특집

IPv6기반 센서 네트워크(6LoWPAN)을 위한 라우팅 프로토콜 기술

임채성, Waleed Mansoor, 김기형, 유승화(아주대학교), 박수홍(삼성전자), 이재호(한국전산원)

I. 서 론

센서 네트워크는 저가의 센서 장치들을 무선으로 상호 연결한 저전력 네트워크로서 유비쿼터스 환경 구축의 핵심 기술로 떠오르고 있다. 이를 위한 대표적인 PHY, MAC 표준으로는 IEEE Std 802.15.4-2003(이하 IEEE 802.15.4)[1]을 들 수 있다. IEEE 802.15.4 표준은 센서 네트워크에 적합한 저전력, 저속, 단거리의 특징을 갖추고 있다. IEEE 802.15.4에 이어 후속 작업으로서 IEEE 802.15.4b TG에서 업데이트가 되고 있으며, 또한 IEEE 802.15.4a를 통해 고속 통신 및 정교한 위치 인식을 지원하는 새로운 PHY를 정의하고 있다.

2004년 12월 발표된 ZigBee 1.0-2004(이하 ZigBee)[2]는 IEEE 802.15.4 네트워크의 상위 계층을 정의하며, 네트워크, APS(Application Support Sublayer), AF(Application Framework), ZDO(ZigBee Device Object) 등으로 구성된다. ZigBee 기술은 누구나 사용할 수 있는 공개 표준이 아니고 삼성, 모토롤라, 필립스 등의 회사가 프로모터로 있는 ZigBee Alliance에 가입한 회원에 한해 사용이 가능하다. 2005년 6월부터는 저변 확대를 위해 일반에게 스펙이 공개되었다.

6LoWPAN는 IETF 인터넷 영역(Area)의 6LoWPAN 워킹그룹(WG)에서 표준화되고 있는 기술로서 LoWPAN(Low-power Wireless Personal Area Networks), 즉 IEEE 802.15.4 표준의 MAC 및 PHY 계층의 상위 계층에 IP 계층을 올려 센서 네트워크상에서 IPv6 패킷을 전송하고자 하는 기술이다. 2004년 11월 61차 IETF 회의에서 BOF가 열렸으며 2005년 3월부터 정식 워킹그룹으로 시작하였다. 6LoWPAN 기술은 기존의 IP 인프라를 재사용할 수 있다는 장점과 더불어 IPv6의 특징으로 들 수 있는 많은 수의 주소 공간과 자동 주소 할당 등의 기능이 센서 네트워크에 특징에 부합하는 점 등으로 인해 가능성을 인정받고 있다.

본고에서는 6LoWPAN을 위한 라우팅 프로토콜 기술을 제시하고자 한다. 먼저 II장에서는 6LoWPAN에 대한 기술적 소개를 한다. III장에서는 6LoWPAN 라우팅 기술을 살펴보고, IV장에서는 6LoWPAN 라우팅 기술을 적용한 테스트베드를 보인다. 그리고 마지막으로 V장에서는 결론을 맺는다.

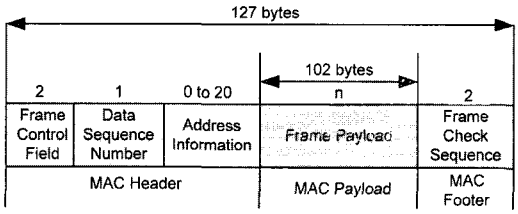
II. 6LoWPAN 소개

본 장에서는 6LoWPAN에 대해서 소개하고자 한다. 먼저 LoWPAN의 특징을 살펴보고, IPv6 적용의 이점과 기술의 목표를 살펴본다. 그 다음 6LoWPAN에서 사용하는 패킷 포맷을 살펴보고 마지막으로 IPv6 주소 자동 할당을 위한 기술을 살펴본다.

1. LoWPAN의 특징

LoWPAN은 제한된 전력 하에서의 저비용 무선 통신을 위한 네트워크로서 IEEE 802.15.4 표준을 따른다. LoWPAN의 주요한 특징은 다음과 같다.

1. LoWPAN의 최대 패킷 크기는 127 바이트에 불과하다. (그림 1)에서 보듯 이중 PHY 및 MAC에서 사용하는 부분을 제외하면 약 102 바이트 정도만이 상위 계층에 의해 사용될 수 있다. 또한 링크 계층 보안 정보가 포함되면 사용가능한 크기는 최하 81 바이트까지 줄어들 수 있다. IPv6 패킷의 크기가 40 바이트인 것을 고려해보면 상당히 작은 크기인 것을 알 수 있다.
2. 낮은 대역폭 및 저전력, 저비용의 특징을 가진다. 2.4 GHz 대역에서 약 250 kbps 정도의 대역폭을 가지며, 장치는 주로 센서 또는 스위치 등에 부착되어 낮은 처리 속도 및 적은 메모리를 가질 것이다. 또한 몇몇 장치는 배터리 모드로 동작할 수도 있다. 이 경우 전력 소비를 줄이기 위해 장치가 주기적으로 슬립 모드에 들어감에 따라 통신이 불가능한 시간이 발생할 수 있다.



〈그림 1〉 IEEE 802.15.4 MAC 프레임 포맷

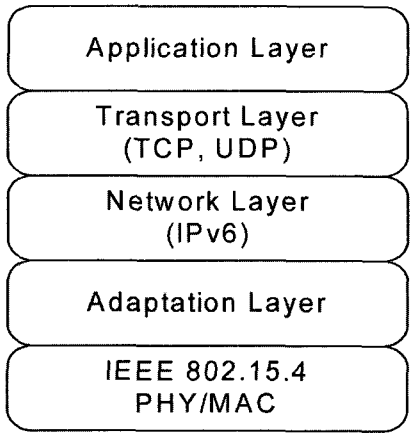
3. 16비트의 짧은 주소와 IEEE 64비트 주소를 둘 다 지원한다.
4. 토폴로지는 스타, 클러스터-트리 그리고 메시 형태를 구성할 수 있다.
5. 저가격, 소형의 특징을 감안할 때 LoWPAN에서는 PC나 기존의 무선 네트워크에 비해 많은 수의 장치들이 배치될 가능성을 고려해야한다.
6. 장치는 배터리의 소모, 물리적 훼손, 무선 환경의 불안정 등으로 신뢰성이 떨어질 수 있다.

2. IPv6 적용의 이점

LoWPAN에 IPv6 기술을 적용하여 얻을 수 있는 이점은 다음과 같다.

1. 이미 기존에 구축된 IP 인프라를 사용 가능하다.
2. IP 기반 기술은 이미 존재하며, 널리 알려져 있고 이미 충분히 검증되어 있다.
3. LoWPAN은 많은 수의 장치들이 배치될 가능성이 높으며 따라서 자동 설정 및 비상태 유지 기술이 요구된다. 그리고 IPv6는 이미 해결책을 가지고 있다.
4. IPv6는 많은 수의 장치가 필요로 하는 충분한 주소공간을 제공할 수 있다.

5. IP 네트워크 기술들은 지적 재산권(IPR)의 측면에서 다른 기술들에 비해 쉽게 접근이 가능하며 선호도가 높다.
6. IP 네트워크에는 이미 진단(Diagnostics), 관리(Management) 등을 위한 툴이 만들어져 있다.
7. IP 기반 장치들은 변환 게이트웨이 또는 프록시 없이 쉽게 다른 IP 기반 네트워크에 연결 가능하다.



〈그림 2〉 6LoWPAN 적응 계층

3. 기술의 목표

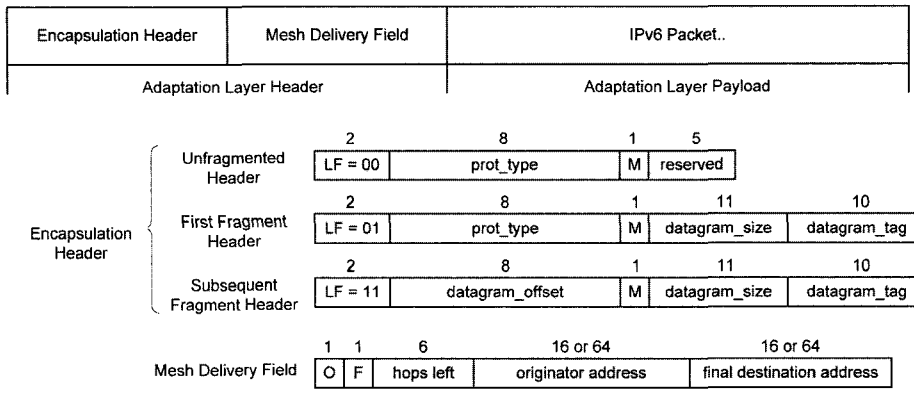
본 절에서는 6LoWPAN이 달성하고자 하는 기술적 목표를 살펴본다. 2.1 절에서 명시한 바와 같이 LoWPAN에서 사용가능한 패킷 크기는 약 81 바이트에 불과하다. 이에 반해 IPv6의 MTU(Maximum Transmission Unit)은 1280 바이트이다. 따라서 (그림2)와 같이 IP 계층과 MAC 계층 사이에 적응 계층(Adaptation Layer)를 두어 패킷의 단편(fragmentation)과 재조합(reassembly)을 수행하도록 한다.

IPv6 기본 헤더가 40 바이트, UDP 헤더가 8바이트, TCP 헤더가 20바이트 크기를 가지므로 이를 그대로 사용한다면 TCP 패킷은 21 바이트만을, UDP 패킷은 33 바이트만을 데이터로 전송 가능하다. 더욱이 적응 계층에서 점유하게 되는 헤더 크기를 고려하면 전송 가능한 데이터는 더 적어지게 된다. 따라서 헤더 압축(compression)을 통해 헤더의 크기를 줄여 더 많은 응용 데이터 공간을 확보하는 것 역시 6LoWPAN 기술의 중요한 목표중 하나이다.

많은 수의 장치들의 설정에 따른 오버헤드를 줄이기 위해서는 IPv6의 주소 자동 설정 기능을 지원해야 한다. 이를 위해 IEEE 64비트 주소로부터 IPv6 인터페이스 아이디를 만들어내는 방법이 필요하다.

LoWPAN의 토폴로지를 메시 형태로 구성하기 위한 라우팅 프로토콜이 필요하다. 기존의 MANET 워킹그룹의 라우팅 프로토콜(AODV[3], DYMO[4] 등)도 사용될 수 있으며, 또는 새로운 라우팅 프로토콜 네트워크를 구성할 수도 있다. 어떤 경우에도 라우팅 컨트롤 패킷은 단편 없이 IEEE 802.15.4 프레임에 들어갈 수 있어야 한다.

IPv6를 LoWPAN 상에서 동작하도록 하는 노력에서 중요한 점은 기존의 프로토콜을 재사용할 수 있도록 해야 한다는 점이다. 그 좋은 예로는 SNMP[5]를 들 수 있다. SNMP 기반의 LoWPAN 관리는 매우 유용한 기술이 될 것이다. 그러나 헤더 압축을 고려하더라도 너무 무거운 응용 계층 프로토콜은 절충될 필요가 있다. 그러한 것들의 예로는 XML 기반의 SOAP[6]를 들 수 있다.



〈그림 3〉 6LoWPAN 패킷 포맷

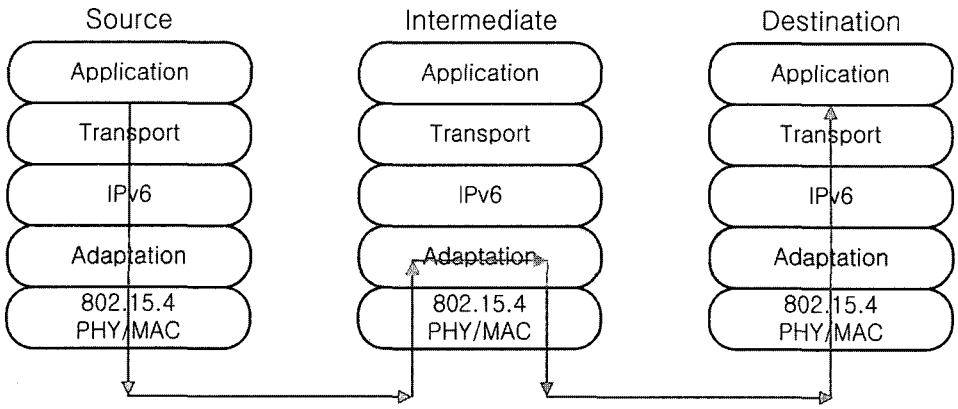
4. 패킷 포맷

본 절에서는 6LoWPAN에서 사용하는 패킷 포맷을 살펴본다. 적응 계층의 헤더는 MAC 헤더 다음에 위치하며 캡슐화(Encapsulation) 헤더와 메시 전달(Mesh Delivery) 필드(캡슐화 헤더의 M 비트가 1로 설정되어 있을 경우에만 사용된다)로 구성된다. 적응 계층의 헤더 부분이 끝나면 IPv6 패킷이 시작된다. (그림3)은 적응 계층 포맷 구조를 보이고 있다.

캡슐화 헤더는 LF(Link Fragment) 필드를 통해 패킷의 단편 유무를 알려준다. prot_type 필드는 적응 계층의 페이로드(payload)가 IPv6 또는 IPv6 헤더의 압축 정보 데이터인지를 알리는 역할을 한다. datagram_tag, datagram_size 그리고 datagram_offset 필드는 패킷 단편에 대한 정보를 담는다. 토폴로지가 메시 형태일 경우 메시 전달 필드가 사용된다. 목적지 노드가 2홉 이상 떨어져 있을 수 있으므로 라우팅이 필요하며, 이를 위해 최종 목적지 주소(Final Destination Address)와 출발지 주소(Originator Address)가 필요하다. 또한 hops left 필드를 통해 최종 목적지까지 도달하는 데에 걸리는 홉 수를 제한하게 된다. hops left 필드는 6비트 크기이므로 6LoWPAN의 최대 직경(Diameter)은 63 홉으로 제한되게 될 것이다. 메시 전달 필드의 O와 F 필드는 각각 출발지와 최종목적지 주소가 16 비트 주소를 사용하는지 또는 64비트 주소를 사용하는지를 나타낸다.

5. IPv6 자동 주소 할당

3절에서 언급한 바와 같이 IPv6 자동 주소 할당 기능은 6LoWPAN에 요구되는 지원 사항에 해당한다. IPv6 주소의 64비트 인터페이스 아이디(Interface Identifier 또는 IID)는 "IPv6 over Ethernet"[RFC 2464]에 정의된 방식대로 장치의 EUI-64 식별자로부터 구할 수 있다. 또한 장치가 16비트 주소를 부여받았을 경우에는 16비트 주소와 16비트 PAN ID를 16비트길이의 '0'과 조합하여 48비트 링크 주소를 생성한 뒤 RFC 2464에 명시된 방법에 따라 IID를 구하는 것도 가능하다.



〈그림 4〉 Sub-IP 라우팅

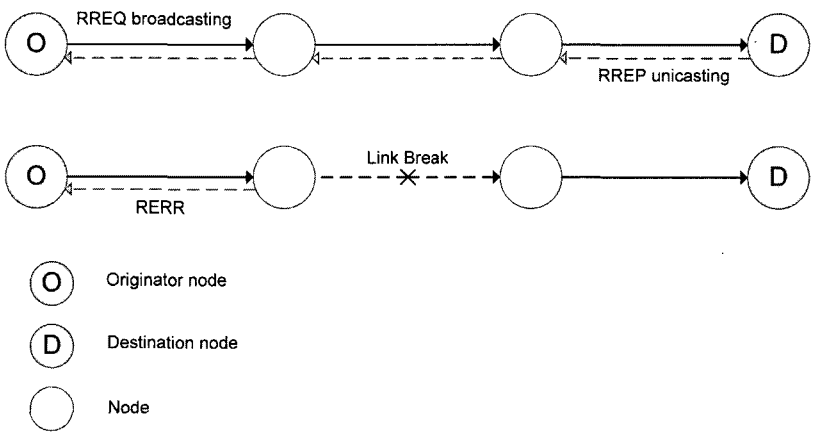
III. 6LoWPAN 라우팅 프로토콜 기술

1. 요구 사항

6LoWPAN에서의 라우팅 프로토콜은 기존 MANET의 그것과 비교하여 아래와 같은 추가적인 요구 사항을 가지게 된다.

1. MANET의 라우팅 프로토콜은 IP 라우팅을 수행하는 반면, 6LoWPAN의 그것은 Sub-IP 라우팅을 수행해야 한다. 즉, 6LoWPAN에서의 라우팅은 IP 계층이 아니고 그 밑의 적응 계층에서 수행된다. 적응 계층에서 라우팅이 수행되면 IP 헤더 압축을 효율적으로 수행가능하며 EUI-64 주소 또는 16비트 주소를 사용함으로서 라우팅 테이블의 크기가 줄어든다.
2. 6LoWPAN의 네트워크 특성을 활용 가능해야 한다. 예를 들어 IEEE 802.15.4 물리 계층에서 제공하는 LQI(Link Quality Indicator)와 같은 값을 활용하면 보다 효율적인 라우팅을 제공할 수 있다. 또한 적은 대역폭을 감안하여 컨트롤 메시지의 크기 및 횟수가 줄어들어야 한다.
3. 전력 소비 및 알고리즘 복잡도를 최소화해야 한다. 6LoWPAN의 장치들이 저가, 소형이며 배터리를 사용할 수 있음을 감안하여 라우팅 프로토콜은 전력 소비 및 알고리즘 수행의 복잡도를 최소화해야한다.
4. 기존에 존재하는 프로토콜(AODV, DYMO 등)들을 가능한 재사용해야 한다. 이미 MANET 워킹 그룹을 통해 연구 및 검증이 된 프로토콜들을 적용함으로서 신뢰성 및 성능의 이점을 가져오도록 해야 한다.

본 장에서는 위와 같은 요구사항을 고려하여 개발된 6LoWPAN 라우팅 프로토콜들을 제시하고자 한다. 라우팅 프로토콜의 명칭은 "6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD)"(이하 LOAD)[7]이며 MANET의 AODV 프로토콜을 6LoWPAN의 특성에 맞춰 간략화하고 최적화시킨 프로토콜이다.



〈그림 5〉 LOAD 기본 동작

2. 기본 동작

(그림 5)는 LOAD의 기본 동작을 나타낸다. 출발지 노드가 아직 경로가 형성되지 않은 목적지 노드로의 경로를 형성하고자 하면 RREQ (Route Request) 패킷을 브로드캐스트로 전송하게 된다. 중간 노드가 RREQ 패킷을 받게 되면 자신의 경로 발견 테이블(Route Discovery Table)에 이미 받고 등록한 RREQ 패킷인지를 확인하게 된다. 만약 이미 받은 RREQ 패킷이라면 버리고 그렇지 않다면 경로 발견 테이블에 기록한 후 RREQ를 브로드캐스트로 재전송하게 된다. 목적지 노드가 RREQ 패킷을 받게 되면 경로 발견 테이블을 검사하여 이미 받은 패킷인지를 확인한다. 이미 받은 RREQ 패킷이 있을 경우에는 기존의 RREQ 패킷에 기록된 경로 비용(cost)과 비교하여 새롭게 도착한 RREQ 패킷이 더 낮은 경로 비용을 가질 경우 RREP 패킷으로 응답하게 된다. 이때 RREP(Route Reply) 패킷은 RREQ 패킷의 출발지 노드를 목적지 노드로 하여 유니캐스트로 전송된다. 중간 노드들은 RREP 패킷을 받으면 경로 비용을 추가하고 재전송하게 된다. 출발지 노드에 RREP 패킷이 도착하게 되면 기존에 받았던 RREP 패킷의 경로 비용과 비교하여 새롭게 도착한 RREP 패킷의 경로 비용이 적을 경우 해당 RREP 패킷이 거쳐온 경로를 경로로 라우팅 테이블에 기록하게 된다. 전송 과정에서 에러가 발생할 경우에는 먼저 링크 에러를 감지한 중간 노드가 지역 경로 복구(Local Repair)를 시도한다. 중간 노드로부터의 지역 경로 복구 시도가 실패했을 경우에는 중간 노드는 출발지 노드에게 RERR(Route Error) 패킷을 전송하여 더 이상 경로가 사용될 수 없음을 알린다.

3. AODV와의 비교

LOAD는 AODV 프로토콜과 유사한 기본 동작을 보이지만 세부적으로는 여러 차이점이 있다. 이는 주로 6LoWPAN 환경에 맞도록 변화된 부분들이다. LOAD와 AODV와의 차이점은 다음과 같다.

1. LOAD에서 중간 노드들은 RREQ 패킷에

대해 RREP로 응답하지 않으며 따라서 "Gratuitous RREP" 기법은 사용되지 않는다. 이를 통해 프로토콜의 복잡도를 줄였다.

2. AODV는 IP 주소를 사용하여 라우팅 하는 것과 달리 LOAD는 EUI-64 또는 16비트 주소를 라우팅에 사용한다. 따라서 LOAD 컨트롤 메시지를 UDP 포트 번호 대신 적응계층 헤더의 prot_type 필드의 값을 통해 구분된다.
3. LOAD는 경로 비용으로 PHY 계층으로부터 제공되는 LQI 값을 활용한다. 하지만 컨트롤 패킷 내에는 경로 비용 정책을 선택하는 필드가 있으므로 다른 경로 비용(홉 카운트 등)을 적용하는 것도 가능하다.
4. AODV에서 사용하는 Hello 메시지는 LOAD에서 사용되지 않는다. 컨트롤 메시지의 증가로 인한 트래픽, 배터리 소모를 줄이기 위함이며, 대신 IEEE 802.15.4에서 제공하는 ACKs, 비컨(beacon) 응답, 패킷 엿듣기(over-hearing) 등의 방법을 통해 대체한다.
5. LOAD에서는 메모리의 소모를 고려하여 Precursor list를 유지하지 않는다.
6. LOAD의 RREQ, RREP, RERR 패킷은 AODV의 패킷에 비해 크기가 작다.
7. LOAD는 RERR 패킷에 에러 코드를 추가하여 오류 상황 분별 능력을 향상시켰다.

4. 경로 비용 계산

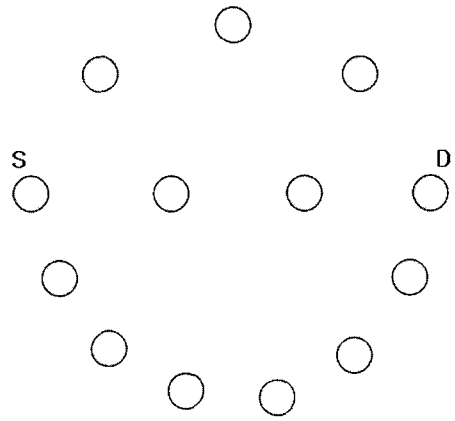
AODV의 경우에는 기본 라우팅 경로 비용 계산 방식으로 최소 홉 카운트 방식을 채택하고 있다. 이 방식은 경로 중 최소의 홉 카운트를 가진 경로를 선택하는 방식으로서, 홉 카운트가 많아질수록 링크 에러의 확률이 높아지며 패킷 전달율이 높아진다는 점에 기인한다.

LOAD의 경우 최소 홉 카운트 방식과 LQI를 조합하여 사용한다. LQI는 IEEE 802.15.4로부터 제공되는 값으로서 링크의 품질을 8비트 범위(0~255)의 값으로 나타낸다. LQI는 일반적으로 링크의 패킷 전달율에 영향을 미치지 않으며 특정 임계값 이하로 LQI가 낮아질 경우에 한해 패킷의 전달율이 급격히 떨어지는 특성을 가진다. 따라서 LOAD는 LQI를 이진 함수(Binary Function)의 형태로 표현하여 사용한다. 그 형태는 다음과 같다.

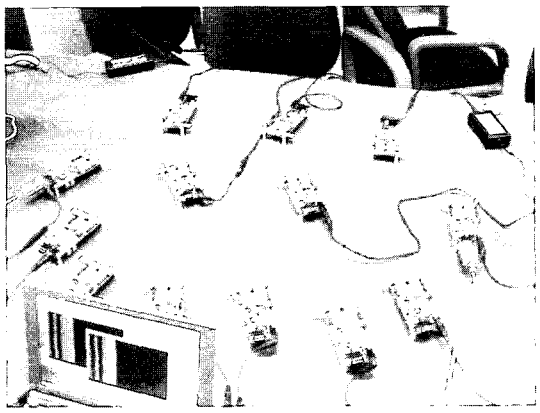
▷ 취약한 링크(Weak Link) : LQI가 임계값(LQIth)에 미달하는 링크
▷ 건전한 링크(Healthy Link) : LQI가 임계값을 초과하는 링크

위와 같은 이진 구분법을 통해 경로 비용 계산의 복잡도가 지나치게 늘어나는 것을 방지하면서도 홉 카운트만을 이용할 때보다 효율적인 라우팅 능력을 가질 수 있다.

홉 카운트와 LQI의 이진 함수 값을 조합하기 위해서는 사전적 비용 계산 방식(Lexical Routing Metric)을 적용한다. 즉, 경로 중 취약한 링크(WL)의 수와 홉 카운트(HC)를 (WL, HC)의 쌍으로 묶은 다음, 왼쪽부터 사전식으로 비교하여 경로의 우열을 판단하게 된다. 예를 들어 A 경로의 취약한 링크의 수가 3, 홉 카운트가 5이며 B 경로의 취약한 링크의 수가 2, 홉 카운트가 6이라고 가정하면, B 경로가 A 경로에 비해 적은 취약한 링크를 가지므로 적은 경로 비용을 가진다고 판단하게 된다.



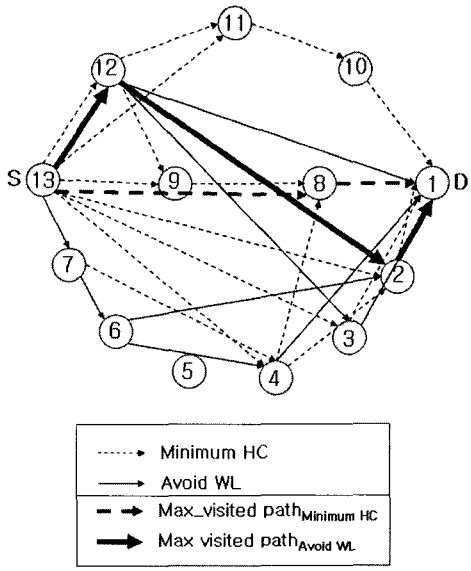
〈그림 6〉 테스트베드 토폴로지



〈그림 7〉 테스트베드 사진

Ⅳ. 테스트베드

본 장에서는 LOAD 프로토콜을 위한 테스트베드를 살펴보고자 한다. 테스트베드를 구축하기 위해 13개의 자체 개발된 6LoWPAN 스택을 다운로드된 Chipcon CC2420DB 보드를 사용하였다. 실내에 테스트베드를 구축하기 위해서 장치들의 전파 출력 세기는 -20DBm으로 설정되었으며 약 200cm² 평방의 지역에 (그림 6)과 같은 토폴로지의 6LoWPAN 네트워크를 구성하였다. (그림 6)에서 S로 명시된 장치가 출발지 노드이며, D로 명시된 장치가 목적지 노드이다.



〈그림 8〉 테스트베드 실험 결과

실험은 최소 홉 카운트 방식(Minimum HC)과 LOAD의 경로 비용 계산 방식(Avoid WL)에 대해 각각 진행하였다. 출발지 노드로부터 목적지 노드에게 40~220ms 간격으로 적응 계층 페이로드 기준 50바이트 패킷을 1000회 전송하여 형성된 경로 및 패킷 전달율을 기록하였으며 각 경로 비용 계산 방식 마다 80회씩 실험을 반복하였다. (그림 7)은 실험에서 형성된 경로의 경향을 보이고 있다.

Ⅴ. 결 론

본 고에서는 IPv6기반 센서 네트워크(6LoWPAN)를 위한 라우팅 프로토콜 기술을 살펴보았다. 이를 위해 먼저 6LoWPAN 기술에 대한 소개 및 주요 기술에 대한 정리를 하였고, 6LoWPAN에서 라우팅 프로토콜을 위해 고려해야할 사항들에 대해서 살펴보았다. 이어서 기존

의 MANET의 AODV를 변형하여 6LoWPAN 환경에 적합하도록 작성된 라우팅 프로토콜에 대해서 살펴보고, 이를 실제 구현하여 테스트베드를 통해 테스트하는 과정 또한 살펴보았다. 6LoWPAN의 라우팅 프로토콜은 MANET 라우팅 프로토콜과 비교하여 저전력, 적은 패킷 크기 등 실제로 고려해야할 사항들이 적지 않으며 따라서 센서 네트워크 분야의 새로운 연구 과제로서 조명되기를 기대한다.

참고문헌

[1] IEEE Computer Society, "IEEE Std. 802.15.4-2003", October 2003.

[2] ZigBee Alliance, "ZigBee Specification 1.0", http://www.zigbee.org/en/spec_download/download_request.asp, December 2004.

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing", RFC 3561, Jul, 2003.

[4] I. Chakeres, E. Belding-Royer, and C. Perkins, "Dynamic MANET On-demand(DYMO) Routing", draft-ietf-manet-dymo-03.txt, Oct, 2005.

[5] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol(SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[8] W3C XML Protocol Working Group, "SOAP Version 1.2", http://www.w3.org/TR/soap/

[7] K. Kim, S. Daniel Park, G. Montenegro, S. Yoo, and N. Kushalnagar, "6LoWPAN Ad Hoc On-Demand Distance Vector Routing(LOAD)", draft-daniel-6lowpan-load-adhoc-routing-02.txt, March, 2006.

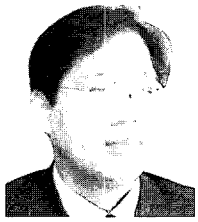
저자소개

임 채 성

2005년 아주대학교 정보컴퓨터 공학부 졸업(공학사)
2006년 아주대학교 정보통신 전문대학원 석사과정
주관심분야 6LoWPAN, 센서네트워크, IPv6

Waleed Mansoor

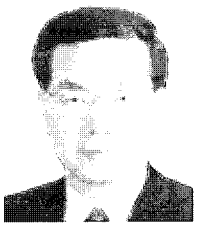
2004년 NUST 졸업 (공학사)
2005년 – 현 재 아주대학교 정보통신 전문대학원 석사과정
주관심분야 6LoWPAN, 센서네트워크, IPv6



김 기 형

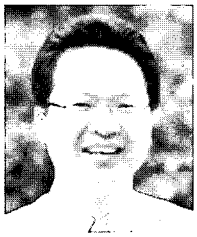
1990년 한양대학교 졸업(공학사)
1992년 한국과학기술원 졸업(공학석사)
1996년 한국과학기술원 졸업(공학박사)
1997년 – 2005년 영남대학교 정보통신공학부 교수
2005년 – 현 재 아주대학교 정보및컴퓨터공학부 교수
주관심분야 6LoWPAN, 센서네트워크, IPv6, 임베디드시스템

저자소개



유 승 화

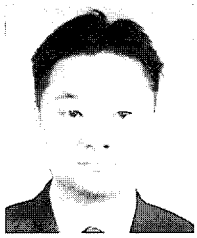
1972년 서울대학교 졸업(이학사)
1980년 University of Kansas 졸업(공학석사)
1983년 University of Kansas 졸업(공학박사)
1983년-1988년 AT Bell 연구소(미) 연구원
1988년-1989년 Amdahl Corporation(미) 수석 연구원
1989년-1999년 삼성전자(주) 전무이사
1999년-현 재 아주대학교 정보컴퓨터 공학부 교수
주관심분야 6LoWPAN, 센서네트워크, RFID, 홈네트워크, 무선인터넷



박 수 홍

1999년 단국대학교 전자공학과
1999년-2002년 OPICOM IPv6기술개발총괄
2004년-2005년 IPv6포럼코리아 Convergence WG 의장
2005년-2006년 무선인터넷포럼 IETF Mobility WG 의장
2002년-현 재 삼성전자 디지털미디어연구소 선임연구원
2005년-현 재 IETF 16ng Working Group 의장
주관심분야 Internet Protoco, Mobility, Wireless Communication

저자소개



이 재 호

1995년 성균관대학교 정보공학과(학사)
1997년 성균관대학교 정보공학과(석사)
2006년 연세대학교 전기전자공학과(박사수료)
1997년-현 재 한국전산원 차세대인터넷팀 책임연구원
주관심분야 IPv6, USN, BcN, Mobile IP

용어해설

Outbound Content Compliance

Outbound Content Compliance, OCC [정보보호]

이메일, IM, P2P, FTP, 웹포스팅 그리고 이외의 메시징 트래픽에 포함되어 내부로부터 유출되는 콘텐츠를 감시하고, 암호화, 필터링 및 차단 기능을 제공하는 솔루션.

OCC는 IDC에서 정의한 기밀정보 유출방지 솔루션으로 공공기관과 산업체의 내부 규정(HIPAA, GLBA, SOX 등) 위반, 조직 내부의 이메일 정책이나 관행에 위반, 지적재산권 유출, 기밀정보 유출, 성인 콘텐츠 유포 등에 대한 방어 기능을 포함한다.

OCC는 크게 이메일 필터링, secure email, 멀티프로토콜 콘텐츠 필터링, 인스턴트 메시징 보안, 전사적 위험 관리(ERM) 등으로 나눌 수 있다. 특히, 멀티프로토콜 콘텐츠 필터링은 기존의 전통적인 이메일 보안을 넘어서 다양한 프로토콜을 통하여 전달되는 메시징 트래픽을 모니터링하여 조직내부의 중요 정보유출을 차단한다.