DHCP 기반 IoT 디바이스를 위한 DNS 네이밍 기술

이근태 ○, 김석화, 정재훈
성균관대학교 전자전기컴퓨터공학과
{keuntaelee, seokhwakim, pauljeong}@skku.edu

DHCP-Based DNS Naming Scheme for IoT Devices

Keuntae Lee○, Seokhwa Kim, Jaehoon (Paul) Jeong
Department of Computer Science and Engineering,
Sungkyunkwan University

요 약

본 논문은 최근 가장 주목 받고 있는 연구 분야 중 하나인 사물인터넷(Internet of Things, IoT)을 위한 DNS 네이밍 서비스 기술에 대해 소개한다. 점차 늘어나는 IoT 디바이스의 수에 따라 DNS 네임을 일일이 수동적으로 설정하는 것은 비효율적이다. 본 논문에서는 이러한 IoT 디바이스들을 위한 DHCP 기반의 DNS 네임 자동설정 기법을 소개한다. 본 논문에서 제안한 DNS 네임 자동설정 기법을 통해 사용자는 쉽고 간편하게 DNS 네임을 등록할 수 있으며, 스마트폰 등의 모바일 스마트 디바이스로 등록된 IoT 디바이스들을 모니터링 및 원격제어 할 수 있다.

1. 서론

최근 가장 주목받고 있는 연구 분야 중 하나인 사물인터넷(Internet of Things, IoT)은 네트워크에 연결된 매우 많은 디바이스를 통해 사용자에게 다양한 서비스를 제공하는 것을 목표로 한다. 미국의 시장조사기관인 가트너(Gartner)는 2014년도에 발표한 Hype Cycle에서 향후 5년에서 10년 정도 가장 유망한 미래의 기술로 IoT를 선정했고, 2018년도까지 80억개의 IoT 디바이스가 증가해서 총 160억개의 IoT 디바이스가 존재할 것이라고 발표했다[1]. 이렇듯 수많은 IoT 디바이스를 관리하기 위해 IoT 디바이스에 대한 Domain Name System(DNS) 네임을 일일이 수동으로 설정하는 것은 비효율적이다. 따라서 본 논문에서는 Dynamic Host Configuration Protocol(DHCP) 기반의 DNS 네임 자동설정에 대해 제안하려 한다.

사물인터넷 디바이스를 위한 IPv6 네트워크 상의 DNS 네임 자동설정 및 네이밍 서비스로는 DNS Name Autoconfiguration(DNSNA)가 제안되었다[2]. 또한 IPv4 네트워크 상의 사물인터넷 디바이스를 위한 네임 자동설정으로는 DNSNAv4가 제안되었다[3].

본 논문에서는 IPv4 인터넷에서 호스트의 네트워킹 자동설정(예, 호스트 IP 주소, 서브넷, 게이트웨이 IP 주소, DNS Domain)을 위한 DHCP 프로토콜을 기반한 DNS 네임 자동설정기법을 설명한다. 또한 DHCP에 관련된 인터넷 표준문서 RFC[4, 5, 6]에서는 호스트들이 중복된 DNS 네임을 사용하고자 할 때 발생하는 DNS 네임 충돌에 대한 해결책을 명확히 제시하고 있지 않다. 본 논문은 이러한 DNS 네임 충돌에 대한 것도 포함하여 IoT 디바이스를 위한 DNS 네임 자동설정 기법을 제시하고자 한다.

2. 본론

2.1 DHCP 기반의 DNSNA 구조도

본 절에서는 DHCP 기반의 DNSNA의 구조에 대해 설명한다. 그림 1은 DHCP 기반의 DNSNA의 구조도이다.

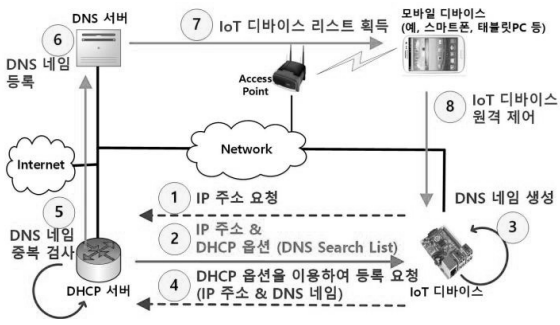

그림 1. DHCP 기반의 DNSNA 구조도

DHCP 기반의 DNSNA의 순서는 다음과 같다. 먼저 IoT 디바이스가 DHCP 프로토콜에 따라 DHCP 서버에게 자신이 사용할 IP 주소를 요청한다. DHCP 서버는 IoT 디바이스에게 필요한 IP 주소를 할당하면서 DHCP 옵션을 이용하여 DNS Search List(DNSSL)를 넘겨준다. IoT 디바이스는 받은 DNSSL를 이용하여 자신의 DNS 네임을 생성한다. 그리고 자신의 할당

받은 IP 주소와 DNS 네임을 DHCP 서버에게 등록하도록 요청한다.

이 때 요청하는 메시지는 기존에 제안된 구조들[2, 3]과 다르다. 본 논문에서 제안하는 DNS 네임 자동설정은 DHCP 옵션을 새롭게 정의하여 IoT 디바이스가 DHCP 서버에게 DNS 네임 등록을 요청하는 방식이다. 이 때 사용되는 옵션과 포맷은 IoT 디바이스를 위한 것들이고 DNS 네임은 기존에 제안된 DNSNA의 네임 포맷을 따른다.

DHCP 서버는 받은 DNS 네임이 중복되는지 검사를 한다. 만약 중복된다면 이름 충돌 방지 솔루션에 따라 처리하도록 한다. 이에 대한 내용은 2.3절에서 다루도록 한다. 만약 IoT 디바이스의 DNS 네임이 중복되지 않는다면 DNS Dynamic Update 기능[7]을 이용하여 DHCP 서버는 DNS 서버에게 IoT 디바이스의 해당 DNS 네임 정보를 업데이트 하도록 요청한다. DNS 서버가 IoT 디바이스들의 DNS 네임을 등록해서 저장한 뒤 사용자는 모바일 디바이스(예, 스마트폰, 태블릿 PC 등)을 이용하여 DNS 서버로부터 사용 가능한 DNS 네임 리스트들을 받아오고 이를 이용하여 필요한 IoT 디바이스들을 원격제어 및 모니터링 할 수 있게 된다.

2.2 DNSNA 네임 포맷

본 절에서는 DNSNA에서 사용되는 DNS 네임 포맷에 대해 설명한다. 그림 2는 IoT 디바이스를 위한 DNS 네임 포맷이며, 우리의 국제인터넷표준화기구인 Internet Engineering Task Force (IETF) 기고서를 참조하였다[8].

unique_id.object_identifier.OID.mic_loc.mac_loc.LOC.domain_name

그림 2. DNS 네임 포맷

- **unique_id** : ASCII 문자로 된 DNS 이름의 고유성을 보장하는 고유한 식별자. 예를 들어, 식별자는 제품명, 시퀀스 번호와 같은 가독성을 갖는 영문 또는 숫자일 수 있다.
- **object_identifier** : 디바이스의 객체 식별자는 상위 아크. 즉, M2M 노드 표시 ID (즉, 관리 조직, 관리, 데이터 국가 코드 및 M2M 노드의 연결)와 네 개의 호의 시퀀스(즉 제조업체 ID, 모델 ID, 일련 ID 및 확장 ID)가 정의되어 있다[9]. 필드는 밑줄 '_' 로 구분된다.
- **OID** : object_identifier가 사용되었음을 나타내는 OID 키워드의 서브도메인이다.
- **mic_loc** : 디바이스의 미시적 위치(예, 중심, 모서리, 코너 등)를 나타낸다.
- **mac_loc** : 디바이스의 거시적 위치(예, 거실 및 주방 등)를 나타낸다.
- **LOC**: mac_loc 및 mic_loc가 사용됨을 나타내기 위한 서브도메인이다.
- **domain_name**: IoT 장치가 있는 네트워크의 DNS 도메인을 나타내는 도메인 서픽스 (Suffix)이다.

2.3 DNS 네임 충돌 방지

본 절에서는 DHCP 기반의 DNSNA 구조에 대한 DNS 이름 충돌은 다음과 같이 세가지 경우를 고려한다. 본 논문의 DNS 네임 충돌 방지는 IoT 디바이스의 서브넷과 IoT 디바이스와 떨어져 있는 다른 서브넷을 고려해서 수행하다. 즉 IoT 디바이스의 서브넷의 DNS 중복 탐지 및 해결은 DHCP 서버를 통해 수행하고, 다른 서브넷에서 DNS 중복 탐지 및 해결은 DNS 서버를 통해 수행한다.

첫째, DNS 등록 요청 메시지의 유효성 및 메시지 데이터의 유효성에 따른 다음과 같이 동작한다. DHCP 서버가 요청 메시지를 수신했지만 유효하지 않은 메시지인 경우 DHCP 서버는 메시지 유형에 따라 두 가지 동작을 수행할 수 있다. 만일 메시지 유형이 유효하지 않으면 DHCP 서버는 이 메시지를 무시한다. 반면에 메시지 유형이 유효하지만 메시지 데이터 자체에 오류가 있는 경우에는 DHCP 서버가 해당 메시지에 대한 오류 코드와 함께 오류 메시지를 IoT 디바이스에게 회신한다. IoT 디바이스는 이러한 오류 메시지를 받으면 DNS 네임 등록요청 메시지를 재생성하고 DHCP 서버에게 등록요청 메시지를 다시 전송한다. 이 프로세스는 다시 실패할 경우를 대비하여 최대 세 번까지 수행 할 수 있다. 등록요청이 세 번을 초과하면 DHCP 서버는 해당 IoT 디바이스의 요청 메시지를 무시하고 일정시간 동안 차단한다. 횟수를 3번으로 정한 이유는 서비스 리소스 문제 때문이다. 만약, 악의적인 목적을 가진 장치가 계속해서 요청 메시지를 보내는 경우, DHCP 서버가 공격자의 공격 때문에 과부하가 걸릴 수 있기 때문이다.

둘째, DNS 등록 요청 메시지가 유효하지만, 등록하고자 하는 DNS 이름이 중복되는 경우이다. IoT 장치는 자신의 DNS 이름과 이에 대응하는 IP 주소를 DHCP 서버에 등록하도록 요청한다. DHCPv4 서버가 요청 메시지를 수신하지만 자신의 DNS 네임 관리 저장소(Repository)에 받은 DNS 이름이 존재하면 DHCP 서버는 중복 DNS 이름을 나타내는 오류 메시지를 해당 IoT 디바이스에게 전송한다. IoT 디바이스는 DHCP 서버로부터 오류 메시지를 받으면, IoT 디바이스는 새로운 unique_id를 선택하여 그림 2의 DNS 네임 포맷에 때라 자신의 DNS 이름을 다시 생성하고 DHCP 서버에 다시 등록하도록 요청합니다. 이러한 과정은 DNS 네임의 고유성을 확인할 때까지 이 프로세스를 반복한다.

셋째, DHCP 서버가 IoT 디바이스의 DNS 네임과 IP 주소를 DNS 서버에게 DNS Dynamic Update[7]를 통해 등록한다. DHCP 서버가 등록하고자 하는 DNS 네임이

DNS 서버에 등록되어 있는지 확인한다. 만약 DNS 네임이 DNS 서버에 등록되어 있으면 DHCP 서버는 IoT 디바이스에게 DNS 네임 중복을 알려주어 새로운 DNS 네임을 생성하여 등록하게 한다. 반면에 DNS 네임이 DNS 서버에 등록되어 있지 않으면 DNS Dynamic Update를 통해 등록한다.

3. 결론

본 논문에서는 DHCP를 기반한 DNSNA에 대해 소개하고 설명하였다. 향후 증가하는 IoT 환경 시대에서 각 IoT 디바이스의 이름을 일일이 수정하는 것은 비효율적이다. 따라서 본 논문에서는 IPv4 및 IPv6에서 사용 가능한 DHCP 또는 DHCPv6를 기반한 DNSNA를 소개하였다. 우리는 본 기술을 통해 향후 IoT 네트워크 산업에 큰 도움을 줄 것으로 예상한다. 향후 연구로는 DHCP를 기반한 DNSNA를 구현하고 테스트하여 IETF 인터넷 기고서를 작성하여 인터넷 표준으로 채택되게 진행할 예정이다.

4. Acknowledgment

본 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 2017R1D1A1B03035885)임. 또한 본 논문은 한국연구재단의 글로벌 리서치 랩 프로그램(2013K1A1A2A02078326)과 과학기술정보통신부의 재원을 받은 CPS글로벌센터의 연구결과물임.

5. 참고문헌

[1] Gartner, Inc., “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020”, http://www.gartner.com/newsroom/id/2636073.

[2] Sejun Lee, Jaehoon (Paul) Jeong, and Jung-Soo Park, “DNSNA: DNS name autoconfiguration for Internet of Things devices”, Proceedings of the 18th International Conference on Advanced Communication Technology (ICACT), 410-416, Feb 2016.

[3] Keuntae Lee, Seokhwa Kim, and Jaehoon (Paul) Jeong, “DNSNAv4: DNS Name Autoconfiguration for Internet-of-Things Devices in IPv4 Networks”, 31th International Conference on Advanced Information Networking and Applications Workshops - Device Centric Cloud (DC2), Taipei, Taiwan, March 27-29, 2017.

[4] M. Stapp, T. Lemon, and A. Gustafsson, “A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR)”, IETF RFC 4701, Oct 2006.

[5] M. Stapp, B. Volz, and Y. Rekhter, “The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option”, IETF RFC 4702, Oct 2006.

[6] M. Stapp and B. Volz, “Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration Protocol (DHCP) Clients”, IETF RFC 4703, Oct 2006.

[7] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, “Dynamic Updates in the Domain Name System (DNS UPDATE)”, IETF RFC 2136, Apr 1997.

[8] Jaehoon Paul Jeong, Sejun Lee, and Jung-Soo Park, “DNS Name Autoconfiguration for Internet of Things Devices”, IETF Internet-Draft, draft-jeong-ipwave-iotdns-autoconf, March 2017.

[9] M2M, “Object Identifier based M2M Device Identification Scheme”, http://www.onem2m.org.