DBpia

논문 15-40-12-10 The Journal of Korean Institute of Communications and Information Sciences '15-12 Vol.40 No.12
http://dx.doi.org/10.7840/kics.2015.40.12.2392

IoT 환경을 위한 Hash 기반 동적 Zigbee PANID 생성 및 충돌 회피 방안

이 재 호◆

Adaptable PANID Generation Scheme for Resolving Address Conflict Based on Hash Mechanism in IoT Environment

Jaeho Lee◆

요 약

무선 저전력 통신과 매쉬 네트워크 기술로 대표되는 Zigbee 표준 기술은 스마트 홈과 스마트 빌딩, 대규모 센서 네트워크 등의 환경에서 Ad hoc 방식에 의하여 통신거리 확장을 목표로 개발되어왔다. 또한 Zigbee 표준 기술은 기본적으로 IEEE 802.15.4 표준 기술을 기반으로 개발되었으며, 네트워크를 구성하는 전체 노드는 IEEE에서 정의하는 48bit의 Unique한 노드 주소를 사용하여 매쉬 통신을 구성한다. 하지만 스마트 라이팅이나 넓은 지역의 센서 네트워크와 같이 광범위한 지역을 대상으로 동작하는 Zigbee 환경에서는 매우 많은 수의 노드가 필요하고 경우에 따라 설치를 담당하는 시공사가 다를 수 있으며, 이 경우 많은 수의 노드에 대하여 Unique한 노드 ID를 제공하기 힘들 수 있다. 이러한 문제를 해결하기 위하여 본 고에서는 넓은 지역에 대규모로 설치되는 많은 노드들에 대하여 각각의 Personal Coordinator 들이 해쉬 기반으로 동적 PANID를 설정하고, 이에 따라 발생될 수 있는 PANID 충돌 문제를 해결하는 기법을 제안하며 이에 대한 성능을 검증한다.

Key Words : Zigbee, ID Conflict, WPAN, IoT, Routing, Auto Configuration

ABSTRACT

Zigbee, which was a representative standard technology for dealing low energy and mesh networks in large deployment area such as smart home, smart building, and massive sensor networks, has been developed and deployed for increasing communication area by using Ad hoc method. It has been originally developed based on IEEE 802.15.4 standard so every node needs 48bit unique address defined by IEEE. However, it is absolutely inefficient to assign an unique address to every communication node where it would be deployed through large-scale network area, e.g., smart lighting and massive sensor networks, because there could be variously multiple companies to deploy network infrastructure and they could have different policy to assign node ID. To prevent the problem, this paper proposes a method of dynamic PANID assignment in overall Personal Coordinators, and also proposes a method for addressing PANID conflict problem which could be derived from dynamic PANID assignment.

◆ First Author : Assistant Professor, Dept. Information and Communications, Seowon University, izeho@seowon.ac.kr, 정회원
논문번호 : KICS2015-09-311, Received September 16, 2015; Revised November 20, 2015; Accepted November 23, 2015

www.dbpia.co.kr

Ⅰ. 서 론

유비쿼터스 핵심 기술로 발전되어온 센서 네트워크 기술은 RFID(Radio Frequency Identification) 및 USN(Ubiquitous Sensor Network)이라는 새로운 키워드와 함께 21세기 초기 기술을 주도하였으며, 특히 통신이론 측면에서 기존의 원거리 고성능 송수신의 전통적인 통신목적과 달리 근거리 저전력이라는 새로운 패러다임을 제시하였다. 이러한 USN 기술은 가정용 홈 네트워크, 스마트 빌딩, 스마트 시티 등의 광범위한 통신 인프라의 새로운 시장을 개척하였으며, 스마트폰, 스마트워치, 스마트밴드 등의 소형화된 개인 기기의 폭발적인 수요로 인하여 인체통신과 웨어러블 통신 등에 사용되어 우리 생활 속의 필수 요소로 각인되고 있다.

또한, 저전력 통신 기술은 IoT(Internet of Things) 시장의 핵심적인 요소로 자리 잡고 있으며, Zigbee[1] 기술 역시 Wi-Fi, Bluetooth 등의 기술과 함께 대표적인 저전력 IoT 핵심 기술로 널리 사용되고 있으며, 현재까지도 표준 기술이 활발히 개발되고 있다.

Zigbee 기술은 IEEE[2]에서 발표한 IEEE 802.15.4[3] PHY(Physical) 및 MAC(Medium Access Control) 통신 방식을 그대로 차용하고 상위 계층에 대한 다양한 프로파일 등의 응용 기술과 각 계층별 인터페이스를 정의하여 표준 기술로 발표하였으며, 또한 산업 현장에서 호환적으로 사용될 수 있도록 Interoperability를 제공하기 위한 인증 절차를 진행하고 있다.

Zigbee 표준 기술의 핵심 기술은 응용 계층의 프로파일이 효율적으로 수행될 수 있도록 중간 계층의 기술을 정의하는데 있으며, 특히 네트워크 계층을 다루는 라우팅 기술이 가장 핵심적인 기술 항목으로 자리 잡고 있다. 이 기술은 비교적 짧은 거리의 통신 반경을 가지는 각 통신 노드들을 Ad hoc 형태로 연결한 후, 종단의 통신 노드가 데이터를 전송할 때 중간 노드들에 의한 데이터 포워딩의 형태로 이루어지는데, 이 때 데이터 전달의 효율성을 극대화시키는 데 주 목적을 둔다.

현재까지 수많은 저전력 라우팅[4-10] 기법이 IEEE 802.15.4 및 이를 포함한 Zigbee 기술에서의 적용성을 목표로 연구되어 왔지만, 현재 산업 현장에서 사용되는 Zigbee 기술은 대부분 DSDV(Destination Sequenced Distance Vector)[4]와 AODV(Ad-hoc On-demand Distance Vector)[5] 등으로 제한적이며, 일부 ZRP(Zone Routing Protocol)[6] 등 Hybrid 형태의 라우팅 기법들도 사용되고 있다.

이와 같이 수많은 라우팅 기법들이 제안되고 그중 일부 방식은 실제로 현장에 채용되어 사용되고 있다. 이들 라우팅 방식은 대부분 포워딩 절차에 대한 오버헤드 감소와 각 링크에 대한 링크 비용의 최적화, 또는 이동성이 강한 환경에 대한 Mobility에 대한 고려를 목표로 대부분 연구되어 왔다.

Zigbee에 적용되는 대부분의 라우팅 방식은 PC(Personal Coordinator)로 명칭되는 통신 노드에 따른 패킷 포워딩으로 이루어지는데, 이때 PC는 해당 패킷에 포함된 목적지 주소를 기준으로 포워딩 결정을 한다. 즉, 각 패킷은 자신의 목적지를 명시하는 주소 형태의 유일한 PANID를 반드시 포함해야 하며, 만약 해당 PANID가 전체 네트워크 내에 유일하지 않는 경우 라우팅 영역에서의 큰 혼란을 야기 시킬 수 있다.

반면에, 실제 산업 현장에서는 Zigbee 네트워크에 대한 시공사의 라우팅 방식에 절대적으로 의존하고 있으며, 이에 따른 유일한 PANID 역시 시공사가 주입하는 주소에 의하여 결정된다. 따라서 만약 Zigbee 네트워크 구축 지역에 복수의 구축 및 시공자가 발생할 경우, 이들의 PANID 유일성에 대한 교류가 이루어지지 않는다면 전체 네트워크 영역에서의 대규모 PANID 충돌 문제가 발생할 수 있다. 또한 스마트 라이팅을 포함한 스마트 빌딩이나 대규모 센서 네트워크를 구축할 경우 위와 같은 문제는 크게 가시화될 가능성이 높으며, 향후 IoT 시대를 맞이하여 대규모 통신 기기들이 다양한 형태로 연계될 경우 문제가 시급해진다.

이처럼 PANID 유일성에 대한 대책은 현실적으로 효율적이지 못한 상태이며, 라우팅 동작의 기준이 되는 Addressing에 대한 연구 자체는 실제로 많은 연구가 진행되고 있지 못하고 있기 때문에, Zigbee 네트워크를 구축하는 대규모 영역에서의 효율적인 PANID 생성과 함께 PANID 충돌 문제에 대한 효율적인 방안에 대한 연구가 절실히 필요하다. 따라서 본 고에서는 IoT 환경과 같은 대규모 PANID 생성이 요구되는 Zigbee 네트워크 환경에 대한 고효율적인 동적 PANID 생성 방안과, 이에 따른 PANID 충돌 회피에 대한 해결방안을 제시한다.

Ⅱ. 연구 배경

MANET 등의 멀티홉 라우팅 기법은 네트워크를 구성하는 통신 노드의 위치적 구조와 요구되는 에너

www.dbpia.co.kr

지 효율, 발생되는 트래픽의 크기와 빈번도, 노드의 이동성 등에 따라 그 방식을 달리 하며, 크게 Proactive 방식과 Reactive 방식으로 구분되고 경우에 따라 이 두 가지 방식의 혼합된 형태인 Hybrid 방식으로 구분된다.

Proactive 방식은, 네트워크를 구성하는 통신 노드들의 토폴로지의 변경상황에 능동적으로 대처하기 위한 방식으로써, DSDV 라우팅 알고리즘으로 대표된다. 이 방식에서의 모든 노드들은 토폴로지상에서 자신의 위치를 기반으로 다른 모든 노드에 대한 Link Cost를 점검 및 연산하고 이를 주기적으로 반복함으로써 최적의 라우팅 경로를 유지하는 기법이다.

이 라우팅 방식은 네트워크 토폴로지가 빈번하게 변경되는 환경에서도 주기적으로 최적의 라우팅 경로를 유지하기 때문에, 모든 노드들은 항상 최적화된 라우팅 경로를 보유하고 있다. 따라서 임의의 노드에서 데이터 전송 요구가 발생할 경우 라우팅 경로 탐색 과정을 별도로 진행할 필요가 없고 비교적 짧은 전송 시간을 보장한다. 하지만 데이터 발생 빈도가 매우 낮은 경우에도 주기적인 라우팅 경로 탐색으로 인한 에너지 소모가 발생하며, 이를 극복하기 위하여 라우팅 경로 탐색 주기를 길게 설정할 경우 이동성이 매우 강한 환경에서 경로 선택 실패율이 높아지게 되는 단점이 있다.

한편 AODV와 DSR(Dynamic Source Routing)[7]으로 대표되는 Reactive 방식은 네트워크 유휴 시간(데이터 전송이 발생되지 않은 시간)에는 라우팅 경로 탐색 절차를 수행하지 않으며, 데이터 전송이 필요할 경우에만 필요에 의해 라우팅 경로 탐색을 수행하는 방식이다. 이 방식은 Proactive 방식과 반대의 성격을 나타내기 때문에, 네트워크 토폴로지 변화가 매우 빈번한 이동형 네트워크 환경에 적합하다. 하지만 Reactive 방식 역시 데이터 전송이 발생된 시점부터 라우팅 경로 설정을 수행하기 때문에 Proactive 방식에 비하여 데이터 전송 지연 시간이 상대적으로 높고, 경우에 따라 전송 성공률 또한 낮아질 수 있다.

Hybrid 방식은 Proactive 방식과 Reactive 방식을 적절하게 혼합하여 사용하는 방식으로써 ZRP, TA-DZR(Traffic Aware Dynamic Zone Routing)[8] 등이 존재한다. ZRP 방식은 임의의 노드에서 특정 거리를 Hop Count로 정의하고, 설정된 임계값 이하의 Hop Count에 해당하는 노드들에 대하여 Proactive 방식을 사용하고, 그 외의 노드들에 대해서는 Reactive 방식을 적용하여 Proactive 방식과 Reactive 방식의 장점을 혼합한 형태로 운영되는 라우팅 기법이다.

하지만 이러한 대부분의 라우팅 기법은 모두 유일한 주소 및 노드 ID를 필요로 하며, Zigbee의 경우 PANID의 유일성을 요구한다. 또한 앞 장에서 기술한 바와 같이 대규모 네트워크를 구성하는 Ad hoc 환경에서는 네트워크를 설치하는 시공사가 상이할 수 있으며, IoT 환경에서는 서로 다른 다양한 네트워크가 혼합된 연결형태가 구성되기 때문에 Zigbee PANID의 유일성에 대하여 시공사의 ID부여정책에 의존할 경우 많은 문제점이 발생될 수 있다.

또한 기존의 많은 센서네트워크 MAC 프로토콜[9-14]에서의 ID 충돌 문제를 해결하기 위하여 연구된 PACMAN(Passive Auto Configuration for Mobile Ad hoc Networks)[15] 등에서는 이러한 통신노드의 동적 ID Assignment 정책에 대하여 연구된 바 있지만, 대체적으로 전체 네트워크에 대한 정보를 알고 있다는 전제 하에 설계된 방식이기 때문에, IoT 환경에서 발생되는 부분적인 네트워크 환경에서는 외부 네트워크의 규모와 환경에 대한 정확한 정보 습득이 불가능하기 때문에 적용이 적합하지 않다. 따라서 부분적인 네트워크 환경에서 효율적인 PANID Assignment 정책을 설계하고, 이후 발생되는 PANID 충돌에 대한 적절한 대체 방안에 대한 연구가 필요하다.

Ⅲ. 동적 ID생성 및 충돌회피 방안

3.1 Motivation

Zigbee 기술에서는 여러 노드들이 Ad-hoc 형태로 상호 통신하며, 임의의 Source 노드로부터 원거리 Destination 노드까지 Hop-by-Hop으로 데이터를 전달할 수 있다. 이러한 네트워크 형태에서 가장 작은 통신 구성을 이루는 네트워크 단위를 Zigbee 에서는 PAN (Personal Area Network) 이라고 정의하며, 하나의 PAN 영역에서는 하나의 PC (PAN Coordinator)를 주축으로 다수의 Leaf 노드가 Star 토폴로지 형태로 PC와 연결된다. 즉, PC는 해당 PAN 내부의 노드들을 직접 제어하며, 인접된 외부 PAN과의 통신을 통하여 Ad-Hoc 통신을 가능하게 한다. 또한, PAN 내의 모든 노드가 송신하는 패킷은 해당 PAN의 PC에게만 전달되어야 하며, 인근 PAN 내의 노드가 이를 수신하지 못하게 하기 위하여 Zigbee 에서는 Unique한 PANID를 정의하고 있다.

하지만, 현재의 Zigbee 표준 기술에는 PANID를 생성하는 방안이 없으며, 대규모 Ad-hoc 네트워크가 존재한다고 가정할 때 임의의 PANID는 원거리에 존재하는 모든 PANID를 알 수 없기 때문에 Unique한

www.dbpia.co.kr

PANID 생성을 보장할 수 없다. 또한, Zigbee 에서 정의하는 PANID는 2byte 체계로 구성되기 때문에 원천적으로 Unique PANID를 생성하는 것이 불가능하며 어떠한 경우에서도 PANID 충돌 문제가 발생할 수 있다. 이를 해결하기 위하여 본 고에서는 지역적인 동적 PANID 생성 방식과 이에 따른 충돌 탐지 및 회피 방안을 다음에 기술한다.

3.2 Hash 기반 동적 PANID 생성

일반적으로 IEEE MAC Address는 48bit로서 Unique 하다고 알려져 있다. 하지만 이는 전체 네트워크 규모에 종속적이며, 무한한 크기의 네트워크 규모가 있다고 가정할 경우 어떠한 크기로도 Unique ID를 정의할 수 없다. Zigbee에서는 단일 PAN에 대한 ID를 PANID로 정의하며, 하나의 PAN 내에는 하나의 PC가 해당 PANID를 소유한다.

본 제안 방식은 Zigbee PANID를 동적으로 생성하되 확률적으로 PANID 충돌 확률을 낮추는 방안을 제시하고, PANID 충돌 탐지 방법과 이에 대한 해결 방안을 제시하는 데 목적을 둔다. 또한 본 절에서는 PANID 충돌 확률을 낮추기 위한 동적 PANID 생성 방안을 아래와 같이 제시한다.

그림 1과 그림 2는 PANID를 생성하는 방안과 초기 PANID를 모든 노드에게 알리는 방안을 도식화하였다. 또한 Zigbee 표준 기술은 IEEE 802.15.4 기반의 PHY/MAC 기술을 사용하며, 모든 노드는 48bit 길이의 IEEE Address를 보유하고 있고 PANID는 기존 표준 기술에서 정의하는 16bit 크기를 사용한다.

IEEE에서 정의되는 MAC Address가 무한대의 노드 수에 모두 Unique한 Address를 제공할 수는 없지만 PANID에 비하여 유일성이 매우 높기 때문에, 본 논문에서는 각 노드가 보유한 IEEE Address를 Seed로 Hash 알고리즘을 사용한다. 또한 Hash 알고리즘을 위하여 사용되는 Hash Table은 PANID 길이와 동일하게 16bit로 결정된다.

이러한 형태로 그림 1과 같이 48bit의 Address를

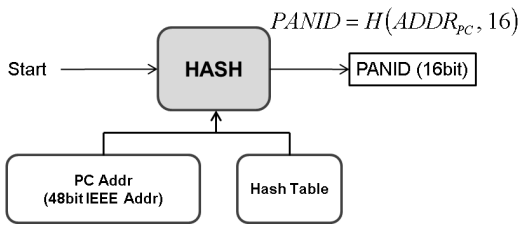

그림 1. Hash 기반의 PANID generation
Fig. 1. Hash-based PANID generation

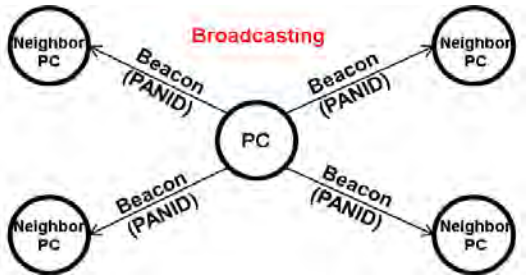

그림 2. PANID broadcasting
Fig. 2. PANID broadcasting

16bit Hash 알고리즘을 거쳐 최종적으로 PANID를 생성할 경우, 이는 16bit 표현 가능 수인 65536 크기의 범위 내에 유일성을 제공하기에, 네트워크 규모가 이 경우의 수 보다 크지 않는 한 유일 PANID를 제공할 수 있으며, 반대의 경우에도 PANID 충돌 확률을 최대한 낮출 수 있다. 이와 같은 절차로 생성된 PANID는 PAN 내의 MAC 계층 통신에서 PC가 주기적으로 송신하는 Beacon 내부에 적재되어 동일 PAN 내의 모든 노드에게 PANID 정보를 알려준다.

본 고에서 제안한 Hash 알고리즘 외에도, 동적 PANID 생성을 위한 또 다른 방법으로는 Random PANID 생성, 장치 내부의 Clock Time Stamp 값을 이용한 PANID 생성, IEEE Address 중 특정 부분(상위 또는 하위)을 2byte 만큼 선택하여 PANID 생성, 또는 IEEE Address를 2byte로 조합하여 PANID를 생성하는 방법이 활용될 수 있지만, 지역적인 네트워크에서 원천적으로 PANID의 유일성을 확보하고 PANID 충돌을 확률적으로 낮추기 위해서는 Hash 방식의 PANID 생성 기법이 효율적이다.

또한 그림 2와 같은 형태로, PANID를 생성한 PC는 자신의 이웃 PC를 대상으로 Discovery 절차 등을 통하여 자신이 생성한 PANID를 알리고, 이를 수신한 이웃 PC는 자신이 생성한 PANID와의 중복 검사를 수행함으로써 1hop 이내의 이웃 PC에 대한 지역적인 PANID 충돌 발생을 방지한다.

3.3 PANID 충돌 탐지 및 회피 방안

앞 절에서 나타낸 Hash 기반 PANID 생성 방식은 2byte로 제한되는 PANID 중복 확률을 최대한 감소시키기 위하여 48bit MAC Address를 기반으로 Hash 테이블을 활용하고, 이를 통하여 PANID를 관리자의 직접 주입 없이 PC 자체적으로 동적 할당 하는 방식이다. 하지만 앞서 설명한 바와 같이 네트워크 규모가 증가할수록 PANID 충돌 확률은 높아지기 때문에 이

www.dbpia.co.kr

에 대한 회피 방안이 필요하다. 본 절은 이러한 문제 해결을 위하여 네트워크를 구성하는 각 PC에서 PANID 충돌을 감지하고 이에 대한 PANID 재할당 방안을 나타낸다.

그림 3과 같이 PC는 외부로부터 수신되는 모든 Packet을 Overhearing 할 수 있으며 또한 대상 패킷의 PANID와 자신의 PANID 충돌 여부를 파악할 수 있다. 따라서 외부의 특정 PAN에서 자신이 종속된 PAN 및 PANID가 수신된 패킷에 포함된 PANID와 동일하다고 발견될 경우 다음의 3가지 방법 중 선택적으로 수행하여 PANID 충돌 문제를 해결할 수 있다.

먼저 PANID 충돌을 발견한 장치는 메시지 송신을 통하여 Source 장치가 PANID를 변경하도록 설정할 수 있다. 이 경우 PANID 변경 요구는 PANID 충돌을 감지한 노드가 실행하며, Source PC는 자신의 PANID를 변경하기 위하여 Hash 기반의 PANID 생성 방식을 다시 실행시킨 후, 자신의 이웃 PC와 PANID 충돌을 발견한 PC 모두에게 자신의 변경된 PANID를 알린다.

두 번째로 PANID 충돌 발견 장치가 자신의 PANID를 변경하는 방법이 존재한다. 이 경우 역시 위와 동일한 방법으로 PANID를 변경하지만, ID 변경을 PANID 충돌 탐지 PC가 진행하기 때문에 Source PC에게는 충돌 발생 자체를 알릴 필요는 없다.

마지막으로 PANID 충돌을 탐지한 PC와 Source PC의 두 장치가 서로 Negotiation 절차에 의하여 PANID를 변경할 장치를 선택하는 방법이 있다. 이 경우 PANID 변경 장치로 선택되기 위하여 고려해야 할 파라미터들이 존재하며, 기본적으로 각 PC가 보유한 자식 노드들의 수와 각 PC에 남아있는 에너지 잔량이 필수적으로 고려되어야 한다. 즉, 임의의 PC가 자신의 PANID를 변경하게 될 경우 자신이 보유한 모든 자식 노드들에게 이를 알려야 하는데, 이 경우 또한 Direct 전송이 아닌 Ad hoc 연결 형태일 가능성도 높기 때문에 이에 대한 고려가 필요하며, 이 동작을 포함하여 이웃 PC에 대한 PANID 변경 전달 등 여러 절차가 요구되기 때문에 PC 자체에 남아있는 에너지 잔량 또한 중요한 요소가 된다.

이와 같은 3가지 해결 방안은 크게 PANID 변경을 수행하는 PC의 주체에 따라 구분될 수 있다. 즉, PANID 충돌을 탐지한 장치가 발생할 경우, 대상 PC에게 요구하거나 자신이 직접 변경하거나 또는 서로 협상하거나에 따라 달라진다. 이러한 방식은 네트워크 환경에 따라 유동적으로 적용할 수 있지만 기본적으로 네트워크 규모와 PANID 충돌이 발생한 두 장치간의 거리는 반드시 고려되어야 한다. 즉, PANID 충돌을 발견한 PC와 Source PC의 거리가 멀고 네트워크 규모가 크며 라우팅 경로가 다양하게 발생할 확률이 높은 환경에서는, PANID 충돌을 발견한 PC가 자신의 ID를 변경하는 방법이 효율적이다. 하지만 소규모 네트워크 환경에서는 Source PC에게 PANID 변경을 요청하여 해당 데이터 전송을 다시 수행하도록 유도하는 방법이 전송 신뢰성 측면에서 효율적이다. 또한 만약 두 PC의 환경 차이가 크지 않을 경우 협상에 의한 방안도 고려되어야 한다.

이러한 형태로 자신의 PANID를 변경한 PC는 자신에게 종속된 PAN 내부의 모든 통신 노드들에게 알리기 위하여 그림 3과 같이 MAC 계층에서 변경된 PANID가 포함된 Beacon을 송신한다. 또한 내부 PAN에 대하여 PANID 변경 적용이 완료된 후, 해당 PC는 네트워크 전체에 대하여 변경된 PANID를 알리기 위하여, 전체 네트워크에 존재하는 모든 PC를 대상으로 Routing 계층에서 Route Discovery 등의 Flooding 절차를 수행한다.

PANID 충돌을 탐지한 PC는 충돌 회피를 위하여 앞서 제시한 3가지 유형 중 선택적으로 PANID 재생

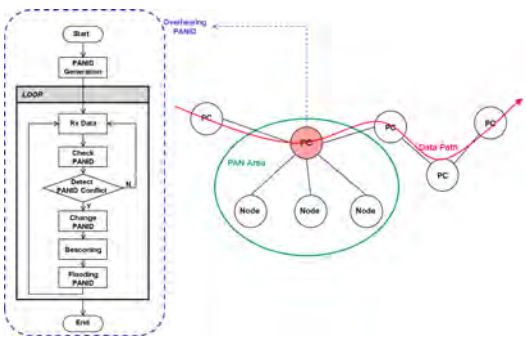

그림 3. PANID 충돌 탐지 방안
Fig. 3. PANID conflict detection method

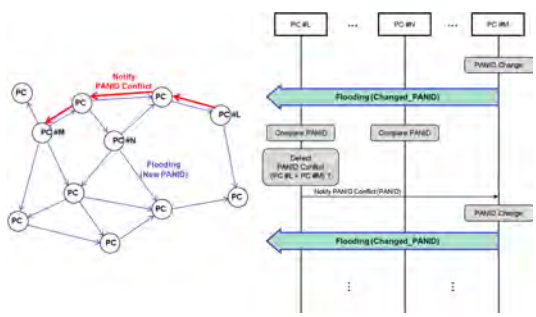

그림 4. PANID 충돌에 대한 Notification
Fig. 4. Notification for PANID conflict

www.dbpia.co.kr

성 절차를 진행하는데, 이때 자신의 PANID를 변경한 PC는 변경된 PANID를 네트워크에 알리기 위하여 그림 4와 같이 Route Discovery 또는 Route Update 등의 기능을 수행하기 위한 Flooding 절차를 수행한다. 또한 이 Flooding 내부에는 자신의 변경된 PANID를 적재한다.

하지만 Flooding 절차 역시 변경된 PANID에 대한 유일성을 보장하지는 못한다. IoT 환경에서는 여러 가지 기기들이 다양한 형태의 직접 및 간접 연결성을 제공하기 때문에, 이기종망 (Heterogeneous Networks)에 대한 연결성(Inter-Connectivity)도 존재할 수 있으며, 또한 단일 Zigbee 네트워크라 할지라도 대규모 환경의 경우 궁극적으로 Clustering 등의 네트워크 분할 기능이 사용될 수 있다. 따라서 변경된 PANID에 대한 Flooding 역시 지역적인 유일성만 보장될 수 있으며, 이를 위하여 본 고에서는 PANID 충돌 탐지 동작을 모든 PC가 항상 수행하되, 충돌이 탐지 될 때마다 PANID 회피 동작을 수행하고, 이를 통하여 네트워크 초기 설치시 Self Organization 단계에 충분한 시간을 두고 전반적으로 모든 PC가 스스로 자신의 PANID 유일성을 찾는 과정을 권고한다.

우선, PANID 충돌을 탐지한 PC는 자신의 PANID를 변경하는데, 이때 변경된 PANID가 전체 네트워크 내의 임의의 PANID와 동일할 경우 추가적인 PANID 충돌이 발생되며, 이는 PANID 변경에 의한 Flooding 메시지를 모든 PC가 수신하여 자신의 PANID와 비교함으로써 탐지할 수 있다. 또한 Flooding 메시지 내의 PANID가 자신의 PANID와 동일함을 감지한 PC는, Flooding 메시지를 송신한 PANID에게 추가적인 PANID 충돌이 발생함을 Notify_PANID_Conflict 메시지를 통하여 알린다. 또한 Notify_PANID_Conflict 메시지를 수신한 PC는 자신의 PANID를 앞 장에서 설명된 방식을 통하여 다시 변경하고 이를 Flooding 한다. 그 후 PANID를 변경한 PC는 Notify_PANID_Conflict 메시지가 더 이상 수신되지 않을 때 까지 위 절차를 반복한다.

3.4 Overhearing에 의한 PANID 충돌 탐지

위와 같은 PANID 탐지 방법은 해당 패킷의 Destination PC 이외에도 중간 Forwarding PC의 overhearing에 의한 방법 또한 가능하다. 매쉬 네트워크와 같은 멀티홉 환경에서의 모든 패킷은 반드시 중간 노드를 거쳐야 하며, Zigbee 환경에서는 네트워크를 구성하는 다른 PC가 그 역할을 수행한다. 즉, 임의의 통신 노드가 원거리에 위치한 특정 destination 노드로 패킷을 전달할 경우, 이 패킷은 주어진 Source 노드 상위의 PC와 함께 destination 노드를 종속하는 Destination PC를 포함하여, 해당 패킷 전달 경로 상에 존재하는 다수의 PC 또한 이 패킷을 전달한다. 따라서 라우팅 경로에 포함된 모든 PC는 해당 패킷을 수신하여 확인할 수 있다.

이와 같이 패킷 Forwarding을 수행한 중간 PC는 패킷에 대한 Overhearing을 통하여 원거리에 존재하는 PC의 PANID를 저장할 수 있고, 만약 Forwarding 되는 패킷의 Source 또는 Destination PANID가 자신의 PANID와 동일할 경우 PANID 충돌을 파악할 수 있다. 또한 만약 서로 다른 경로에서 전달된 두 패킷의 Source 또는 Destination ID에서 동일한 PANID가 Overhearing에 의하여 탐지된 경우, 이 PC는 PANID 충돌 사실을 파악할 수 있다. 따라서 이 PC는 패킷 내

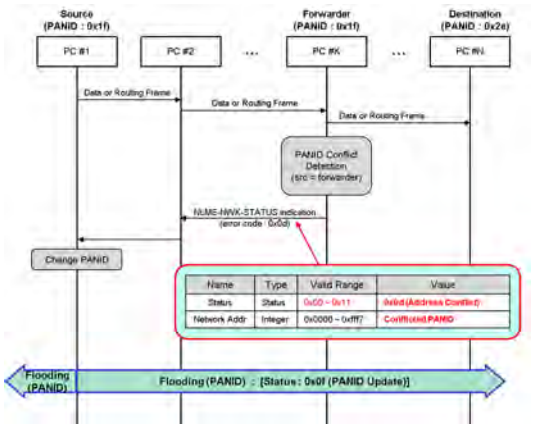

그림 5. Forwarder에 의한 PANID 충돌탐지 및 회피 절차
Fig. 5. PANID conflict detection and avoidance process by forwarder

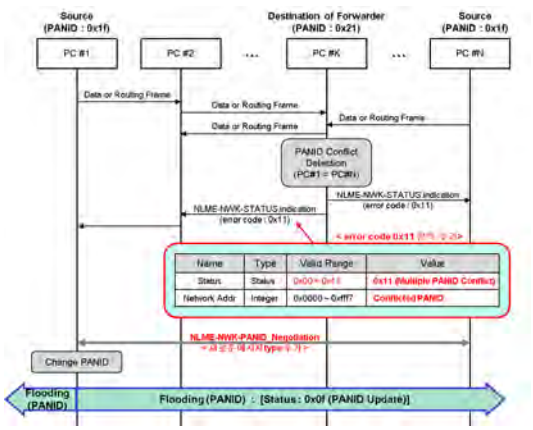

그림 6. 제3의 PC에 의한 PANID 충돌탐지 및 회피 절차
Fig. 6. PANID conflict detection and avoidance process by 3rd-Party PC

www.dbpia.co.kr

의 PANID가 자신의 PANID와 중복되지 않더라도 PANID 충돌을 파악한 후 대상 PC에게 PANID 변경 요청을 수행할 수 있다. 그림 5와 6은 위와 같이 Forwarding 절차를 수행하는 중간 PC가 PANID 충돌을 탐지하는 2 가지 경우에 대한 예시를 나타내었다.

Ⅳ. 성능 평가

제안하는 Hash 기반 동적 PANID 생성 방식은 IEEE 802.15.4 표준 기술에서 정의한 16bit PANID의 유일성을 확보하기 위하여 48bit MAC Address와 Hash 테이블을 사용한다. 이는 16bit라는 물리적 길이의 한계로 인하여 PANID의 유일성을 원천적으로 제공할 수는 없지만, IEEE에서 정의한 MAC Address를 사용한 Hash 특성과 PANID Broadcasting 방안을 활용하기 때문에 지역적인 유일성은 어느 정도 보장이 가능하다.

대규모 네트워크 환경이나 이기종 네트워크가 혼합된 IoT 환경의 경우, PC 자체의 동적 PANID 생성 방식은 원천적으로 충돌문제가 발생될 수 있다. 하지만 다양한 네트워크 환경을 구성하는 모든 통신 노드에 유일한 주소 및 PANID를 수동으로 주입하는 방식은 네트워크 구축의 효율성과 편의성 측면에서 매우 열악할 수 있기 때문에, 본 고에서는 PC 자체에서의 동적 PANID 생성 방식을 제안하고 PANID 중첩에 대한 충돌 탐지 방안과 이에 대한 회피 방안을 제안한다.

식 (1)과 같이, 전체 네트워크를 구성하는 PC의 수를 N, 전체 PANID의 평균을 μ라고 정의할 때, PANID의 중첩 확률은 분산에 의존적이며 아래와 같이 표현된다.

$$S^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i-\mu)^2 \tag{1}$$

또한 모든 PAIND 값에 대한 경우의 수를 k, 임의의 PC 수를 n으로 설정할 때, n개의 PC에서 충돌이 발생할 확률 $P_c(n)$ 및 전체 N개의 PC에서의 총 충돌 수에 대한 기대값 $E_c(n)$ 값은 아래와 같이 표현된다.

$$\begin{aligned} P_c(n) &= 1 - {}_kP_n\, k^{-n} \\ &= 1 - \frac{k!}{k^n(k-n)!} \end{aligned} \tag{2}$$

$$\begin{aligned} E_c(n) &= \sum_{n=2}^{N}(1-P_c(n))n \\ &= \sum_{n=2}^{N}\left(1-\frac{k!}{k^n(k-n)!}\right) \end{aligned} \tag{3}$$

이와 같이 이론적 충돌수에 대한 기대값에 대한 충돌 확률은 PANID의 크기가 16bit로 고정되어 있기 때문에 원천적으로 낮추기 어렵지만, 모든 PC가 이웃하는 PC의 PANID를 Broadcast 형태로 수신하고 이를 인지한 후 Hashing 기법을 적용할 경우, 지역적인 PANID 충돌 확률은 크게 낮출 수 있다. 대부분의 Zigbee 네트워크 환경에서 발생되는 데이터는 종단 노드에서 원격 Gateway 노드로 전달되거나 또는 근거리에 위치한 PC로의 패킷 전달이 대부분이기 때문에, 이러한 지역적 PANID 충돌 억제 방안은 실제 환경에서 높은 이득을 나타낼 수 있다.

그림 7은 전체 네트워크에 존재하는 PC의 수를 16bit PANID의 허용 크기(65,535)를 초과시켜 80,000 PC로 설정한 후, 이로 인하여 반드시 발생되는 PANID 충돌에 대한 각 PC의 탐지율을 측정하여 나타내었다. 또한 본 실험에서는 MD5 Hashing 기법을 활용할 경우에 대한 PANID의 충돌 탐지율을 Proactive 방식과 Reactive 방식 모두에 적용하여 결과를 도출하였으며, 각 PC에 발생되는 트래픽의 Destination PANID는 Random하게 발생시켰다. 이러한 결과는 트래픽이 증가할수록 원거리 라우팅 확률이 높아지고, 이에 대한 PANID 충돌 탐지율 또한 높아지는 현상을 나타낸다.

본 실험에서 트래픽 발생이 낮아 원거리 PANID 충돌에 대한 탐지율이 낮은 경우에도, 지역적인 라우

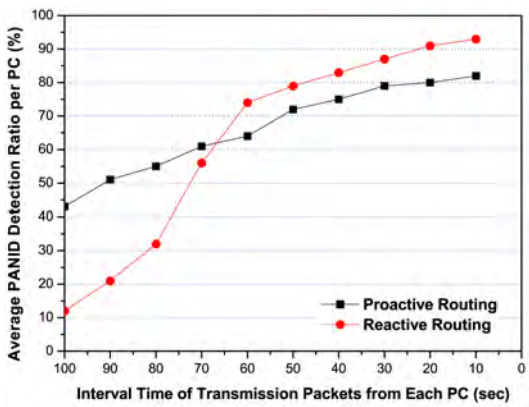

그림 7. 트래픽에 따른 PANID 충돌 탐지율
Fig. 7. PANID conflict detection ratio according to traffic

www.dbpia.co.kr

팅 측면에서는 PANID의 유일성이 보장되기 때문에 지역적 데이터 전달에는 문제가 되지 않는다. 다만 원거리 데이터 전달 요구가 발생한 경우 초기 라우팅 탐색에는 혼란이 발생할 수 있지만, PANID 충돌 여부는 중간 Forwarding PC에서 파악할 수 있으며 이에 대한 PANID 변경 요청 또한 수행되기 때문에, 이후 발생되는 데이터 전달에는 문제없이 라우팅 절차가 수행된다.

그림 8은 그림 7과 동일한 환경에서 각 PC의 트래픽 발생을 고정시킨 후, 시간에 따른 PANID 충돌 탐지율을 도식화하였다. 이 실험 역시 Proactive와 Reactive 라우팅 방식에 모두 적용하였으며, 각 PC에 발생되는 트래픽의 Destination PANID 역시 그림 7과 동일하게 Random 발생 방법을 적용시켰다.

이 실험에서는 각 라우팅 방식에서 발생되는 PANID 충돌 탐지 결과의 차이점을 관찰하기 위하여, 초기 Route Discovery 등의 절차로 인한 라우팅 영역에서의 Flooding 수행을 생략한 후 Proactive 및 Reactive 라우팅 방식 고유의 특징에서 발견되는 PANID 충돌 탐지를 확인하였다. 또한 네트워크 운영 중 발생되는 신규 PC에 의한 PANID 충돌 회피 동작 여부를 판단하기 위하여, 모든 PANID는 총 실험시간 내에 2~3회 자신의 PANID를 변경하였다.

Proactive 라우팅 방식은 주기적인 Route Update로 인하여 불필요한 Flooding 절차가 수행되는 단점이 있지만, 모든 PC가 항상 최적화된 경로를 인지하기 때문에 일반적으로 즉각적인 데이터 전달이 가능하다. 이러한 특성으로 인하여 Reactive 라우팅에 비하여 PANID 충돌에 대한 탐지 및 회피 시간이 상대적으로 빠르다는 결과를 나타내었다.

반면 Reactive 라우팅 방식은 데이터 전달 요구가 발생할 경우에 On-demand 형태로 데이터 전달 경로를 확인한다. 따라서 원거리 PC의 PANID가 변경되어 PANID 충돌이 발생하더라도 즉각적으로 탐지할 수 없으며 충돌 회피 또한 Proactive 라우팅 방식에 비하여 시간적 비용이 요구된다. 하지만 Reactive 라우팅 방식은 데이터 전달이 요구될 때에만 라우팅 경로를 탐색하기 때문에 트래픽이 낮은 환경에서 에너지 효율이 높다는 장점이 있고, 또한 PANID 충돌 역시 지역적인 데이터 송수신에서는 발생하지 않기 때문에 발생되는 트래픽의 근거리 Destination PC에 대해서는 원거리 PANID의 충돌이 발생하여도 라우팅 수행에는 문제가 없다.

마지막으로 그림 9는 그림 7에서 확인된 PANID 충돌에 대한 참고적 실험으로써, Destination PANID가 Random하게 변경되는 트래픽 환경에서 패킷 수가 증가함에 따라 실제로 중첩된 PANID 수를 나타내었다. 이 실험 역시 트래픽이 높아질수록 원거리 데이터 전달 요구가 높아지며, 이에 따라 PANID 충돌 탐지 빈도수가 높아지기 때문에 전체적인 PANID 중첩 개수는 트래픽에 따라 감소함을 알 수 있다. 하지만 본 실험에 적용된 총 PC 수는 16bit로 제한된 PANID 허용 크기를 초과하기 때문에, 이 범위를 초과한 PC의 수량에 대한 PANID 충돌 수는 특정 수준 이하로 감소되지 않음을 알 수 있다. 또한 전체적인 데이터 전달에 대한 전송 성공률 역시 PANID 충돌에 대한 영향을 크게 받지 않음을 알 수 있다.

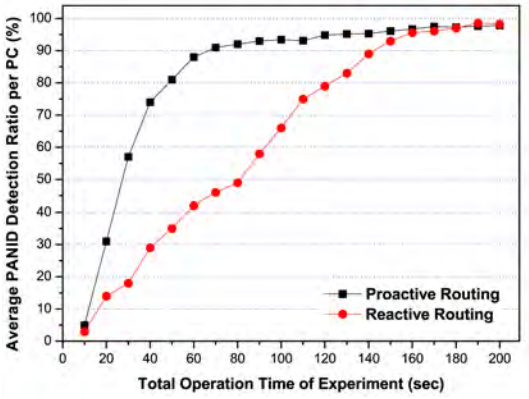

그림 8. 시간 경과에 따른 PANID 충돌 탐지율
Fig. 8. PANID conflict detection ratio in time domain

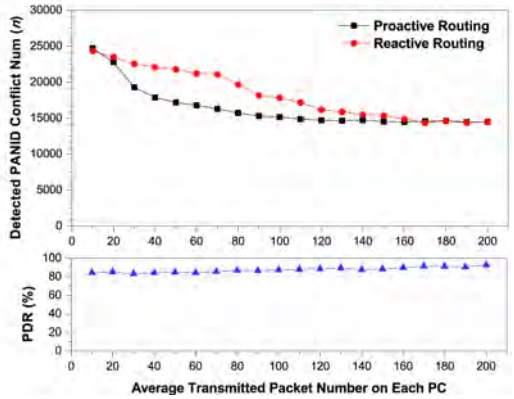

그림 9. PANID 충돌 탐지 수 및 전송 성공률(PDR)
Fig. 9. Number of PANID conflict detection and PDR

V. 결 론

대규모 센서 네트워크 또는 많은 통신 노드 수가 필요한 대형 빌딩의 Smart Lighting 등의 환경에서는

www.dbpia.co.kr

PANID 유일성 보장을 각 노드마다 주입시키는 ID체계에 의존하기 힘들고, 또한 새로운 노드의 추가 등의 관리 및 유지보수 측면에서도 PANID 유일성에 대한 일차원적 고려는 효율성 측면에서 매우 열악하다. 본 고에서는 이러한 문제를 해결하기 위하여 Hash 기반의 동적 PANID 설정 방안을 제시하였고, 불가피하게 발생되는 PANID 충돌에 대한 효과적인 탐지 및 회피 방안을 제안하였으며, 이에 대한 성능을 검증하였다.

수많은 네트워크 기술에서 끊임없이 제시되었던 Addressing 문제는 향후에도 지속적으로 연구되어야 할 테마임이 자명하며, 본 고에서 제시한 방식 이외에 전체 네트워크 관점에서의 Addressing 체계 방안, 그리고 이를 토대로 발전될 수 있는 Auto Configuration 방안은 대규모 네트워크를 목표로 연구되는 수많은 네트워크 기술과 접목이 용이하며 발전 가능성 역시 높은 분야이기에, 향후 다양한 네트워크 기술 관점에서 공통된 연구 진행이 요구될 것으로 사료된다.

References

[1] Zigbee Specification, Zigbee Alliance Inc., Sept. 2012.

[2] http://www.ieee.org

[3] IEEE, *IEEE Standard for Local and Metropolitan Area Networks*, Part 15.4 (Low-Rate Wireless Personal Area Networks), Sept. 2011.

[4] C.-C. Chiang, H.-K. Wu, W. Liu, and M. Gerla, "Routing in clustered multihop, mobile wireless networks with fading channel," in *Proc. IEEE SICON*, pp. 197-211, Apr. 1997.

[5] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. IEEE WMCSA '99*, pp. 90-100, Feb. 1999.

[6] Z. J. Haas, M. R. Pearlman, and P. Samar, *The zone routing protocol (ZRP) for ad hoc networks*, Internet Draft, draftietf-manet-zone-zrp-04, 2002.

[7] D. B. Johnson and D. A. Maltz, "Dynamic source routing in Ad-Hoc wireless networks," *Mob. Comput.*, vol. 353, pp. 153-81, 1996.

[8] J. Lee, "A new routing scheme to reduce traffic in large scale mobile ad-hoc networks through selective on-demand method," *Wirel. Netw.*, vol. 20, no. 5, pp. 1067-1083, 2014.

[9] L. Wang and S. Olariu, "A two-zone hybrid routing protocol for mobile ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 15, pp. 1105-1116, 2004.

[10] C. Busch, et al., "Approximating congestion + dilation in networks via "Quality of routing" games," *IEEE Trans. Comput.*, vol. 61, no. 9, pp. 1270-1283, 2012.

[11] J. Lee, "A traffic-aware energy efficient scheme for WSN employing an adaptable wakeup period," *Wirel. Pers. Commun.*, vol. 71, no. 3, pp. 1879-1914, Aug. 2013.

[12] N. Saxena, A. Roy, and J. Shin, "A qos-based energy-aware MAC protocol for wireless multimedia sensor networks," in *Proc. VTC*, pp. 183-187, May 2008.

[13] C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and H. Tian, "RAP: A real-time communication architecture for large-scale wireless sensor networks," in *Proc. IEEE RTSS*, pp. 55-66, Dec. 2001.

[14] J. Lee, "A massive transmission scheme in contention-based MAC for wireless multimedia sensor networks," *Wirel. Pers. Commun.*, vol. 71, no. 3, pp. 2079-2095, Aug. 2013.

[15] K. Weniger, "PACMAN: passive autoconfiguration for mobile ad hoc networks," *IEEE JSAC, Wireless Ad Hoc Networks*, vol. 23, pp. 507-519, 2005.

이 재 호 (Jaeho Lee)

2005년 : 고려대학교 전자컴퓨터공학과 석사

2008년~2013년 : 고려대학교 전기전자전파공학과 박사

2011년~2013년 : 서일대학교 겸임교수

2013년~2015년 : LG전자 차세대 표준연구소 선임연구원

2015년~현재 : 서원대학교 정보통신공학과 조교수

<관심분야> WPAN, 센서네트워크, MANET, MAC, WBAN, Bluetooth, Wi-Fi, ITS, Localization

www.dbpia.co.kr