제어를 포함한 방범시스템, 욕실 냉·온수의 온도조절 및 ON/OFF, 조명 ON/OFF 제어기, 아파트 단지내 진·출입 및 주차관리 시스템 등 다양한 기기들로 구축되기 때문에 외부의 해킹 공격형태 및 피해 양상 역시 유선에서 무선까지 매우 다양하게 나타날 수 있다.

스마트 홈 환경에서는 가스누출, 온도조절 오작동 과 급격한 온도 상승으로 화재 유발과 분산 서비스 거부 공격(DDoS)으로 네트워크 마비로 스마트 홈 시스템 제어 불능 등 예기치 못한 상황이 발생할 수 있다.

실제로 외국에서 스마트 홈이 설치된 아파트 단지 내에서 멀리 떨어지지 않은 맞은편 아파트 옥상에서 노트북에 설치된 해킹 프로그램으로 전원 ON/OFF를 마음대로 제어하여 장난을 치는 해킹 사고가 있었다. 스마트 홈에 거주하는 사용자들은 이유도 모르고 전원이 ON/OFF 되는 상황을 지켜보고만 있어야 했고 해커는 장난치듯이 몇 분 동안 이 작업을 하였다. 해커는 이 작업을 하기 위해 미리 관리실에서 가정으로 통하는 유선에 백도어로 사용될 무선 AP와 그 AP를 통해 유선으로 통하는 트래픽을 분석하기 위해 정보 수집을 위해 소형 PDA을 연결해 놓고 무선으로 트래픽을 전달 받았다. 맞은편 아파트에 있는 해커는 전원 ON/O FF하는 코드를 알아내어 스마트 홈에 전원을 마음대로 ON/OFF 조작하는 사례가 있었다. 단순한 전원 ON/OFF 하는 조작하는 해킹사고였다고는 하나 그 이상의 해킹 사고를 유발할 수 있다고 생각된다[1,2].

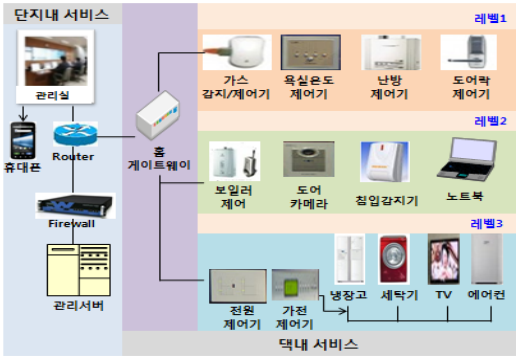
그러므로, 기존의 관리자 중심의 보안 서비스로는 보안에 아무런 지식이 없는 일반 사용자들이 사용하는 스마트 홈 시스템에 정밀한 보안을 유지하는 것은 어려운 실정이다.

스마트 홈 게이트웨이를 통해서 댁내에 설치된 가전제품을 불법 접근할 수도 있고, 중간에 설치된 방화벽, IDS, IPS, 웹 필터 등 보안 솔루션들을 우회하여 무선접속을 통해 스마트 홈 가전제품을 직접 접근하여 공격할 수 있다[3,4].

이와 같은 침해에 기존의 보안시스템으로는 스마트 홈 시스템에 적절히 침입에 대응하는 것이 부족한 상태이기 때문에 침해에 대응할 수 있는 침입감지 및 차단시스템이 절실히 필요한 상황에서 좀 더 체계적인 보안을 강화할 수 방안을 찾고자 댁내에 스마트 홈에 가전제품별 보안을 강화할 수 방안을 찾고자 본 논문에서는 유·무선에서 침입할 수 있는 경로를 분석하여 대응방안을 연구하였다.

2.2 스마트 홈 시스템의 위험수준별 분류

본 논문에서는 침입 트래픽을 분석하고 대응하기 위해 스마트 홈에 설치되는 가전제품들을 해킹 공격을 당했을 때 인간에게 피해를 주는지에 따라서 위험수준에 따라 먼저 제품들을 분류하였고, 사전에 위험수준에 따라 데이터베이스를 구축하기 위해 위험 수준별 레벨1~레벨3까지 분류했다.



[그림 3] 위험수준에 따라 스마트 홈 가전제품 분류
[Fig. 3] Smart home classification according to risk level

위험도가 가장 높은 제품들을 레벨1로, 사용자에게 피해는 없지만 중간 경유지 역할을 할 수 있는 제품들을 레벨2에, 단순히 ON/OFF 역할만 가지고 작동하는 제품들을 레벨3으로 분류될 수 있도록 분류 기준을 정했다.

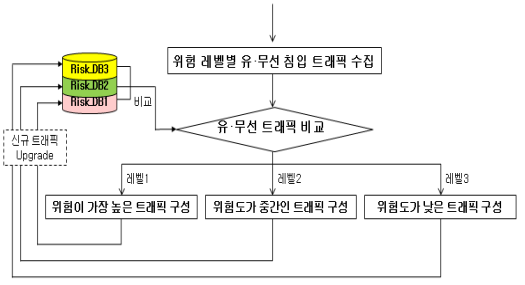
침입대응 알고리즘은 그림3에 레벨별로 접근하는 트래픽 분석을 기반으로 위험수준을 결정하였다.

사전에 침입 트래픽 분석을 위해 초기단계이지만 이제까지 유선에서 발생한 침입 트래픽을 데이터베이스로 구축하는 작업을 수행해 놓았다[4,5].

2.3 보안점검 알고리즘의 구성

스마트 홈에 설치된 가전제품을 위험도에 따라 분류하여 배치하였고, 사전에 유선·무선에서 발생한 해킹 사례를 기반으로 초기 데이터베이스 자료로 해킹 트래픽을 위험수준별로 구분하여 데이터베이스로 구축하여 놓았다.

트래픽 분석은 위험수준에 따라 레벨별 접근하는 트래픽 중에서 정상 트래픽을 먼저 분류해 내고 비정상적인 트래픽이라고 인정되는 것은 데이터베이스와 상호 연동하여 분석 작업을 정밀하게 구성하였다.



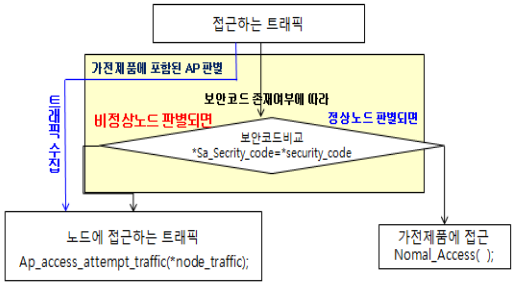
[그림 4] 유·무선 침입 트래픽 수집, 분석 위험수준별 Database 구축
[Fig. 4] Wire·wireless intrusion traffic collection, analysis risk level Database building

침입 트래픽 파일에서 위험 명령어를 찾아내기 위해 침입한 트래픽을 어셈블리 프로그램으로 구성 분석 작업을 실행하여 비정상적인 설정 지시를 내리는 명령, 메모리 오버플로우 유발시키는 명령, 가전제품의 오동작을 유발시키는 명령, 삭제를 유발하는 명령 등 위험 명령들을 찾아내도록 알고리즘을 구성하였다[6,7].

3. 침입대응 알고리즘의 설계 및 성능 평가

3.1 침입대응 알고리즘의 설계

초기 단계에서 접근하는 트래픽에 담겨있는 보안코드를 비교하여 정상적인 접근인지, 비정상적인 접근인지를 판별하는 작업을 수행하는 작업을 한다.

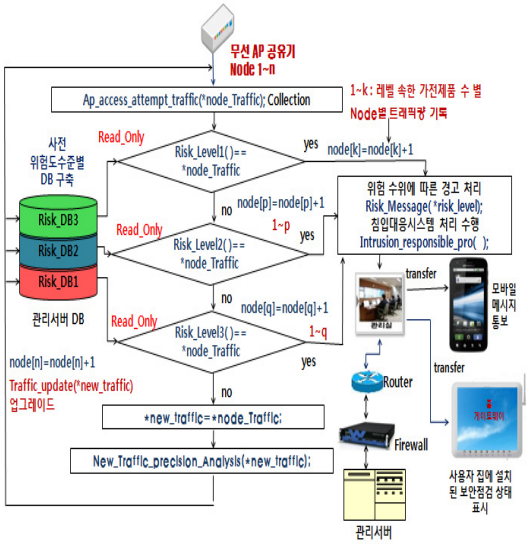


[그림 5] 정상접근인지 비정상접근인지 판별
[Fig. 5] normal or abnormal approach determination

다음 단계로 비정상적인 접근으로 판별되는 트래픽들을 수집을 하고 트래픽을 가전제품의 위험수준에 따라 레벨별로 분류하여 데이터베이스로 구축해 놓은 정보를 기반으로 그림 6 알고리즘이 수행되도록 구성하였다.

그림 6은 스마트 홈의 각각의 가전제품으로부터 트래픽을 수집하는 작업을 Ap_access_attempt_traffic(*node_traffic); 함수로 했으며, 수집된 *node _traffic을 먼저 보안점검 프로그램을 통해 여러 가지 위험을 유발하는 명령들을 찾아내고 데이터베이스에 구축된 트래픽과 같은 침입 트래픽이 있는지 비교(Risk_Level1()==*node_traffic)를 레벨별로 수행하고 해당 레벨에 침입 트래픽이 발생한 경우 관리서버로부터 침입차단을 Intrusion_responsible_ pro(); 함수로 수행하도록 하였다. 비정상적인 트래픽 침입 사실을 댁내 보안점검 상태 시스템에 설치된 표시기에 표시하고 사용자의 모바일로 침입 사실 Risk_Message (*risk_level) 함수로 알려준다.

그리고 각각의 레벨별 발생하는 트래픽의 양을 가전제품의 수에 따라 누적하여 node[k]=node[k] +1;, node[p]=node[p]+1, node[q]=node[q]+1, 새로운 트래픽 양을 누적 node[n]=node[n]+1 하여 위험도를 차트와 트래픽 양을 그림 7에 스마트 홈의 게이트웨이 표시기부분에 표시하도록 하여 사용자가 표시기를 통해 실시간으로 확인할 수 있도록 하였다.



[그림 6] DB에 구축된 침입 트래픽과 실시간 수집된 트래픽 비교 분석 침입 판별
[Fig. 6] DB on built attack traffic and collected real-time traffic comparative analysis to determine

그림 7은 스마트 홈 게이트웨이 표시기 부분에 위험수준을 표시해 주는 부분으로 보안에 아무런 지식이 없는 스마트 홈 사용자가 실시간으로 댁내 설치된 스마트 홈 가전제품에 접근 하는 비정상적인 트래픽 수를 그래프와 수치적으로 확인해 볼 수 있도록 하였고, 위험 수위가 높을 때는 강제로 OFF할 수 있도록 했고, 초기설정 작업을 통해 사용자가 기본 설정을 하도록 하였다.

위험수준별 구성한 데이터베이스와 일치하는 비정상적인 트래픽을 발견시 위험수준별로 경고 처리와 침입대응 시스템별로 처리를 수행하도록 하였고, 데이터베이스에 저장된 트래픽과 일치하지 않을 때는 새로운 트래픽으로 분류하여 다시 분석 작업을 수행하고 새로운 해킹 트래픽으로 인지시키고 데이터베이스에 업그레이드 하였다.

[그림 7] 댁내에 설치된 스마트 홈 게이트웨이에서 위험수준 표시
[Fig. 7] home on built smart home gateway risk level display

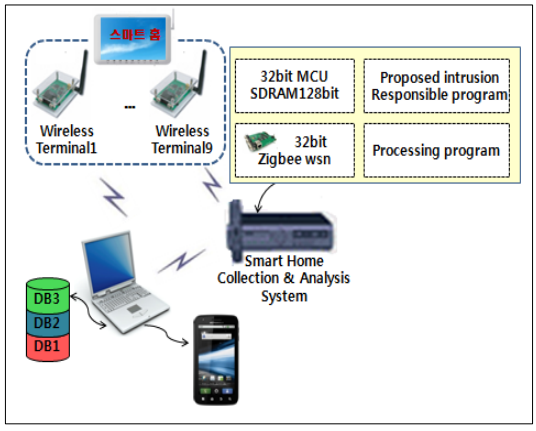
3.2 침입대응 알고리즘 실행과 성능 평가

스마트 홈에 설치된 제품들을 실험을 위해 그림 8에서 볼 수 있듯이 노드 1~9까지로 배치하였다.

[그림 8] 스마트 홈에 실험을 위해 센서노드 배치
[Fig. 8] Smart home for experiments placed the sensor nodes

각각의 노드에 무선으로 접근하는 트래픽을 노드별로 트래픽을 수집하여 분석을 위해 데이터베이스에 저장된 위험수준별 트래픽과 비교하여 비정상적인 트래픽을 찾아내도록 하였고, 새롭게 발생한 트래픽은 분석 작업을 다시 정밀하게 하여 새로운 위협 트래픽으로 분류하여 데이터베이스로 업그레이드 하도록 하였다.

실험을 위해서 실제 스마트 홈에 가전제품을 배치해 놓고 실험을 할 수 없는 어려운 환경이라서 가전제품 대신 무선센서노드를 배치하였다.



[그림 9] 침입대응 시스템의 하드웨어 구성도
[Fig. 9] Hardware configuration of Intrusion system

본 논문에 실험을 위해 Wireless Terminal을 9개 배치하고 Wireless Terminal로부터 트래픽을 수집하여 분석하기 위해 Smart Home Collection & Analysis System을 구성하였고, Smart Home Collection & Analysis System은 기본 시스템(32bit MCU, 128bit SDRAM)과 제안한 침입대응 프로그램을 수록하여 구성하였고, 데이터베이스 구축 스마트 홈 서버로 노트북(Samsung Sense)을 사용하였다.

무선으로 접근하는 트래픽 수를 위험수준 레벨별로 소속된 센서노드에서 트래픽을 수집할 수 있도록 하였고, 평가를 위해 레벨별 트래픽 수를 각각 누적하도록 하였다.

각각의 노드의 비정상적 접근 트래픽 수를 측정하여 많은 접근을 시도하는 노드에 침입이 집중되고 있는 것으로 파악하여 해킹을 감지로 나타내주는 보조 알고리즘을 구성하였다. 그림 10은 실험을 통해 비정상적인 접근을 시도하는 트래픽 수로 해킹을 감지한 결과를 보여주고 있다.

성능 평가를 위해 접근하는 비정상적인 트래픽의 수로서 알고리즘의 성능을 평가하는데 주안점을 두었지만 핵심적으로 제안하고자 한 것은 기존 논문에서 관리자 중심의 보안관리 체계에서 들어난 문제점들을 개선하고자 댁내 스마트 홈 시스템에 보안점검 프로그램을 내장하여 일반 사용자들도 실시간으로 트래픽 발생 상황을 확인하므로 위협에 직접적으로 조치를 취하도록 하였고, 정밀한 분석 및 2차적인 대응은 관리 서버에서 할 수 있도록 하여 보안을 강화할 수 있는 방안을 제안하였다.

Ap node access traffic count

노드 ID	Ch1	Ch2	...	Ch9
node1	3	2	...	5
node2	2	3	...	2
node3	3	2	...	1
node4	25	15	...	11
node5	1	4	...	2
node6	23	16	...	22
node7	4	3	...	1
node8	2	3	...	2
node9	1	4	...	1

해킹인지

[그림 10] 노드 접근 트래픽 수로 해킹 감지
[Fig. 10] Access traffic the number of nodes detecting hacking

4. 결 론 및 향후 연구 방향

본 논문에는 스마트 홈 시스템의 위험수준별 트래픽 분석하여 데이터베이스로 구축해 놓고, 실시간으로 AP 노드에 접근하는 트래픽과 데이터베이스에 트래픽과 비교분석을 통해 위험수준별 불법접근을 찾아내어 차단하고 모바일로 사용자에게 통보되도록 하였다. 노드에 접근하는 트래픽의 수를 파악하여 해킹 감지할 수 있도록 보조 알고리즘을 구성하였다.

현재 스마트 홈에 설치되는 가전제품들은 스마트 홈 게이트웨이의 제어에 의해 무선으로 조정되도록 구성되어 있다. 제안한 침입대응 알고리즘을 포함한 시스템을 스마트 홈 시스템에 각각의 가전제품에 추가시켜 표준화 작업이 무엇보다도 우선적으로 시행되어야 할 것으로 보인다.

어떠한 형태로 스마트 홈의 침입이 발생할지 예측하기 어려운 상태이지만 스마트 홈에 설치되는 가전제품들의 특성과 유무선 네트워크 위험도를 정확히 분석하여 침입대응 할 수 있는 시스템이 갖추어져야 한다.

향후 연구해야 할 것은 스마트 홈의 위험분석을 위한 데이터베이스를 구축하여 실시간으로 발생하는 트래픽을 분석하여 위험을 찾아내고 침입을 대응할 수 있는 초석을 만들었으나 많은 침입사례를 예측할 수 없었기 때문에 보다 정밀하게 침입에 대응 할 수 있는 알고리즘 보완이 필요하며 스마트 홈에 사용되는 가전제품에 개별적으로 보안인증을 강화할 수 있는 방안을 연구해 볼 것이다.

References

[1] Hwang-Rae Kim, Yeon-i Kang, “Monitoring-based Intrusion Detection System for Ubiquitous Sensor Network”, Korea Aerospace Industries. 2010.

[2] Jong-Hu Lee, Jae cheol Ryu,"Intrusion detection system for home network security", 2007. HN FOCUS vol.8

[3] Jae Hak Yu, Yong Hwa Jeong, “A Study on Hierarchical Distributed Intrusion Detection for Secure Home works Service*",Information Security Institute, 2008. 2

[4] Jong-Hu Lee, Jae Cheol Ryu, “TSC system(주) ZigBee home network Introduction and building example”, 2007. HN FOCUS vol.8

[5] Du Seop Eom, “Military applications of RFID/Sensor Networks”, 2010. 2

[6] Jae Geun Park, “Home Network Security", 2004. 7

[7] Jeong-Tae Kim, Hye Jung Park, ui hyeon Baek, “Trends of Home Server & Gateway Technology", Electronic Communications Trend Analysis, 2005. 12

강 연 이(Yeon-i Kang) [정회원]

- 2004년 8월 : 단국대학교 산업정보대학원 석사
- 2011년 현재 : 공주대학교 컴퓨터공학부 박사과정
- 2009년 9월 ~ 현재 : 단국대학교 강사
- 2008년 9월 ~ 현재 : 공주대학교 강사

<관심분야>
네트워크보안, 임베디드 시스템, 네트워크 프로그램

김 황 래(Hwang-Rae Kim) [정회원]

- 1982년 9월 : 중앙대학교 전자계산학과 이학사
- 1991년 2월 : 중앙대학교 대학원 컴퓨터공학과 공학석사
- 2007년 9월 : 대전대학교 대학원 컴퓨터공학과 공학박사
- 1983년 3월 ~ 1994년 2월 : 한국전자통신연구원 선임연구원
- 1994년 3월 ~ 현재 : 공주대학교 컴퓨터공학부 교수

<관심분야>
컴퓨터네트워크, 네트워크보안, 네트워크생존성관리