The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 6, pp.1-6, Dec. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.6.1
JIIBC 2014-6-1

리버스 프록시 기반 IoT 서비스 도메인 설계

Design of Smart Service based on Reverse-proxy for the Internet of Things

박지예*, 강남희**

Jiye Park*, Namhi Kang**

요 약 최근 사물인터넷, IoT(Internet of Things)는 초연결 사회 실현을 위한 핵심 기술로 주목받고 있다. 이에 ICT 산업과 다수의 표준화 기구에서는 IoT 현실화를 위해 많은 노력을 기울이고 있다. 그 중 IETF CoRE 워킹그룹에서는 IoT 장치를 위한 프로토콜로 CoAP을 표준화 하였으며, CoAP 옵션의 일부분으로 포워드 프록시 사용을 제공하고 있다. 포워드 프록시는 CoAP을 지원하지 않는 레거시 장치를 위한 프로토콜 번역을 수행, 메시지 릴레이를 위한 목적으로 사용된다. 하지만 인터넷 환경의 클라이언트와 자원이 제한적인 IoT 환경 내 CoAP 서버 간 통신 시스템 구조가 실제 서비스 도메인에 적용되는 경우, 배터리 절약을 위한 Sleep mode 서버에서의 응답문제, URI 할당 및 접근 문제, DoS 문제 등이 발생한다. 이를 해결하기 위해 본 논문에서는 리버스 프록시 기반 IoT 시스템을 제안한다. 본 제안 시스템에서는 정적인 IoT 환경과 동적인 IoT 환경을 모두 고려하였다. 상기 문제를 해결한 제안 시스템 구조는 실제 IoT 서비스를 효율적으로 제공 할 수 있을 것으로 예상된다.

Abstract The IoT (Internet of Things) is considered as a core technology to realize interconnected world. At this, companies composing ICT industry and standard organizations make efforts to accelerate it. IETF CoRE(Constrained RESTful Environment) working group standardized CoAP (Constrained Application Protocol) for the constrained device. CoAP has RESTful architecture and CoAP option is provided to use forward-proxy. The forward-proxy is used to translate protocol and perform requests on behalf of the client. However, communication between Internet based client and LLN(Low-power and Lossy Network) based CoAP server architecture has limitations to deploy real IoT service. In this architecture, problems like response delay, URI assignment and DoS attack can be occurred. To solve these problems, we propose the reverse-proxy based system. We consider both of static IoT and mobility IoT environments. Finally, our proposed system is expected to provide efficient IoT service.

Key Words : Internet of Things, Reverse-proxy, URI assignment, Resource discovery.

Ⅰ. 서 론

사물인터넷, IoT(Internet of Things)는 인터넷을 기반으로 모든 사물을 연결하고자 하는 패러다임이다. IoT는 인프라의 발전, 인터넷에 연결되는 사물의 수 증가를 기반으로 초연결사회 실현을 위한 핵심으로 전망되고 있다[1]. 사물 인터넷은 스마트 홈, 스마트 헬스케어, 스마트 시티 등 많은 분야에 적용될 수 있다. 개인이 소유한 장치

*학생회원, 덕성여자대학교 전산정보통신학과
**정회원, 덕성여자대학교 디지털미디어학과(교신저자)
접수일자 : 2014년 8월 6일, 수정완료 : 2014년 9월 14일
게재확정일자 : 2014년 12월 12일

Received: 6 August, 2014 / Revised: 14 September, 2014
Accepted: 12 December, 2014
**Corresponding Author: kang@duksung.ac.kr
Dept. of Digital Media, Duksung Women's University, Korea

와 공공의 장치가 인터넷을 기반으로 연결되어 맞춤형 서비스로 제공될 수 있으며(예, [2]) 경제적 파급 효과는 2020년 까지 1.9조 달러에 이를 것으로 예측 된다[3]. 이에 IoT 생태계를 구성하고 있는 칩셋 제조사, 단말 제조사, 통신 사업자, 서비스 사업자 등 사업자는 IoT 현실화를 위한 가치 체인을 형성하고 있다.

IoT 현실화를 위한 연구는 ETSI, ITU-T, IETF, 3GPP등과 같은 표준화 기구에서도 활발히 진행되고 있다. 그 중, IETF CoRE(Constrained RESTful Environments) 워킹그룹에서는 IoT를 구성하는 작은 임베디드 장치를 위한 어플리케이션 프로토콜 CoAP(Constrained Application Protocol)을 표준화 하였다[4]. CoAP 프로토콜은 RESTful 구조를 가지는 UDP기반 프로토콜로서, GET, PUT, POST, DELETE와 같은 함수를 사용하며 RESTful 구조 웹 프로토콜인 HTTP와 많은 유사성을 가지고 있다. 또한 CoRE 워킹그룹에서는 CoAP 기반 장치와 CoAP을 지원하지 않는 장치 간 통신을 위한 프로토콜을 번역, 클라이언트의 요청 포워딩, 서버로부터의 응답 릴레이 등을 위한 용도로 프록시 사용을 제안하였다.

프록시는 포지션에 따라 클라이언트 측을 위한 포워드 프록시와 서버측을 위한 리버스 프록시로 구분된다. 각각의 프록시는 현재 웹 시스템에서 사용되는 장치로 다음 그림1과 같은 구조를 가진다.

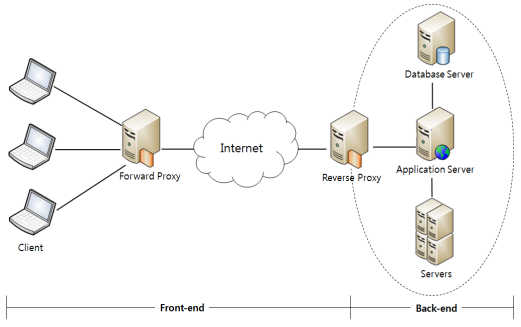


그림 1. 프록시 기반 웹 서비스 시스템 구조
Fig. 1. Proxy based web service system architecture

웹 시스템에서 포워드 프록시는 클라이언트에 의해 설정된다. 웹 서버로 데이터 요청 시 포워드 프록시를 통해 요청이 포워딩되며 웹 캐싱을 통해 응답 시간을 줄이고 네트워크 자원을 절약할 수 있는 장점이 있다. 반면 리버스 프록시는 서버 사이드 프록시로 엑세스 컨트롤, 로드 밸런싱(예, [5], SPOF(Single Poing Of Failure) 방지를 위한 용도로 사용된다.

CoAP 프로토콜에서는 포워드 프록시를 이용하기 위한 방안으로 Proxy-Uri 옵션을 제공한다. CoAP 프로토콜을 사용하는 IoT 장치는 서비스에 따라 서버와 클라이언트 역할을 모두 수행할 수 있다. 클라이언트가 CoAP 기반 IoT 장치인 경우 포워드 프록시는 유용하게 사용될 수 있다. 하지만 자원이 제한적인 IoT 환경 특성상 클라이언트가 인터넷 환경에서 브라우저를 이용하여 CoAP 서버에 데이터 요청을 하는 경우, 포워드 프록시의 도움만으로는 원활한 통신을 하는데 많은 제약이 있다. 따라서 제한된 환경 내 CoAP 서버를 위한 리버스 프록시에 대한 고려가 이루어져야 한다.

IoT의 환경적 특성을 고려한 본 논문에서는 일반적인 IoT 시스템에서 웹 브라우저를 이용하는 클라이언트가 CoAP 서버로 데이터 요청 시 발생할 수 있는 문제를 제시하고, 이를 해결할 수 있는 리버스 프록시 기반 IoT 서비스 도메인을 설계한다.

본 논문은 다음과 같이 구성된다. 2장에서는 IoT의 환경적 특성에 대해 자세히 설명하고 리버스 프록시가 고려되지 않았을 경우 발생 될 수 있는 문제 대해 기술한다. 3장에서는 상기 문제를 해결하기 위한 시스템을 제안한다. 마지막으로 4장에서는 결론을 맺는다.

II. 제안 시스템 배경

IoT는 노트북, PC 등 컴퓨팅 성능이 좋은 장치로 구성된 TCP 기반 인터넷 환경과 확연이 구분되는 두 가지 특징을 가진다. 첫째, 장치는 이기종의 임베디드 형태로 구성된다. 따라서 대다수의 기기는 메모리, CPU, 배터리와 같은 자원이 제한 되어있다. 장치는 자원이 제한적인 정도에 따라 3개의 클래스로 구분 된다[6]. Class 0에 해당하는 장치는 10 KiB 이하의 RAM, 100 KiB 이하의 ROM을 갖는 초경량 장치로, 인터넷 환경과 통신하기 위해서는 프록시나 게이트웨이와 같은 인프라 장치의 도움이 필요하다. 또한, IoT 장치는 배터리를 절약하기 위한 방안으로 자원 제약성을 고려한 스케줄에 따라 Sleep mode를 상태를 갖는다.

둘째, IoT를 구성하고 있는 네트워크는 127 byte의 MTU 사이즈를 갖는 IEEE 802.15.4와 같은 저 전력 네트워크로 구성된다[7]. LLN(Low power and Lossy Network)으로 분류되는 IoT 네트워크 환경은 기본 1500

byte의 MTU를 갖는 인터넷 환경에서 대량의 데이터 요청이 들어올 경우, 쉽게 과부하가 발생될 수 있다.다음 그림 2는 일반적인 IoT 구조를 나타낸다.

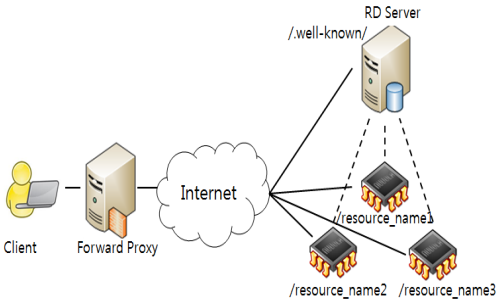


그림 2. 일반적인 IoT 7시스템 구조
Fig. 2. Common IoT system architecture

RD(Resource Directory) 서버는 리소스 디스커버리 기능을 통해 각 센서의 도메인 네임, 리소스 네임, 리소스 타입 등을 저장 한다[8]. RD 서버에 저장된 정보는 클라이언트로부터 Coap://domain_name/.well-known/ URI 요청 시 /resource_name 의 형태로 이용할 수 있는 센서 정보를 전송 받는다.

CoAP 센서는 설정된 기능 및 서비스에 따라 특정 도메인에 속하며 RD 서버에 저장된 리소스 네임을 참조하여 CoAP://domain_name/resource_name 형태의 URI를 갖는다.

상기 구조는 인터넷 기반 클라이언트와 CoAP서버 간 통신의 일반적인 시스템 구조이지만 실제 서비스를 제공하는 경우 다음과 같은 문제가 발생된다.

- **Sleep Mode 센서**

정해진 스케줄에 따라 Sleep Mode로 상태 변환된 센서로 데이터 요청이 올 경우, 클라이언트는 요청에 대해 즉시 응답 받을 수 없다. 따라서 Wake up 메시지 전송, 응답 과정이 추가적으로 필요하다. 이는 데이터를 전송받는데 까지 걸리는 시간 증가의 요인이 된다.

- **URI 할당 및 접근 방법**

센서에는 네트워크 환경에 따라 공인, 사설 IP 주소가 각각 할당이 되어 있다. RD 서버에 입력된 도메인 네임과 리소스 네임을 참조 하여 생성된 Coap://domain_name/resource_name 형태의 URI는 현재 DNS 시스템에서 고유 IP 주소를 가진 /resource_name 센서로 요청이 전달되는 것이 아니라 도메인의 IP로 요청이 전달된다. 따라서 동일한 도메인을 갖는 센서 /resource_name1과/resource_name2로 전송되는 요청의 경우 모두 domain_name 서버로 설정된 IP로 전송되므로 구분되지 않는다.

직관적인 방법으로, 각각의 센서에 도메인을 부여하여 Coap://resource_name.com와 같은 형태로 접근 할 수 있다. 하지만 이 역시 160억 개로 증가될 것으로 예상되는 IoT 장치에 모두 도메인 주소를 할당하기에는 많은 무리가 있다. 또한 이동성이 있는 헬스케어 센서의 경우 호스팅 정보는 위치에 따라 변경되는 IP 정보를 시시각각 반영해야 하는 어려움이 있다.

- **DoS 공격**

IoT 장치는 메모리, CPU, 배터리와 같은 자원이 매우 한정되어 있다. 따라서 성능이 좋은 인터넷 환경으로 부터 DoS 공격이 발생하는 경우 쉽게 공격 받을 수 있다.

Ⅲ. 제안 시스템

본 장에서는 IoT 환경적 특성을 고려한 URI 기반 통신 시스템을 제안한다. 크기가 작고 가벼워 휴대하기 쉬운 장치 특성에 따라 스마트 홈과 같이 한정된 공간 내에 장치가 존재하는 경우와 스마트 헬스케어와 같이 각 장치가 이동성을 갖는 환경으로 나누어 제안한다.

1. 스마트 홈

스마트 홈은 다양한 성능을 가진 장치들로 구성된다. 제안 서비스 도메인은 다음 그림 3과 같다.

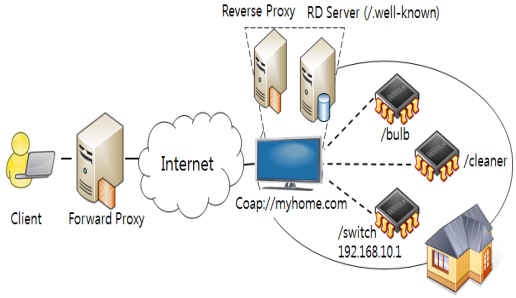


그림 3. 스마트 홈 제안 시스템 구조
Fig. 3. Proposed smart home system architecture

각 센서는 자원 경량화 정도에 따라 일정시간 sleep mode 상태로 유지되며, sleep mode 상태 변환 전, 리버스 프록시에 가장 최근의 센싱 정보를 전송한다. 본 제안 서비스 도메인에서는 비교적 컴퓨팅 성능이 뛰어나고 전력 공급이 안정적인 스마트 TV가 리버스 프록시의 역할을 수행한다. 또한 스마트 TV는 집안의 각 센서를 정보를 등록하고 관리하는 RD 서버 역할을 수행할 수 있다.

다음 그림 4는 클라이언트가 센서 정보 요청 시 수행되는 동작의 흐름을 나타낸다.

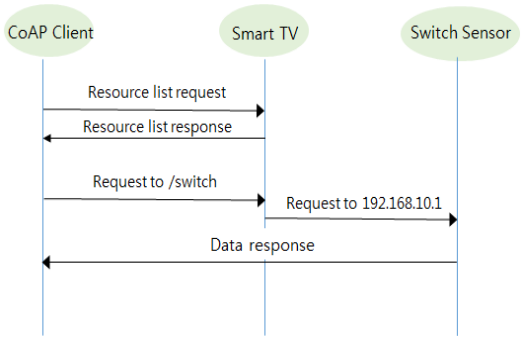


그림 4. 제안 시스템 메시지 흐름
Fig. 4. Proposed smart home system message flow

IoT 홈 네트워크에 접속하고자 하는 클라이언트는 Coap://myhome.com/.well-known/ 요청을 통해 RD 서버, 즉, 스마트 TV가 관리하고 있는 센서 리스트에 대에 대한 리소스 네임을 전송 받는다. 클라이언트는 Coap://myhome.com/switch path를 가진 센서에 대한 센싱 정보를 요청한다. 요청은 리버스 프록시 역할을 수행하는 스마트 TV로 전송된다. 스마트 TV는 Coap://myhome.com/switch -> 192.168.10.1 로 설정되어 있는 가상 호스팅 테이블을 참조하여 실제 센서에 데이터를 요청한다. switch 센서는 센싱 정보를 리버스 프록시에 전송하고 이는 클라이언트로 포워딩 된다.

센서가 sleep mode 상태일 경우, 리버스 프록시는 최근 전송받은 센싱 정보를 클라이언트에 전송하고, 일정 시간 이상 지난 정보일 경우 센서에 데이터 요청을 위한 wake up 메시지를 전송한다. 포워드 프록시의 캐싱 기능과는 달리, 리버스 프록시에서의 데이터 캐싱 기능은 Sleep mode 상태로 돌입하기 직전, CoAP 서버의 최신 센싱 정보를 저장하기 위한 용도로 사용된다. 리버스 프록시에서의 캐싱 기능을 통해 경량화 된 장치의 배터리 소모를 줄일 수 있다.

리버스 프록시 역할을 수행하는 스마트 TV를 통해 메시지 요청이 전달되므로, 인터넷 환경으로부터 자원이 제한적인 장치에 직접 접근하는 것을 사전에 차단하여 다량의 데이터로 인한 DoS 공격에 대응 하여 LLN 내부를 보호할 수 있다.

2. 스마트 헬스케어

제안하는 스마트 헬스케어 시스템은 다음 그림 5와 같이 센서를 부착한 사용자의 이동으로 개인 도메인이 병원과 같은 공공 장소의 IoT 도메인과 겹치게 되는 구조를 가진다.

본 장에서는 '사용자'를 헬스케어 센서를 부착하고 있는 스마트 헬스케어 서비스 유저로, '클라이언트'는 인터넷 기반 환경에서 브라우저를 통해 환자의 상태를 모니터링하는 의사로 각각 구분하여 기술한다.

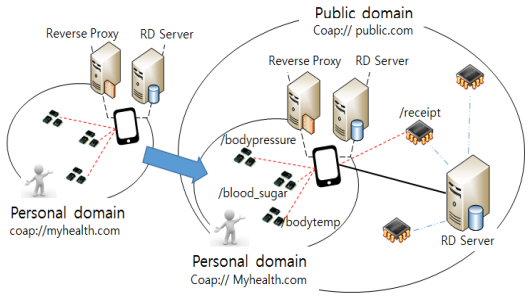


그림 5. 스마트 헬스케어 시스템 구조
Fig. 5. Proposed smart healthcare system architecture

제안 시스템에서 개인 도메인에 속하는 헬스케어 장치는 public IP 주소가 할당 되어 있으며 위치 이동에 따라 IP주소가 변경된다. 또한 사용자의 스마트폰은 리버스 프록시와 RD 서버 역할을 수행할 수 있다.

위치 이동으로 인해 센서의 아이피가 변경되는 경우, 센서는 스마트폰의 RD 테이블에 새롭게 리소스 등록을 한다. 따라서 클라이언트는 헬스케어 센서의 IP 주소 변경에 상관없이 Coap://myhealth.com/.well-known/ 요청을 통해 통신이 가능한 센서 정보를 전송 받을 수 있다. 리버스 프록시 기능을 하는 사용자의 스마트 폰은 업데이트 된 RD 정보를 참조하여 센서의 경로가 되는 리소스 네임과 실제 IP가 입력되는 가상 호스팅 테이블을 생성하고, 특정 센서의 데이터 요청 시 이를 실제 센서로 포워딩 한다.

사용자의 이동으로 Coap://myhealth.com의 도메인을 가지는 personal domain이 Coap://public.com 도메인을 가지는 public IoT domain 환경과 겹치게 되는 경우, 스마트폰은 Coap://public.com의 RD 서버로 리소스 디스커버리 메시지를 전송하여 전송받은 정보를 토대로 public.com 도메인을 가지는 센서 중 클라이언트가 이용할 수 있는 센서에 대한 정보를 자신의 RD에 저장한다. 스마트 폰은 RD에 저장된 데이터를 가상 호스팅 테이블을 업데이트 한다. 가상 호스팅 테이블은 다음과 같은 형태를 가진다.

표 1. 가상 호스팅 테이블
Table 1. Virtual Hosting table

Resource path	Resource IP
/bodypressure	203.252.3.x
/blood_sugar	203.252.3.x
/bodytemp	203.252.3.x
/receipt	203.252.4.x

따라서 클라이언트는 자신의 스마트폰을 이용하여 Coap://myhealth.com/receipt 형태의 URI를 이용하여 외부 도메인에 속한 센서를 personal domain의 리소스처럼 접근하여 사용할 수 있다.

Ⅳ. 결 론

본 논문에서는 일반적으로 알려진, 인터넷 클라이언트와 IoT 서버환경 간 시스템 구조에서 실제 서비스 제공 시 발생할 수 있는 Sleep mode의 IoT 서버 응답 문제, URI 할당 및 접근 문제, DoS 공격 등의 문제점을 기술하였다. 또한 이를 해결하기 위한 방안으로 리버스 프록시 기반 IoT 서비스 도메인 구조를 제안하였다. 제안 시스템에서는 정적 IoT 환경과 동적 IoT 환경을 고려하였으며 각각 서비스 도메인에서 리버스 프록시와 RD 서버기능을 할 수 있는 장치를 통해 URI 기반 접근성을 높이고 Sleep mode 상태 서버 접속에서 발생되는 응답 지연 문제를 해결하였다. 또한 리버스 프록시에서의 Access control을 통해 IoT 도메인에서 발생하는 DoS를 경감시켰다.

References

[1] L.Tan, N. Wang, “Future Internet: The Internet of Things”, Int, Conf of ICACTE 2010, August 2010.

[2] W. Jung, N. Kang, “A Compoment-Based Framework for Structural Embedding of Mobile Agent System”, Journal of the Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 12 No. 6, pp. 33-42, 2012

[3] The Internet of Things, Worldwide, Gartner, Inc. 2013.

[4] Z. shelby, K. Hartke, C. Bormann, “The Constrained Application Protocol (CoAP)”, RFC 7252

[5] H. Noh, N. Kang, “Efficient Buffer Managerment scheme for Mitigation Pssibility of DDoS Attack”, Journal of the Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 12 No. 2, pp. 1-7, 2012

[6] M. Kovatsch, “CoAP for the Web of Things : From Tiny Resource-constrained Devices to the Web Browser”, Int, Workshop on the Web of Things (WoT 2013), Sept. 2013.

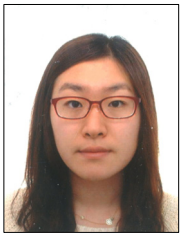
[7] A. Mayzaud, R. Badonnel, I. Chrisment, “Monitoring and security for the Internet of Things”, Emerging Managerment Mechanisms for the Future Internet (pp. 37-40), 2013.

[8] Z. Shelby, C. Bormann, S. Krco, “CoRE Resource Directory” Draft, IETF, December 2013.

본 연구는 덕성여자대학교 2013년도 교내연구비 지원에 의해 수행되었음

저자 소개

박 지 예(학생회원)



- 2013년 : 덕성여자대학교 컴퓨터시스템학과 졸업
- 2013 ~ 현재 : 덕성여자대학교 전산정보통신학과 석사과정

<관심분야 : Security for Internet of Things, Web of Things>

강 남 희(정회원)

- 1999년 3월 ~ 2001년 2월: 숭실대학교 공학석사
- 2004년 12월 : University of Siegen, 공학박사
- 2009년 3월 ~ 현재 : 덕성여자대학교 디지털미디어학과 조교수

<주관심분야 : 인터넷통신, 통신보안>