사물인터넷 환경에서 안전하고 경량화된 RPL 라우팅 프로토콜

오 하 영
숭실대학교
정보통신전자공학부 조교수

Ⅰ. 서 론

사물인터넷 서비스는 사물 (Things)의 연결을 통해 고객들에게 새로운 서비스를 제공함으로써 제품의 본연의 가치를 높여주기 때문에 최근 매우 각광받고 있는 기술이다. IoT시장 규모 및 성장 가능성 분석결과, 2020년 글로벌 IoT시장은 5조 달러 이상의 규모로 성장할 것으로 기대되며, 국내 IoT시장도 30조 원에 이를 것으로 전망된다고 한다.

사물인터넷 기술의 서비스 사례로는 Sen.se사의 집과 가족 모니터링 시스템 (i.e., Mother와 Cookies), nest사의 온도조절장치 (nest thermostat), 특정 동작 인식 기능을 학습하는 DropCam등이 있다.

IoT가 응용될 수 있는 단말은 저전력, 초소형 및 경량적이여야 한다는 특성때문에 지금까지 폐쇄적이고 개별적으로 이용되어 오던 센서 네트워크에 일차적으로 접목가능하다[1-2]. 센싱된 정보가 스마트폰, 스마트 TV와 같은 다양한 스마트 기기들과 연동된다면 새로운 개인중심의 생활밀착형 서비스를 제공할 수 있고, 특히 2020년에는 약 240억대의 단말이 인터넷에 연결될 수 있기 때문에 이를 통해 스마트 홈, 스마트 그리드, 헬스케어, 지능형 교통서비스 등과 같은 IoT기반의 다양한 서비스가 창출될 수 있다.

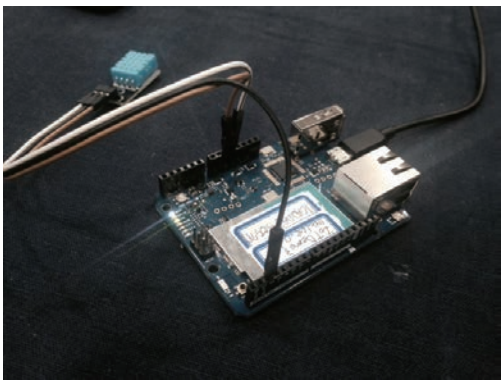
물론, 최근 스마트 기기들은 가속도계, GPS, 근접센서, 카메라 등 자체 내장된 센서 등을 활용하여 새로운 응용서비스를 만들어 내는 능력과 프레임워크를 제공하고 있기 때문에 사용자와 개발자의 편의에 따라 내장 센서의 값을 활용할 수 있다[23]. 하지만 스마트폰 센서의 크기나 가격, 제한된 공간 등으로 다양한 센서들을 모두 내장시킬 수는 없으며, 따라서 사용자들의 지속적인 욕구를 충족시키기엔 한계가 있다. 이런 이유로 인해 최근에는 사물인터넷과의 연동을 통해 외부에 위치하고 있는 다양한 센서를 활용하여 정보를 수집하거나 스마트 기기에서 원격

으로 제어 할 수 있는 기술개발에 대한 관심과 논의가 뜨거운 상황이다. 일례로 이동성을 가진 스마트폰들은 주변에 산재해 있는 고정된 다양한 환경 및 기상 센서들로부터 정보를 수집하여 현재 위치의 실시간 온 · 습도를 포함한 환경정보를 다양하게 활용할 수 있다[2].

사물인터넷의 3대 주요 기술은 센싱 기술, 유무선 통신 및 네트워크 인프라 기술, 서비스 인터페이스 기술이다[1]. 센싱 기술은 센서로부터 정보를 수집 · 처리 · 관리하고 정보가 서비스로 구현되기 위한 기법들을 지원한다. 네트워크 종단간(end-to-end)에 사물인터넷 서비스를 지원하기 위해서는 근거리 통신기술(WPAN, WLAN 등), 이동통신기술(2G, 3G 등)과 유선통신기술(Ethernet, BcN 등) 등의 유무선 통신 및 네트워크 인프라 기술이 필요하다. 최종적으로 사용자에게 사물인터넷 서비스를 제공하기 위해서는 정보를 센싱, 가공/추출/처리, 저장, 판단, 상황 인식, 인지, 보안/프라이버시 보호, 인증/인가, 디스커버리, 객체 정형화, 오픈 API, 오픈 플랫폼 기술 등을 포함하는 서비스 인터페이스 기술이 필요하다.

최근에는 인프라가 없는 (Infra-less) 환경에서 디바이스들끼리 정보를 직접 주고받을 수 있는 기기 간 직접(device-to-device) 통신기술들이 다양한 무선망에서 발전되어 오고 있다[3-6],[23]. 셀룰러 네트워크에서는 기기 간 직접통신 기술로써 3GPP에서 LTE (Long-Term Evolution)에 직접통신을 적용하기 위해 최근 표준화를 시작했고[4-5], 비면허 대역에서는 기존의 무선랜 표준을 확장하여 와이파이 다이렉트의 802.11u 기술이 개발되었다[6-7]. 또한 IEEE 802.15.8에서는 대상 인식 통신 표준화 작업이 진행 중이다. 기기 간 직접통신의 대표적인 장점들은 i) AP 및 기지국등과 같은 중간노드를 거칠 필요가 없기 때문에 전송횟수, 통신거리 및 지연시간 감소를 시킬 수 있고, ii) IoT단말기들끼리 센싱된 정보, 이웃탐색 및 IPv6주소 등의 새로운 종류의 근접 기반 자원들도 서로 쉽게 공유할 수 있는 환경을 새로 만들 수 있다는 점 등을 들 수 있다[8].

특히, 최근에는 〈그림 1〉과 같이 아듀이노 (Arduino)



〈그림 1〉 아듀이노를 활용한 오픈소스 IoT의 예

칩을 다양한 센서에 연결하고 노트북으로 아듀이노 칩에 전력제공 및 웹을 통해 센싱된 변화 값 확인 등을 위한 현실적인 오픈소스 IoT플랫폼이 각광받고 있다[21].

하지만, IoT환경에서는 단말기가 특히 저전력, 경량화 및 불안정한 통신 상황등 이란 특성들을 가지기 때문에 기존의 자동 주소 설정을 포함한 IPv6 이웃발견 (Neighbor Discovery) 기법, 기기 간 통신 및 라우팅 프로토콜과 다르게 디자인되야 한다[23].

'서비스'에 초점을 맞춘 나머지 간과되고 있는 핵심 요소인 보안을 필수적으로 고려해 줘야한다.

또한, '서비스'에 초점을 맞춘 나머지 간과되고 있는 핵심 요소인 보안을 필수적으로 고려해 줘야한다. 편리함을 제공해준다는 큰 이유로 IoT에 대한 산학연의 관심사는 주로 '서비스'에만 초점이 맞춰져 왔다. 하지만, 개별 특성에 관련된 모든 센싱 데이터가 안전한 보안 절차 없이 쉽게 외부로 노출될 수 있기 때문에 문제가 심각하다. 한 예로, 구글에게 3조 4천 억원 (32억 달러)에 인수된 nest사의 온도조절장치 IoT제품은 보안이 전혀 고려되어있지 않아 최근에 많은 공격을 당했다[20].

IoT보안은 크게 구현 시 보안 요구사항을 고려하여 반영하는 시스템 보안 관점과 키 관리를 통한 암호학적 관점이 있다. 실제 해킹은 시스템의 취약성과 암호학적 취약성을 구분하지는 않기 때문에 모두 공격 대상이 될 수 있다. 예를 들어, 디바이스 보안 취약성으로는 pin노출, ROM코드 노출 등을 들 수 있고, Firmware프로그램의 취약성으로는 buffer overflow, integer overflow등을 들 수 있다. 기타, 프로토콜 취약성으로는 openSSL의

heartbleed등을 들 수 있다.

근접 기반 경량화 자동 주소 설정 및 IPv6 이웃 발견기법 측면에서는 두 개 이상의 IoT 단말기들이 물리적으로 근접한 위치에 있을 때 각 IoT 단말기가 경량화된 IPv6주소를 자동으로 설정하고 상대 IoT를 발견 후 기반 시설을 거치지 않고 IoT 기기 간 직접통신을 하는 것을 고려해야 한다. 이러한 근접 기반 경량화 자동 주소 설정 및 IPv6 이웃 발견기법을 구현하기 위해서는 우선적으로 수많은 주변 IoT들이 자동으로 각각 설정한 IPv6주소가 겹치지 서로 겹치지 않는지 찾아내는 디스커버리 프로토콜을 설계하는 것이 매우 중요하다. 하지만, 적절한 시간 내에, 가능한 적은 양의 무선 자원을 사용하고, 배터리 소모를 최소화하면서 경량화 자동 주소 설정을 탐색하고 목적지까지 데이터를 안전하게 전송해줄 수 있는 프로토콜을 설계하는 것은 간단한 일이 아니다[10-15].

특히, 이러한 방식으로 수많은 IoT 기기들이 원하는 IoT 단말기 및 중복되지 않은 IPv6주소를 발견하지 못하거나 목적지까지 경로 유지가 되지 않을 경우 접속을 끊고 다시 연결해야하는 과정을 반복해야 하고 이러한 과정에서 많은 양의 유니캐스트 정보가 전달되야 하므로 매우 비효율적이라 할 수 있다.

오버헤드를 줄이기 위한 기존 연구들로는 웹 서비스인 http로 단말기 수준 (device level)까지 접근하고 데이터 전송 측면에서 해결책을 제시한 CoAP (Constrained Application Protocol)[16]과 제어 메시지를 줄이기 위한 RPL (Routing Protocol for Low-power and Lossy Networks)[8], Kunjan Patel[17], PSR[18] 및 Hu She[19]등이 있다. 기존 연구들은 데이터를 목적지로 경량화하게 전송하기 위해서 제어 메시지 타입을 다양하게 구분하거나 제한된 시간 동안만 비콘을 주기적으로 주고받아 데이터 전송 전체 경로를 설정하는 데 초점을 맞추었다.

반면 [23]에서 제안된 기법은 해시함수(hash function) 기반 블룸필터 표현법을 활용하여 노드들끼리 주고받는 메시지 양을 줄이는 것을 물론 노드 식별 주소, 이웃 발견 및 라우팅 경로 등을 경량화하게 모두 표현하여 궁극적으로 전체 제어 메시지의 오버헤드를 줄이는 것을 목표로 했다. 저전력 손실 네트워크에서 경량화된 주소를 가진 IoT 단말기들이 RPL(Routing Protocol for Low-power and lossy networks)[8] 기반으로 동작할 때 루프[9], 경로 손실등과 같은 문제가 생겨도 유연하고 작은 오버헤드로 경로를 다시 재탐색하여 빠른 시간 내에 원하는 이웃 IoT단말기를 찾아 목적지까지 데이터를 견고하게 전송할 수 있다.

하지만, 기존연구[23]도 보안관점에서는 고려하지 않았기 때문에 안전성 측면에서 미흡한 실정이다. 본 논문에서는 IPv6에서 향상된 mCGA (modified Cryptographically Generated Address) 및 기존 연구 [23]를 기반으로 사물인터넷 환경에서 향상된 RPL기반 안전하고 경량화된 라우팅 프로토콜을 제안한다.

본 고의 구성은 다음과 같다. 2장에서 관련연구를 소개한다. 3장에서는 사물인터넷 환경에서 향상된 RPL기반 안전하고 경량화된 라우팅 프로토콜 대하여 설명한다. 4장에서는 성능평가 결과를 보여주며, 마지막으로 5장에서는 본 논문을 정리하며 마친다.

Ⅱ. 관련 연구

IoT기반 저전력 통신을 위한 라우팅 프로토콜은 경로 설정을 위한 제어메시지관점 (control plane) 및 데이터 전송관점 (data plane)에 따라 크게 〈표 1〉과 같이 나뉠 수 있다.

1) CoAP (Constrained Application Protocol)

M2M 관련 표준화가 가속화 되어가고 있는 가운데, IETF(Internet Engineering Task Force) 내의 CoRE(Constrained RESTful Environments) 워킹그룹에서는 2010년부터 6LoWPAN의 상위 애플리케이션 계층 프로토콜 CoAP(Constrained Environments Application Protocol)의 표준화 활동을 시작해왔다[16]. CoAP은 '코앱'이라고 불리며 http를 단말기 자체 제어로 바로 사용하는 것이 목적이다. CoAP는 표준들 상위의 트랜스포트와 애플리케이션 계층을 위한 응용 프로토콜로 이를 활용하면 웹 서비스로 단말기 자체에 접근할 수 있다.

〈표 1〉 IoT based protocols for Low-power communications

Data Plan	Control Plane
6LoWPAN (IPv6 over Low-power WPAN) –Fragment Forwarding Technique	
CoAP(Constrained Application Protocol) – M2M communication in constrained networks – Connect smart objects to the Internet – A bulk data transfer mechanism over UDP – Avoid fragmentation, retransmission of TCP to minimize state maintenance and power usage – Its own loss detection and retransmission to avoid the problems TCP has in wireless networks – Goal: *HTTP equivalent* for WSNs (Representational State Transfer : REST)	*RPL (Routing Protocol for Low-power and Lossy Networks)* – Each node builds a directed acyclic graph through which packets can be efficiently routed to sink nodes. – From the sink, RPL builds routes to nodes inside the network which can distribute data to sensor nodes. – ContikiMAC used as radio cycling protocol. – Energy consumption is measured using Contiki's built-in power profiler.

CoAP을 적용할 수 있는 대상 노드들은 노드가 저성능의 CPU를 가질 뿐만 아니라 작은 용량의 램 및 롬 을 가지는 제한적인 노드를 대상으로 하고 있다. 또한, 사물인터넷을 구성하는 기기들의 상태 전송이라는 이벤트를 비동기적 (asynchronous)으로 전송할 수 있는 Representational State Transfer (REST) 아키텍처를 기반으로 Resource Discovery, 멀티캐스트 지원, 비동기 트랜잭션 요청 및 응답 등을 지원하기 위한 프로토콜이다.

특히, CoRE 워킹그룹에서 제정하려는 CoAP의 표준화 영역은 TCP와 UDP를 포함하는 트랜스포트 계층을 포함한 상위 애플리케이션 계층에서 M2M 노드들 사이에서 어떻게 리소스 이벤트(예: 온도, 습도)에 대한 요청을 하고 이벤트가 생겼을 경우 어떻게 비동기적으로 리소스 이벤트를 노드에게 전송할 지에 대한 방법을 설계하는 부분이다.

HTTP를 이용하기는 하지만 CoAP이 기존의 HTTP와 다른 점은 UDP 환경 하에서 유니캐스트와 멀티캐스트 양쪽을 지원해야 한다는 점과 CoAP은 경우에 따라 노드가 클라이언트, 서버, 프록시의 역할을 할 수 있다는 것이다.

2) RPL (Routing Protocol for Low-power and Lossy Networks)

RPL(IPv6 Routing Protocol for Low-power Lossy Networks)은 IETF의 ROLL(Routing Over Low-power and Lossy networks) 워킹 그룹에서 표준화를 진행 중인 IPv6 라우팅 프로토콜로 Ripple(리플)이라 읽는다. RPL은 IEEE 802.15.4[14], 전력선 통신등 저전력과 잡음이 매우 심한 네트워크 환경에 적합하도록 설계되었으며, 여러 응용들의 다양한 요구사항을 수용하기 위해 다양한 라우팅 메트릭을 지원한다. 이를 위하여 각 응용의 요구조건을 달성하기 위한 라우팅 메트릭, 경로 최적화 등에 해당하는 기능은 Objective Function(OF)로 분리하였으며 표준에서 정의하는 내용들은 다양한 OF에 공통적으로 사용하는 일반적인 내용들을 정의하고 있다[8],[23].

RPL객체는 목적지 기반 방향성은 있지만 사이클이 없는 여러 개의 그래프(DODAGs: Destination Oriented Directed Acyclic Graphs)로 구성된다. 노드의 랭크는 루트 DODAG로부터 얼마나 멀리 위치하고 있는지를 알려준다. DODAGs 를 만들기 위해 각 노드들은 로컬 링크 정보 및 랭크를 담은 DAG Information Object(DIO)라는 제어메시지를 주기적으로 보낸다. DIO를 수신한 노드들은 DODAG루트까지 최소의 비용으로 전송할 수 있는 부모 노드를 선택하기 위해서 새로운 DODAG에 참여하거나 기존의 DODAG를 유지한다.

RPL은 크게 데이터 저장 금지 모드(non-storing mode), 데이터 저장 가능 모드(storing mode) 및 데이터가 위로 전송되는 것을 막는 기법 이렇게 3가지 전송기법이 있다. 저장 금지 모드에서는 근접한 말단 노드들끼리 통신을 하고자 하는 경우에도 DODAG루트까지 올라갔다가 데이터가 수신노드에게 전송되야 한다는 특징이 있고, 저장 모드에서는 루트까지 올라가지 않아도 공유하고 있는 근접 상위노드만 통과하여 해당 노드에게 데이터를 전송할 수 있다는 특징이 있다. 하지만 어떤 종류든 RPL에서는 아래와 같이 3가지의 문제가 발생한다[24].

- RPL기법에서는 노드들이 에너지를 절약하기 위해서 잠자는 모드(sleeping mode)로 들어가서 제때 응답을 안 하거나 저전력 및 데이터 손실이 존재할

수 있는 환경이기 때문에 데이터 성공율 매우 낮은 편이다. 결과 데이터 전송에 문제가 생긴 경우 DIO 제어메시지를 활용하여 문제를 알리고 해결한다.

- RPL에서는 루프문제(loop problem)를 완벽하게 해결할 수 없다. 따라서 loop이 발생되면 실시간으로 탐지하여 문제 있는 부분을 유연하게 피하고(loosely avoidance) 다양한 제어메시지들을 활용하여 작은 오버헤드로 최대한 빨리 해결 하는 게 필요하다. 예를 들어서 RPL에서는 랭크가 감소하는 부분으로만 데이터가 전송 되야 루프(loop)이 발생되지 않는 것을 의미한다. 만약 어느 순간 랭크가 증가되는 쪽으로만 데이터가 전송된다면 이는 loop이 발생될 확률이 높아질 수 있다는 것을 의미한다. 따라서 각 응용의 요구조건을 달성하기 위한 라우팅 메트릭, 경로 최적화 등에 해당하는 기능인 Objective Function(OF)을 잘 디자인하여 문제가 생긴 부분만 지역적으로 해결하던지 아니면 전체적으로 해결해야할지 결정해야한다.
- RPL은 ISA 100.11a혹은 wireless HART등에 비해서 동적으로 변화하는 환경(dynamic environment)에서 데이터를 저전력으로 전송할 수 있는 기법을 제안했다. 하지만 여전히 끈어짐에 대한 대응방법이 매우 약하다. 비록 문제가 발생했을 경우 DIO poisoning이라는 방식으로 문제를 해결하려고 하지만 문제가 생길 때마다 매번 DODAG들을 새로 유지하고 업데이트하는데 오버헤드가 들기 때문에 완벽한 해결책이 되지 못한다.

저전력 손실 네트워크을 구성하는 LLN(Low-power and Lossy Networks) 라우터는 한정된 메모리를 사용하는 제한 조건을 가지고 있기 때문에 목적지 경로 정보를 유지할 수 없으며 다만 적은 수의 디폴트 라우터 정보만을 유지한다. 예를 들어, IEEE 802.15.4 상에서 IPv6 기반 네트워크 프로토콜 표준화에서는 저전력, 저가, 저기능(8bit-microprocessors, 수 KB RAM), 저속(~ 250 kbps) 의 제한된 환경을 고려하고 있다[23].

따라서 제한된 환경에서도 LLN 라우터가 암호화된 IPv6 경량화 주소 및 LLN 내에 목적지까지의 연결성 정보 및 데이터그램 전달을 위한 경로 정보를 안전하게 유지해야 한다. 더불어 데이터그램 전달을 위해 IPv6 소스 라우팅이 필요하다. 따라서 본 연구에서는 기존 연구[23]을 확장하여 사물인터넷 환경의 RPL 라우팅 도메인 내에서 RPL 라우터들끼리 데이터그램 전달을 위해 IoT 단말기의 안전하고 경량화된 자동 주소 설정을 포함한 IPv6 이웃 발견 기법 및 light-weight 라우팅 프로토콜 개발하는데 목표를 둔다.

3) 기타 경량화 라우팅 프로토콜

Kunjan Patel[17]은 센서 네트워크에서 유니캐스트 수행 시 다양한 응답 메시지 (acknowledgement)들과 한정된 시간 내 (timeout schemes) 에서만 라우팅 프로토콜이 동작하게 하여 불필요한 메시지 양을 줄이는 경량화 라우팅 프로토콜을 제안했다. 하지만 제한된 시간동안에만 데이터를 전송할 수 있기 때문에 성능향상에 한계가 있고 다양한 응답 메시지를 주기적으로 주고 받아야하기 때문에 총 전달되는 제어 메시지 양은 여전히 많다.

[18]에서는 모바일 무선 네트워크 환경에서 소스에서 목적지까지 모든 경로를 알 수 있는 경량화 된 소스 라우팅 프로토콜 (PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks)을 제안했다. 이 기법은 작은 오버헤드로 토폴로지에 대한 많은 정보를 활용할 수 있도록 이진트리 기반 라우팅 프로토콜 상에서 동작한다. 하지만 이진트리 구조로 변형이 가능한 토폴로지에서만 동작한다는 한계점이 있으며 물리적으로 주어진 토폴로지를 이진 트리화하기 위해서 필요한 제어 메시지 양들을 고려하면 역시 총 전달되야 하는 제어 메시지 양이 여전히 크다는 것을 알 수 있다.

Hu She[19]는 자동차 무선 네트워크 환경에서 실시간으로 발생하는 트래픽 지역적 정보를 경량화하게 수집하는 기법을 제안했다. 이를 위해 주기적인 비콘 메시지로 링크상태를 측정하고 데이터를 효율적으로 전달하는 기법을 제안했다. 움직이는 자동차 무선 네트워크 환경에서 최소의 전송 횟수로 데이터를 목적지로 성공적으로 전송할 수 있지만 이를 위해 주기적으로 제어 메시지를 주고

받아 링크 상태를 확인하고 저장해야하기 때문에 역시 총 전달 및 저장되야 하는 제어 메시지 양은 많이 줄이지 못했다는 한계점을 지닌다.

기존 연구들은 데이터를 목적지로 경량화하게 전송하기 위해서 제어 메시지 타입을 다양하게 구분하거나 주기적으로 주고받아 데이터 전송 전체 경로를 설정하는 데 초점을 맞추었다.

반면 제안하는 기법은 기존 연구[23]을 확장하여 mCGA를 바탕으로 안전한 IPv6주소를 설정했다. 결과, 제안하는 기법은 블룸필터 및 mCGA 기반 노드 식별 주소, 이웃 발견 및 라우팅 경로등을 경량화하고 안전하게 모두 표현하여 궁극적으로 전체 제어 메시지의 오버헤드를 줄였다.

4) CGA

CGA는 기본적으로 공개 암호키의 암호를 이용한 cryptographic hash를 계산하여 IPv6주소의 interface를 생성하는 것이다. 이러한 결과로 생성되는 IPv6주소는 암호화하여 생성되기 때문에 CGA라 불린다. 이런 생성에 의해 상응하는 비밀 키는 주소로부터 보내지는 메시지들을 서명하기 위해 사용된다[24].

5) Node.js를 고려한 현실성 논의

IoT 실제 환경을 만들 수 있는 방법은 기존의 Node.js 기반 solution들을 활용하는 방법과 Node.js자체로 만드는 방법이 있다.

Node.js는 확장성 있는 네트워크 애플리케이션(특히 서버 사이드) 개발에 사용되는 소프트웨어 플랫폼이다. Node.js는 작성언어로 자바스크립트를 활용하며 Non-blocking I/O와 단일 스레드 이벤트 루프를 통한 높은 처리성능을 가지고 있다. 특히, Node.js는 내장 HTTP 서버 라이브러리를 포함하고 있어 웹서버에서 아파치 등의 별도의 소프트웨어 없이 동작하는 것이 가능하며 이를 통해 웹서버의 동작에 있어 더 많은 통제를 가능케 한다[22].

Node.js기반 solution이란 많은 플러그인들을 활용하여 인터넷으로 노드를 제어하는 기술이다. 반면, Node.js 자체로 만드는 방법은 Node.js는 외부 접근 언어인 자바스크립트를 직접 수정하여 원하는 목적 데로 서비스하는 것이다.

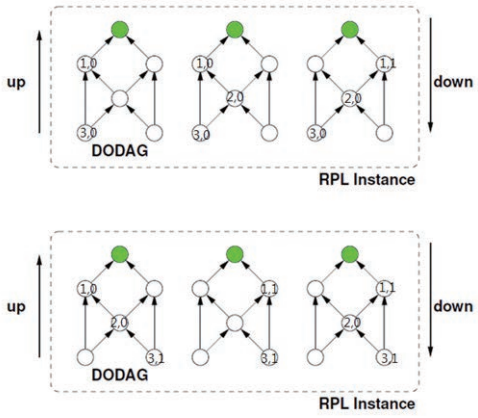
Node.js는 많은 기능을 표현하기 위해 내부적으로는 C언어로 되어 있다. 하지만, C언어는 절차 지향적 언어로 지역적 시간 개념을 바탕으로 동기화되어 있다는 것을 가정한다. 반면, IoT환경은 사용자가 언제 다양한 이벤트를 발생시킬지 모르기 때문에 비동화 프로토콜이 필요하다. 즉, C언어는 한 노드입장에서 절차적으로 진행하는 경우는 충분하지만, 외부환경인 네트워크 시간개념으로 확장하면 비동기화 개념이 필요하기 때문에 이벤트 제어(event handler) 및 메시지 제어 (message handler)가 필요하다. 예를 들어, 사용자가 버튼을 누를 수 있는 사실은 알겠지만, "언제" 누를지는 모른다. 따라서, 이벤트 제어를 통해 실제로 이벤트가 발생하면 동작할 수 있도록 만들어야한다. 결과, Node.js는 내부적으로는 C언어로 외부적으로는 자바스크립트로 구성된다.

Ⅲ. 사물인터넷 무선 환경에서 향상된 RPL기반 안전하고 경량화된 라우팅 프로토콜

3.1 블룸필터 (Bloom filter)와 향상된 랭크기법 기반 경량화된 IPv6 주소 설정 및 경량화 라우팅 프로토콜

IoT단말기들이 급격하게 증가되고 초연결성을 지원하기 위해서는 센싱데이터, IPv6주소 및 이웃탐색 등의 주고받는 메시지 양이 급격하게 증가될 것이다. 반면 IoT단말기들 및 LLN라우터들은 초경량화, 저전력 및 손실등의 특성이 있기 때문에 최소한의 데이터를 저장하고 있어야 하고 목적지까지 일관된 경로로 데이터를 전송하는 것은 어려운 일이다. 따라서 노드식별자에 주소를 압축하여 의미는 부여하되 경량화 된 표기법이 필요하다.

경량화 된 IPv6주소 설정을 위해 본 연구에서는 블룸필터 및 향상된 랭크기법을 활용 한다[23]. 기존의 향상된 RPL (enhanced RPL : eRPL)기법[23]에서는 rank는 같거나 낮은 조건에서 relative location값이 같거나, 크거나, 작아지거나 상관없이 다양한 조합을 반복하면서 견

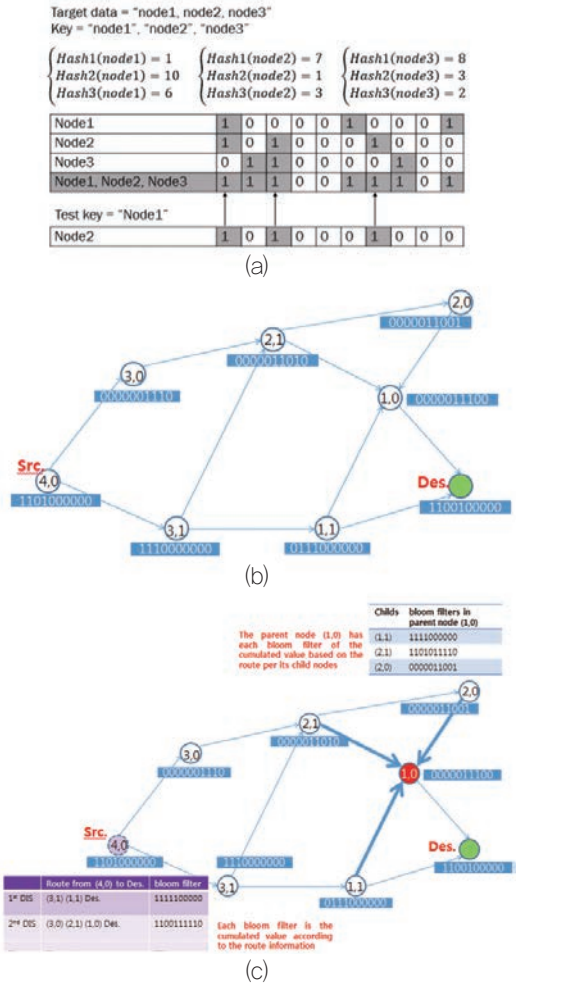


〈그림 2〉 An enhanced RPL based light-weight routing protocol[23]

고한 경로로 데이터를 전송할 수 있도록 만들어준다. 〈그림 2〉에서 알 수 있듯이 제안하는 기법에서는 경량화된 IPv6주소를 활용하여 각 소스 노드에서 목적지 경로까지 총 3개의 다중 경로를 활용할 수 있다는 것을 보여준다.

〈그림 3(a)〉는 블룸필터 결과 생성된 노드 구분자들을 바탕으로 IPv6주소를 대신하여 노드를 식별하는 과정을 보여준다. 예를 들어, 1번, 6번 및 10번 자리에 '1'비트로 설정된 경우 노드 1을, 1번, 3번 및 7번 자리에 '1'비트로 설정되면 노드 2번, 2번, 3번 및 8번 자리에 '1'비트로 설정되면 노드 3번을 나타낸다. 만약 소스에서 목적지까지 노드 1번, 2번 및 3번을 경유하여 경로설정 제어 메시지 패킷이 전송됐다면 목적지가 가지고 있는 블룸필터는 1,2,3,6,7,8,10번 자리에 모두 '1'비트로 설정된 최종 결과만 가지고 있게 된다. 목적지는 자신의 원 홉 반경 내의 주변 노드들 중 어떤 노드를 경유하여 경로설정 제어 메시지 패킷이 전송됐는지 판단하기 위해 최종 블룸필터에 '1'비트로 체크된 자리들과 각 이웃 노드들의 블룸필터를 대입하여 판별한다.

〈그림 3(b)〉는 소스에서 목적지까지 데이터를 전송할 수 있는 다양한 경로가 존재할 때 각 노드를 10비트의 블룸필터로 표현한 멀티 홉 시나리오를 보여준다. 〈그림 3(c)〉는 소스에서 목적지 노드의 전 노드인 (1,0)까지 데이터를 전송할 수 있는 각각의 다중 경로들을 블룸필터 테이블에서 관리하는 과정을 보여준다.



〈그림 3〉 (a) Bloom filter based light-weight IPv6 address, (b) The multi-hop scenario with Bloom filter based light-weight IPv6 addresses (c) Light-weighted various routing routes establishment in eRPL

하지만, 블룸필터 값만으로는 중복되거나 노드 식별 정확도가 떨어질 수 있기 때문에 기존 기법[23]에서는 상대적인 자녀노드의 위치를 표현할 수 있는 향상된 랭크를 추가로 활용하여 이 문제를 해결했다. 해당 코드에는 이웃노드들의 이름 집합을 축약한 정보만이 담겨 있으므로 코드로부터 이웃노드들 이름을 유일하게 복구할 수 없다. 대신 특정 이웃노드의 이름이 송신자의 이웃노드리스트 집합에 포함되었는지의 여부만 알 수 있다. 따라서 축약된 블룸필터 코드를 이용하여 이웃노드의 존

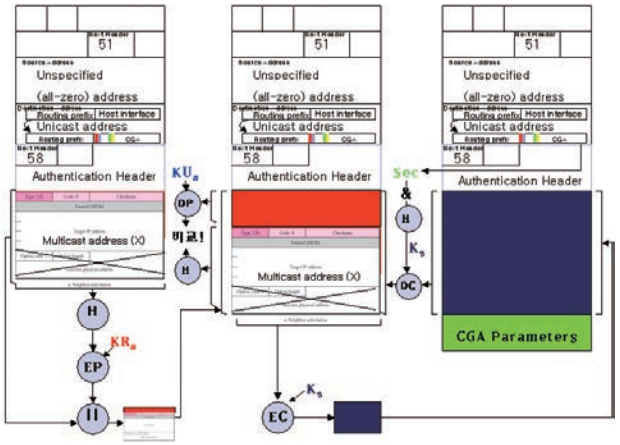
CGA는 기본적으로 공개 암호키의 암호를 이용한 cryptographic hash를 계산하여 IPv6주소의 interface를 생성하는 것이다.

재 유무를 테스트할 때 정보의 손실로 인해 오류가 발생할 수 있다. 이웃노드가 존재하지 않지만 존재한다고 판단한 경우는 거짓 양성(false positive) 오류가 발생했다고 할 수 있으며 이웃노드가 존재하지만 존재하지 않는다고 판단한 경우는 거짓 음성(false negative) 오류로 분류할 수 있다. 이때, 이웃노드 발견이 실패하는 경우를 막기 위해서 거짓 음성 오류가 발생하지 않도록 향상된 랭크를 반영하여 축약된 블룸필터 코드를 설계했다. 즉, 같은 블룸필터에 속한 여러 개의 이웃 노드들이 존재해도 부모 노드로부터 각 자식 노드들의 상대적인 위치는 다르기 때문에 이를 표현하고 있는 향상된 랭크 식별자는 블룸필터의 부정확성을 해결해줄 수 있다.

결과, 기존 기법에서는 전체경로 및 상대적인 자식 위치를 함축하고 있는 블룸필터를 활용하여 경량화된 IPv6 주소, 이웃 노들 발견 및 경량화 라우팅 프로토콜 설정할 수 있다. 이 기법에서는 각 부모 노드가 블룸필터로 함축화 된 다양한 자식경로들을 유지하기 때문에 손실이 많은 사물인터넷 기반 무선 네트워크에서 다양한 에러가 많이 발생해도 바로 다른 지역적으로 가능한 경량화 된 경로를 활용하여 견고성을 높였다. 하지만, IPv6주소 자체에 암호화가 걸려있지 않기 때문에 보안측면에서 한계점을 가진다.

3.2 블룸필터 (Bloom filter) 기반 경량화된 이웃탐색 기법

일반적으로 근접 단말기의 발견을 위해 통신 단말기는 자신의 식별자(identifier)가 포함되어 있는 비콘(beacon) 등의 신호를 주기적으로 방송해야하고 이웃노드들의 발견을 위해서는 추가적으로 이웃노드들의 정보가 포함된 메시지도 알려야 한다. 그러나 이웃노드들의 이름 및 리스트를 그대로 방송하면 너무 많은 양의 정보를 전달하게 되어 저전력 손실 네트워크에서는 적합하지 않다. 또한, 암호화되어있는 않은 IPv6 주소를 주기적으로 방송하게 되면 메시지의 기밀성 (confidentiality) 보장과 replay attack을 막지 못한다.



〈그림 4〉 mCGA (modified Cryptographic Generated Address)

[23] 기법에서는, 이웃노드 리스트 광고에 필요한 비트수를 줄이기 위해 소스와 목적지 사이에 설정된 경로상의 이웃 노드들에 대한 정보를 〈그림 3(c)〉의 축약된 블룸필터 코드로 표현하여 블룸필터 테이블에서 관리한다. 예를 들어, 노드 (1,0)의 블룸필터기반 이웃관리 테이블에는 자식 노드들인 (2,1), (2,0), (1,1) 및 목적지 노드가 들어있다. 노드 (1,0)은 목적지 노드만 제외하고 각 자식노드들의 상대적인 위치를 고려한 노드 블름 필터 값과 해당 노드까지 데이터를 전송될 때 거쳐 온 노드들의 전체 경로를 함축한 블룸 필터 값을 테이블에 관리한다. 만약 노드 (1,0)이 1111000000라는 블름 필터로 데이터를 받았다면 노드 (1,0)의 주변 노드들의 블름 필터 (0000011010), (0111000000) 및 (0000011001) 중에서 (1,1)에 해당되는 (0111000000)만 포함할 수 있기 때문에 데이터가 소스, (3,1), (1,1)을 거쳐서 (1,0)으로 왔다는 것을 알 수 있다.

> mCGA 생성을 통해 호스트는 ND서비스 및 비 상태 주소 자동생성 서비스 등을 위해 IPv6 기본헤더 뒤에 붙는 ICMPv6메시지에 기밀성을 제공한다.

3.3 mCGA를 활용한 안전한 RLP프로토콜

표준화 그룹에서 제안한 기존 CGA는 공개키를 이용한 전자서명을 통해 인증을 제공해주지만 여전히 메시지의 기밀성(confidentiality) 및 replay attack등의 측면에서 한계점을 가진다. 따라서 제안하는 기법에서는 기존 연구[23]에 추가로 modified CGA를 고려한다. mCGA 생

성을 통해 호스트는 ND서비스 및 비 상태 주소 자동생성 서비스 등을 위해 IPv6 기본헤더 뒤에 붙는 ICMPv6 메시지에 기밀성을 제공한다. 이를 위해 〈그림 4〉와 같은 동적인 Sec과 Mask값을 이용하여 송신자는 symmetric key를 만들어 암호화 한다. 또한 기본적으로 공개 암호키의 암호를 이용한 cryptographic hash를 계산 시 mac address값과 time stamp값을 추가하여 IPv6주소의 interface를 생성함으로써 IP-Mac Binding 공격과 재현 공격을 막는다.

Ⅳ. 결 론

본 논문에서는 사물인터넷 환경에서 IoT 디바이스의 안전하고 경량화된 자동 주소 설정을 포함한 IPv6 이웃 발견 기법 및 향상된 RPL기반 경량화 라우팅 프로토콜을 제안했다.

제어 메시지 전송 횟수 및 사이즈를 줄여서 경량화 라우팅 프로토콜들을 제안했던 기존 연구들과 달리 본 연구에서는 노드 식별 IPv6주소, 이웃발견 과정 및 데이터 전송을 위한 라우팅 경로에서 발생하는 총 제어 메시지 양을 줄이는 RPL기반 향상된 경량화 라우팅 프로토콜을 제안했다. 특히, 편리성만 주로 고려하고 보안의 중요성은 언급하지 않은 기존 연구들과 달리, 안전한 IPv6주소 활용의 가능성을 사물인터넷 환경에서 처음으로 고려했다.

추후 연구로는 제안한 기법이 다른 기법들에 비해서 전력소모량, IPv6주소, 메시지 오버헤드 등의 안정성 및 경량화를 성능평가 할 예정이다.

이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 한국연구재단에서 부여한 과제번호 : NRF-2014R1A1A1003562)

참 고 문 헌

[1] 장원규, 이성협, “국내외 사물인터넷 정책 및 시장동향과 주요 서비스 사례”, 동향과 전망 : 방송 · 통신 · 전파 통권 제64호 2013. 07

[2] 고정길, 홍상기, 이병복, 김내수 “스마트 디바이스와 사물인터넷(IoT) 융합 기술 동향”, 전자통신동향분석 제28권 제4호 2013년 8월

[3] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklś, and Z. Turnyi, “Design aspects of network assisted device-to-device communications,” IEEE Commun. Mag., vol. 50, no. 3, pp. 170–177, Mar. 2012.

[4] 계원, 이현, 장성철, “기기 간 직접통신을 위한 모바일 어플리케이션 및 서비스 디스커버리 프로토콜”, 한국통신학회논문지 (J-KICS) '13-10 Vol.38A No.10

[5] L. Lei, Z. Zhong, C. Lin, and X. Shen, “Operator controlled device-to-device communications in LTE-Advanced networks,” IEEE Wireless Commun. Mag., vol. 19, no. 3, pp. 96–104, June 2012.

[6] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, “Device-to-device communications with Wi-Fi Direct: overview and experimentation,” IEEE Wireless Commun., vol. 20, no. 3, pp. 1–8, June 2013.

[7] IEEE, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 9: interworking with external networks, IEEE Std. 802.11u, 2011.

[8] IETF, “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” RFC 6550, Mar. 2012.

[9] J.H. Lim et al., “A Closed-Loop Approach for Improving the Wellness of Low Income Elders at Home Using Game Consoles,” IEEE Communications Magazine, vol. 50, no. 1, Jan. 2012, pp. 44–51.

[10] 전자신문, “삼성-퀄컴 글로벌 반도체 기업, 헬스케어 시장 주도권 다툼 치열,” 2012. 7. 4.

[11] DailyTech, “스마트폰과 무선 센서 네트워크를 사용한 지능형 주차 서비스,” 2008. 7. 14.

[12] Wireless Sensor Network Blog, “Valarm offers an affordable remote sensor and monitoring solution for Android devices,” 2013. 4. 13.

[13] J. Ko et al., “Connecting Low-power and Lossy Networks to the Internet,” IEEE Communications Magazine, vol. 49, no. 4, Apr. 2011, pp. 96–101.

[14] IETF, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," RFC 4944, Sep. 2007.

[15] J. Ko et al., "Wireless Sensor Networks for Healthcare," Proc. IEEE, vol. 98, no. 11, Nov. 2010, pp. 1947–1960.

[16] Z. Shelbyet al., "Constrained Application Portocol (CoAP)," IETF CoRE Working Group, Internet-Draft, ver. 18, June 2013.

[17] Kunjan Patel, Lim Jong Chern, C.J.Bleakley and Wim Vanderbauwhede, "MAW: A Reliable Lightweight Multi-Hop Wireless Sensor Network Routing Protocol," 2009 International Conference on Computational Science and Engineering

[18] Zehua Wang, Yuanzhu Chen and Cheng Li, "PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks," Vehicular Technology, IEEE Transactions on (Volume:63, Issue: 2)

[19] Hu Shen, Xiaodong Wang, Yanqiang Sun, Yanrong Ding, Xingming Zhou, "LALO: A Link-Aware Lightweight Routing Protocol for Data Delivery in Vehicular Ad Hoc Networks," Ubiquitous Intelligence and Computing Lecture Notes in Computer Science Volume 6406, 2010, pp 459–473

[20] https://nest.com/thermostat/life-with-nest-thermostat/

[21] http://www.arduino.cc/

[22] http://ko.wikipedia.org/wiki/Node.js

[23] 오하영, "사물 인터넷 기반 기기 간 통신 무선 환경에서 향상된 RPL 기반 경량화 라우팅 프로토콜", 정보처리학회지 3권 10호, 357p~363, 2014년 10월

[24] http://en.wikipedia.org/wiki/Cryptographically_Generated_Address

오하영

- 1998.03~2002.02 덕성여자대학교
- 2001.11~2004.02 신한금융지주회사 e-신한
- 2004.03~2006.02 이화여자대학교 컴퓨터공학 석사
- 2006.09~2013.02 서울대학교 컴퓨터공학 박사
- 2010.04~2010.10 U.C. Berkeley 방문연구원
- 2013.03~2013.08 서울시립대학교 연구교수
- 2013.09~현재 숭실대학교 정보통신전자공학부 조교수

〈관심분야〉
소셜 정보망, 추천시스템, 무선 네트워크 및 비디오 스트리밍