

## Mobile Ad-hoc 네트워크 기술 동향

심재화\*, 이훈재<sup>o</sup>

\*<sup>o</sup>동서대학교 정보통신공학과

e-mail: abyss1110@gmail.com\*, hjlee@dongseo.ac.kr<sup>o</sup>

## Technical Trends in Mobile Ad-hoc Networks

JaeHwa Sim\*, HoonJae Lee<sup>o</sup>

\*<sup>o</sup>Dept. of Information and Communication Engineering, Dongseo University

### ● 요약 ●

최근 고정된 네트워크가 아닌 센싱 노드를 기반으로 한 유비쿼터스 센서 네트워크의 관심이 높아지고 있는 추세이다. 센서 네트워크에서는 넓은 지역의 정보 수집이나 망 기반시설이 갖추어 지지 않은 곳의 정보 수집 및 가공과 통신을 위하여 배터리로 구동되는 센싱 노드를 사용한다. 배터리로 구동되는 센싱노드는 통신을 위해 저전력을 사용하기 때문에 근거리 통신만 가능하다. 이러한 거리 제약을 극복하기 위해 멀티 홉 릴레이 기능을 이용한 이동 Ad-hoc 네트워크가 많이 사용된다. 본 논문에서는 이동 Ad-hoc 네트워크에서 운용되어지는 프로토콜과, 기존 망과의 연동을 위해 쓰이고 있는 기술에 대해 알아보고, 이동 Ad-hoc 네트워크상에서의 보안 기술을 고찰 하고자 한다.

키워드: MANET, Ad-hoc Network trend

### I. 서론

최근 스마트폰(smart phone)의 등장과 함께 유비쿼터스 센서 네트워크(USN, Ubiquitous Sensor Network)에 대한 관심이 높아지고 있다. 센서 네트워크에 사용하는 센싱 엔진은 광범위한 환경 모니터링이나 고정된 인프라가 없어 망 구성이 어려운 곳에서 많이 사용되어진다. 이 같은 환경에서 발생할 수 있는 통신 거리 제약을 극복하기 위하여 센싱 엔진 간 이동 Ad-hoc 네트워크(MANET, Mobile Ad-hoc Network)의 멀티홉 릴레이가 구현되고 있다[1].

고정된 기반 네트워크가없는 열악한 환경에서도 MANET은 배터리로 운영되는 이동노드들 간에 무선 인터페이스를 통하여 자율적인 네트워크를 가능하게 만들었으며 이는 순간적인 네트워크 인프라 구축을 가능하게 만들었다.

MANET의 핵심적인 구성 요소는 이동노드이다. MANET의 이동노드는 무선 인터페이스를 사용하여 이동 호스트 컴퓨팅 기능과 라우팅 기능을 동시에 갖는다. 이에 기지국(BS, Base Station)이나 액세스포인트(AP, Access Point)와 같은 중재자(centralized coordinator)가 없이도 즉흥적으로 망 구성이 가능하다.

이동노드를 통한 망 구성을 하는 MANET은 동적 네트워크 특성을 갖는다. 이동노드간의 연결성, 전파 상태, 트래픽 및 사용자의 이동패턴에 따라 네트워크 토폴로지가 끊임없이 변화 하므로 네트워크의 구성유지가 어렵고 제반 기술의 적용이 용이치 않다. 또한 사용자의 이동패턴, 트래픽 종류, 또는 배터리를 사용하는 이동 노드의 에너지 잔량 등에 따라 노드의 일부 또는 전체가 가변

적으로 네트워크에 나타나거나 사라진다.

따라서 이동 Ad-hoc 네트워크 기술은 하위 계층의 전파 전파, 전파 간섭 및 전력 제어에서부터 링크계층의 다중 접속 및 자원 할당, 네트워크 계층의 라우팅, 트랜스포트 계층의 연결 설정 및 유지, 그리고 보안 및 상위 계층 애플리케이션에 이르기까지 다양한 기술적 해결 요구사항을 갖는다. 또한 기존의 인터넷이나 이동 통신망 또는 무선 랜과의 상호 연동을 위한 IP 이동성이나 주소 관리, 망 관리 기술들도 앞으로 해결해야 할 문제들이다[2].

이에 본 논문에서는 이동 Ad-hoc 네트워크 구성 프로토콜 [3][4][6] 및 기존 네트워크 연동 기술, 그리고 무선 네트워크로서의 Ad-hoc 네트워크의 보안 관련 기술 동향에 대하여 알아보하고자 한다.

### II. 이동 Ad-hoc 네트워크 기술 동향

#### 1. 이동 Ad-hoc 라우팅 프로토콜

이동 Ad-hoc 네트워크는 이동노드의 이동 패턴과 트래픽 종류, 링크 품질 또는 전력 여유 등에 따라 토폴로지가 수시로 변하므로 특정 노드로 찾아가기 위한 경로의 설정과 유지가 어렵다. 노드들의 이동 패턴에 따라 직접적인 통신이 가능한 이웃 노드들의 집합 또는 그룹이 함께 변하므로 각 노드는 주기적으로 자신의 존재를 broadcasting하여 직접적인 통신이 가능한 이웃 노드 또는 그룹의 정보를 항상 유지 한다.

이를 위한 이동 Ad-hoc 라우팅 프로토콜은 테이블 관리 (Table-driven 또는 proactive) 방식과 요구기반 (On-demand 또는 Reactive) 방식으로 나뉜다.

### 1.1 테이블 관리 방식

테이블 관리 라우팅 방식은 모든 이동 노드들이 항상 최신의 루트 정보를 유지하며, 라우팅 정보를 주기적으로 또는 네트워크 토폴로지 상의 변경이 있을 때마다 네트워크 전체로 전파시켜 각 노드들이 자신의 라우팅 정보를 변경한다. 테이블 관리 방식 라우팅 프로토콜은 망 변동이 있을 때마다 업데이트 하여 패킷 발생 시 지연 없이 항상 최신의 루트를 통해 라우팅 할 수 있는 장점이 있지만, 망 변동이 심할 경우 라우팅 테이블을 갱신하기 위한 오버헤드가 커서 배터리 운용에 어려움이 있다는 문제점이 있다. 테이블 방식의 라우팅 프로토콜로는 OLSR(Optimized Link State Routing), DSDV(Destination Sequenced Distance Vector), WRP(Wireless Routing Protocol), 그리고 CGSR(Clusterhead Gateway Switching Routing)이 있다.

### 1.2 요구 기반 방식

요구 기반 방식은 트래픽이 발생하는 시점에서 루트를 탐색하는 방법으로서 프로액티브 라우팅 방식의 단점인 제어 메시지의 오버헤드를 감소시킬 수 있다. 또한, 루트 정보는 루트 상의 각 노드에 저장되는 일정 기간 동안 해당 루트가 사용되지 않을 경우 노트로부터 삭제된다. 요구 기반 방식은 트래픽이 발생하는 시점에서 루트를 탐색하기 때문에 루트 탐색에 추가적인 시간이 필요하며, 이는 트래픽 전송 지연을 야기하는 단점이 있다. 요구 기반 방식 프로토콜에는 AODV(Adhoc On-demand Distance Vector), DSR(Dynamic Source Routing) 등이 있다.

## 2. 기존 네트워크와의 연동

이동 Ad-hoc 네트워크의 구성은 독자적이면서 유동적이다. 이동노드에 의존하는 이동 Ad-hoc 네트워크는 인터넷 서비스가 요구되거나 재난 구조 및 센서네트워크로 운용 될 때에는, 센싱 노드를 통해 얻어진 데이터나 멀티 홉에 의해 전달된 데이터를 기존 유무선 네트워크에 연결해 전송할 필요가 있다. 따라서 Ad-hoc 네트워크와 기존의 인터넷, 무선 LAN 또는 이동 데이터 통신 네트워크와의 상호연동에 관한 연구는 매우 중요하며, 현재 다양한 연구가 진행 중이다[2].

### 1.1 인터넷 또는 무선 랜과의 연동

인터넷과의 연동은 이동 Ad-hoc 네트워크와 인터넷의 경계면에서 Ad-hoc 라우팅 프로토콜과 Ad-hoc 게이트웨이를 두어 구현하며, 이때 Ad-hoc 게이트웨이는 인터넷 라우터와 연결되도록 구성한다. Ad-hoc 게이트웨이와 이동 Ad-hoc 노드간의 인터페이스는 Ad-hoc 네트워크와 동일한 무선 인터페이스를 가지며, Ad-hoc 게이트웨이와 유선 인터넷 라우터간의 인터페이스는 인터넷 인터페이스를 따른다.

### 1.2 이동통신 네트워크와의 연동

Ad-hoc 네트워크 개념을 이동통신 셀룰러 망에 적용하고자 하

는 연구가 다수 진행되어 오고 있으며 그 중에 대표적인 것으로 iCAR와 A-GSM, Multihop Cellular Network(MCN)이 있다. iCAR(an integrated Cellular and Ad-hoc Relay)는 밀집지역(hot spot)의 셀의 과부하를 로드 밸런싱으로 풀기 위해 ARS(Ad-hoc Relay Station)라는 제 3의 중계 노드(relay node)를 사용하고 있다. ARS는 네트워크 사업자에 의해 필요한 곳에 놓여 기지국과 단말 사이의 통신을 중계하는 역할을 하게 된다. MCN은 배타적으로 멀리 떨어져 있는 기지국에 접속하기 위하여 브리징 프로토콜(bridging protocol)을 추가한 이동 단말기를 통해 다중 홉 통신을 함으로써 기지국의 수와 단말 또는 기지국의 송신 범위를 줄이고자 한다.

### 1.3 IP 이동성

이동 Ad-hoc 네트워크가 기존의 IP 기반에서 동작하는 경우 IP 이동성 문제가 발생한다. 특히, 이동노드가 움직여서 다른 지역으로 이동하였을 때, 통신이 불가능해지므로 새로운 위치에서 IP 주소를 새로 획득하거나 사용자가 새로 설정해 주어야 한다. 이러한 IP 이동성 문제를 해결하기 위하여 IETF에서 제안된 것이 이동 IP이다. 이동 IP는 서브넷이 달라지는 다른 위치에서도 자신의 고유 IP 주소를 가지고 서비스를 지속하기 위하여 변경된 위치에서의 IP 주소 식별과 해당 접속점으로서의 라우팅을 위한 메커니즘을 가진다.

그러나 기존의 이동 IP 규격은 이동 노드와 외부 에이전트(Foreign Agent)가 직접적인 연결을 갖는 싱글 홉 통신을 전제로 하므로 이동 Ad-hoc 네트워크에서의 다중 홉 통신에 그대로 적용하기가 어렵다. 이에 대한 대표적인 연구로는 MIPMANET이나 Mobile IP/AODV 등이 있다. Mobile IP/AODV는 에이전트 발견 절차와 등록 절차와 같은 기존의 이동 IP 절차를 수행하면서 요구 기반 방식의 Ad-hoc 라우팅 프로토콜에 의한 다중 홉 라우팅을 수행한다.

## 3. Ad-hoc 네트워크에서의 보안 기술

Ad-hoc 네트워크의 인증 기술로는 중앙 서버의 역할을 수행하는 신뢰 기관이나 베이스 스테이션을 이용하는 방식과, 아이디를 이용하는 방식이 많이 사용된다. 데이터 안전성은 타원 곡선을 이용한 공개키와 세션키 분배를 통해서 암호화 하는 방식의 연구가 진행되고 있다.

### 3.1 인증 기술

이동 Ad-hoc 네트워크는 임의 디바이스 접근으로 이루어지기 때문에 아이디와 패스워드 방식을 적용하기에는 어려운 특징을 지니고 있다. 그러므로 Ad-hoc 네트워크 구성에 신뢰기관이나 베이스 스테이션을 할 수 있는 모바일 디바이스를 정해서 인증을 제공하는 방식을 활용한다.

#### 3.1.1 신뢰기관 및 베이스 스테이션

통신에 참여하는 모바일 디바이스는 신뢰 기관 및 베이스 스테이션의 정보를 제공하여 공인인증서를 발급 받거나 인증 정보를 다른 모바일 디바이스에 제공하여 통신에 참여한 디바이스에 세션

키를 분배한다. 그러나 신뢰 기관이나 베이스 스테이션 모델은 Ad-hoc네트워크를 구성하는 많은 모바일 디바이스 중 신뢰 기관 역할을 수행할 디바이스를 선택하는데 어려움이 있다.

### 3.1.2 공인인증서를 이용한 인증

모바일 디바이스는 공인인증서를 가지고 있으며, 전자 서명을 통해서 인증을 제공하는 방식이다. 이와 같은 방식은 공인 인증서를 신뢰 할 수 있어야 하며, 모바일 디바이스가 공개키 연산이 가능해야하는 단점이 있다. 또한 공인 인증서를 체크하기 위해서 인증서 체인을 통해 상위 기관의 전자 서명을 검증할 수 있는 방안이 필요하게 된다.

### 3.1.3 아이디를 이용한 인증

ID-Password 인증방식은 가장 일반적인 인증 방식 중 하나로, 인증 서버에 ID와 Password를 저장하여, 인증 요청시 저장된 정보를 활용하여 인증을 수행한다. 그러나 Ad-hoc 네트워크에서는 ID와 Password를 저장하여 유지 하는 것이 어려움으로, ID를 이용하여 인증하는 방식을 주로 사용한다. ID를 이용한 인증 방식은 ID를 기반을 두어 세션키를 생성하거나 인증할 수 있는 인자를 생성하는 방식이다.

### 3.2 데이터 보호 기술

이동 Ad hoc 네트워크에서는 빈번한 통신경로의 변경으로 공유키를 이용하는 암호기술은 적용하기 어려움이 있으며, 공개키를 이용하는 경우 각 노드의 인증서를 다시 검증해야 하기 때문에 통신량이 증가하게 된다. 이와 반대로 아이디 기반의 보안 기술은 공유키 및 사전 정보 없이 상대방의 아이디를 이용하여 보안 인자를 생성해 통신을 하므로 안정성을 제공 할 수 있다. 이에 센서 노드의 아이디를 기반으로 하여 세션키나 인증할 수 있는 인자를 만드는 방법을 이용하고 있는 중이다.

Ad-hoc 네트워크에서는 그룹키 방식에 대한 연구도 진행 되어야 한다. Ad-hoc 네트워크를 이룬 모바일 디바이스는 하나의 그룹 안에서는 동일한 그룹 키를 이용하여 통신의 효율성을 높일 수 있다. 그러나 Ad-hoc네트워크 특성을 감안 한다면, 그룹 키의 전 방향성과 후방향성의 안정성을 제공하는 키 관리가 필요하다. 또한 빈번한 키 갱신을 고려한 효율성을 제공할 수 있어야한다.

## III. 결론 및 향후 방향

최근 센서 네트워크의 발달로 이동 Ad-hoc 네트워크에 관한 관심이 부쩍 증가 하였다. 본 논문에서는 보안이나 효율적 라우팅 프로토콜에 대한 기술적인 부분에 있어서 자세히 논의 할 수 없었지만, 최근 이동 Ad-hoc 네트워크의 운용과 네트워크 인증과 데이터 보호기술에 대하여 간략히 내용을 알아보았다.

망 구성이 어려운 지역에서도 통신을 가능 하게 하는 장점을 가지고 있지만, 배터리로 운용되는 센싱 노드는 복잡한 라우팅 프로토콜의 제어 메시지가 증가 할수록 오버헤드가 증가하는 단점을 보였다. 몇몇 다른 논문에서는 효율적인 라우팅 프로토콜과 저전력 문제해결에 관한 기술들을 제시하고 있지만 아직까지는 저전력 센싱노드의 배터리 문제와 효율적 라우팅 프로토콜의 문제를 함께 해결 할 수 있는 방안이 부족해 보이는 실정이다. 이에 센싱 노드의 배터리에 관하여 효율적인 라우팅 프로토콜에 관한 정책 수립이 필요하며 기존 보안 인증 및 키 생성의 개선이 요구된다.

## 참고문헌

- [1] tkcho, and jhlee, "The Study on the OLSR(Optimized Link State Routing Protocol) Implementation in the Mobile Ad-hoc Networks," Journal of KIEE Vol. 60, No. 3, pp. 161-161, Sep 2011.
- [2] Technical Trends on Mobile Ad-hoc Networks, <http://ettrends.etri.re.kr/>
- [3] C. Perkins, Mobile ad hoc networking terminology, Internet Draft, Internet Engineering Task Force, Oct 1997.
- [4] V. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proc. IEEE INFOCOM '97, Kobe, Japan(1997).
- [5] sikang, "A study on Authentication and Key Generation for secure Wireless Communication in Ubiquitous Environment," Dec 2008.
- [6] mskang, dwkum, and yzcho, "Performance Evaluation of AODV and OLSR Routing Protocol According to Node's Mobility Model", Journal of KICS, Vol. 36, No.7, July 2011.