특집

이동 Ad-hoc 네트워크에서 노드의 제약 및 응용에 따른 확장된 멀티캐스트 프로토콜 연구

김기일(충남대학교 컴퓨터과학과), 김상하(충남대학교 교수)

I. 서 론

이동 Ad-hoc 네트워크 (Mobile Ad-hoc Networks)는 패킷 데이터를 전송하는 무선 인터페이스를 사용하는 이동 노드들로 구성되는 네트워크로써 중앙 집중적인 관리 없이 노드들의 자발적 참여로써 네트워크가 형성된다. 이를 위하여 네트워크의 노드들은 라우터 및 호스트로써 동작이 가능하며 이를 통하여 다중 홉 무선 통신이 가능하게 된다[1].

현재 이러한 이동 Ad-hoc 네트워크에서 고려되고 있는 대표적인 응용들로는 회의실과 같은 공간에서의 독자적인 화상 회의, 군사 작전을 위한 응용, 그리고 재난 구조를 위한 응용과 같이 인프라스트럭처의 사용이 불가능하거나 또는 임시적으로 구성되는 독자적 네트워크상에서의 응용들이 주로 고려되고 있다. 이러한 응용 지원을 위하여 적용되는 통신의 가장 큰 특징은 일-대-일 통신 보다는 일-대-다 또는 다-대-다 통신이 주로 사용된다는 것이다. 특히, 이동 Ad-hoc 네트워크는 노드들의 그룹 단위의 협력적 관계로써 동작하는 동시에 노드들의 분산된 동작에 기반을 둔 네트워크이므로 해당 응용들의 사용 빈도수는 점차 증가할 것으로 예상된다.

이러한 이동 Ad-hoc 네트워크에서의 무선 네트워크는 유선망과는 달리 대역폭이 상대적으로 작기 때문에 그룹 통신을 지원하기 위한 프로토콜은 자원의 효율적 사용을 가장 중요하게 고려하여야만 한다. 이러한 이유로 인하여, 그룹 통신을 멀티캐스트를 통하여 지원하기 위한 다양한 메커니즘이 제안되었다. 왜냐하면, 멀티캐스트 메커니즘은 네트워크의 형태에 상관없이 가장 효율적인 그룹 통신 방법이기 때문이다.

현재 제안되고 있는 멀티캐스트 메커니즘들은 노드의 이동성으로 인한 네트워크 토폴로지의 변화에 상관없이 각 수신자들에게 효율적으로 데이터 전송을 위한 데이터 전송 구조를 구성하는 것에 초점이 맞추어져 있다. 현재 제안되어 있는 프로토콜들은 데이터 전송 구조의 형태에 따라, 트리기반, 메쉬기반 그리고 두 메커니즘을 통합한 혼합 구조로 나누어지게 되며, 대표적인 프로토콜로는 MAODV (Multicast Ad-hoc On-Demand Distance Vector), ODMRP (On-Demand Multicast Routing Protocol), MCEDAR (Multicast Core-Extraction Distributed Ad-hoc Routing) [1] 등이 있으며 보다 많은 프로토콜들이

학교 및 연구소에서 연구 되고 있다.

이러한 멀티캐스트 라우팅 프로토콜에 대한 연구와 병행하여 최근에는 멀티캐스트 확장에 대한 연구가 계속되고 있다. 특히, 이동 Ad-hoc 네트워크는 노드의 배터리에만 의존한 적은 전력의 디바이스들의 임의적인 집합으로 구성되기 때문에 멀티캐스트를 지원하기 위하여서는 전력의 소비를 최적화하기 위한 확장 방안에 대한 연구가 필수적이라 할 수 있다. 또한, 이동 Ad-hoc 네트워크의 제약사항에 관한 연구와 더불어 군사 망과 같은 실제 멀티캐스트가 적용될 응용 측면에서 각 그룹 멤버들에게 서비스 질 보장, 안전한 통신을 제공하기 위한 멀티캐스트의 확장 방안 또한 많은 연구자들의 주목을 받고 있다. 이러한 멀티캐스트 프로토콜의 확장은 현재 진행되고 있는 멀티캐스트 메커니즘을 실제 망에 적용하기 위하여 반드시 고려되어야 할 사항에 해당하는 것으로 이동 Ad-hoc 네트워크에서의 멀티캐스트 서비스를 위하여 필수적이라 할 수 있다. 이에 현재 진행 중인 연구를 중심으로 관련 프로토콜들을 비교 분석 함으로써 각 프로토콜의 장단점을 알아보고자 한다.

본고는 다음과 같이 구성된다. Ⅱ장에서는 에너지 효율성을 고려한 멀티캐스트 라우팅 프로토콜에 대하여 살펴본다. 또한, QoS 보장 및 안전한 멀티캐스트를 위한 연구는 각각 Ⅲ장과 Ⅳ장에서 설명한다. 마지막으로, Ⅴ장에서는 결론을 맺는다.

Ⅱ. 에너지 제약을 고려한 멀티캐스트

이동 Ad-hoc 네트워크에서의 노드들은 배터리에 대하여 의존적이기 때문에, 네트워크의 수명을 증가시키기 위하여 배터리의 전력을 최적화할 수 있는 프로토콜이 필요하다. 이러한 기능의 추가는 결과적으로 네트워크의 수명을 증가시키는 동시에 이로 인한 패킷의 손실을 줄일 수 있기 때문에 패킷 전송률과도 많은 관계가 있게 된다. 이번 장에서는 대표적인 연구들을 살펴본다.

1. Energy-Efficient Reliable Broadcast and Multicast Protocols

[2]에서는 BIP (Broadcast Incremental Power), BLU (Broadcast Least Unicast), BLiMST (Broadcast Link-based Mimimum Spanning Tree)의 3가지 알고리즘을 기반으로 하는 효율적 에너지 사용 기반의 멀티캐스트 메커니즘이 제안되었다. 이러한 메커니즘들은 패킷-에러 확률을 고려하여 해당 링크 상에서 신뢰성 있게 데이터를 전송하기 위하여 필요한 예상되는 에너지를 결정한다. 노드 i에서 노드 j의 패킷의 신뢰성 있는 전송을 위하여 필요한 에너지는 다음과 같이 정의되게 된다.

$$E_{ij(reliable)} = \frac{E_{ij}}{(1-p_{ij})} \quad (1)$$

식 (1)에서 p_{ij}는 패킷-에러 확률을 나타내고, $1 / (1-p_{ij})$는 노드 i에서 노드 j까지의 필요한 재전송 횟수이다. E_{ij}는 노드 i에서 노드 j까지의 패킷 전송을 위하여 필요한 에너지양이다. 제안된 메커니즘에서는 $E_{ij(reliable)}$값을 멀티캐스트 트리 구성을 위한 알고리즘의 기준 값으로 적용함으로써 효율적인 에너지 기반 트리를 만들게 된다.

2. A Distributed Power-Aware Multicast Routing Protocol

[3]에서는 유니캐스트 라우팅 프로토콜의 라

우팅 정보와 에너지 관련 파라미터를 고려하여 최소 에너지 비용 트리를 구성하는 방안을 제안하였다. 이러한 트리 구성을 위하여 각 노드에서는 각 노드에서 현재 사용가능한 송수신기 및 노드에서 각 노드로 전송 시 필요한 에너지의 양을 이용하게 된다. 이러한 정보를 이용하여 각 노드 i에서 노드 j로의 거리를 구하게 된다. 따라서 이러한 거리의 값을 최소화 할 수 있는 트리를 구성함으로써 에너지를 고려한 전송 트리를 구성하게 된다.

이러한 트리를 구성하기 위한 비용 C는 다음과 같이 주어지게 된다.

$$C = \frac{(P_{1,2} + P_{2,3} + ... + P_{j-1,j})}{\min(K_1, K_2, ... K_j)} \quad (2)$$

식 (2)에서 K_i는 노드 i에서 사용가능한 전송자의 수이며, $P_{i,j}$는 노드 i에서 노드 j로 전송하기 위하여 필요한 전력량을 나타낸다. 노드 i에서 노드 j로의 거리는 다음과 같이 표현된다.

$$D_{i,j} = \frac{P_{i,j}}{\min(K_i, K_j)} \quad (3)$$

이러한 $D_{i,j}$를 기준으로 송신자에서 각 수신자까지 경로 중 가장 적은 값을 갖는 경로를 선택하게 된다.

3. Energy-Efficient Multicast Routing Protocol

[4]에서는 메쉬 기반의 E^2MRP (Energy-efficient Multicast Routing Protocol)을 제안하였다. 제안된 메커니즘은 두 단계로 구성된다. 첫 번째 단계는 각 패킷당 소요되는 최소 전력을 구하게 된다 (MECP 단계). 사용되는 에너지는 거리에 비례하기 때문에 거리를 고려하여 각 패킷당 소요되는 최소 에너지를 이용하여 송신자로부터 최종 목적지까지 패킷을 전송하는데 소요되는 전체 단-대-단 전력을 최소화하는 것이다. 이 최소 에너지를 이용하여 메쉬를 구성하게 된다. 이후, 최소-최대 노드 비용을 계산한다. 이러한 계산을 위하여 시간 t까지 사용된 에너지의 양이 사용된다. 이를 바탕으로 경로 상에 보다 많은 에너지를 가진 노드들로 구성된 경로 설정을 하게 된다 (MMNC 단계).

이러한 두 단계는 계속적으로 서로 바뀌게 된다. 먼저, MECP 알고리즘을 적용함으로써 몇 개의 경로 집합이 설정되게 되고 메쉬가 구성되게 된다. 메쉬가 구성된 다음, CFS (Cost Function Switch)라고 불리는 타이머가 설정되게 된다. CFS가 종료되기 전에 시스템은 MMNC 상태로 전위된다. 이 단계에서 MMNC 기능으로 인하여 메쉬가 다시 설정되게 되고 CFS 타이머가 다시 설정된다. 이전과 마찬가지로 타이머가 종료되기 이전에 MECP 상태로 전의되게 되며 계속적으로 이 과정이 반복되게 된다.

4. Energy-Efficient Cluster Adaptation of Multicast Protocol

[5]에서는 전력을 최적화 할 수 있는 클러스터 기반의 메커니즘이 제안되었다. 각 클러스터는 클러스터-헤드를 가지고 있고 이 클러스터-헤드는 슈퍼-노드 네트워크에 연결되어 있는 구조를 가지고 있다. 클러스터-헤드에 수는 에너지 소비에 절대적 영향을 미치기 때문에, 적당한 클러스터 수를 조절하는 것이 필요하다.

이러한 클러스터 수 조절을 위한 네트워크 초

기화 과정에서 각 노드는 자신을 클러스터-헤드로 정의하고 가장 강력한 전력 레벨로 비콘 메시지를 주기적으로 전송한다. 각 노드는 증가 추세에 있던 노드들의 수가 줄어들게 되거나 또는 전력 레벨이 특정 최대치를 넘게 되면 자신의 전력 레벨을 한 단계 높이게 된다. 각 노드는 첫 번째 자신의 ID보다 큰 ID를 가진 클러스터-헤더에 참가하게 된다. 이러한 클러스터를 만듦으로써 클러스터내의 각 노드는 같은 클러스터 안에 있는 다른 모든 노드들에게 접근이 가능하게 된다. 에너지의 소비를 맞추기 위하여, 각 노드들은 돌아가면서 클러스터-헤드가 된다.

5. 요약 및 고려사항

위의 각 프로토콜에서 살펴 본 봐와 같이 효율적인 에너지 사용을 위한 멀티캐스트 프로토콜의 기본적인 개념은 멀티캐스트 트리 구성 시 가장 짧은 홉 수를 기준으로 하는 기존의 메커니즘과는 달리 각 노드 사이에서의 전력의 사용량을 기준으로 하는 새로운 트리 구조 및 메쉬 구조를 만드는 것에 초점이 맞추어져 있다. 이러한 구조의 기본적인 생각은 데이터 전송에 참가하는 노드의 수를 제한함으로써 전체적인 멀티캐스트 전송을 위한 에너지 사용을 최소화 하는 것이다. 이러한 접근 방법은 효율적 에너지 사용을 위한 적절한 접근 방법이라 할 수 있다.

하지만, 지금까지의 메커니즘들의 경우에는 이동성에 대한 고려가 부족한 상태이다. 즉, 이동으로 인한 링크의 단절과 이를 복구하기 위한 시그널링으로 인한 에너지의 소모 등에 대한 고려가 부족한 동시에 각 노드의 배터리 소모를 균형 있게 조절 할 수 있는 메커니즘의 추가가 요구된다. 또한, MAC 레이어와의 연동을 위한 구조 또한 고려되어야만 한다.

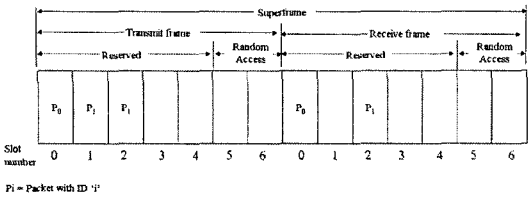
III. QoS 보장을 위한 멀티캐스트 프로토콜

이동 Ad-hoc 네트워크에서 QoS를 보장한다는 것은 단-대-단 지연, 가용 자원 대역폭, 버퍼, 그리고 멀티캐스트 세션에 대한 계산적 자원과 같은 파라미터를 보장함을 의미한다. 이동 Ad-hoc 네트워크에서 QoS를 보장하기 위한 대표적 프로토콜로는 wireless Ad-hoc real-time multicast protocol, multicast priority scheduling, 그리고 an efficient core migration protocol for QoS in mobile Ad-hoc networks 이 있다. 이번 장에서의 위의 프로토콜들을 기준으로 QoS 보장을 위한 요구 사항 및 각 프로토콜의 특징을 살펴본다.

1. Wireless Ad-hoc Real-time Multicast Protocol

WARM (Wireless Ad-hoc real-time multicast)는 멀티캐스트 메쉬상의 CBR (Constant Bit Rate) 트패픽에 대한 QoS를 보장하기 위하여 제안된 프로토콜이다. 이 프로토콜은 멀티캐스트 세션에 대한 전송 스케줄링 문제에 초점을 맞추고 있다. 이를 위하여 수신자 노드는 시간 분할 다중 접속의 타임 슬롯들을 예약하며 멀티캐스트 멤버인 이웃 노드를 통하여 멀티캐스트 메쉬에 접속하게 된다.

이러한 프로토콜은 두 가지 트래픽 타입(CBR, VBR)을 가지며 각 프레임은 예약 부분과 임의 접근 부분으로 구성되어 있다. 노드에 의하여 전송된 패킷들은 해당 프레임에 대하여 연속적으로 번호가 매겨지게 된다. 각각의 노드는 멀티캐스트 세션에 대하여 여러 정보를 유지하게 된다.



〈그림 1〉 WARM에서의 TDMA 프레임 구조

각각의 노드는 자신이 미리 예약해 놓은 슬롯의 수가 임계치 보다 적어지게 되면 다른 노드를 통하여 다시 멀티캐스트 세션에 연결을 시도하게 된다. 이를 위하여 각 노드들은 상태 정보를 주기적으로 전송하게 되며 이러한 정보는 다른 신호 채널 상에서 이루어지게 된다.

만약, 현재 예약되어 있는 수신 채널의 수가 현재 트래픽에 기반하여 노드에 의하여 결정된 수신 슬롯의 정해진 수보다 작게 되면 노드는 시그널링 메시지를 통하여 보다 많은 수신 채널 확보를 수행한다. 이후, 노드는 요구되는 여분의 수신 채널, 이 수신 채널을 사용하게 될 잠재적 부모 노드, 손실된 패킷의 시퀀스 번호에 대한 정보를 신호 메시지에 추가하게 된다. 각 노드는 신호 정보를 받는 모든 노드들에 관한 이웃 데이터베이스를 유지하게 된다. 연결 과정은 다음과 같다.

1단계 : 노드는 손실된 패킷의 프레임-시퀀스 번호를 결정한다. 그리고 기존 노드와 1홉 이내에 있는 이웃 노드에서 이 프레임을 이미 전송한 노드를 찾는다.

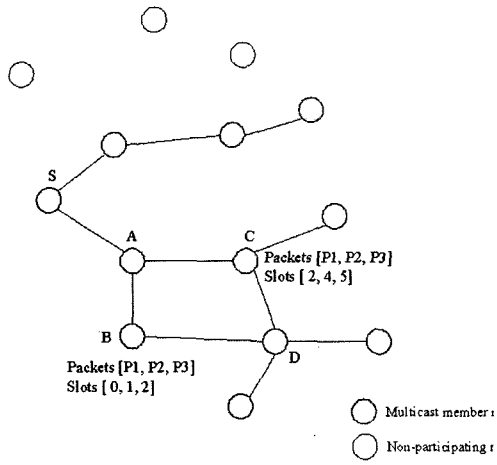
2단계 : 이 노드와의 SIR (Signaling-to-Interference Ratio)를 비교하여 이 값이 임계치 큰 경우에, 해당 노드는 이 노드로부터 데이터를 받게 된다.

3단계 : 만약 위의 과정에도 패킷을 손실하게 되면, 자신의 홉보다 1홉 작은 이웃 노드를 확인한 뒤 손실된 패킷을 릴레이 하기 위하여 전송 슬롯을 추가하게 된다.

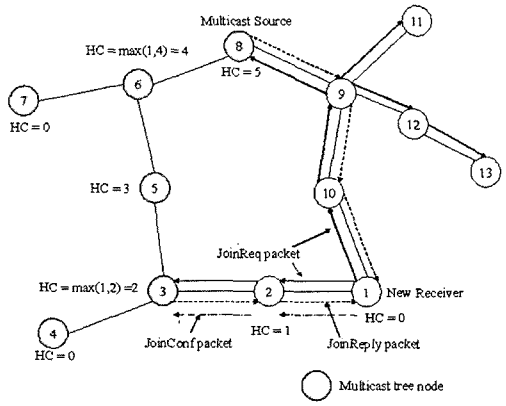
<그림 2>는 송신자 S에서부터 수신자들에게 데이터 전송 과정을 보여준다. A에서 전송된 패킷은 B, C에서 아무런 충돌 없이 수신되게 된다. 노드 B는 P1, P2를 슬롯 0번을 통해, P3을 슬롯 1번을 통해 각각 전송하게 된다. 반면 노드 C는 P1, P2를 슬롯 2, 4번을 통하여 전송하게 되고 P3을 슬롯 5번에 전송하게 된다. 노드 B는 노드 D의 부모노드이다. 노드 B에서 보내진 패킷 P1, P2는 노드 D의 슬롯 0, 1로 문제없이 수신되게 된다. 그러나 슬롯 2번에서, 노드 B와 C가 동시에 전송한다. 따라서 노드 D의 슬롯 2번에서 충돌이 발생하게 된다. 두 노드가 보낸 패킷은 노드 D의 슬롯 2번에서 충돌이 발생하게 된다. 노드 D는 P3을 전송한 다른 부모 노드를 찾게 된다. 노드 C가 슬롯 5번으로 P3을 전송한 것을 알 수 있다. 노드 C에서 슬롯 5가 사용되고 있지 않으며 슬롯 5의 SIR이 적당하다면, 노드 D는 노드 C를 자신이 부모 노드로 결정하고 슬롯 5번으로부터 패킷 P3을 수신하게 된다.

2. Multicast Priority Scheduling Protocol

MPSP (Multicast Priority Scheduling Protocol)는 이동 Ad-hoc 네트워크상에서의 멀티캐스트 트래픽을 위한 패킷 스케줄링 메커니즘이다. MPSP의 목표는 제한된 단-대-단 지연을 보장하면서 멀티캐스트 패킷 전송을 제공하는 것이다. 이 메커니즘은 단-대-단 지연 안에 높은 패킷 전송을 보장하는 우선순위 스케줄링을 사용하는



〈그림 2〉 WARM을 통한 패킷 전송 예



〈그림 3〉 MPSP에서 HC의 전파 예

DLPS (Distributed Laxity-Based Priority Scheduling) 프로토콜에 기반하고 있다.

MPSP는 트리나 메쉬 기반의 멀티캐스트 프로토콜들에서 동작이 가능하다. 각 노드는 스케줄링 테이블 (ST)라 불리는 테이블을 유지한다. 이 테이블에는 노드에 의해 전송된 패킷 정보, 우선순위 인덱스 값에 의하여 정렬된 이웃노드들에서의 패킷 정보가 포함되어 있다. 우선순위 인덱스는 패킷의 우선순위를 나타낸다. MPSP 프로토콜은 피드백 메커니즘, 우선순위 인덱스 계산, 스케줄링 테이블 갱신, 백-오프 메커니즘으로 구성된다.

<그림 3>는 그룹 참가 과정을 보여준다. 새로운 노드 NR (node 1)이 JoinReq 패킷을 전송함으로써 경로 탐색을 시작한다. 이것은 멀티캐스트 노드인 3과 8에 도착하게 되며 두 노드는 JoinReply 패킷을 전송하게 된다. Node 1은 3을 선택하게 되고 hopCount (HC) 값을 0으로 설정한 JoinConf메시지를 전송하게 된다. 노드 2가 이 메시지를 받게 되며 HC값을 1 증가시키며 다음 전송하는 데이터 패킷에 이 정보를 삽입한다. 노드 3은 이 패킷을 받고 노드 1에 대한 HC정보를 갱신한다. 노드 3은 이미 노드 4에 접속되어 있기 때문에, 노드 3으로부터의 HC는 1이다. 노드 3에서의 멀티캐스트 세션에 대한 새로운 HC 값은 max(1,2) = 2로 결정된다. 이 값은 노드 3에 의해 전송되는 멀티캐스트 패킷에 의하여 전송된다. 노드 5와 6은 값은 방법으로 새로운 HC를 계산한다. 노드 6인 HC값이 4로 정해진 패킷을 전송하는 경우, 멀티캐스트 송신자인 노드 8은 패킷을 받게 되고 노드 6을 통한 최대 홉은 5로 설정한다. 이러한 각각의 HC값에 의하여 패킷의 우선순위 인덱스가 결정되게 된다. 이러한 우선순위 인덱스는 식 (4)에 의하여 결정되게 된다.

$$PI = \frac{PDR}{M} * ULB \qquad (4)$$

식 (2)에서 PDR은 패킷이 속하는 플로우의 패킷 전송률이고 ULB는 (정해진 지연 - 현재 노드에서의 시간) / 멀티캐스트 패킷이 전송되기 위

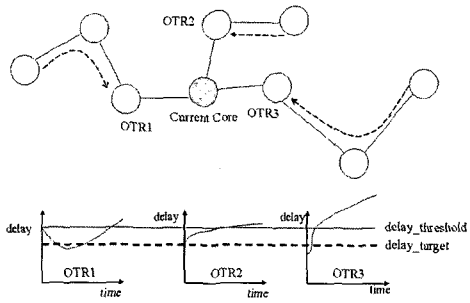
한 남아 있는 최대 홉 수로 정의된다. 또한, M은 멀티캐스트 세션을 위한 패킷 전송률을 나타내는 사용자 정의 파라미터이다.

3. An Efficient Core Migration Protocol for QoS in Mobile Ad-hoc Networks

제안된 QoS에 기반한 코어 이동 프로토콜[8]은 그룹 공유 트리를 이용한다. 이 프로토콜은 각 트리의 마지막 노드가 멀티캐스트의 원하는 서비스 질에 만족할 수 있도록 새로운 트리를 구성하는 방법을 찾게 된다.

통신을 위한 비용을 줄이기 위하여 코어 선택 알고리즘은 오직 현재 코어에서만 동작하게 된다. 만약, 예를 들어, 서비스 질 평가의 값이 지연이라면, 코어는 각 노드들에 대한 지연의 값을 보장하게 된다. 이러한 지연은 코어까지의 지연 + 각 노드에서 전송되는 ACK 메시지의 지연으로 계산되게 된다. 만약 평균 지연 시간이 주어진 임계치 값을 넘어가게 되면 현재의 코어 노드는 근처에 있는 노드들 중에서 보다 좋은 코어 후보 노드들 중에서 하나를 선택하게 된다. 따라는 코어의 이동은 점진적으로 일어나게 되며 이동 Ad-hoc 네트워크의 동적인 이동성 특성을 맞출 수 있게 된다.

<그림 4>는 지연에 따른 코어 결정 알고리즘의 예를 보여준다. 그림에서 볼 수 있듯이 현재 코어에서의 지연 측정 결과 OTR3에서의 평균 지연 시간이 가장 크기 때문에 현재의 코어 노드가 OTR3으로 결정되게 된다면 평균 지연 시간을 줄이는데 보다 좋게 된다. 따라서 현재의 코어 노드는 OTR3으로 전체적인 지연을 줄이기 위하여 OTR3으로 이동하게 된다.



〈그림 4〉 코어에서의 지연 측정 결과에 따른 코어 결정 알고리즘

4. 요약 및 고려 사항

현재의 QoS 보장을 위한 멀티캐스트의 확장 측면은 기본적으로 예약을 통한 무선 자원 확보를 통한 QoS 제공을 위한 MAC 레벨에서의 메커니즘과 QoS 보장을 위한 효율적인 멀티캐스트 트리 구성에 초점이 맞추어져 있다. 멀티캐스트 트리 구성시는 이전의 효율적 에너지 사용을 위한 트리 구성과 마찬가지로 각 링크의 비용을 해당 QoS 파라미터로 설정한 뒤 이를 기준으로 트리를 구성하게 된다.

이러한 멀티캐스트 프로토콜의 확장 역시 많은 오버헤드로 인하여 아직까지 동적 환경이 변화에 대한 연구는 아직 많은 연구가 필요한 부분으로 남아 있다. 이러한 이동성과 더불어 무선 네트워크 환경의 변화에 적응할 수 있는 프로토콜이 개발도 필요할 것으로 예상된다.

Ⅳ. 안전한 데이터 전송을 위한 멀티캐스트 프로토콜

이동 Ad-hoc 네트워크가 군사 작전과 같은 특수한 환경에서 동작되는 경우에 멀티캐스트 프

로토콜은 무엇보다 안전한 데이터 전송을 위한 보안에 초점이 맞추어져야만 한다. 특히, 이동 Ad-hoc 네트워크에서의 노드에서의 기본적인 데이터 전송은 브로드캐스팅에 의존하게 되므로 임의의 노드에서 쉽게 이러한 데이터를 가로챌 수 있기 때문에 이러한 보안에 대한 고려는 반드시 필요하게 된다.

특히, 이동 Ad-hoc 네트워크의 동적인 토폴로지 특성은 여러 가지 문제점을 야기한다. 첫 번째는 이동 Ad-hoc 네트워크는 기존의 네트워크와는 달리 신뢰할 만한 중앙 집중적 인프라스트럭처가 없다. 이와 더불어 이동으로 인하여 각 노드는 임의의 노드와 많은 연결의 설정 및 해제가 빈번하게 된다. 마지막으로 이동 Ad-hoc 네트워크 환경에서 공격자는 각 이동 노드 자체를 획득할 수 있기 때문에 이에 대한 고려 또한 필요하다. 이번 절에서는 이러한 문제점을 최대한 극복하고자 제안된 멀티캐스트 프로토콜의 확장 프로토콜들을 살펴본다.

1. Secure Multicast over Multihop Wireless Ad-hoc Networks

[9]에서는 안전한 멀티캐스트를 위하여 그룹 멤버들의 물리적으로 안전 트리를 유지하는데 초점이 맞추어져 있다. 이 안전한 멀티캐스트 트리는 인가된 그룹 멤버들에게 그룹 키를 안전하게 포워딩하기 위하여 사용된다. 그룹에 참가함으로써 안전한 멀티캐스트 트리를 구성하기 위한 단계는 다음과 같다.

1단계 : 그룹 참가 요청 메시지를 브로드캐스트 한다.

2단계 : 그룹 참가에 대한 응답들을 수신한다.

3단계 : 인증, 등록, 키 설정 : 인증을 요청하는 노드와 중간 노드는 상호 인증을 하게 된다. 인증 과정은 공용 키 설정 과정을 유도한다. 이후, 두 노드는 정보 접근을 위한 상호 검사를 하게 된다. 이러한 접근 권한은 서비스-접근 증명서를 사용함으로써 이루어진다.

4단계 : 암호화된 데이터 수신

5단계 과정의 증명서는 서비스를 나타내며 인증된 엔티티로부터 검사된 메시지이다. 이러한 증명서를 위한 형식은 다음과 같다.

[DataId | Issuer | TypeOfService | ValidityPeriod | SequenceNumber | UserPublicKey | Signature]

만약 노드 A가 그룹 참가를 요청하게 되면 해당 노드는 다른 그룹 멤버들에게 서비스 권한 증명서를 전송한다. 노드 A가 노드 B에 접속했다고 가정하자. 만약 A의 증명서가 노드 B에 저장되어 있는 증명서 폐기 리스트의 시퀀스 번호가 [MinSN, CurrentSN] 사이에 있다면 A는 그룹 참가가 허락된다. 만약 CRL에 있다면 이것은 거부될 것이다. 만약, A의 증명서의 SN이 노드 B의 CRL안의 MinSN보다 작다면, A는 송신자로부터 승인을 받아야 하거나 또는 높은 SN을 가진 증명서를 받아야 한다.

2. Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographical Location Information

효율적인 키 분배 메커니즘의 기본은 오직 인

증된 그룹 멤버들만 특정 시간에 유효한 키를 가져야 한다는 것을 보장해야만 한다. 이를 위하여 계층적 구조의 키 분배 알고리즘이 제안되었다. 하지만, 이 구조 하에서 그룹의 참가나 탈퇴가 발생한 경우에는 이러한 키는 반드시 갱신되어야 하므로 빈번한 갱신으로 인한 계산의 복잡성이 증가하게 되고 이것은 노드의 수명을 단축시키게 된다.

이에 대응하기 위하여 [10]에서는 물리적인 위치 정보를 이용한 효율적 에너지 기반의 키 분배 메커니즘을 제안한다. 이는 멀티캐스트 그룹의 멤버들 사이의 공간적 상관성을 검사함으로서, 에너지를 고려한 효율적인 키 분배 메커니즘을 만들 수 있게 된다. [10]에서는 계층적인 트리 구조를 구성하기 위하여 K-평균 알고리즘을 사용하는 메커니즘을 제안한다. 이 알고리즘은 다음과 같다.

1단계 : 초기에는 하나의 클러스터에 모든 점들을 할당한다.
2단계 : K-평균 알고리즘을 이용하여 각 클러스터를 두 개의 클러스터로 나눈다.
3단계 : 각 클러스터에 할당되는 점의 수를 조절한다.
4단계 : 2단계와 3단계를 계속 반복하여 클러스터에 할당된 점의 수가 2 또는 1이 되도록 한다.
5단계 : 하나의 점으로 가능하면 합병한다.
6단계 : 클러스터의 계층화를 트리의 계층화로 매핑 한다.

3. GKMPAN : An Efficient Group Rekeying Scheme for Secure Multicast in Ad-hoc Networks

[11]에서는 이동 Ad-hoc 네트워크에서 안전한 멀티캐스트를 위한 효율적이고 확장성 있는 키 재설정 프로토콜을 제안하였다. 이 메커니즘에서 그룹 키는 각 멤버들에게 안전한 홉간의 전달 방법을 사용하여 분배된다. 이미 구현된 대칭형 키에 기반을 둔 확률적인 메커니즘은 그룹 키 분배를 위한 맴버들 간의 안전한 채널들을 구현하는데 사용된다. 또한, GKMPAN은 효율적으로 미리 설정된 키들을 갱신하기 위한 분산된 메커니즘을 포함한다. GKMPAN의 가장 큰 특징은 각 노드는 만약 이전의 키 재설정 과정이 완벽하게 이루어지지 않더라도 현재의 그룹 키를 혼자 구성할 수 있다.

GKMPAN에서 가장 고려하고 있는 공격은 그룹 멤버 간에 교환되는 키 분배 메시지를 엿들음으로서 그룹 키를 알아내는 그룹 키 복구 공격이다. 이를 위하여 프로토콜은 4가지 단계가 존재한다.

1단계 : 키 미리 분배-이동 Ad-hoc 네트워크가 구현되기 이전에, 모든 노드는 키 서버로부터 키의 서브 집합을 얻게 되고 이러한 키들은 키를 암호화하기 위한키로 사용된다.
2단계 : 인증 노드 취소-키 서버가 노드를 인증을 취소하고자 할 때 네트워크에 이 사실을 브로드캐스트 한다.
3단계 : 안전한 그룹 키 분배-키 서버는 새로운 그룹 키 K를 생성하고 분배한다. K는 홉 전달 방식으로 모든 노드들에게 전달되게 되며, 미리 구현된 키를 KEK (Key Encryption Key) 방식으로 안전하게 전달한다.
4단계 : 키 갱신-노드가 그룹 키 K를 받고 확인

한 뒤, 노드는 K에 기반하여 자신의 KEK를 갱신한다.

V. 결 론

이동 Ad-hoc 네트워크에서의 유니캐스트 라우팅 프로토콜 개발과 더불어 효율적인 그룹 통신을 위한 멀티캐스트 라우팅 프로토콜이 개발도 매우 시급한 문제로 인식되고 있다. 이를 위하여 다양한 메커니즘이 제안되었으나 이들을 실제 망에 적용하는 경우 야기 될 수 있는 제한적 에너지 공급 문제, QoS 보장, 그리고 안전한 그룹 통신을 위한 연구들은 아직 초기화 단계에 있다. 특히 그룹 통신을 위한 응용들의 관점에서 살펴 볼 때 네트워크의 수명의 최대화, 멀티미디어 데이터 전송을 위한 QoS 보장, 무선 네트워크의 브로드캐스팅에 기반한 데이터 전송으로 인한 보안 문제들은 향후 응용에서 반드시 고려되어야 하므로 이에 대한 프로토콜 확장은 필수적이다.

본 논문에서는 위의 세 가지 관점에서 멀티캐스트 프로토콜 확장 방안에 대한 기존의 연구들을 살펴보았다. 하지만, 결론적으로 아직까지 제안된 모든 프로토콜들은 이동 Ad-hoc 네트워크의 가장 큰 특징인 노드의 이동성에 의한 네트워크 토폴로지의 변화에 완벽하게 대응하지는 못하고 있다. 그러나, 계속적인 연구가 진행되고 있는 봐 이에 대한 해결 방안이 곧 개발 될 것으로 예상된다.

참고문헌

[1] C. M. Cordeiro, H. Gossain, and D. P. Agrawal, "Multicast over Wireless Mobile Ad-hoc Networks: Present and Future Directions," IEEE Networks, pp. 52 - 59, January/February 2003.

[2] S. Banerjee, A. Misra, J. Ye, and A. Agrawala, "Energy-Efficient Broadcast and Multicast Trees for Reliable Wireless Communications," in Proc. of IEEE WCNC, March 2003.

[3] J. E. Wieselthier, G. D. Nguyen, and A. Ephermides, "Multicasting in Energy-Limited Ad-hoc Wireless Networks," in Proc. of IEEE MILCOM, pp. 18 - 21, October 1998.

[4] H. Jiang, S. Cheng, Y. He, and B. Sun, "Multicasting along Energy-Efficient Meshes in Mobile Ad-hoc Networks," in Proc. IEEE WCNC, pp. 807 - 811, March 2002.

[5] C. Tang, C. S. Raghavendra, and V. Prasanna, "Energy Efficient Adaptation of Multicast Routing Protocols in Power-Controlled Wireless Ad-hoc Networks," in Proc. of IEEE International Symposium on Parallel Architecture, Algorithms, and Networks, pp. 80 - 85, May 2002.

[6] G. D. Kondylis, S. V. Krishnamurthy, S. K. Dao, and Gregory J. Pottie, "Multicasting Sustained CBR and VBR Traffic in Wireless Ad-hoc Networks," in Proc. of IEEE ICC, pp. 543 - 549, June 2000.

[7] I. Karthigeyan, B. S. Manoj, and C. Siva Ram Murthy, "Multicast Priority Scheduling Protocol for Ad-hoc Wireless Networks," Technical Report, Department of Computer Science and Engineering, Indian Institute of Technology, January 2004.

[8] M. Kochhal, L. Schwiebert, S. Gupta, and C. Jiao, "An Efficient Core Migration Protocol for QoS in Mobile Ad-hoc Networks," in Proc. of IEEE International Conference on Performance Computing and Communications, pp. 387-391, 2002.

[9] G. Lin, and G. Noubir, "Secure Multicast over Multihop Wireless Ad-hoc Networks," in Proc. of Mobile Ad-hoc Networks Workshop (MADNET), March 2003.

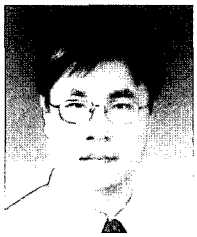
[10] L. Lazos, and R. Poovendran, "Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographical Location Information," in Proc. of IEEE International Conference on Acoustics Speech and Signal Processing, April 2003.

[11] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN:An Efficient Group Rekeying Scheme for Secure Multicast in Ad-hoc Networks," in Proc. of First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, pp. 42 - 51, August 2004.

저자소개

김 기 일

2000년 충남대학교 컴퓨터과학과 학사
2002년 충남대학교 컴퓨터과학과 석사
2005년 충남대학교 컴퓨터과학과 박사 예정
주관심분야 MANET, 센서 네트워크, 멀티캐스트, QoS



김 상 하

1980년 서울대학교 화학과 학사
1984년 University of Houston 화학과 석사
1989년 University of Houston 전산학과 박사
1989년 HNSX SuperComputer Inc. 자문위원
1990년 - 1991년 시스템 공학 연구소 선임연구원
1992년 - 현 재 충남대학교 교수
주관심분야 이동 네트워크, 인터넷 프로토콜, QoS