홈 네트워크에서 DDoS Attack 방지 및 보안 통신 가능한 Secure Coordinator 구현을 위한 연구

황지온*, 이평수*, 박세현*

*중앙대학교, 전자전기공학부

Implementation of the Secure Coodinator against DDoS Attack in Home Networking

Zi On Hwang*, Pyung Soo Lee*, Se Hyun Park*

*School of Electrical and Electronic Engineering, Chung-Ang University, Cipher Internet-World Lab.

요 약

본 논문에서는 하나의 네트워크로 연결되어진 가정내의 모든 가전 기기 및 PC 관련 제품들을 인터넷 접속을 통해 제어 및 데이터 전송을 가능하게 하는 홈 네트워크에서 DDoS Attack을 방지하고 보안 통신을 가능하게 하는 Secure Coordinator를 구현하였다. 여러 가전기기들은 진화를 거듭하여 데이터 통신 및 원격 제어가 가능하게 되었고 대부분의 전자 장비들과 연결되어 하나의 Network를 구성하고 있다. 이러한 데이터 통신은 아직 암호화 통신이 이루어지지 않아 쉽게 외부로 유출 될 수 있을뿐만 아니라 악의적인 사용자의 DDoS Attack 에 의해서 내부 Network는 쉽게 무력화 될 수 있다. 본 논문에서는 Secure Coordinator를 통한 DDoS Attack 방지 및 암호화 통신을 구현하였으며, 본 시스템을 통해 기존 시스템의 수정 없이 서버 및 클라이언트 앞단에 모듈처럼 삽입하는 방식으로 설계가 되어 있어 Home Networking 뿐만 아니라 서버/클라이언트 어플리케이션에 많은 활용이 기대되어 진다.

I. 서론

1960년대 말 최초로 인터넷이 등장하고 두 대의 컴퓨터를 연결하여 정보를 교환할 수 있음을 보여줬을 때, 그것은 많은 컴퓨터 전문가들에게 조차 놀라운 일로 받아들여졌다. 그러나 최근에는 정보 교환의 영역이 컴퓨터뿐만 아니라 가전기기로까지 확대되어지고 있고 이러한 가전기기가 점차 지능화되고 통신망 기술이 발달하면서 집안의 가전기기를 이용한 네트워크를 구축하는 움직임이 활발해 지고 있다. 이러한 홈 네트워크에 대한 요구에 따라 가정에서는 HomeRF, HomePNA, IEEE 1394, Home Bluetooth, Ethernet등이 활발히 연구되고 있다. 또한 컴퓨터와 가정의 다른 기기들을 하나로 연결할 수 있는 미들웨어로서 UPnP나 Jini, Havi 등이 연구되어 지고 있다.[1] 네트워크의 획기적인 발전과 함께 성장해온 홈 네트워크의 연구가 활발히 진행되어짐에 따라 홈 네트워크 보안에 대한 필요가 요구되고 있다. 현재 홈 네트워크의 개발에 비하여 보안관련 연구는 상대적으로 미비한 상황이다.[2] 이는 원격으로 제어되는 전자기기의 원하지 않는 동작을 초래할 뿐만 아니라 가정내의 데이터 유출 및 홈 네트워크의 무력화로 큰 피해를 야기할 위험이 존재한다. 본 논문에서는 이러한 여러 가지 보안적 문제점을 해결할 수 있는 Secure Coordinator를 구현하여 DDoS Attack을 방지하고 통신 및 제어 데이터의 기밀성과 무결성을 보장한다.[3] Secure Coordinator는 기존 장치에 모듈 방식으로 삽입되는 것으로 모든 동작이 이루어지므로 다른 홈 네트워크 장비의 변

경 없이 시스템 구축이 가능하다.

II. 본론

1. Implementation of the Secure Coordinator

기존에 Home Networking에서는 모든 패킷이 Plane Text로 통신이 이루어지기 때문에 악의적인 제 3자가 패킷을 훔쳐보거나 패킷 변경의 위험이 존재할 수 있다. 특히 외부에서 댁내 전자기기를 제어한다거나 데이터를 변경할 경우 이러한 악의적인 공격은 치명적 피해를 야기할 수 있다. 이러한 위험을 방지하기 위해 Secure Coordinator는 원격 제어 모듈과 Home network segment를 SSL로 암호화하여 데이터 교환을 수행한다.[4]

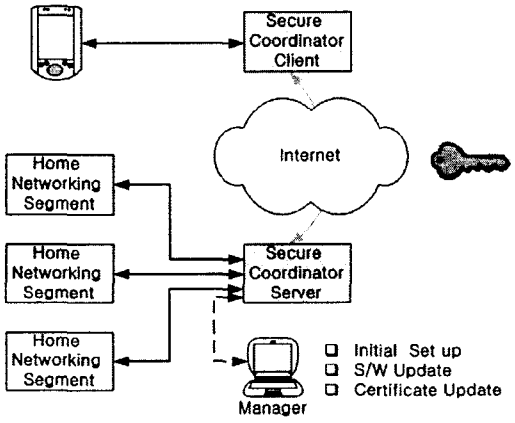

그림 1: Structure of Secure Coordinator

Secure Coordinator 는 SCS, SCC로 구성되어 있고 각 모듈의 기능은 다음과 같다.

SCS(Secure Coordinator Server) :

Secure Coordinator Client와 SSL 접속을 이루고, Home Network 외부 접속 기기에서 전달받은 데이터를 Home Network Segment에 전송한다. 인증서와 개인키를 내장하고 SCC의 인증서와 서명을 검증한다.

SCC(Secure Coordinator Client) :

Secure Coordinator Server와 SSL 접속을 이루고, Home Network 내부의 기기를 컨트롤하기 위한 데이터를 암호화하는 작업을 수행한다. 개인키와 인증서를 내장하고 있고 SCS의 인증서와 서명을 검증한다.

1)Implementation of the Secure Coordinator Server(SCS)

SCS는 Home Network Segment 간의 통신을 관리하고 Home network 외부에 위치하는 원격 제어 모듈에서 유입되는 데이터를 복호화하고 DDoS Attack을 방지하기 위해서 각 Segment에 정기적인 Request 신호를 전송하는 역할을 수행한다.

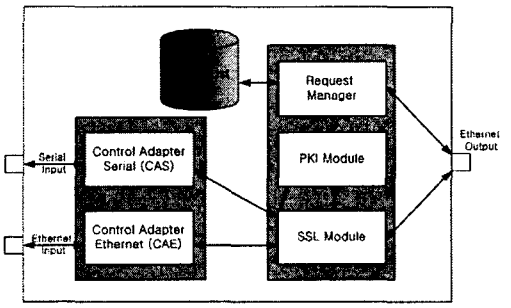

그림 2: Structure of Secure Coordinator Server

각 보안모듈은 상호 작용에 의해서 데이터 및 제어 패킷의 인증 및 암호화를 수행한다. 각 모듈의 세부 동작은 다음과 같다.

Control Adapter Ethernet (CAE) :

Home network segment로부터 데이터 패킷을 받아 SSL 모듈로 전달하고, SSL 모듈에서 보내지는 제어 패킷을 Home Network Segment로 전달하는 프로세스이다. 암호화 기능은 수행하지 않고 통과하는 모든 패킷을 bypass 하는 기능을 수행한다.

Control Adapter Serial (CAS) :

Home network segment중에서 Serial Output만을 지원하는 기기를 위해서 만들어진 포트이다. 시리얼 포트를 통해서 데이터 패킷을 받아 SSL 모듈로 전달하고, SSL 모듈에서 보내지는 제어 패킷을 Home Network Segment로 전달하는 프로세스이다. CAE 와 동일한 기능을 수행한다.

SSL Module :

SSL 모듈은 SSL 패킷을 보내거나 받는 프로세스이다. CAE 또는 CAS로부터 데이터를 받아들이고, 세션키를 이용해 암호화한 후 Secure

Coordinator Client로 전송한다. SSL을 통해 SCC 부터 전송된 데이터 패킷을 세션키를 이용해서 복호화 한 후 CAE 또는 CAS로 전달한다. CAS와 CAE 중 최초에 데이터 패킷을 SSL 모듈로 전송하는 쪽이 계속되는 패킷 전송 포트로 이용된다. SSL 모듈은 초기 setup시 SCC 에 대한 정보 (IP 주소, port 번호, 인증서 등)를 관리하고 SCC와 SSL 세션을 맺고 관리하는 역할을 한다. SSL 세션을 맺을 때 SCC의 인증서를 검증하도록 하는 SSL 옵션을 이용하여 검증한다. 인증서에 의한 검증을 수행하는 주기는 설정에 따라 변경될 수 있다. SSL 세션 성립 후에는 세션키를 이용하여 데이터를 암호화 한다. 다음 그림 3 는 SSL 모듈의 입출력 신호를 나타낸다.

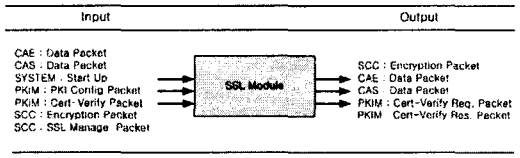

그림 3: Signal of SSLD

PKI module (PKIM):

인증서와 관련된 작업을 수행하는 프로세스이다. 인증서 및 개인키 파일에 관련된 작업을 수행하고 기타 설정사항을 셋팅하는 역할을 수행한다. SCS와 SCC는 인증 메시지를 교환함으로서 상호 인증작업을 수행하게 된다.

Request Manager Module(RMM) :

DDoS Attack을 방지하기 위해서 Request Message 전송을 관리하는 모듈이다. RMM은 데이터베이스에 관리되고 있는 SCC의 정보를 이용하여Request를 전송하여 DDoS Attack을 방지한다.

SCS 는 접속된 SCC 의 개수만큼 쓰레드가 생성되고 각 쓰레드는 각각 Home Network Segment 와 개별적인 통신을 수행한다.

2)Implementation of the Secure Coordinator Client(SCC)

SCC는 Home Control Equipment 와 Home network segment 사이의 통신을 중계하는 역할을 수행한다. 본 논문에서는 CE(Control Equipment)에 SCC를 탑재하여 구현하였다. 즉 SCC를 별도의 모듈로 구현하지 않고 소프트웨어 적으로 CE에 탑재하였다.

SCC는 Control Adapter Ethernet (CAE), SSL Module(SSLM), PKI Module(PKIM) 으로 구성되어 있고 대부분 SCS와 동일한 기능을 수행한다. 다만 SCS는 SCC가 접속할 경우 스레드를 생성하여 각 SCC와 연결을 맺으나 SCC는 하나의 프로세스만으로 SCS에 접속을 수행한다. SCC는 다음 그림 4 과 같이 구성되어 있다.

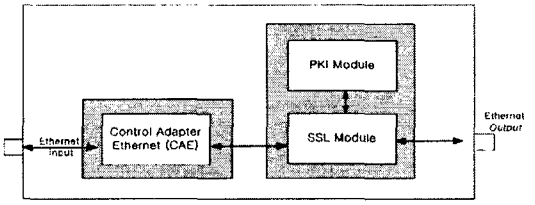

그림 4: Structure of Secure Coordinator Client

SCC 는 SCS와 서명메시지 교환을 통해서 상호 인증이 수행하면 암호화된 데이터 및 제어패킷을 교환한다. SCC의 서명메시지도 SCS의 서명메시지와 동일한 포맷으로 되어 있다.

3)Against DDoS Attack in Home Networking

DDoS(Distributed Denial of Service) Attack은 사용자들에게 피해를 준다는 점에서 크래킹의 한 종류라고 할 수 있다. 하지만 요즘 인터넷으로 배포되는 공격 프로그램을 이용하면 전문 지식이 없어도 공격이 가능하기 때문에 그 방법이 비교적 간단하지만 그 피해 범위와 정도는 매우 광범위하다. DDoS의 주요 공격 대상은 시각적인 서비스를 하는 웹서버나 라우터, 네트워크같은 기반 시설이다. DDoS는 한 사용자가 시스템의 리소스를 독점하거나 모두 사용, 또는 파괴함으로써 다른 사용자들이 이 시스템의 서비스를 올바르게 사용할 수 없도록 만드는 것을 말한다. 이런 의미에서 시스템의 정상적인 수행에 문제를 일으키는 모든 행위를 DDoS라 할 수 있다. 이러한 DDoS Attack이 일어나는 방법은 매우 다양하다. 일반적인 Server/Client 모델은 클라이언트가 서버에 Request를 요청하게 된다. 이러한 서버/클라이언트의 특성을 이용해서 불특정 다수의 가상 클라이언트의 요청이 이루어지게 되면 서버는 정당한 클라이언트의 접속요청에 응답을 수행하지 못하는 상황이 발생하게 된다.[6] 본 논문에서는 이러한

취약성을 방지할 수 있는 방법으로 서버/클라이언트의 접속 프로토콜을 수정하여 구현함으로써 DDoS Attack을 방지 할 수 있는 Secure Coordinator를 개발하였다.[7] 다음 그림 5 에서는 본 논문에서 구현한 Secure Coordinator 의 Request/Response 흐름도이다.

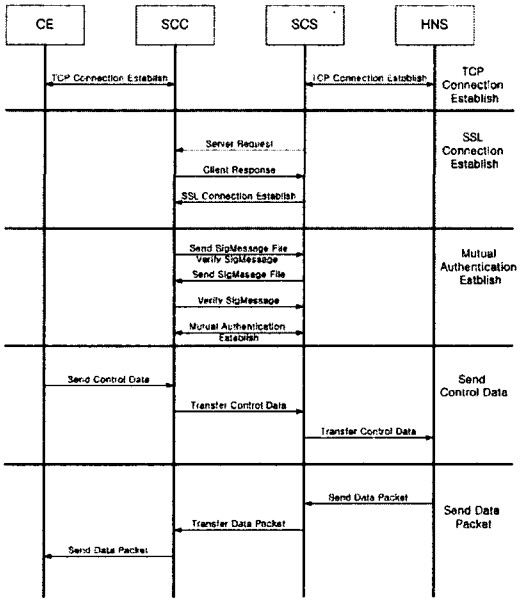

그림 5: Request/Response Procedure

CE(Control Equipment)와 SCC(Secure Coordinator Client), SCS(Secure Coordinator Server)와 HNS(Home Network Segment)는 내부 네트워크로 TCP Connection을 맺는다. 그리고 SCS는 데이터 베이스에 저장되어 있는 SCC ACL를 참고하여 각 SCC에 Request Message를 전송한다. Request Message를 전송한 SCS는 일정 시간동안 Response 가 없을 경우 Request Message를 재전송하게 된다. SCS의 Request 에 SCC가 Response 를 하지 않게 되면 SCS는 계속 Request를 요청하게 된다. 사용되지 않는 SCC에게는 필요 없는 Request 가 지속되게 되면 네트워크 및 시스템의 Resource가 불필요하게 낭비되기 때문에 본 시스템에서는 다음과 같은 알고리즘을 사용하여 Request 재전송하기 위한 Wait Time을 계산하였다. 일반적으로 한번 Response 응답이 있는 CE는 다음번에도 재접속할 확률이 높기 때문에 가중치를 높게 산정하여 재전송 시간을 감소시키는 방법이다. Request Message 에 대한 Response 가 없을 경우 재전송하기까지의 시간을 n 이라고 할 때 Response 가 없으면 n * 2 만큼으로 시간이 증가한다. 마찬가지로 이전의 Request 에 대한 Response 가 존재하게 되면 n / 2 로 시간이 감소하게 된다. 이는 한번 접속한 CE는 이후에 재접속할 확률이 더 커지므로 이에 대한 환경요인을 적용한 결과이다. Response 가 없을 경우 n 이 무한정 커질 수 있으므로 n의 최대값을 N이라 설정하고 n이 N 보다 커지게 되면 더 이상 증가하지 않고 N으로 설정하게 된다. 다음 그림 6은 Request를 재전송하는 시간이 2배만큼 증가하는 것을 나타낸 그림이다.

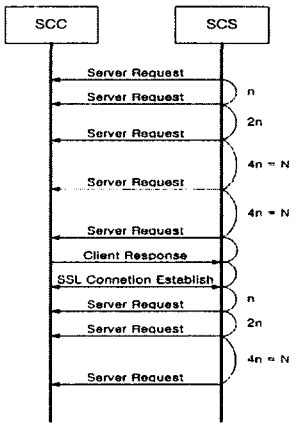

그림 6: Calculation of Request Interval Time

SCS가 Request를 요청하기 때문에 SCS의 ACL에 존재하지 않은 IP에서의 요청메시지는 무시되며 이러한 방법으로 Secure Coordinator Server/Client 는 DDoS Attack에 저항력을 가지고 있다. 다음 그림 7은 Secure Coordinator의 전체적인 구성을 그림으로 나타낸 것이다.

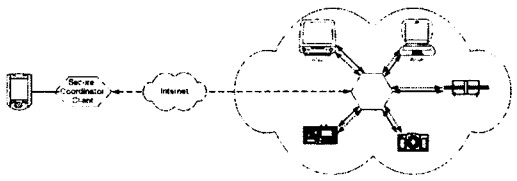

그림 7: Structure of Secure Coordinator

2 Secure Coordinator의 동작 및 실행 화면

SCS 는 DB에 저장되어 있는 ACL의 IP 주소로

규칙적인 Request Message를 전송한다. 이때 대기하고 있던 SCC는 Response Message를 전송한다. Response를 전송받은 SCS는 해당 SCC와의 통신을 위해서 스레드를 하나 생성하고 대기한다. 이때 SCC가 먼저 인증메시지를 전송하면 SCS는 인증메시지를 검증한 다음 자신의 인증메시지를 생성하여 SCC에게 전송한다. SCC가 SCS의 인증메시지 검증에 성공하게 되면 상호인증이 완료되어 SSL Connection을 맺게 된다. 다음 그림 8 은 SCC가 인증메시지를 검증하는 화면이다.

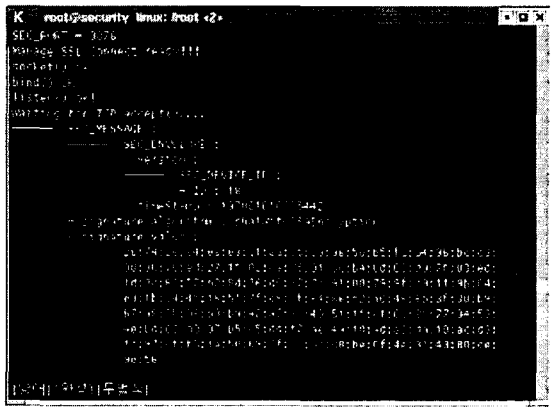

그림 8: Verify Authentication Message

상호인증이 완료된 이후에 SCC는 데이터를 암호화하여 Home Network Segment에 제어신호를 전송한다. 상호인증이 완료된 이후의 모든 데이터들은 SSL로 암호화되어 전송되기 때문에 중간에 패킷이 누출되어도 데이터가 위조되거나 변조될 위험이 없다. (그림 9)

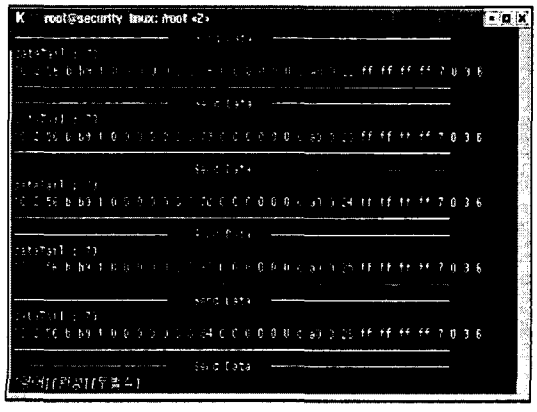

그림 9: Send Control Packet

Ⅲ. 결론

홈 네트워킹 기술은 최근에 이슈가 되고 있으며 다양한 솔루션이 급속도로 제시되고 있다. 즉, 기구축된 전화선로를 이용하는 HomePNA 기술, IEEE 1394 기술, 전력선 통신기술과 같은 유선기술과2.4GHz 주파수 대역을 이용하는 WLAN, Bluetooth, HomeRF와 같은 무선기술등이 다양하게 전개되고 있으며 홈네트워킹은 차세대 주요 통신시장으로 부상할 것이 자명하다. 그러나 현재의 홈 네트워킹은 보안적으로 아주 취약한 상태이고 DDoS와 같은 단순한 공격에도 홈 네트워크가 쉽게 무력화 될 위험이 있다. 또한 외부의 네트워크를 통해서 가정용 기기를 제어할 수 있기 때문에 해킹을 통한 공격이 이루어질 경우 심각한 위험을 초래할 수 있다. 이에 본 논문에서는 Secure Coordinator를 구현하여 암호화 통신을 통한 데이터 위변조 방지와 DDoS Attack를 방지하였다.

참고문헌

[1] "8802-11 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", ISO/IEC

[2] David Bagby, et. al., "Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol across Distribution Systems Supporting IEEE 802.11 Operation", internet draft, January 2003

[3] Rigney, et. al., "Remote Authentication Dial In User Service", IETF, RFC2865, April 1997

[4] Pat R. Calhoun, et. al., "Diameter Base Protocol", IETF Internet Draft, December 2002

[5] Perkins. C, "IP Mobility Support for IPV4 revised", IETF, RFC3220, January 2002

[6] Mick Seaman, et. al., "Port-Based network Access Control", IEEE, June 2001

[7] Metz. C, "AAA protocol: Authentication, Authorization, and Accounting for the Internet", IEEE computing, IEEE, Vol3 Issue 6, Nov/Dec 1999, Page(s): 75-79