

## Mobile Ad-hoc Network에서 영역기반 보안 멀티캐스트 기법 연구\*

양 환 석\*

### *A Study on Region-based Secure Multicast in Mobile Ad-hoc Network*

Yang Hwanseok

#### 〈Abstract〉

MANET is a network composed only mobile network having limited resources and has dynamic topology characteristics. Therefore, every mobile node acts as a route and delivers data by using multi-hop method. In particular, group communication such as multicast is desperately needed because of characteristics such as battery life of limited wireless bandwidth and mobile nodes. However, the multicast technique can have different efficient of data transmission according to configuring method of a virtual topology by the movement of the nodes and the performance of a multicast can be significantly degraded. In this paper, the region based security multicast technique is proposed in order to increase the efficiency of data transmission by maintaining an optimal path and enhance the security features in data transmission. The group management node that manages the state information of the member nodes after the whole network is separated to area for efficient management of multicast member nodes is used. Member node encrypts using member key for secure data transmission and the security features are strengthened by sending the data after encrypted using group key in group management node. The superiority of the proposed technique in this paper was confirmed through experiments.

Key Words : Multicast, Mobile Ad-hoc Network, Region-based Routing, Data Encryption

### I. 서론

MANET(Mobile Ad-hoc Network)은 어떠한 인프라스트럭처의 도움 없이 무선 단말기로만 자가 구성된 네트워크로서 특수한 상황에서 빠르게 네트워크 구축이 필요할 때 사용되어 왔다. 따라서 네트워크에 참여하는 모든 노드들은 라우터의 역할을 수행해야

하며, 데이터 전달은 다중 홉(multi-hop) 방식으로 이루어진다[1-2]. MANET은 제한된 대역폭과 노드들의 이동으로 인한 동적인 토폴로지, 높은 송수신 오류 비율 등의 특징 때문에 멀티캐스트와 같은 효율적인 그룹 통신 프로토콜이 필요하다. MANET에서의 멀티캐스트는 네트워크 계층의 IP 멀티캐스트와 응용 계층의 오버레이 멀티캐스트로 구분된다[3]. 네트워크 계층의 멀티캐스트는 모든 노드가 멀티캐스팅 서

\* 중부대학교 정보보호학과 조교수

비스를 인식해야하며, 멀티캐스트에 참여하지 않는 노드들에 대해서도 관리를 해야 한다. 또한 노드들의 이동이 빈번하게 발생하면 노드들의 상태를 유지해야 하는 비용이 많이 발생하며 멀티캐스트 효율성이 떨어진다. 오버레이 멀티캐스팅은 가상 멀티캐스트 토폴로지를 만들어 서비스하는 것으로 라우팅 프로토콜에 독립적인 장점을 갖고 있지만 최적의 경로를 이용하여 데이터를 전달하기 어려운 단점을 가지고 있다[4]. 그리고 악의적인 노드들에 의해 데이터 전달을 방해하는 공격이 이루어진다면 멀티캐스트 서비스가 불가능한 상태에 빠질 수 있다. 따라서 효율적인 데이터 전달을 위한 가상 토폴로지 구성과 보안에 대한 연구가 필요한 실정이다.

본 논문에서는 오버레이 멀티캐스트에서 데이터 전달의 효율성을 높이면서 보안 멀티캐스트를 제공하기 위한 기법을 제안하였다. 본 논문에서는 최적의 경로를 설정하기 위해 전체 네트워크를 영역으로 분할한 후 멀티캐스트 멤버 노드들을 관리하기 위해 각 영역에 그룹관리노드를 연결수와 배터리 양을 조합하여 선출하였다. 그리고 그룹관리노드들 중에서 멤버 노드가 가장 많은 그룹관리노드를 인증관리노드로 지정하였으며, 그룹키를 발급하는 역할을 수행한다. 그룹관리노드들이 영역내의 이동하는 멤버 노드들 관리함으로써 데이터 전달시 최적의 전달 경로를 유지할 수 있게 하였다. 그리고 데이터 전송시 멤버 노드는 그룹관리노드로부터 발급받은 멤버키로 암호화한 후 데이터를 전송하고 이를 수신한 그룹관리노드는 그룹키를 이용하여 재암호화한 후 데이터 전송을 수행하기 때문에 악의적인 노드들의 멀티캐스트 참여를 차단시킬 수 있게 하였다. 본 논문에서 제안한 멀티캐스트의 우수한 성능을 실험을 통해 확인할 수 있었다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET에서 그 동안 연구되었던 멀티캐스트 기법에

대하여 살펴보고 3장에서는 본 논문에서 제안한 영역기반 보안 멀티캐스트 기법에 대하여 설명하였다. 4장에서는 모의실험을 통해 제안한 기법의 성능을 확인하고 마지막으로 5장에서는 결론을 맺는다.

## II. 관련연구

### 2.1 네트워크 계층 멀티캐스트

네트워크 계층 멀티캐스트 기법은 멀티캐스트 데이터 전송을 위해서는 네트워크를 구성하는 모든 노드들이 멀티캐스트 서비스를 인식하고 있어야 하며, 멀티캐스트에 참여하지 않는 노드들도 데이터 전달 경로를 구성하는 기법이다. 이 기법은 데이터 포워딩 방식에 따라 트리 기반 방식과 메시 기반 방식으로 분류할 수 있다[5]. 트리 기반 방식으로는 MAODV(Multicast Ad hoc On-Demand Distance Vector), AMRIS(Ad Hoc Multicast Routing Protocol Utilizing Increasing id-numberS) 등이 있다[6-7]. MAODV 기법은 RREQ와 RREP 메시지를 사용하여 멀티캐스트를 위한 트리를 구성한다. 멀티캐스트 그룹에 최초로 조인한 노드가 리더가 되어 주기적인 그룹 HELLO 메시지를 브로드캐스트함으로써 최신의 라우팅 정보를 유지한다. 또한 노드들간의 최단 경로를 멀티캐스트 트리로 생성하기 위하여 여러 노드로부터 MACT (Multicast Activation) 메시지를 이용하게 된다.

메시 기반 방식은 노드들의 이동성을 고려하여 다중 전송 경로를 허용하였으며, ODMRP(On-Demand Multicast Routing Protocol), FGMP(Forwarding Group Multicast Protocol) 등이 있다. ODMRP 프로토콜은 멀티캐스트 그룹에 대한 포워딩 그룹을 라우팅 제어 메시지를 이용하여 결정한다. 포워딩 그룹에

속하지 않는 노드들은 자신이 수신한 멀티캐스트 패킷을 무시하게 된다. 멀티캐스트를 위한 메시지 구성 방법은 멀티캐스트에 조인을 원하는 노드가 자신의 정보를 담은 조인 질의를 방송하고 이를 수신한 노드는 라우팅 테이블에 해당 정보를 저장하고 중복 저장을 방지하기 위해 노드의 주소와 순서번호를 저장한다. 조인 질의를 수신한 노드는 이를 브로드캐스트하며 같은 방법으로 조인 질의를 최초로 브로드캐스트한 노드까지 조인 응답 메시지를 전송하면서 포워딩 노드들이 메시지를 구성하게 된다.

## 2.2 응용 계층 멀티캐스트

응용 계층 멀티캐스트 기법은 오버레이 멀티캐스트라고도 불리우며 네트워크 계층 멀티캐스트 기법의 단점을 보완하기 위하여 제안된 기법이다. 즉, 멀티캐스트 데이터 전송의 효율성을 높이기 위하여 응용 계층에 가상 멀티캐스트 토폴로지를 구성하여 멀티캐스트 서비스를 제공한다. 이는 응용 계층에서 동작하기 때문에 라우팅 프로토콜에 비의존적이며, 상위 수준의 다양한 기능을 추가로 제공할 수 있는 장점이 있다[8]. 응용 계층 멀티캐스트 기법으로는 AMRoute(Ad hoc Multicast Routing Protocol), PAST-DM(Progressively Adapted Sub-Tree in Dynamic Mesh) 등이 있다[9].

AMRoute 기법은 멀티캐스트를 위해 메시지 생성과 트리 생성 두 단계로 구성된다. 먼저 인접한 노드들 간의 양방향 터널을 이용하여 메시지를 생성한다. 이렇게 생성된 메시지 구조는 노드들의 이동으로 인한 토폴로지의 변화에도 영향을 받지 않고 고정된다. 이 메시지를 기반으로 주기적인 멀티캐스트 트리를 생성한다[10].

PAST-DM 기법은 AMRoute 기법에서 고정된 가상의 메시지를 생성하기 때문에 발생하는 비효율성을

피하기 위해 제안된 것으로서 주기적인 가상의 메시지 구성 기법을 제안하였다[11]. 즉, 각 이동 노드는 링크 상태 정보를 주기적으로 송수신함으로써 멀티캐스트 그룹의 모든 노드들에 대한 정보를 수집하고 이를 이용하여 가상의 메시지에 대한 전체 토폴로지 정보를 얻게된다. 이를 기반으로 여러 서브 그룹을 생성하고 각 서브 그룹에서 서브 트리를 생성하여 자식 노드에게 유니캐스트 방식으로 데이터를 전달하게 된다.

## III. 영역기반 보안 멀티캐스트 기법

본 장에서는 네트워크 토폴로지 변화에 큰 영향을 받지 않으면서 낮은 오버헤드와 높은 확장성을 제공하고 보안성을 향상시킨 영역기반 보안 멀티캐스트 기법 RSM(Region-based Secure Multicast)을 제안하였다.

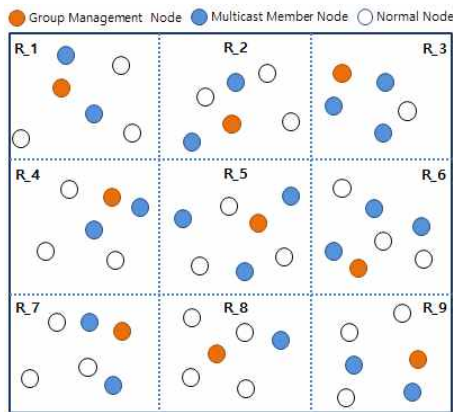
### 3.1 RSM 구조

MANET에서 IP 멀티캐스트 프로토콜은 모든 이동 노드들이 멀티캐스트를 위해서 노드들에 대한 상태 정보를 유지해야 하는 어려움과 높은 오버헤드가 발생하는 문제점이 있다. 그리고 오버레이 멀티캐스트 프로토콜은 네트워크 토폴로지 변화에는 유연하게 대처할 수 있지만 멀티캐스트 그룹에 속해 있는 노드들과의 데이터 전송시 불필요한 전송이 발생할 수 있으며, 주기적인 제어 메시지로 인해 네트워크 성능이 떨어질 수 있다.

RSM(Region-based Secure Multicast) 기법은 멀티캐스트에 참여하는 이동 노드들의 이동성에 큰 영향을 받지 않으면서 안전한 데이터 전송을 제공하기 위해 먼저 전체 네트워크를 3×3개의 영역으로 구분하

였다. 영역의 개수는 노드들의 전송 범위와 전체 네트워크 크기를 고려하여 결정하였다. 전체 네트워크를 구성하는 노드들은 일반 노드, 멤버 노드, 그룹관리노드, 인증관리노드로 구성되어 있다. 일반 노드는 멀티캐스트에 참여하지 않고 MANET을 구성하는 노드들이다. 멤버 노드는 멀티캐스트에 참여하는 노드이고 그룹관리노드는 각 영역 내에 멀티캐스트에 참여하는 멤버 노드들에 대한 상태 정보를 관리하는 노드이다. 마지막으로 인증관리노드는 멀티캐스트에 참여하는 노드들이 데이터 전송을 할 때 사용하는 그룹키를 발급해주고 관리하는 노드로서 그룹관리노드들 중에서 선출된다. 각 영역의 그룹관리노드에 의해 멀티캐스트 멤버 노드들이 관리되기 때문에 노드들의 이동에 큰 영향을 받지 않으면서 불필요한 전달을 줄일 수 있고, 최적의 경로로 데이터를 전달할 수 있게 된다.

<그림 1>는 본 논문에서 사용하는 RSM의 구조를 보여주고 있다.



<그림 1> RSM 네트워크 구조

### 3.2 RSM 그룹 관리

본 논문에서 제안한 기법은 네트워크가 수시로 변

화하는 동적인 특성에 강인함을 제공하고 제어 메시지의 양을 줄임으로써 네트워크 성능을 향상시키기 위하여 멀티캐스트 그룹의 멤버 노드들에 대한 효율적 관리를 영역을 기반으로 한 그룹 관리 기법을 제안하였다.

먼저, 전체 네트워크를 일정 영역으로 분할한 후 각 영역별로 멀티캐스트 그룹에 참여하는 노드들 중에서 링크 수와 배터리 수명 값의 조합이 가장 높은 노드를 그룹관리 노드로 선출한다. 그룹관리노드는 영역내의 멀티캐스트 그룹에 참여하는 멤버 노드들에 대한 정보를 유지하고, 각 멤버 노드들에게 데이터 전송시에 사용할 멤버키를 발급해주는 역할을 담당한다. 이렇게 선출된 그룹관리 노드들은 전체 네트워크에 자신의 존재를 알리기 위해 GroupManager를 방송한다. 그룹관리 노드는 자신의 이웃에 존재하는 그룹관리 노드들에 대한 정보를 이웃그룹관리노드 테이블(Neighbor Group Management Node Table)에 저장하게 된다. 그룹관리 노드들은 주기적으로 자신의 상태 정보를 이웃 그룹관리 노드들에게 방송하게 된다. <그림 2>는 그룹관리 노드의 상태정보 교환 pseudo 코드를 보여주고 있다.

```
while()
{
    for( i=0; i<N ;i++ ) {
        rcv_msg[i] = SendtoStatus(NeighborManager_List);
        if(rcv_msg[i])
        {
            Sendtorcv_msg[i].addr(MemberList);
            initTimer();
        }
    }
    rcvfromMember();
    update(Member_Table);
}
```

<그림 2> 그룹관리 노드의 상태정보 교환 pseudo 코드

그룹관리노드는 자신이 관리하는 영역내의 멀티캐스트 멤버 노드들에 대한 상태 정보를 유지하는 역할을 한다. 그룹관리노드들이 멤버 노드들에 대한 상태

를 정확히 관리하고 있어야만 노드들의 이동에 큰 영향을 받지 않으면서 데이터 전달의 효율성을 높일 수 있기 때문이다. 따라서 주기적으로 멤버 노드들에 대한 상태 업데이트 정보를 수신하여 그룹 멤버십 테이블(Group Membership Table)을 갱신한다. <그림 3>은 그룹 멤버십 테이블의 구조를 보여주고 있다.

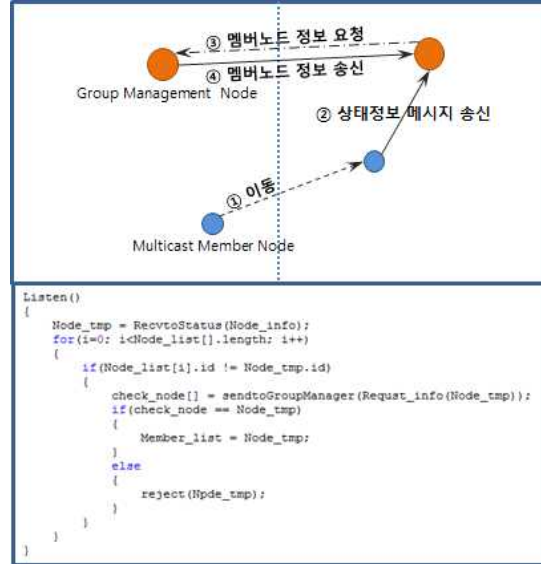
Node ID	Region_Enter_Time	Previous Region	Member_Key_Issue	Member_Join_Time
3	04:20:17	R_2	04:21:01	03:49:54
6	04:21:58	R_7	04:22:49	03:30:19
...	...	...	...	...
1	04:24:11	R_3	04:24:56	04:01:10

<그림 3> 그룹 멤버십 테이블 구조

상태 업데이트 메시지는 그룹관리노드에서 발급한 멤버키로 암호화하여 전송하게 된다. 만약 일정 시간 동안 특정 멤버 노드로부터 상태 업데이트 정보를 수신하지 못한다면 해당 노드에 대한 정보를 그룹 멤버십 테이블에서 삭제하게 된다. 반대로 멤버 노드가 다른 영역으로 이동한 경우 해당 영역의 그룹관리노드는 해당 노드에 대한 정보가 그룹 멤버십 테이블에 존재하지 않게 된다. 그룹 멤버십 테이블에 존재하지 않는 멤버 노드로부터 상태 업데이트 메시지를 수신하면 해당 멤버키를 발급해준 그룹관리노드로부터 해당 노드의 멤버 노드의 여부를 점검한 후 그룹 멤버십 테이블에 해당 노드의 정보를 삽입하게 된다. 이와 같은 방법을 통해 멀티캐스트 그룹 멤버 노드들을 관리하며, 멤버키를 이용하여 노드들에 대한 인증 과정을 거침으로써 악의적인 노드의 멀티캐스트 참여를 차단할 수 있게 된다. <그림 4>는 멤버 노드의 영역 이동에 따른 그룹관리노드의 멤버 노드 관리 방법과 pseudo 코드를 보여주고 있다.

### 3.3 보안 멀티캐스트 기법

보안 멀티캐스트 기법은 크게 두 단계의 암호화 과

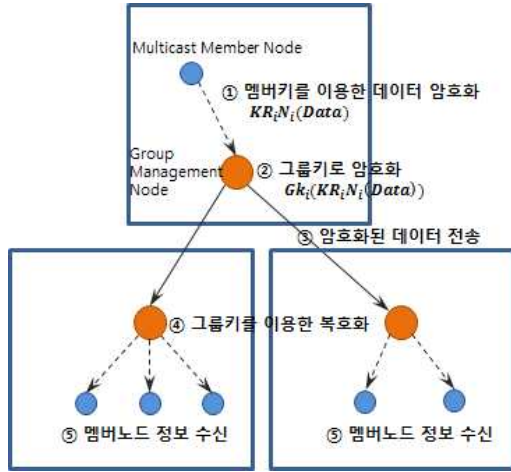


<그림 4> 멀티캐스트 멤버노드 이동 관리

정으로 구성되어 있다. 첫 번째 단계는 멀티캐스트 그룹내에 데이터 전송을 원하는 멤버 노드는 전송하고자 하는 데이터를 자신이 속해있는 영역의 그룹관리노드로부터 발급받은 멤버키를 이용하여 암호화한 후 암호화된 데이터를 그룹관리노드에게 전송하게 된다. 두 번째 단계는 멤버 노드로부터 수신된 암호화된 데이터를 그룹관리노드는 인증관리노드로부터 발급받은 그룹키를 이용하여 다시 암호화한 후 자신의 이웃그룹관리 테이블에 저장되어 있는 이웃 노드들에게 데이터를 전송하게 된다. 이렇게 암호화된 정보를 수신한 그룹관리노드들은 자신들이 관리하는 멤버 노드들에게 패킷을 전송하면 멤버 노드들은 해당 데이터를 자신의 멤버키를 이용하여 복호화하게 된다. <그림 5>는 보안 멀티캐스트 데이터 전송 과정을 보여주고 있다.

인증관리노드가 그룹관리노드에게 인증서를 발급해주는 과정은 다음과 같다.

단계 1 : 그룹관리노드 R1은 인증관리노드에게 암



<그림 5> 멀티캐스트 데이터 전송과정

```

SendMsg()
{
    if(*data) {
        while(*data != NULL)
        {
            GroupManager(Encrypt(KRiNi(*data)));
        }
    }
}

GroupManager(*data)
{
    while(*data != NULL)
    {
        cryptData=Encrypt(GKi(*data));
        SendtoMsg(MemberList(cryptData));
    }
}
    
```

<그림 6> 데이터 암호화 및 전송 pseudo 코드

호키쌍  $((G_{Ri}, P_{Ri}), P)$ 을 생성하여 그룹키 발급 요청

단계 2 : 그룹키 요청을 수신한 인증관리노드에서는 그룹관리노드 확인 후 그룹키  $(GK_{Ri}(H(k, M)))$  생성

단계 3 : 수신한 그룹키  $(GK_{Ri}(H(k, M)))$ 를 이용하여 멤버 노드들에게 멤버키  $(K_{Ri, Ni})$ 를 발급

이러한 과정으로 발급된 키를 이용한 멤버 노드들이 멀티캐스트 데이터를 전송할 수 있기 때문에 악의적인 노드들에 의한 데이터 위변조 공격을 차단 및 데이터 전달을 배제시켜 보안 멀티캐스트를 제공한다. <그림 6>은 멤버 노드에서 데이터를 암호화해서 전송하는 pseudo 코드를 보여주고 있다.

법의 성능을 측정하기 위해 모의실험을 하였다. NS-2 시뮬레이터를 이용하여 성능 평가를 실시하였으며, 모의실험을 위한 환경은 다음과 같다. 먼저 실험에 사용한 네트워크의 크기는 1000×1000, 데이터 전송 범위 250m로 하였다. 실험에 사용한 이동 노드 모델은 random-way point 모델로서 0 ~ 20 m/s 사이의 속도로 이동하고 pause time은 10초로 하였다. 전체 모의실험의 시간은 300초로 하였다. <표 1>에서는 모의실험을 위한 환경변수 값들을 보여주고 있다.

<표 1> 실험에 사용한 환경 변수

Parameter	Value
Number of Nodes	50, 100, 150, 200
Multicast Group Size	20, 30, 40, 50,
MAC Protocol	IEEE 802.11 DCF
Packet Size	CBR 512 bytes

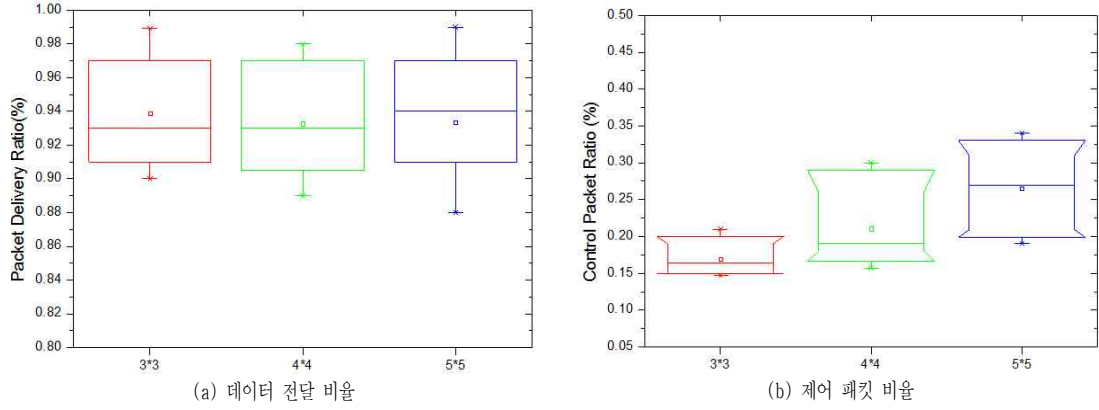
#### IV. 모의실험 및 결과

##### 4.1 실험 환경

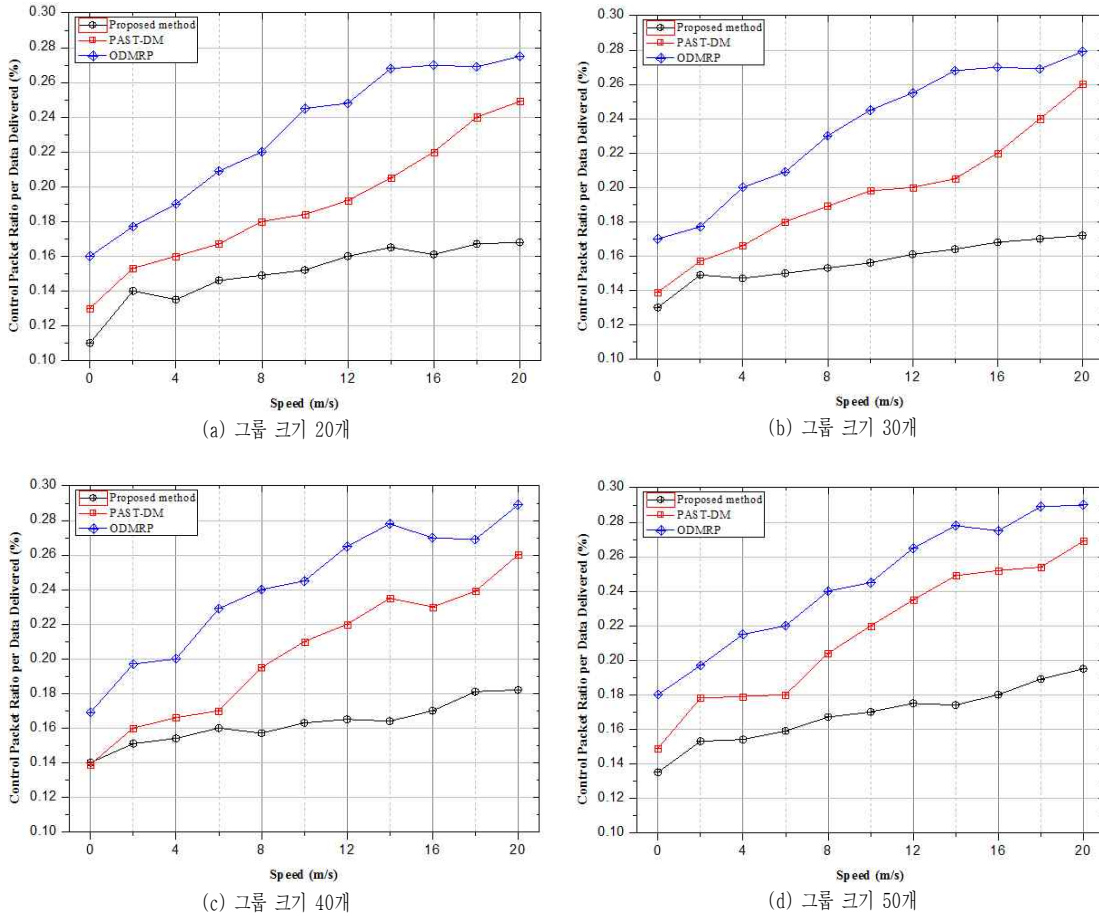
본 논문에서 제안한 영역기반 보안 멀티캐스트 기

##### 4.2 실험 결과

본 논문에서는 제안한 영역기반 보안 멀티캐스트 기법의 우수한 성능을 측정하기 위하여 ODMRP, PAST-DM 기법들과 비교 실험을 하였으며, 성능 평

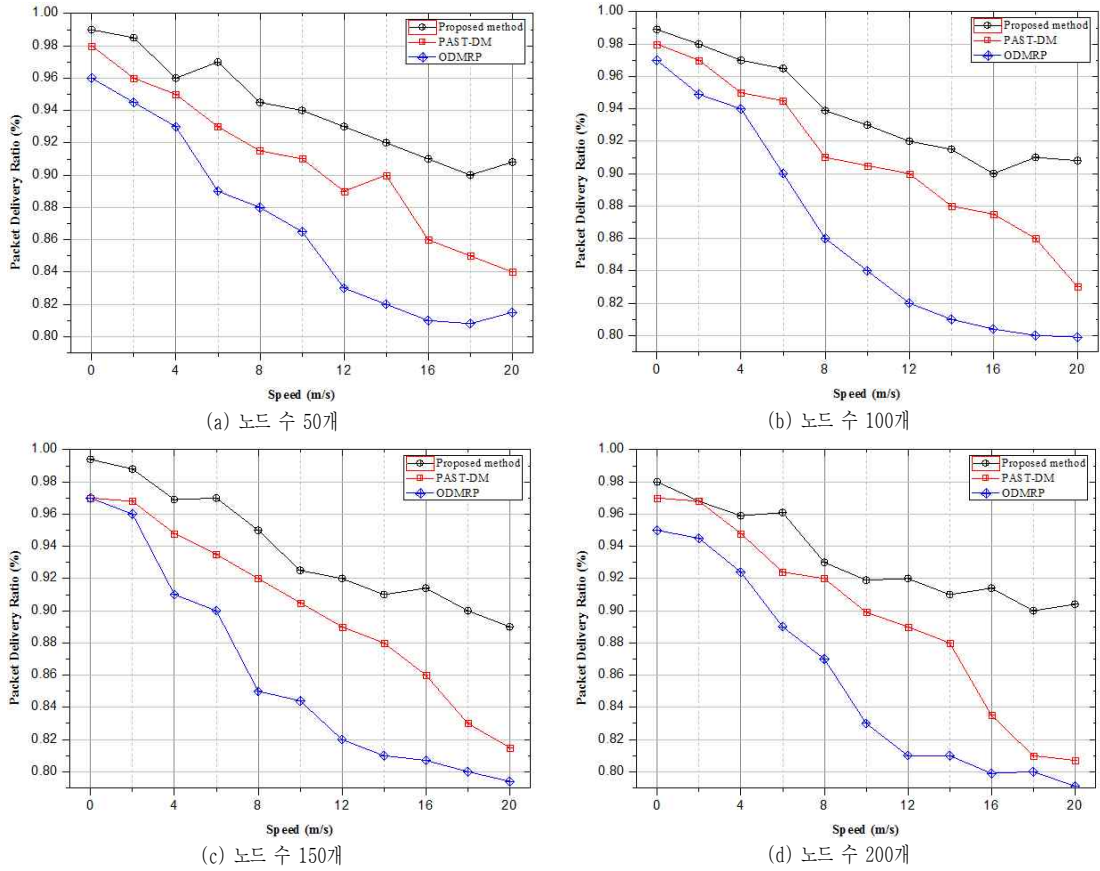


<그림 7> 네트워크 영역 개수에 따른 성능 측정



<그림 8> 그룹 크기에 따른 제어 패킷 비율





<그림 9> 노드 수에 따른 패킷 전달 비율

가 기준은 노드 수와 이동 속도에 따른 데이터 전달 비율과 멀티캐스트 그룹 크기에 따른 제어 패킷 비율로 설정하였다. 그리고 네트워크 영역의 개수에 따른 데이터 전달 비율과 제어 패킷의 비율을 측정하여, 최적의 네트워크 분할 크기를 확인하였다.

<그림 7>는 네트워크 영역 개수에 따른 데이터 전달 비율과 제어 패킷의 양을 측정하였다. 그림에서 보듯이 데이터 전달 비율은 네트워크의 분할 개수에 큰 영향을 받지않고 비슷한 성능을 보여주었으나, 제어 패킷의 양을 측정한 실험에서는 네트워크 크기에 비해 상대적으로 많은 영역으로 분할될수록 제어 패킷의 양은 크게 증가하였다. 이는 각 영역에 존재하

는 그룹관리 노드들과 멤버 노드들 그리고 각 그룹관리 노드들간의 제어 메시지가 증가하기 때문에 이러한 결과를 얻게 되었다. 따라서 최적의 네트워크 영역 분할은 각 노드들의 전송 범위를 고려한 최소한의 영역 구성이 효율적임을 확인할 수 있었다. 이는 식 1에 의해 계산된 크기  $N \times N$ 의 영역으로 분할하면 된다.

$$P(N) = \sqrt{\frac{Size_X \times Size_Y}{r^2}} \times \omega_p \tag{1}$$

$$w = \begin{cases} 1, & \rho \geq 0.9 \\ 0.8, & 0.65 \leq \rho \leq 0.89 \\ 0.6, & \rho \leq 0.64 \end{cases}$$



여기서  $r$ 은 데이터 전송범위를 나타내며,  $w$ 는 전체 네트워크에 존재하는 노드의 밀도( $\rho$ )에 따른 가중치이다.

<그림 8>에서는 노드 50, 100, 150, 200개가 있는 상황에서 이동 속도에 따른 데이터 전달 비율을 측정하였다. 이는 노드들의 이동에 따라 멀티캐스트 경로 설정 성능을 측정하기 위한 실험이다. 실험 결과에서 보여주듯이 ODMRP 기법의 성능이 가장 좋지 않았고 노드들의 수와 이동이 증가함에 따라 그 결과가 더욱 좋지 않았는데 이는 멀티캐스트에 참여하지 않는 노드들에 대한 상태 정보까지도 유지해야하기 때문에 빈번한 이동으로 인한 경로 유지가 어려워 데이터 전달 비율이 상당히 떨어졌다. PAST-DM 기법은 주기적인 상태 정보 교환을 통해 구성된 메시지를 이용한 데이터 전달의 효율성은 향상되었으나, 노드들의 이동으로 인해 특정 노드에 자식 멤버 노드가 집중되는 경우에 채널 간섭과 경쟁으로 인한 성능 저하가 유발되었다. 제안한 기법은 노드들의 이동이 빈번하더라도 각 영역내의 그룹관리노드에 의해 주기적으로 멤버 노드들이 관리되기 때문에 노드 수에 큰 영향을 받지 않으면서 멀티캐스트 멤버 노드들에 대한 데이터 전달 비율이 가장 우수한 결과를 보였다.

멀티캐스트 그룹 크기에 따른 제어 패킷 비율을 측정한 결과는 <그림 9>에서 보여주고 있다. 전체 네트워크의 패킷 중에서 제어 패킷이 차지하는 비율이 높다면 이는 네트워크의 성능이 떨어진다는 것을 의미한다. 그림에서 확인할 수 있듯이 ODMRP 기법은 멀티캐스트 데이터 전달을 위한 포워딩 그룹 결정을 위한 제어 메시지와 멀티캐스트에 조인하기 위한 제어 메시지 그리고 메시지 구성을 위한 응답 메시지 등 멀티캐스트 그룹관리 및 데이터 전송을 위한 제어 패킷의 비율이 매우 높다. PAST-DM 기법은 노드들 이동에 강건한 메시지 구성을 위한 이웃 노드들 간의 주기적인 제어 메시지 때문에 많은 오버헤드가 발생하고,

이동에 따라 그 비율은 더욱 높아지는 결과를 보였다. 제안한 기법은 노드들의 이동이 높더라도 각 영역 내에 멤버 노드를 관리하는 그룹관리노드와는 상태 정보만을 주고받으면 되기 때문에 제어 메시지의 양은 높지는 않았으나, 노드들의 이동 속도에 비례하여 제어 패킷이 다소 증가하는 결과를 보였다.

## V. 결론

MANET에서 제한된 무선 대역폭과 노드들의 이동성이 고려된 효율적인 멀티캐스트는 매우 중요한 분야 중에 하나이다. 특히 가상 토폴로지를 이용하는 오버레이 멀티캐스팅에서는 최적의 경로를 이용한 데이터 전송이 그 성능을 좌우하기 때문에 가상 토폴로지 구성 및 관리 기법이 매우 중요하다 할 수 있다. 따라서 본 논문에서는 효율적인 멀티캐스트를 위해 가상 토폴로지 구성 및 관리를 위하여 전체 네트워크를 일정 영역으로 나눈 후에 각 영역의 멀티캐스트 멤버 노드를 관리하는 구조를 제안하였다. 각 영역내의 멤버 노드들에 대한 상태 및 위치를 주기적으로 점검함으로써 데이터 전달을 위한 최적의 경로를 유지할 수 있었다. 그리고 악의적인 노드들의 멀티캐스트 참여를 차단하기 위하여 멤버 노드들은 그룹에 참여하기 위해서는 그룹관리노드로부터 멤버키를 발급 받아야만 멀티캐스트에 참여하도록 하였다. 그리고 인증관리노드에서는 멤버 노드들을 관리하는 그룹관리노드들에 대한 신뢰를 검사하여 그 보안성을 더욱 향상시켰다. 제안한 멀티캐스트 기법의 성능을 측정하기 위하여 ODMRP 기법, PAST-DM 기법과 비교 실험하였으며, 실험을 통해 노드들의 빈번한 이동에도 우수한 데이터 전달 성능을 확인하였다. 하지만 본 논문에서는 멤버 노드들이 특정 영역으로의 집중 때문에 무의미한 제어 패킷이 증가하는 문제점이 발

생하였다.

향후 영역내의 멤버 노드들이 집중이 되는 경우 그룹관리노드에 부하집중에 대한 분산 방법 연구가 수행되어야 할 것이다.

## 참고문헌

- [1] 김정삼, "무선 센서네트워크에서 네트워크수명 극대화 방안," 디지털산업정보학회지, 제10권, 제4호, 2014, pp. 47-59.
- [2] Biradar RC, M. S., "Ring mesh based multicast routing scheme in MANET using bandwidth delay product," Wireless Personal Communication, 2012, pp. 117-146.
- [3] 양환석, "MANET에서 P2P 성능 향상을 위한 위치기반 라우팅 기법에 관한 연구," 디지털산업정보학회지, 제11권, 제2호, 2015, pp. 37-45.
- [4] Subburaj. V, Dr. K. Chitra, "IDS for Detection and Prevention of Dynamic mobile node positioning based on Logical Distance Measures," International Journal of Engineering Research and Development, Vol. 3, Issue 7, 2012, pp. 27-32.
- [5] Z. J Hass and M. R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," ACM/IEEE Transactions on Networking, August, 2001, pp. 427-438.
- [6] Vaidya B, Y. S., "Robust and secure routing scheme for wireless multihop network," Personal and Ubiquitous Computing, 2009, pp. 457-469.
- [7] Kashihara S, H. T., "Data delivery method based on neighbor nodes information in a mobile ad hoc network," The Scientific World Journal, 2012, pp. 1-13.
- [8] Huang, J, "MOEAQ: a QoS-aware multicast routing algorithm for MANET," Expert Systems with Applications, 2010, pp. 1391-1399.
- [9] Yang S, Y. C., "Toward reliable data delivery for highly dynamic mobile ad hoc networks," IEEE Transactions on Mobile Computing, 2012, pp. 111-124.
- [10] K. Shankar and S. Audithan, "Analysis of QoS Multicast Protocols for MANETs," in 2nd International Conference on Current Trends in Engineering and Technology, ICCTET'14 IEEE 2014 IEEE Conference Number, 2014, pp. 472-474.
- [11] B. Singh and R. Hans, "TCP and UDP Based Performance Analysis of AODV, DSR and DSDV Routing Protocols Under Different Traffic Conditions in Mobile AdHoc Networks," International Journal of Future Generation Communication and Networking, Vol 8, No. 2, 2015, pp. 73-92.

■ 저자소개 ■



양 환 석  
Yang Hwanseok

2011년 9월~현재  
중부대학교 정보보호학과 조교수  
2006년 2월~2011년 2월  
호원대학교 사이버수사경찰학과  
연구교수  
2005년 2월 조선대학교 전산통계학과  
(이학박사)  
1998년 2월 조선대학교 전산통계학과(이학석사)  
관심분야 : 정보보호, 침입탐지시스템,  
MANET  
E-mail : yanghs@joongbu.ac.kr

논문접수일: 2016년 8월 4일
수정일: 2016년 8월 17일
게재확정일: 2016년 8월 26일