디지털산업정보학회 논문지 제13권 제4호-2017년 12월
http://dx.doi.org/10.17662/ksdim.2017.13.4.013

범용적으로 적용 가능한 네트워크제어서버 기반의 상호인증 및 그룹핑 프로토콜 설계

박 중 오*

Design of Mutual Authentication and Grouping Protocol Based On Network Control Server Applicable to General Purpose

Park Jungoh*

〈Abstract〉

In order to protect personal information and important information (confidential information, sales information, user information, etc.) in the internal network, companies and organizations apply encryption to the Server-To-Server or Server-To-Client communication section, And are experiencing difficulties due to the increasing number of known attacks and intelligent security attacks. In order to apply the existing S / W encryption technology, it is necessary to modify the application.

In the financial sector, "Comprehensive Measures to Prevent the Recurrence of Personal Information Leakage in the Domestic Financial Sector" has been issued, and standard guidelines for financial computing security have been laid out, and it is required to expand the whole area of encryption to the internal network. In addition, even in environments such as U-Health and Smart Grid, which are based on the Internet of Things (IoT) environment, which is increasingly used, security requirements for each collection gateway and secure transmission of the transmitted and received data The requirements of the secure channel for the use of the standard are specified in the standard. Therefore, in this paper, we propose a secure encryption algorithm through mutual authentication and grouping for each node through H / W based Network Control Server (NCS) applicable to internal system and IoT environment provided by enterprises and organizations. We propose a protocol design that can set the channel.

Key Words : Interval Encryption, IoT(Internet of Things), Network Control Server, Mutual Authentication, Secure Channel

Ⅰ. 서론

최근 국내 비교적 안전하다고 여겨지는 금융권은 물론 사용자의 개인정보 및 의료기록정보 등을 취급하고 있는 병원과 내부망을 이용하여 서비스를 제공하는 일반 기업 및 공공 분야에서도 사용자의 중요 정보에 대한 사고가 꾸준히 증가하고 있다. 이로 인하여 사용자와 각 분야의 기업들도 정신적 피해는 물론 금전적 피해도 발생한다.

이에 따라 국내에서는 “국내 금융분야 개인정보 유출 재발방지 종합대책”을 내 놓으며 내부 보안규정의 수준 향상을 위해 감독당국이 금융협회와 공동으로 “금융전산 보안 표준지침”을 마련하고, 특히 외부망과 중간망까지 되어 있던 암호화를 내부망 전 구간 까지 암호화를 수행 하도록 확대 되었다. 국내뿐만 아니라 해외의 경우 대표적인 검색포털인 Y사의 경우 미 국가안보국(NSA)해킹으로 수백만 건의 데이터 유출사고가 발생함에 따라 최고 경영자(CEO)는 전 영역에서 네트워크 및 데이터 통신에 대해 암호화하도록 조치하였다.

이처럼 증가하고 있는 각종 유출사고 및 보안 사고에 대응하기 위하여 각 산업분야 별로 다양한 보안솔루션 및 보안규정 등을 구축하여 운영하고 있지만 가용성 측면과 여러 가지 제약 사항들로 인하여 많은 어려움을 겪고 있다. 현재 운영되고 있는 대부분의 시스템에서 CT, MRI, PACS, EMR, OCS 등과 같이 환자의 개인정보 및 의료기록 등을 관리하는 시스템의 경우 소스 수정이 불가능한 환경으로 인하여 데이터 전송 간 외부 노출에 취약한 형태로 방치가 되고 있다. 그 밖에 수많은 외산 패키지 등 많은 제약 사항을 가지고 있는 구조의 어플리케이션 역시 보안통신을 통한 민감 데이터에 대한 보호가 미비한 실정이다. 또한 정책적으로 기존에 허가를 받아 사용 중인 의료장비의 경우 보안성 강화의 목적으로 소스 수정 등의 작업을 진행할 경우 장비 변경에 대한 허가를 다시 받아야 하는 불편함이 존재한다. 또한 기존의 S/W 적용 방식은 지속적으로 변화하고 있는 IT 인프라의 변화를 적극적으로 반영하지 못하고 있으며, 다른 플랫폼으로의 서버이관 및 국가 표준 알고리즘 변경이나 암호키 길이 증가 등 암호화 알고리즘의 변화 등과 같은 시스템 업그레이드 시 매번 소프트웨어를 재구매하여 신규로 적용해야 하는 재정적 낭비와 일력 소모의 악 순환을 초래한다.

기존 적용 방식은 민감 데이터의 암·복호화를 위해 어플리케이션 자체 서비스에 영향을 주는 단점이 존재하며, 이로 인하여 서비스 가용성 및 성능을 경감시켜 암호화 도입 적용에 있어 많은 인프라 제약을 받고 있다.

또한 최근에는 의료/헬스케어 및 지능형 스마트 홈, 스마트그리드 등 다양한 영역에서 사물인터넷 게이트웨이가 적용되는 범위가 지속적으로 확대되고 있다. IoT 환경의 경우도 표준상에 전송 구간에 대한 보안채널 설정과 전송단의 게이트웨이에 대한 보안 요구사항이 명시되어있다.

이에 따라 2장에서는 사물인터넷 게이트웨이에 대한 개요 및 보안요구사항에 대하여 서술하며, 3장에서는 네트워크제어서버를 통한 각 노드간의 상호인증 및 생성된 세션키를 통한 그룹키 생성/갱신을 제안한다. 4장에서는 안전성 분석 및 보안성 분석을 통하여 해당 시스템의 성능평가결과를 나타내었으며 5장 결론에서는 향후 연구방향을 제시한다.

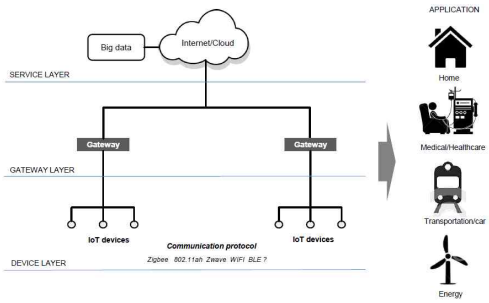
Ⅱ. 관련연구

2.1 사물인터넷 게이트웨이 개요

사물인터넷의 환경의 게이트웨이의 역할은 데이

* 성결대학교 파이데이아학부 조교수

터를 전달(bypass)하는 저전력의 경량 게이트웨이부터 각 디바이스의 인증 및 키관리 등 다양한 기능을 제공하고 있다. 사물인터넷환경에서 게이트웨이 기반의 서비스는 <그림 1>과 같은 구조를 가지고 있으며, 사물인터넷은 크게 세 개의 계층(Layer)으로 구분한다.



<그림 1> 사물인터넷 게이트웨이 기반 서비스 개념도

디바이스 계층은 다양한 기능을 가진 IoT 사물 즉 디바이스와 센서들로 구성되어 있으며, 각 디바이스 및 센서들은 Zigbee나 Wi-Fi, Bluetooth, 무선랜 등 다양한 네트워크 프로토콜로 통신한다[1-3].

두 번째 게이트웨이 계층은 각 디바이스나 센서와 같은 IoT사물과 사람 및 다양한 형태의 서비스 플랫폼들과의 연결성(Connectivity)과 메시징(Messaging) 서비스를 제공한다. 서비스 계층의 경우 이용환경 별로 다양한 형태로 존재한다. 최근엔 디바이스 계층에서 수집되는 대량의 데이터를 의미있는 정보로 활용하기 위하여 빅데이터와 연계하여 다양한 서비스를 제공한다[4].

2.2 사물인터넷 게이트웨이 주요 기능 및 보안요구사항

사물인터넷 게이트웨이는 사물 간 연결 및 메시지 교환 지원, 수집데이터 처리/전송, 다양한 네트워크 프로토콜간 변환기능, 사물디바이스 관리 기능, 리소스 관리기능, 서버 플랫폼 연동기능, 보안기능 등 다양한 기능을 가지고 있다. 또한 사물인터넷 게이트웨이는 하드웨어 자원이나 통신방식 및 보안 구조가 상이한 환경에서 디바이스와 네트워크간의 연결성 및 데이터를 전달하는 초연결성 지원이 가능해야하며, 다양한 프로토콜 환경을 수용해야 한다. 사물인터넷 게이트웨이 자체를 보호하기 위한 기능뿐 아니라 사물네트워크의 보안을 강화하기 위한 방안 및 사물기기의 접근제어, 보안 터널링, 인증서 관리 등 추가적인 보안관리 기능이 요구된다[5].

IoT 환경의 특성상 게이트웨이는 수많은 디바이스 및 센서와 연결되어 수많은 양의 데이터가 수신되고, 제어 및 관리가 이루어지고 있으며 외부 서비스 플랫폼 환경과의 연결점 역할을 담당함으로 다양한 보안위협에 노출되는 빈도 및 침해 가능성이 증가된다. 이에 따라 정보보안의 3대요소인 기밀성, 무결성, 가용성의 침해 가능성 또한 증가한다. 사물인터넷 게이트웨이는 충분히 악의적인 공격 및 위협의 대상이 될 수 있으며 기존 환경에 비해 다양하고 지능적으로 변화되고 있는 공격으로 인하여 대응에 대한 어려움은 점점 심화되고 있다. 보안위협은 게이트웨이 기기를 대상으로 위협, 게이트웨이와 기기간, 게이트웨이 간, 게이트웨이와 외부 환경 간 네트워크를 대상으로 한 보안위협, 그리고 게이트웨이의 서비스를 대상으로 한 보안 위협으로 나눌 수 있다[1, 6].

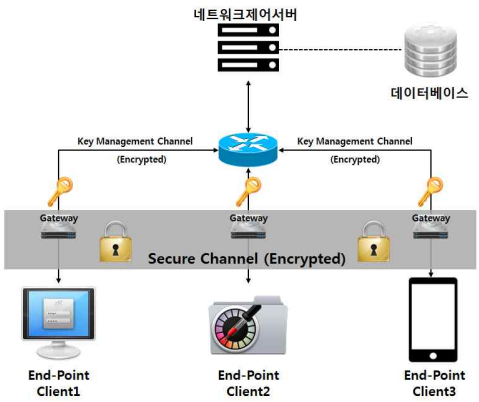
사물인터넷 게이트웨이의 주요 보안요구사항은 <표 1>과 같다.

<표 1> 사물인터넷 게이트웨이 주요 보안요구사항

웜, 바이러스와 같은 악성코드 감염이나 외부 해킹 공격을 탐지하고 방어할 수 있는 기능을 제공해야 한다.
인가된 사용자 및 기기가 허락된 자원에만 접근하도록 인증 및 접근제어 기능을 제공해야 한다.
송수신 데이터의 위변조를 방지하기 위한 데이터 무결성 검증 기능을 제공해야 한다.
송수신 데이터는 불법적인 스니핑 또는 도청 방지를 위해 암호화된 형태로 전송되어야 한다.
이종 네트워크 프로토콜간 변환 과정에서 데이터 기밀성을 유지하고, 악의적인 위·변조를 방지할 수 있어야 한다.
자신의 도메인 또는 다른 도메인에 존재하는 기간 상호 인증을 지원하는 기능을 제공해야 한다.
임의의 메시지를 주입하여 발생할 수 있는 보안위협에 대응할 수 있어야 한다.

Ⅲ. 네트워크제어서버 기반의 상호인증 및 그룹키 생성 및 관리

본 연구에서 제안하는 시스템은 내부망을 이용하는 서비스나 IoT 환경에서 End Point 앞단의 네트워크제어서버를 중심으로 각 End Point의 클라이언트(디바이스 및 센서)들과의 상호인증을 통하여 세션설정 및 그룹키 생성과 갱신을 수행한다. <그림 2>는 제안 시스템의 구성도이다.



<그림 2> 제안시스템 구성도

네트워크제어서버에서 각 노드들에 대한 ID와 Password, IV값을 관리하며, 이를 기반으로 각 노드들은 PBKDF2 키유도 함수를 통하여 상호인증을 수행하며 세션키를 생성한다. 상호인증이 완료된 클라이언트간의 Secure Channel을 확보를 위하여 서버와 클라이언트간의 안전한 인증정보 교환을 통하여 그룹 세션키 생성을 통하여 안전한 통신이 가능하다. 제안된 프로토콜의 약어표는 <표 2>와 같다.

<표 2> 약어표

약 어	설 명
$Device_{ID}$	Device ID
$User_{ID}$	User ID
$User_{PW}$	User Password
IV	Initial Vector Value
C	Count
$DLen$	Data Length
N	Natural Number
$Server_{ID}$	Server ID
$Client_{N\_skey}$	Client N's Session Key
GS_{GN_skey}	Group GN's Session Key
GN	Group Name
$Notify\ MSG$	Notify Message
$Hash(T)$	Timestamp's Hash Value

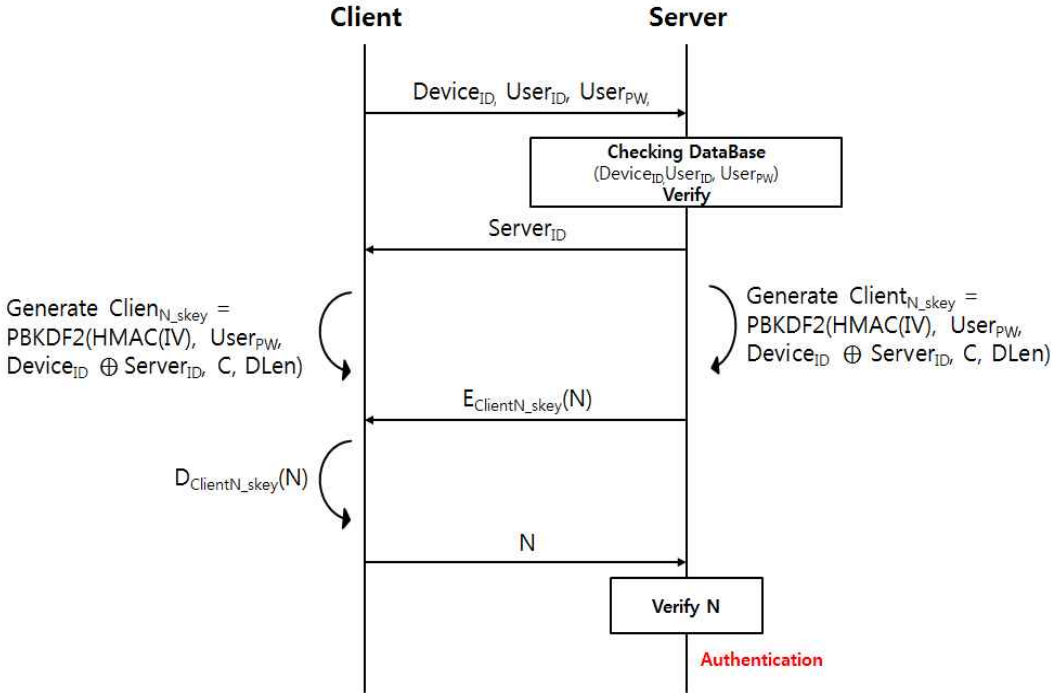
3.1 상호인증 기반의 세션 생성

서버는 End Point 클라이언트의 ID, Password를 등록 및 관리하며, 추가적으로 각 클라이언트에 대한 IV값 또한 관리한다. 서버는 클라이언트의 식별값을 수신 받아 서버의 Database 조회를 통하여 해당 클라이언트에 대한 인증을 수행한다. 세부적인 상호인증 기반의 세션 생성 절차는 <그림 3>과 같다.

1. 클라이언트는 자신의 $Device_{ID}$, $User_{ID}$, $User_{PW}$를 서버로 전송하여 상호인증 요청 메시지를 전송한다.

2. 서버는 Database를 조회하여 전송 받은 클라이언트의 식별값의 유효여부를 판단한다.

Checking Database
$(Device_{ID},\ User_{ID},\ User_{PW})$ (1)



<그림 3> 상호인증 기반의 세션 생성 절차

3. 서버는 클라이언트 식별값의 유효여부를 검증한 이후 세션키 생성 Seed 값인 $Server_{ID}$를 클라이언트로 전송한다.

4. $Server_{ID}$를 수신한 클라이언트는 PBKDF2() 키유도함수를 통하여 수식 (2)와 같이 $Client_{N_skey}$를 생성한다.

Generate $Client_{N\_skey}$ = PBKDF2 $(HMAC(IV), User_{PW},\ Device_{ID} \oplus User_{ID},\ C,\ DLen)$ (2)

5. 서버 또한 PBKDF2() 키유도 함수를 통하여 수식 (2)와 같이 $Client_{N_skey}$를 생성한다.

6. 서버는 클라이언트의 인증을 위하여 생성된 $Client_{N_skey}$키로 N을 암호화 하여 전송한다.

$E_{ClientN\_skey}(N)$ (3)

7. 클라이언트는 생성한 $Client_{N\_skey}$ 키로 수신한 암호문 $E_{ClientN_skey}(N)$을 복호한 후 복호화문 N을 서버로 전송한다.

$D_{ClientN\_skey}(N)$ (4)

8. 서버는 수신한 N값과 자신이 생성한 N값을 비교하여 동일하다면 클라이언트에 대한 인증을 완료하여 세션을 생성한다.

3.2 그룹키 생성 및 갱신 프로토콜 설계

상호인증이 완료된 클라이언트들은 안전한 데이터 통신을 위하여 클라이언트간의 그룹을 생성할 수 있다. 그 과정에서 각 클라이언트들은 서버와 공유하고 있는 세션키를 활용하여 그룹키를 생성한다. 또한 각각의 클라이언트는 생성된 그룹키를 이용하여 안전한 데이터 통신을 할 수 있도록 한다.

생성되는 그룹의 목록은 네트워크제어서버에서 관리하며, 클라이언트의 요청 유형에 따라 그룹가입 및 그룹탈퇴 시 마다 그룹키를 갱신하고 재배포한다.

3.2.1 그룹키 생성

상호인증이 완료된 각 클라이언트는 서버와 상호인증 과정에서 생성한 세션키를 활용하여 그룹키를 생성한다. 그룹키 생성 상세 프로토콜은 <그림 4>와 같다.

1. 그룹을 생성하고자 하는 클라이언트는 서버로 자신의 식별값을 전송한다.

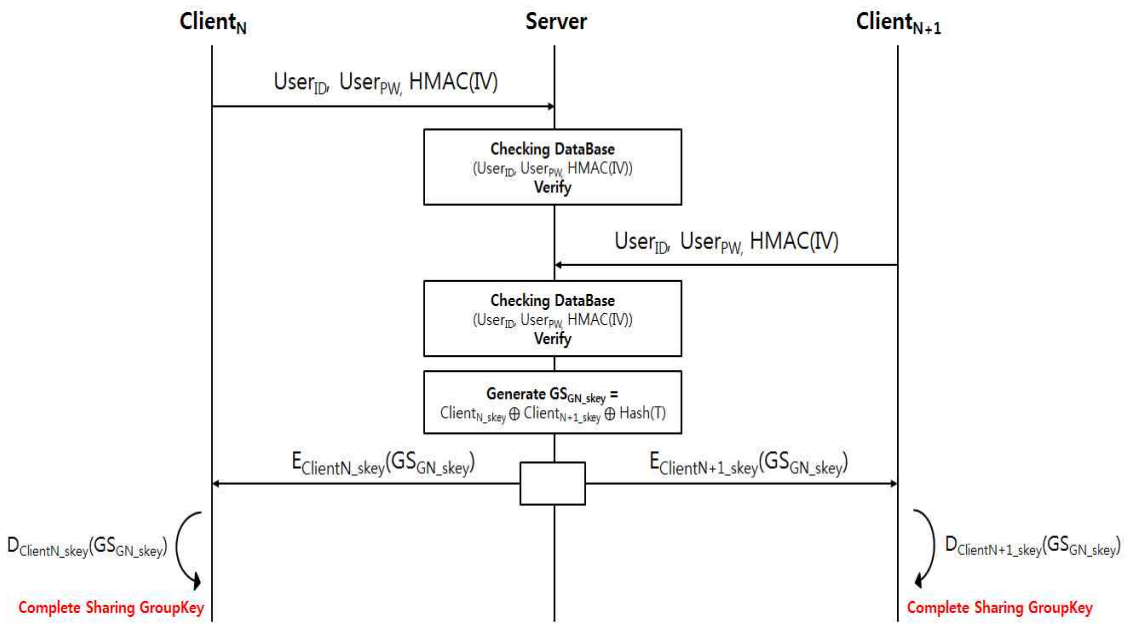
$$User_{ID,} User_{PW,} HAMC(IV) \quad (5)$$

2. 서버는 Database를 조회하여 전송 받은 클라이언트의 식별값의 유효여부를 판단한다.

Checking Database

$$(User_{ID,} User_{PW,} HAMC(IV)) \quad (6)$$

3. 클라이언트의 식별값의 유효여부를 검증한 후 그룹요청이 들어온 클라이언트들의 세션키와 그룹



<그림 4> 그룹키 생성 프로토콜

키의 유효시간 관리를 위하여 $Hash(T)$ 값을 활용하여 그룹키를 생성한다.

$$\textbf{Generate } GS_{GN\_skey} = Client_{N\_skey} \oplus Client_{N+1\_skey} \oplus Hash(T) \quad (7)$$

4. 서버는 생성된 그룹키 값인 GS_{GN_skey}를 그룹 요청이 들어온 각 클라이언트의 세션키로 암호화하여 전송한다.

$$E_{ClientN\_skey}(GS_{GN\_skey}) \quad (8)$$

5. 서버로부터 암호문 $E_{ClientN_skey}(GS_{GN_skey})$을 받은 각 클라이언트는 자신의 세션키를 활용하여 복호화문을 획득하며, 최종적으로 그룹키를 공유한다.

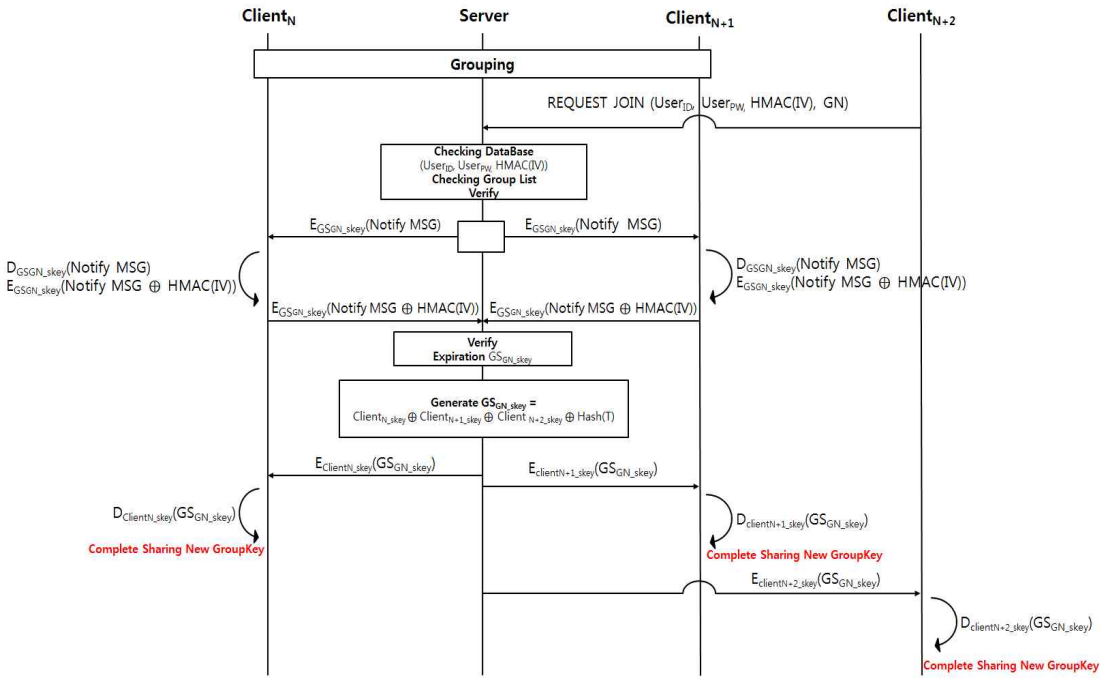
$$D_{ClientN\_skey}(GS_{GN\_skey}) \quad (9)$$

3.2.2 그룹키 갱신(그룹 가입)

이미 그룹핑된 그룹에 서버와 상호인증이 완료된 새로운 클라이언트가 가입 요청을 하는 경우 서버는 해당 클라이언트의 식별값의 유효성을 한번 더 검증하고, 요청한 해당 그룹의 클라이언트들에게 그룹키 갱신을 위한 요청 및 키 배포를 한다. 그룹키 갱신(그룹 가입)에 대한 상세 프로토콜은 <그림 5>와 같다.

1. 기존 그룹에 가입을 원하는 클라이언트는 자신의 식별값과 가입하고자 하는 그룹의 식별값인 GN을 서버로 전송한다.

$$\textbf{REQUEST JOIN } (User_{ID,} User_{PW,} HAMC(IV), GN) \quad (10)$$



<그림 5> 그룹키 갱신(그룹 가입) 상세 프로토콜

2. 요청을 받은 서버는 클라이언트의 식별값의 유효여부를 판단한 후 그룹리스트를 확인하여 GN과 동일한 그룹을 확인한다.

Checking Database
$(User_{ID,}User_{PW,}HAMC(IV))$ (11)

3. 서버는 식별값 검증 후 기존 그룹에 속한 클라이언트들에게 새로운 클라이언트의 그룹가입에 대한 $Notify\ MSG$를 기존 그룹키로 암호화하여 전송한다.

$$E_{GS_{GN\_skey}}(Notify\ MSG) \quad (12)$$

4. 암호문을 수신한 각 클라이언트는 기존 그룹키로 전송받은 암호문을 복호화하여 가입요청 메시지를 확인하고, 한번 더 자신의 유효성 여부 확인을 위해 $HAMC(IV)$ 식별값과 Exclusive OR 연산한 값을 기존 그룹키로 암호화하여 서버로 전송한다.

$$D_{GS_{GN\_skey}}(Notify\ MSG) \quad (13)$$

$$E_{GS_{GN\_skey}}(Notify\ MSG \oplus HMAC(IV)) \quad (14)$$

5. 암호문 $E_{GS_{GN_skey}}(Notify\ MSG \oplus HMAC(IV))$을 수신한 서버는 기존 그룹키로 복호화 하여 원문을 검증한 후 기존 그룹키인 $E_{GS_{GN_skey}}$를 해지한다.

6. 서버는 새롭게 가입요청 한 클라이언트의 세션키 값과 그룹키 유효시간 정의를 위해 $Hash(T)$을 포함하여 새로운 그룹키를 생성하고, 그룹 멤버들에게 새로 갱신된 그룹키를 각 클라이언트의 세션키로 암호화하여 전송한다.

Generate GS_{GN_skey} = $Client_{N\_skey} \oplus Client_{N+1\_skey} \oplus Client_{N+2\_skey} \oplus Hash(T)$ (15)

$$D_{ClientN\_skey}(GS_{GN\_skey}) \quad (16)$$

7. 각 클라이언트는 자신의 세션키로 수신한 암호문을 복호화하며 최종적으로 새롭게 갱신된 그룹키를 공유한다.

$$D_{ClientN\_skey}(GS_{GN\_skey}) \quad (17)$$

3.2.3 그룹키 갱신(그룹 탈퇴)

이미 그룹핑되어 동일한 그룹키를 공유하고 있는 그룹에서 특정 클라이언트가 탈퇴하는 경우가 발생할 수 있다. 그룹 탈퇴의 경우 공유하고 있는 그룹키에 대한 갱신이 필요하다. 탈퇴를 하고자 하는 특정 클라이언트의 식별값을 통하여 탈퇴 이전에 해당 클라이언트에 대한 검증 과정을 거친 후 탈퇴 프로세스를 수행한다. 이에 대한 상세 프로토콜은 <그림 6>과 같다.

1. 기존 그룹에서 탈퇴를 원하는 클라이언트는 자신의 식별값과 탈퇴하고자 하는 그룹의 식별값인 GN을 서버로 전송한다.

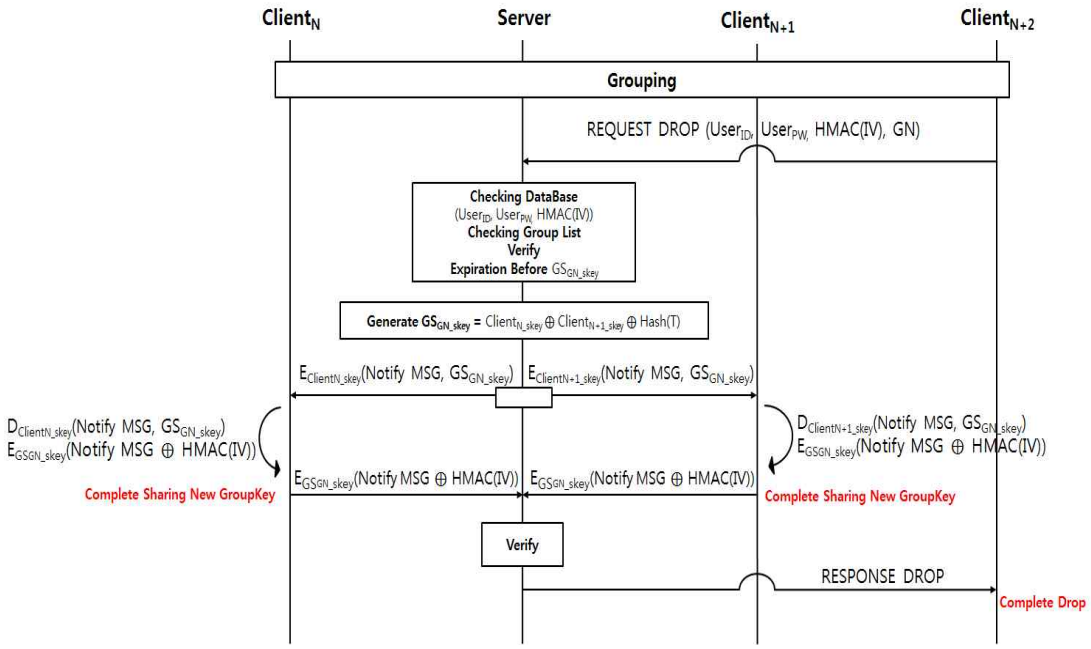
REQUEST DROP
$(User_{ID,}User_{PW,}HAMC(IV), GN)$ (18)

2. 요청을 받은 서버는 클라이언트의 식별값의 유효여부를 검증한 후 그룹리스트를 확인하여 GN과 동일한 그룹 유효여부를 확인한다.

Checking Database
$(User_{ID,}User_{PW,}HAMC(IV))$ (19)

3. 클라이언트의 유효여부를 확인한 후 서버는 기존의 그룹키인 $E_{GS_{GN_skey}}$를 해지한다.

4. 서버는 탈퇴 요청한 클라이언트를 제외하고, 기존 클라이언트들의 세션키와 그룹키의 유효시간



<그림 6> 그룹키 갱신(그룹 탈퇴) 상세 프로토콜

정의를 위해 $Hash(T)$값의 연산을 통하여 새로운 그룹키를 생성한다. 생성된 새로운 그룹키를 각 클라이언트의 세션키로 암호화하여 전송한다.

Generate $GS_{GN\_skey} = Client_{N\_skey} \oplus Client_{N+1\_skey} \oplus Hash(T)$ (20)

$D_{ClientN\_skey}(GS_{GN\_skey})$ (21)

5. 각 클라이언트는 자신의 세션키로 수신한 암호문을 복호화하며 최종적으로 새롭게 갱신된 그룹키를 공유한다.

$D_{ClientN\_skey}(GS_{GN\_skey})$ (22)

6. 최종적으로 서버는 그룹 탈퇴 요청을 한 클라이언트에게 RESPONSE DROP 메시지를 송신하여 그룹 탈퇴를 완료한다.

Ⅳ. 성능분석

4.1 안전성 분석

본 절에서는 제안된 프로토콜에 대한 안전성 및 성능 분석한다. 일반적인 사물인터넷 환경에서 발생 가능한 공격기법을 기준으로 분석하였으며, 한국정보통신기술협회(TTA)의 사물인터넷 게이트웨이 보안 요구사항 표준문서인 TTAK.KO-12.0297의 보안 요구사항을 반영하여 안전성을 분석하였다.

4.1.1 메시지 재사용 및 위·변조

인가되지 않은 공격자가 각 노드 간 전송되어 지는 메시지를 탈취하여 공격자의 의도대로 위·변조하여 재사용 하는 위협으로 각 클라이언트는 자신의 식별값($Device_{ID}$, $User_{ID}$, $User_{PW}$, $HAMC(IV)$)

을 통하여 서버와 상호인증과정에서 생성된 세션키의 유효시간 범위 내에서 안전성을 보장하고 있다. 공격자가 메시지 재사용 및 메시지 위·변조하여 전송한다고 할지라도 서버는 클라이언트와 공유하고 있는 세션키로 공격자의 암호문에 대한 검증이 가능하다.

4.1.2 세션 하이재킹

노드 간 활성화 되어 있는 세션을 중간에 가로채어 이후 통신과정에서 가로챈 세션을 이용하여 공격하는 방법으로 서버와 클라이언트에서 세션키를 생성할 때 $Hash(T)$ 값을 이용하여 생성하기 때문에 유효시간에 따라 갱신되기 때문에 안전성을 보장받을 수 있다.

4.1.3 위장공격

인가되지 않은 사용자가 인가된 사용자인 것처럼 위장하는 공격 방법으로 서버는 클라이언트에 대한 식별값($Device_{ID}$, $User_{ID}$,$User_{PW}$,$HAMC(IV)$)을 등록 및 관리를 하고 있으며, 이를 통하여 상호인증이 이루어졌기 때문에 공격자는 클라이언트의 식별값을 획득해야 하는 정도의 노력이 감수되기 때문에 위장공격에 대하여 안전성을 보장한다.

4.1.4 세션키에 대한 기밀성 및 무결성 보장

서버와 클라이언트가 공유하고 있는 세션키 및 그룹키에 대한 기밀성 및 무결성은 초기 상호인증 과정에서 서버의 식별값($Server_{ID}$)과 클라이언트의 식별값($Device_{ID}$, $User_{ID}$,$User_{PW}$,$HAMC(IV)$)을 통하여 인증을 수행하며, 이후 그룹키 생성 또한 클라이언트의 식별값과 그룹키 생성과정에 포함되는 $Hash(T)$ 값을 통하여 외부 공격에 의하여 기밀성 및 무결성을 보장하고 있다.

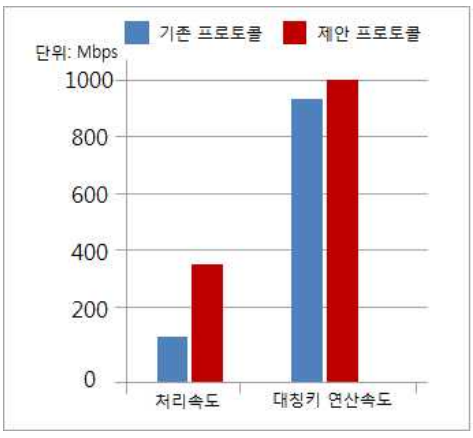
4.2 성능 분석

제안된 프로토콜의 성능을 분석하기 위해 기존의 SSL을 이용한 VPN 오픈소스를 기준으로 분석하였다. 성능평가 항목으로는 처리속도, 대칭키 연산속도, 패킷 송수신 성공률, 암호화 강도를 분석하였다.

<표 3> 성능 분석표

	기존 프로토콜	제안 프로토콜
처리속도	150Mbps	378Mbps
대칭키 연산속도	950Mbps	1,000Mbps
패킷 송수신 성공률	98%	99.27%
암호화 강도	128bit	128bit

처리속도측면에서 기존의 오픈 VPN 프로토콜 대비하여 네트워크제어서버를 통하여 보안채널을 형성하여 약 2배이상 처리속도 향상을 보이고 있으며, 또한 대칭키 암호화 속도와 패킷 송수신 성공률도 미세하게 상승하였다.



<그림 7> 성능분석 도식화

Ⅴ. 결론

본 논문에서는 사물인터넷 환경 및 범용적 환경에서 각 클라이언트(디바이스 및 센서)와 게이트웨이 간의 안전한 통신을 위하여 상호인증을 수행한다. 인증이 완료된 클라이언트 간의 안전하고 효율적인 통신을 위하여 그룹을 생성하고, 생성된 그룹에 속한 클라이언트 간의 동일한 그룹키를 안전하게 공유할 수 있도록 한다.

제안된 프로토콜은 인증 수행과정에서 서버와 클라이언트의 식별값을 통하여 키에 대한 기밀성 및 무결성을 보장하고 있다. 공유하고 있는 세션키의 유효시간을 통하여 안전성을 보장하고 있으며, 제안 프로토콜은 성능적인 측면 보다는 안전성에 초점을 맞추어 제안되었다. 또한 사물인터넷 게이트웨이 표준 보안요구사항을 수용할 수 있도록 제안되었으며 성능적인 측면에서 약간의 향상을 보인다.

향후 상호인증을 통하여 공유한 각 클라이언트의 세션키에 대한 갱신 방법에 대한 연구가 필요할 것으로 보이며 세션키와 그룹키를 활용한 데이터 전송에 대한 상세 프로토콜및 성능적 측면의 고도화를 위한 연구를 진행할 계획이다.

참고문헌

[1] TTA, “IoT 보안게이트웨이 보안요구사항,” TTA.KO-12.0297, 2016. 12.

[2] 김나언, Nguyen Duc Lam, 김서향, 김종권, “공공안전 환경을 위한 사물인터넷 통신망 기술 개요,” KICS, Vol.34, No.6, 2017, pp.35-42.

[3] 양태훈, 이영석, 김상대, 김천용, 김상하, “사물인터넷에서 근거리 무선 통신 기술을 활용한 정보 수집 시스템 비교 분석 연구,” 한국통신학회 학술대회논문집, Vol.8, No.6, 2017, pp.1288-1289.

[4] 신승혁, “오픈소스 하드웨어를 이용한 경량 IoT 센서 게이트웨이에 관한 연구,” Journal of KIIT, Vol. 13, No.10, 2015, pp.85-90.

[5] 이영석, “안전한 사물 인터넷 환경을 위한 인증 방식,” JKIIECT, Vol.8, No.1, 2015, pp.51-58.

[6] Lionel Nkenyereye, 장종욱, “IoT 게이트웨이 기반의 이벤트 중심 접근 방식 응용프로그램 설계,” JKIICE, Vol.20, No.11, 2016, pp.2119-2124.

■ 저자소개 ■

박 중 오
(Park Jungoh)

2000년 7월 : 성결대학교 컴퓨터공학과 졸업
2003년 3월 : 명지대학교 전자계산교육 석사
2011년 8월 : 숭실대학교 컴퓨터공학 박사
2016년 3월~현재 : 성결대학교 파이데이아학부 조교수

관심분야 : PKI, Network security, 암호학
E-mail : jopark02@sungkyul.ac.kr

논문접수일 : 2017년 10월 27일
수 정 일 : 2017년 11월 20일
게재확정일 : 2017년 11월 23일