정 보 보 호 학 회 지
제24권 제4호, 2014. 8

사물 인터넷 환경에서의 센서 네트워킹 보안 기술 분석

신 수 민*, 김 학 범**

요 약

최근 IT 업계의 큰 화두가 되고 있는 사물 인터넷(Internet Of Thing : IoT)은 아직까지 기술 개발 및 초기 도입단계에 있다. 급속한 IT 기술의 발전에 따라 모든 사물을 연결하는 초 연결 사회로서의 길이 열린 지금, 열린 가능성만큼 보안 취약점 또한 나날이 증가해가고 있다. 본 논문에서는 사물 인터넷 환경 하에서 센서 네트워킹 보안을 위한 기술로 XMPP와 IEEE의 P21451-1-4에 대하여 분석하였다.

Ⅰ. 서 론

최근 스마트폰, SNS의 등장 및 사용율의 증가로 인해 초 연결 사회(Hyper Connected Society)라는 개념이 생기면서 사물 인터넷(Internet Of Thing : IoT) 또는 만물인터넷(Internet of Everything : IoE) 시대로 도래하고 있다. 사물 인터넷이란 우리 주변에 존재하는 모든 사물들이 센서와 네트워크 등의 요소를 통해 상호 통신 및 인터넷 연결로 각종 정보를 주고받는 개념으로서, 단순히 사용자 위주의 환경에서 탈피하여 세상에 존재하는 모든 물적 요소에 IT기반의 환경을 구축하여 인간 생활의 풍요로움은 물론, 다양한 산업 분야 활성화의 원동력이 될 차세대 기술 개념으로 각광받고 있다.

정보통신 분야 전문 시장조사 업체인 가트너(Gartner)에서는 2014년 가장 주목해야 할 10대 전략 기술 중 하나로 사물인터넷을 꼽았다. 영국의 시장조사 업체인 ABI리서치는 오늘날 인터넷에 연결된 기기의 대수가 100억 대 이상이며, 2020년에는 300억 대 이상 증가할 것으로 예상했다(ABI Research, 2013. 5. 9) [1]. ABI의 운영이사인 피터 쿠니(Peter Cooney)는 “오늘날의 스마트 폰, 태블릿 및 노트북, PC 등과 같이 허브 역할을 하는 장치들이 IoE 생태계 활성화에 중추적이고 필수적인 구성요소가 될 것이며, 2020년에는 이들 디바이스의 총 설치 기반의 60 %를 차지하는 노드 또는 센서 타입 장치에 의해서 미래의 성장이 좌우될 것이다.”라고 언급했다.(ABI Research, 2013. 5. 9) [1].

이처럼 사물인터넷은 그 성장가치와 잠재력이 무궁무진하나 그 영역과 기능이 확산되면 될수록 보안에 대한 위협 또한 증가되는 추세이다. 사물인터넷이 적용되는 환경(가상의 사이버 환경에서 물리적 환경으로 확장)의 확대로 인해 적용되는 개체에 대한 관리적 어려움은 보안의 취약성을 증가시키고, 무선 환경의 구조적 취약성으로 인해 데이터 유출 및 해킹에 대한 대응이 어려우며, 대부분의 장치가 센서를 기반으로 동작하게 됨에 따라 사용자들로 하여금 관련 정보를 확인 할 수 있는 여건이 부족한 취약성 등을 내포하고 있다.

본 고에서는 XMPP를 활용한 사물인터넷 환경에서의 센서 네트워킹 보안을 위한 통신 기술을 소개함으로써 사물인터넷 보안 기술 적용 방안에 대해서 기술하고자 한다.

Ⅱ. XMPP

2.1. XMPP 소개

2.1.1 XMPP

확장 메시징 및 현재 상태 프로토콜(XMPP, Extensible Messaging and Presence Protocol)은 XML 기반의 메시지 지향 미들웨어 통신 프로토콜이다. 1999년에 재버(Jabber)라는 오픈소스 커뮤니티에서 개발된 프로토콜로써 인터넷 엔지니어링 태스크 포스(IETF)는 IETF 인

* 동국대학교 국제정보대학원 (2014125538@dongguk.edu)
** 동국대학교 국제정보대학원 / (주)이너버스 (khb0305@dongguk.edu)

스턴트 메시징 및 프레즌즈 기술과 같은 핵심 프로토콜을 공식화하기 위해 2002년에 XMPP 워킹 그룹을 형성했다. XMPP 워킹 그룹은 4건의 RFC(RFC 3920, RFC 3921, RFC 3922, RFC 3923)를 제안하였고, 2004 년에 표준으로 승인되었다. 현재 XMPP 기반의 소프트웨어가 인터넷을 통해 널리 배포되고 사용사례로는 몇년 전 구글(google.com)이 XMPP를 채택하여, googletalk 이라는 인스턴트메신저 서비스를 시작하면서 널리 알려지는 계기가 되었다 [2] .

〔표 1〕 XMPP 관련 RFC 표준

구분	내용
RFC 3920	XMPP : Core
RFC 3921	XMPP : Instant Messaging and Presence
RFC 3922	Mapping the XMPP to Common Presence and Instant Messaging
RFC 3923	End-to-End Signing and Object Encryption for XMPP.

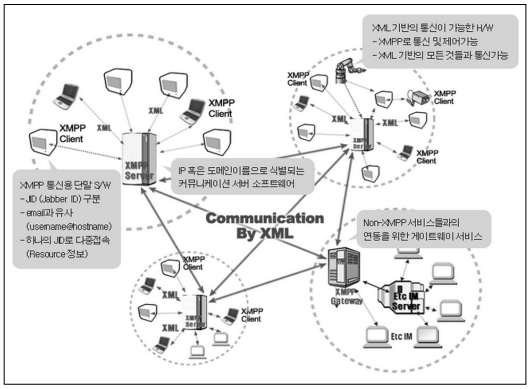
2.1.2 XMPP 특징

- 분산화 : XMPP 네트워크의 구조는 전자메일과 비슷하다. 누구든지 자신만의 XMPP 서버를 구동할 수 있으며 중앙 마스터 서버는 존재하지 않는다.
- 개방형 표준 : 국제 인터넷 표준화 기구는 XMPP란 이름을 규정했다. (최신 규격은 RFC 6120 및 RFC 6121) 이 규격의 지원을 추가하기 위해 로열티가 따로 들지 않으며 개발은 단일 업체에 한정되지 않는다.
- 보안 : XMPP 서버는 공개 XMPP 네트워크 (이를테면 회사 인트라넷)와 분리할 수 있으며 강력한 보안 (SASL, TLS를 통해)을 코어 XMPP 규격에 추가할 수 있다.
- 유연성 : 기기 간 상호 운용성을 유지하기 위해 사용자가 직접 만든 기능을 XMPP 최상단에 빌드할 수 있으며 일반 확장 기능들은 XMPP 표준 재단이 관리한다 [2] .

2.2 XMPP Core

2.2.1 Architecture

XMPP는 클라이언트-서버 모델로 구성된다. 클라이언트는 XMPP를 활용하여 TCP 소켓 연결을 통해 서버에 엑세스하게 되고, 서버는 TCP 연결을 통해 상호 통신하는 구조로 구성되어 있다. [그림 1]에서는 XMPP 구조에 대해 도식하고 있으며, 각 요소별 역할 및 기능은 다음과 같다.



〔그림 1〕 XMPP 구조 [3]

- 서버(Server) : XMPP 통신을 위한 지능적인 추상화 계층으로써 인가된 클라이언트, 서버 또는 다른 엔티티들로부터 XML 스트림 형식 내의 세션 또는 연결을 관리하며, 적절한 주소로 XML 스탠자를 라우팅 한다.
- 클라이언트(Client) : TCP 소켓을 통해 서버에 직접 연결하며, 복수개의 자원은 JID의 자원 구별자에 의해 구분되는 각각의 인가된 클라이언트에 의해 서버에 동시적으로 연결이 가능하다. 클라이언트와 서버 간의 연결을 위한 통신 포트로는 5222을 사용한다.
- 게이트웨이(Gateway) : XMPP를 non-XMPP 메시징 시스템의 프로토콜로 번역하고, 반환된 자료를 XMPP로 번역한다.
- 네트워크(Network) : 각 서버는 네트워크 주소로 구별되고, 서버 간 통신은 클라이언트-서버 프로토콜의 직접적인 확장으로 상호 통신하는 서버들의 네트워크로 구성된다 [4] .

2.2.2 Addressing

모든 엔티티는 XMPP를 활용한 통신에서 종단으로 간주되며, 각각의 엔티티는 그 자신의 고유한 주소를 갖게 되는데 이를 JID(Jabber ID)로 정의한다. 유효한 JID는 도메인, 노드, 자원 식별자 등과 같은 정렬된 요소 집합을 포함한다〔4〕.

- 도메인 식별자(Domain Identifier) : 가장 첫 번째 식별자이며, 네트워크 게이트웨이나 주 서버 이름을 대표하는 요소로서 <123@abc.com> 과 같은 방식으로 사용될 경우 abc.com에 해당되는 부분.
- 노드 식별자(Node Identifier) : 두 번째 식별자이며, 도메인의 세부적인 식별을 위해 사용되는 요소로 도메인 식별자와는 '@'로 구별되며, <123@abc.com> 과 같은 방식으로 사용될 경우 123에 해당되는 부분.
- 자원 식별자(Resource Identifier) : 세 번째 식별자로서 도메인 식별자 뒤에 '/'로 구별하여 사용되며, <123@abc.com/test> 과 같은 방식으로 사용될 경우 test에 해당되는 부분.

〔표 2〕 식별자 표기방식

Item	Value
jid	[node "@"] domain ["/" resource]
domain	fqdn / address-literal
fqdn	(sub-domain 1*("." sub-domain))
sub-domain	(internationalized domain label)
address-literal	IPv4address / IPv6address

2.2.3 Streams and Core Stanzas

XML Stream은 네트워크 상의 두 엔티티 간에 XML 요소들을 교환하기 위한 컨테이너라고 볼 수 있으며, <stream>과 </stream> 태그를 통해 정의된다. Initial Stream 같은 경우 클라이언트와 서버 사이의 연결을 위한 세션과 같은 개념으로 볼 수 있으며, 연결이 이루어진 후 추가적인 Stream을 통해 상호간의 각종 요소를 교환하는 방식으로 통신이 진행된다.

XML Stanza는 XML Stream 상에서 한쪽의 엔티티가 다른 쪽의 엔티티에게 보내는 구조화된 정보의 개별적 의미 단위로 볼 수 있다. Stanza는 <message/>, <presense/>, <iq/> 와 같이 3가지 요소로 구별된다〔4〕.

- <message/> : 일종의 push 개념과 같이 한 엔티티가 다른 엔티티에게 정보를 전달할 때에 전달의 의미로 사용되며, 사용 예로는 이메일을 보낼 때와 같이 <message from/>, <message to/> 등으로 사용할 수 있다.
- <presence/> : 기본적으로 브로드캐스트 또는 "발간-구독" 방식으로 볼 수 있으며, 복수의 엔티티들이 구독하고자 하는 단일 엔티티에 대한 정보를 받을 수 있는 개념으로 이해 할 수 있다.
- <iq/> : Info/Query 또는 IQ로 사용하며, "요청과 응답" 방식으로 유사한 개념으로 http 방식이 있다.

Ⅲ. Sensei/IoT* 기술 소개(P21451-1-4)

3.1. P21451-1-4 표준

P21451-1-4는 ISO, IEC, IEEE가 공동으로 참여하는 ISO/IEC/IEEE 21451[IEEE 1451.x] (Smart Transducer Interface for Sensors and Actuators) 표준에서 사물인터넷 환경 하 센서 네트워크를 위한 현재 개발 중에 있는 표준이다〔5〕.

〔표 3〕 ISO/IEC/IEEE21451 Standards

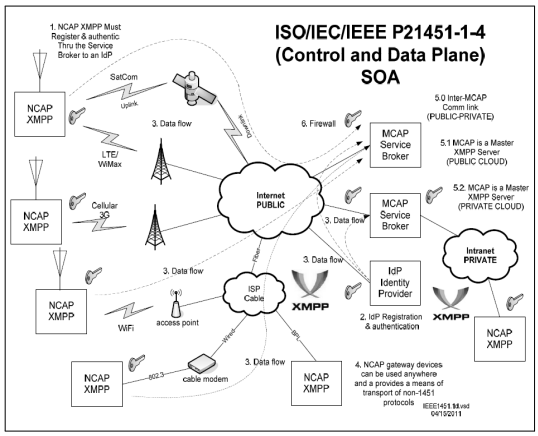
구분	내용
21450	공통적인 기능, 통신 프로토콜들과 전자데이터시트변환(TEDS) 포맷 표준
21451-1	네트워크 지원 응응 프로세서(NCAP)에 대한 정보 모델 표준
21451-2	마이크로 프로세서 통신 프로토콜과 전자데이터시트(TEDS) 포맷 변환 표준
21451-4	혼합 모드 통신 프로토콜과 전자데이터시트변환(TEDS) 포맷 표준
21451-5	무선 통신 프로토콜과 전자데이터시트변환(TEDS) 포맷 표준
21451-7	RFID 시스템 통신 프로토콜과 전자데이터시트변환(TEDS) 포맷 표준

P21451-1-4은 다수의 속성들과, 패킷 전환을 포함하며, 세계적으로 유일한 인증과 패킷 검사 및 정책 통제,

암호화 등을 제공할 뿐만 아니라 상호운영성(Interoperability)을 보장하고 높은 확장성(High Scalability) 제공 및 내재된 보안 기능을 통해 기술 불가지론적이고 프로토콜에 독립적인 심층 보안(Defense-in-depth) 기능을 제공한다〔6〕.

3.1.1 P21451-1-4 Architecture

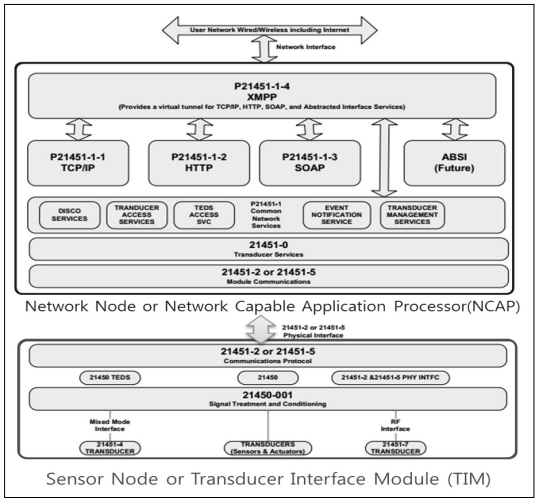
P21451-1-4는 전에 XMPP를 기반으로 한 센서 네트워크를 위한 기술이며, 다음과 같이 활용이 가능하다. 클라이언트 측인 NCAP(Network Capable Application Processor)은 다양한 매체를 통해 서버 측인 MCAP와 연결되어 상호통신 하는 구조로 되어 있다.



〔그림 2〕 ISO/IEC/IEEE P21451-1-4 SOA〔7〕

NCAP은 네트워크 노드라 지칭할 수 있으며, 이는 센서 노드인 TIM(Transducer Interface Module)과 21451-2(Serial Interface) 또는 21451-5(Wireless Interface) 표준을 이용해 상호 통신을 하게 된다.

NCAP은 21450(Transducer Services) → 21451-1 (Common Network Services) → 21451-1-4 (XMPP Services)를 통해 XMPP 서비스를 활용하여 사용자 네트워크 또는 인터넷으로 통신할 수 있다〔7,8〕.

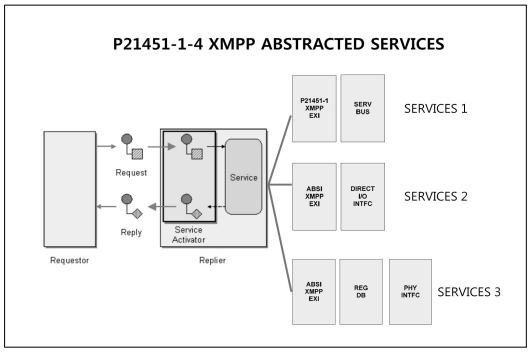


〔그림 3〕 ISO/IEC/IEEE P21451 Network Connection Diagram〔7〕

3.1.2 IoT 환경 하 적용되는 P21451-1-4 유형

사물인터넷 환경 하에 적용되는 P21451-1-4의 추상적인 서비스 유형에는 다음과 같은 것들이 있다〔7〕.

- Gateway (P21451-1 over XMPP)
- Direct I/O (XMPP)
- Legacy Device Adapters (MODBUS over XMPP)
- Server-to-Server (OPC UA over XMPP)



〔그림 4〕 P21451-1-4 XMPP SERVICES

3.1.3 P21451-1-4 요청/응답 방식

P21451-1-4에서의 데이터 요청 및 응답방식은 노드 탐색과, 인터페이스 그리고 센서 데이터로 분류할 수 있다. 먼저, 노드를 찾기 위한 요청 및 응답으로써 MCAP

은 NCAP/TIM 자원의 목록을 요청한다.

요청을 받은 NCAP/TIM은 응답 메시지를 전송하게 되고 이를 통해 노드에 대한 검색이 완료되게 된다. 노드 검색이 완료된 이후 MCAP과 NCAP/TIM 사이에 인터페이스에 대한 요청과 응답 처리과정이 진행되고 식별된 인터페이스에 대해 센서 데이터 요청/응답 과정이 이뤄지면서 통신하게 된다〔7〕.

```
[NCAP/TIM Discovery(Request)]
 <iq type='get' from=' requester@example.org' to='responder@example.org' id='info1'>
   <query xmlns='https://jabber.org/protocol/disco#info'>
     <identity category gateway type='ncap name='ncapid'>
       <feature var='urn:xmpp:iot:interoperability'/>
       <feature var='urn:xmpp:iot:sensordata'/>
       <feature var='http://jabber.org/protocol/disco#info'/>
       <feature var='http://jabber.org/protocol/disco#items'/>
     <identity>
   </guery>
 </iq>

[NCAP/TIM Discovery(Response)]
 <iq type='result' from='responder@example.org' to='requester@example.org'>
   <accepted xmins='urn:xmpp:iot:interoperability'/>
   <accepted xmins='urn:xmpp:iot:sensordata'/>
 </iq>

[Getinterfaces(Request)]
 <iq type='get' from='requester@example.org' to='responder@example.org' id='1'>
   <getInterfaces xmlns='urn:xmpp:sn:interoperability'/>
 </iq>

[Getinterfaces(Response)]
 <iq type='result' from='responder@example.org' to='requester@example.org'>
   <getInterfacesResponse xmlns='urn:xmpp:sn:interoperability'>
     <interface name='XMPPIoT.Sensor.Temperature'/>
     <interface name='XMPPIoT.Sensor.Temperature.History'/>
     <interface name='XMPPIoT.Identity.Clock'/>
     <interface name='XMPPIoT.Identity.Location'/>
     <interface name='XMPPIoT.Identity.Manufacturer'/>
     <interface name='XMPPIoT.Identity.Name'/>
     <interface name='XMPPIoT.Identity.Version'/>
   </getInterfacesResponse>
 </iq>

[SensorData(Request)]
 <iq type='get' from='requester@example.org' to='responder@example.org' id='1'>
   <req xmlns='urn:xmpp:iot:sensordata' seqnr='1' identity='true'/>
 </iq>

[Sensordata(Response)]
 <message from='responder@example.org' to='requester@example.org' >
   <fields xmlns='urn:xmpp:iot:sensordata' seqnr='1' done='true'>
     <node nodeId='Device01'>
       <timestamp value='2013-03-07T16:24:30'>
         <string name='_ID' identity='true' automaticReadout='true' value='1234567'/>
       </timestamp>
     </node>
   </fields>
 </message>
```

〔그림 5〕 p21451 Requests / Responses

3.2. P21451-1-4가 제공하는 보안 기능

3.2.1 Packet Filtering / Inspection

XMPP는 Low-Level에서의 패킷 필터링과 패킷 검사를 지원하며, 패킷레벨에서의 정책 시행을 포함한다. 패킷 변환 작업의 일부로 요청된 기능 및 필터링의 유효성 검사를 포함한다. 이것은 침입 차단에 있어 매우 효과적이라는 의미이다.

예를 들어서 변환 처리에서 Modbus TCP를 사용하는 경우 패킷의 원자 구조가 XML 형태로 변경이 된다. 이것은 웹페이지 상에서 직접적으로 사용되거나 모바일 장치(안드로이드, IOS)로 전송이 가능하다.

패킷을 볼 수 있다는 사실은 명령들이 평가될 수 있다는 것을 의미하고 이것은 패킷이 정보를 읽거나 변경할 수 있는 권한이 부여되는 것을 확인할 수 있는 기회를 부여한다는 것을 말한다〔9〕.

3.2.2 데이터 암호화 / 압축

P21451-1-4는 추가적으로 전송계층보안(TLS, Transport Layer Security)을 제공한다. 전송계층보안을 통해 데이터 변조 및 도청으로부터 안전한 응용 프로토콜을 확보하는 방법을 제공한다〔10〕.

또한 사물 간 의사소통 시 제한된 메모리로 통신할 수 있도록 효율적 XML 교환(EXI, Efiicient XML Interchange)을 통해 압축된다〔11〕.

P21451-1-4는 서비스 브로커와 XMPP 메시지 번환을 활성화 시키는데 사용되는 메타데이터의 요청과 응답과 같은 XMPP 서버에 대한 외부 서비스들을 정의한다.

3.2.3 Single Sign On

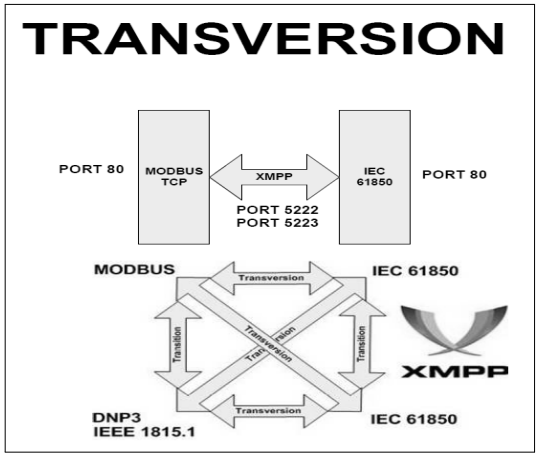
P21451-1-4는 통합인증(SSO, Single Sign-On)을 위한 ID 공급자(IdP, Identity Provider)의 사용으로 외부 서비스를 정의할 수도 있다. IdP 메커니즘은 휴대기기에 대한 활용을 용이하게 할 수 있다. 모든 장치들은 서비스 브로커에 등록되어야 하고, 각각 서로의 장치의 정보를 공유하기 위해 IdP를 사용하여 인증되어야 한다〔6〕.

3.2.4 Packet Transversion

패킷 전환에 대한 내용은 [그림 6] Packet Transversion에 묘사되어 있다. 이것은 기존 XMPP 프로토콜에 대한 변화를 의미한다. 패킷 변환작업은 기술에 얽매이지 않고 프로토콜에 독립적이기 때문에 기존 프로토콜에 상호 운용성(inter -operability)을 제공한다. XML 형태로 있는 동안에 데이터들은 사용자들과 장치들 또는 어플리케이션 등에게 압축되어 메타데이터 형식으로 전송되고 공유될 수 있다〔6〕.

웹 서버는 안드로이드 또는 IOS와 같은 모바일 장치들과 통신할 수 있도록 BOSH (Bidirectional- streams over Synchronous HTTP)〔12〕 위에 XMPP를 사용하는 REST(Representational State Transfer)〔13〕를

제공 할 수 있다.



〔그림 6〕 Packet Transversion

XML 데이터는 종단에서 이진 스트림 값으로 복원될 수 있다. 80번 포트를 사용하는 기존 데이터들은 5222과 5223 포트를 통해 전송될 수 있다. 만약 보안 기능이 없는 Modbus TCP 또는 DNP3과 같은 기존 프로토콜이 XMPP를 활용해 전송 될 수 있다면 패킷흐름은 종단에서 오직 XMPP 트래픽에 의해 한정될 수 있다.

3.3. XEP IoT EXTENSIONS

이처럼 P21451-1-4 기술은 XMPP를 활용한 사물인터넷 기반의 센서 네트워크 통신 및 보안 기술을 제공하는데 이는 기존 XMPP의 확장 프로토콜인 XEP(XMPP Extension Protocols)를 사용함으로써 구현된다.

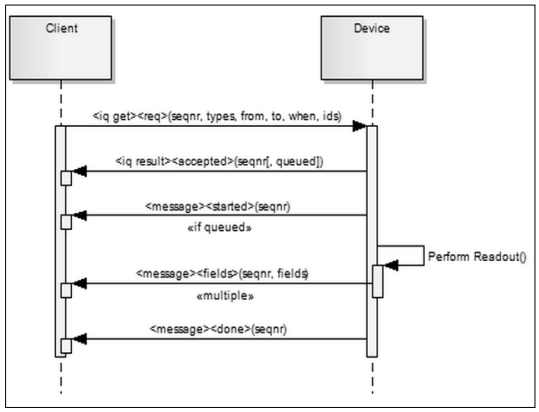
XEP는 기본 기술에 구현된 기술적 세부 사항을 제거한 추상화된 하드웨어 모델을 포함하며, 매우 제한된 메모리 양 또는 리소스를 바탕으로 한 센서들을 위해 디자인되었다. 따라서 단순함이 가장 중요하다. 센서 네트워크는 다양한 아키텍처와 사용 사례를 포함하고 있는 이유로 인해 여러 종류로 나뉘게 되는데, 현재까지 진행중인 IoT 관련 XEP는 다음과 같다〔14〕.

〔표 4〕 XMPP EXtensions of IoT

Number	Name
XEP-0000	Battery Powered Sensors
	Discovery
	PubSub
	Events
	Interoperability
	Tables
XEP-0322	EXI Compression
XEP-0323	SensorData
XEP-0324	Provisioning
XEP-0325	Control
XEP-0326	Concentrators
XEP-0332	HTTP over XMPP
XEP-0336	Dynamic Forms
XEP-0337	Event Logging
XEP-0347	Discovery

3.3.1 SensorData

XEP-0323 Sensor Data는 XMPP 네트워크 상에서 센서 데이터를 상호 교환하는 공통된 프레임워크에 대해서 기술하고 있다. 센서 데이터 응용 프로그램에 대한 가장 일반적인 사용 케이스는 계기판으로써 이것은 다음과 같은 요청과 응답 메커니즘에 의해 동작한다〔15〕.



〔그림 7〕 Sensor Data 동작 방식

3.3.2 Provisioning

XEP-0324 Provisioning은 XMPP 프로토콜을 사용한 사물인터넷 상에서의 접근권한 및 사용자 권한을 효율적으로 프로비저닝하는 아키텍처에 대해 설명한다. XEP-0324는 XMPP를 기반으로 사물의 인터넷 서비스를 효율적으로 프로비저닝을 가능하게 하기 위해 다음과 같은 중요한 작업을 정의한다〔16〕.

- 어떤 사물들은 사물을 알고 있다.
- 어떤 사물들은 사물과 데이터에서 데이터를 읽을 수 있다.
- 어떤 사물들은 사물과 일부를 컨트롤 할 수 있다.
- 네트워크 상의 사용자 컨트롤.
- 네트워크 상의 서비스 컨트롤.
- 네트워크의 일반적인 사용자 권한(Boolean User Privileges)을 제어.

위 작업들은 다음과 같은 방식으로 구현된다.

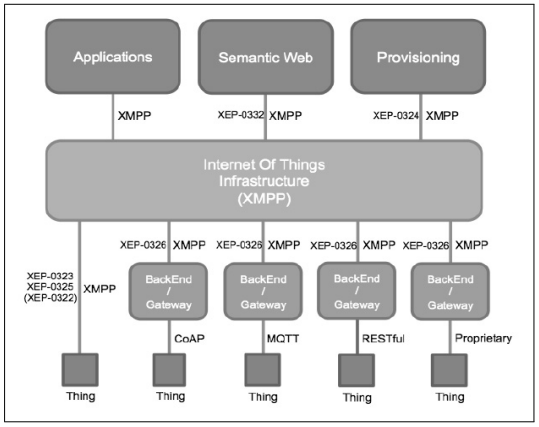
〔표 5〕 XEP-0324 Use Case

구분	내용
신뢰 위임	JID 또는 하위 도메인 주소, 인증서/토큰 등을 통해 클라이언트/서버를 액세스함으로써 신뢰관계 형성
우정 (프렌드쉽)	프렌드쉽 요청 수락 / 거부 및 기존 프렌드쉽 해제, 추천 등에 대한 내용
장치 판독	센서로부터 데이터를 읽어오며, 그 과정에서의 노드 및 필드 제한에 대한 내용 기술
장치 제어	장치 제어 작업에 대한 액세스 권한 및 장치 확인 작업
캐쉬	프로비저닝 서버에 캐시가 쌓이는 것을 피하기 위한 캐시 제거에 대한 내용 기술
서비스	서비스 토큰 획득 및 서비스에 대한 사용자 액세스에 대한 내용
사용자 권한	사용자가 서비스에 액세스할 수 있는 권한 부여 및 성능향상을 위한 서비스의 사용자 권한 전체 다운로드 및 내부 권한 검사 시행

3.3.3 Concentrators

XEP-0326 Concentrators는 센서 네트워크의 한 부분으로써 하위 세트의 장비들을 한 곳으로 모아주는 기능을 수행한다. Concentrators는 다양한 크기를 가질 수 있으며(소형, 중형, 대형) 다양한 데이터 소스들과 함께 작동한다. 이 사양은 센서 네트워크 아키텍처에서 가용한 모든 유형의 집선기들의 일반적인 개념의 관점에서 다음을 정의한다〔17〕.

- 집선기는 다양한 데이터 소스들과 함께 작동한다.
- 효율적으로 데이터 소스와 그 내용의 효과적 관리는 XEP의 중요한 부분이 된다.
- 대량의 개체를 다룰 수 있는 능력
- 이해당사자 간의 효과적 동기화
- 집선기에 의해 통제되는 개체와의 효율적인 상호작용



〔그림 8〕 Concentrators 개념도

3.3.4 EXI(Efficient XML Interchange)

XEP-0322 EXI는 XML 문서와 프레그먼트들에 대한 효율적인 압축방법을 제시한다. EXI 압축을 활성화하면 서버와 클라이언트가 일련의 파라미터들에 의해 동의할 경우 사전에 핸드쉐이크를 요구하게 된다. EXI는 Normal XMPP 포트 또는 전용 이진 EXI 포트를 통해 스트림 압축(XEP-0138)을 사용한 EXI 압축을 활성화하는 방식과 클라이언트 측에서 서버에 접속하여 처음부터 직접 EXI를 사용하여 시작하는 방식으로 사용할 수 있다〔11〕.

이러한 방식의 EXI는 센서 네트워크와 같은 어플에 있어 매우 중요한 요소이다. 압축을 통해 데이터 패킷 사이즈를 줄임으로써 제한된 메모리로 센서들 간에 효율적인 의사소통을 가능하게 하기 때문이다.

3.3.5 Discovery

XEP-0347 Discovery는 XMPP 프로토콜 기반 아키텍처 상에서 사물들(Things)이 그들의 소유자에 의해 설치되고 탐색되어지며, 네트워크 상에 존재하는 사물들과 연결되는 방법들에 대해 기술하고 있다. 사물들은 다음과 같은 수명주기를 통해 식별되고 연결될 수 있다 [18].

① 생산 : 사물의 생산과정에서 XMPP 서버의 도메인과 주소, JID와 같은 매개변수가 사전 구성 및 설치 후 수동 입력 또는 장치에 의해 자동 탐색되어야 함

② 설치 : 물리적 설치 및 전력 연결과 통신 인프라 연결 이외에, 설치 단계에서는 생산 환경에서 사물들이 구성할 수 없는 값들을 수동으로 구성될 수 있어야 함

③ XMPP 서버 탐색 : XMPP 서버의 주소가 사전 구성되지 않았다면, 사물은 DHCP, Multicast DNS, SSDP/UPnp 등을 통해 반드시 로컬 주변의 요소를 찾기 위해 시도함.

④ XMPP 서버 연결 : XMPP 서버가 탐색되면, 연결이 진행된다. 만약 다중의 XMPP 서버가 탐색되면, 클라이언트 측에서는 목적에 맞는 최적의 서버를 선택할 수 있음.

⑤ 사물 레지스트리 탐색 : 만약 사물 레지스트리가 사전 구성되지 않았다면, 반드시 하나는 탐색되어야 함. 사물 레지스트리는 XEP-0114 또는 JID를 통해 접속할 수 있는 XMPP 클라이언트를 사용해 서버 컴포넌트에게도 호스팅 될 수 있음.

⑥ 사물 등록 : 사물 레지스트리가 탐색되었고 친구가 되었을 경우(befriended), 사물은 레지스트리에 자신을 등록 가능.

⑦ 자기소유(self-owned) 사물 등록 : 만약 사물이 자기소유일 경우, 정상으로 레지스트리에 자신을 등록 가능하며 장치에 대한 소유권 주장이 필요치 않음. 이것은 공개적으로 사용되어야 하는 사물들을 설치할 경우에 유용할 수 있음.

⑧ 집선기(Concentrator)에 사물 등록 : 사물 등록 요청 시 사물의 JID 식별을 위해 사용되는 3가지 속성(노드 Id, 소스 Id, 캐쉬 Type)을 추가함으로써 사물을 집선기에 등록 할 수 있음.

⑨ 사물의 소유권 청구 : 사물의 소유자는 소유권을 주장하기 위해 사물 레지스트리에서 제공된 정보를 제공해야 한다. 정보 추측의 가능성을 피하기 위해 정보는 충분이 길어야 하며 전송 문제를 해결하기 위해 QR코드를 제시함.

⑩ 레지스트리로부터 사물 제거 : 소유자는 삭제 요청을 레지스트리에 전송함으로써 사물을 제거 할 수 있음.

⑪ 프로비저닝 서버 탐색 : 액세스 권한 및 사용권한 제어를 위한 프로비저닝 서버 탐색(XEP-0324) 참조.

⑫ 신뢰 위임 : 프로비저닝 서버가 탐색되었고 친구가 되었을 경우(befriended), 사물은 서버에게 신뢰를 위임할 수 있음.

⑬ 레지스트리 내의 사물 메타 정보 갱신 : 사물의 소유권이 청구되고 레지스트리 내에 공공 사물로 선택되었을 경우, 언제든지 메타 정보를 갱신할 수 있음.

⑭ 레지스트리 내의 공공 사물 검색 : 자기 소유 사물을 포함한 공공 사물에 대해 소유권이 청구된 누구든지 사물 레지스트리 내에 공공 사물 검색이 가능함. 단, 소유권 청구가 되지 않았거나, 레지스트리로부터 제거된 사물에 대해서는 검색이 불가.

⑮ 레지스트리로부터 사물 등록 해제 : 레지스트리에 사물 등록 취소 요청을 보냄으로써 사물 등록을 해제함.

⑯ 사물 부인 : 사물의 소유자는 소유자가 없는 상태를 반환함으로써 사물을 부인할 수 있음.

Ⅳ. 결 론

사물인터넷은 세계적으로 아직까지 도입 초기 단계이며 그 활용방안이 무궁무진하여 IT 및 관련 업계에 엄청난 영향을 가져올 것으로 예상된다. 하지만 빛이 있으면 그림자 또한 생기듯이 잠재적 발전 가능성과 업계의 새로운 성장 동력임에는 분명하나, 이를 악용하는 사례들 또한 심심치 않게 등장하는 바, 보안에 대한 각별한 주의가 요구되는 실정이다. 따라서 본 논문에서는 사물인터넷 환경을 구성하는 주 요소인 센서 네트워크 보안을 위한 Sensei/IoT* (P21451-1-4) 기술에 대해서 소개하였다. 이는 현재 나와 있는 IoT 관련 프로토콜

(MQTT, MQTT-S, CoAP, REST API, XMPP) 중 XMPP를 활용한 기술로 상호 운영성(Interoperability)과 높은 확장성(High Scala bility) 및 내재된 보안 기능(Security)을 제공한다. 이 기술은 아직까지는 표준화를 위한 개발 및 실험단계에 있으나, 향후 이를 적용한 실제 사례와 솔루션 등이 등장 할 것이라 예상된다.

참 고 문 헌

[1] “More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020”, [Online] Available: https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne

[2] Wikipedia, "XMPP", [Online] Available: http://en.wikipedia.org/wiki/XMPP

[3] http://www.xmpp.co.kr/?q=node/72

[4] RFC-3920, “Extensible Messaging and Presence Protocol (XMPP) : CORE”, [Online] Available: http://tools.ietf.or g/html/rfc3920

[5] Craig K. Harmon, “ANSI-HSSP Global Supply Chain Security Standardization” 2010. [Online]. Available: http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/Homeland%20Security%20Standards%20Panel/ANSI-HSSP%20Ninth%20Annual%20Plenary%20Meeting/Panel%204%20-%20Global%20Supply%20Chain%20Security/Harmon%20Panel%204.pdf

[6] William J. Miller, “Intrusion Prevention for Sensor Net works, M2M & the Internet of Things (IoT), ISO/IEC/IE- EE P21451-1-4”, February 2013. [Online] Available: http://csrc.nist.gov /cyberframework/rfi_comments/mact_part_3_022613.pdf

[7] William J. Miller, "XMPP, Big Data, and the Smart Grid" 2013, [Online] Available: http://ewh.ieee.org/conf/sege/2013/William-Miller-Talk.pdf

[8] Kang Lee, “Smart Sensor Network and Sensor Smart Sensor Network and Sensor-RFID Standards for Supply Chain“ 2010. [Online] Available: http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/Homeland%20Security%20Standards%20Panel/ANSI-HSSP%20Ninth%20Annual%20Plenary%20Meeting/Panel%204%20-%20Global%20Supply%20Chain%20Security/Lee%20Panel%204.pdf

[9] William J. Miller, "Protocol Transfor mation Defense Against Cyber Attack" 2012, [Online] Available: http://www. controlglobal.com/articles/2012/ cyber-attack-defense/

[10] Ian Paul, “70-plus XMPP messaging services now securing chats with TLS encryption” 2014. [Online]. Available: http://www.pcworld.com/article/2157180/xmpp-services-push-encrypted-connections-by-default.html

[11] P. Waher and Y. DOI, "XEP-0322 : Efficient XML Interchange (EXI) Format," 2014. [Online]. Available : http://xmpp.org/extensions/xep-0322.html

[12] Ian Paterson, Dave Smith, Peter Saint-Andre, Jack Moffitt, Lance Stout, Winfried Tilanus, “XEP-0124: Bidirectio nal-streams Over Synchronous HTTP (BOSH)” 2014. [Online]. Available : http://xmpp.org/extensions/xep-0124.html

[13] 임형준, 송찬호, 백문기, 이규철, “사물인터넷에서 서비스 연동을 위한 양방향 REST 어댑터 설계”, 정보과학회논문지(컴퓨팅의 실제 및 레터 제20권 제1호), Jan 2014.

[14] XMPP Standards Foundation (XSF), “ XMPP Extensions”, [Online] Available : http://xmpp.org/xmpp-protocols/xmpp-extensions/

[15] P. Waher, “ XEP-0323: Internet of Things - Sensor Data” 2014. Available : http://xmpp.org/extensions/xep-0323.html

[16] P. Waher, “XEP-0324: Internet of Things - Provisioning” 2014. Available : http://xmpp.org/extensions/xep-0324.html

[17] P. Waher, “XEP-0326: Internet of Things - Concentrators” 2014. Available :http://xmpp.org/extensions/xep-0326.html

[18] P. Waher, Ronny Klauck, “XEP-0347: Internet

of Things - Discovery” 2014. http://xmpp.org/extensions/xep-0347.html

〈저 자 소 개〉

신 수 민 (Su-Min Shin)
학생회원

2014년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 모바일 보안, 침투테스트, ISMS, 개인정보보호

김 학 범 (Hak-Beom KIM)
정회원

1992년 1990년 8월 : 중앙대학교 대학원
전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원(KISA) 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2011년 9월~2013년 3월 : (주)지엔에스인증원 ISMS본부장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2013년 4월~현재 : ㈜이너버스 연구소장
<관심분야> 통합로그 시스템, 빅데이터 보안, 클라우드 컴퓨팅 보안, 개인정보보호, PIMS