이동 애드혹 네트워크에서 라우팅 방식과 무관한 이기적인 노드 관리 방안

(A Routing Independent Selfish Node Management Scheme for Mobile Ad Hoc Networks)

안 상 현 † 유 영 환 †† 이 재 훈 †††
(Sanghyun Ahn) (Younghwan Yoo) (Jaewoon Lee)

요 약 현재 이동 애드혹 네트워크(mobile ad hoc network; MANET)의 라우팅 프로토콜들은 모든 노드들이 자발적으로 다른 노드들로부터의 패킷을 포워딩하는데 참여한다고 가정하고 있다. 그러나 하나의 MANET이 여러 관리 기구에 속한 노드들로 구성될 경우, 이동 노드가 자신의 에너지를 절약하기 위해서 다른 노드들로부터의 패킷을 고의적으로 포워딩하지 않을 수도 있으며 이로 인해 네트워크 성능이 저하될 수 있다. 본 논문에서는 노드가 자발적으로 패킷 포워딩에 참여하도록 하는 PIFA(Protocol-Independent Fairness Algorithm)라는 크레딧 지불(credit payment) 기법을 제안한다. DSR과 같은 소스 라우팅(source routing) 방식에서만 사용할 수 있었던 기존 방법들과는 달리 PIFA는 기반이 되는 라우팅 프로토콜의 종류와 무관하게 사용될 수 있다. 시뮬레이션을 통해, PIFA가 이기적인(selfish) 노드로 하여금 패킷 포워딩에 참여하게 함으로써 네트워크 성능이 저하되지 않게 함을 알았다.

키워드 : 이동 애드혹 네트워크, 이기적인 노드, 크레딧 지불 기법

Abstract Existing routing protocols for mobile ad hoc networks (MANETs) have assumed that all nodes voluntarily participate in forwarding others' packets. In the case when a MANET consists of nodes belonging to multiple organizations, mobile nodes may deliberately avoid packet forwarding to save their own energy, resulting in network performance degradation. In this paper, to make nodes volunteer in packet forwarding, a credit payment scheme called Protocol-Independent Fairness Algorithm (PIFA) is proposed. PIFA can be utilized irrespective of the type of basic routing protocols, while previous methods are compatible only with source routing mechanisms like DSR. According to simulation results, we can know that PIFA can prevent network performance degradation by inducing selfish nodes to participate in packet forwarding.

Key words : Mobile ad hoc network, Selfish node, Credit payment scheme

1. 서 론

이동 애드혹 네트워크(mobile ad hoc network; MANET)는 고정된 통신 인프라스트럭쳐나 기지국(base station)이 없는 무선 네트워크이다. 고속의 이동성이나 제한된 배터리 전력과 같은 이동 기기의 특징으로 인해 MANET에서의 라우팅은 유선 네트워크에서의 라우팅과 차이가 있다. 가장 대표적인 MANET 라우팅 프로토콜로는 AODV[1]와 DSR[2]이 있다. AODV는 RREQ(route request) 메시지를 브로드캐스트함으로써 새로운 경로를 발견하는 반면, DSR은 소스 라우팅을 수행한다.

LBAR(Load-Balanced Ad hoc Routing)[3], DLAR (Dynamic Load-Aware Routing)[4], SLA(Simple

· 본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업의 지원에 의한 것임
· This research was partially supported by the MIC(Ministry of Information and Communication), Korea, under the Chung-Ang University HNRC-ITRC(Home Network Research Center) support program supervised by the IITA(Institute of Information Technology Assessment)
† 종신회원 : 서울시립대학교 컴퓨터과학부
ahn@venus.uos.ac.kr
(Corresponding author)
†† 비 회 원 : University of Cincinnati, Dept. of ECECS post doc.
ymomo@ececs.uc.edu
††† 종신회원 : 동국대학교 정보통신공학과
jaehwoon@dongguk.edu
논문접수 : 2005년 10월 8일
심사완료 : 2005년 12월 21일

Load-balancing Approach)[5]와 같은 라우팅 방식들에서는 MANET 환경에서의 부하 균등화(load balancing)를 고려하고 있다. LBAR과 DLAR은 네트워크 트래픽 상황을 검사함으로써 부하가 가장 작은 경로를 찾으려고 하는 반면, SLA는 사용되는 라우팅 프로토콜과 무관하게 동작할 뿐만 아니라 트래픽이 병목 지점을 우회하도록 하는 추가적인 모듈로 정의된다.

상기한 알고리즘들은 모두, MANET에 있는 모든 노드들이 공통의 목적을 갖고 자발적으로 다른 노드들로부터의 패킷을 포워딩해준다고 가정하고 있다. MANET은 원래 구조 작업이나 전쟁터와 같이 위험한 곳에서 사용(즉, 모든 노드가 한 관리 기구에 의해서 관리됨)되도록 설계되었기 때문에 이러한 가정이 타당하다고 볼 수 있다. 그러나 요즘은 MANET이 다양한 민간 응용을 지원할 것으로 예상되기 때문에 노드들이 단일 관리 기구에 속하지 않을 수도 있다. 따라서 일부 이기적인(selfish) 노드들이 다른 노드들과 협력하지 않을 수도 있고 또한 자신의 에너지를 절약하기 위해서 다른 노드들로부터의 패킷을 포워딩하려고 하지 않을 수도 있다. 이런 상황에서는 위에서 언급한 라우팅 프로토콜들이 제대로 동작하지 못할 수도 있다.

이런 일이 발생하지 않도록 [6]에서는 PPM(Packet Purse Model)과 PTM(Packet Trade Model)을 제안했으며, 이 제안들은 이기적인 노드 방지 방법에 상업 거래 개념을 처음으로 도입하였다. 다른 노드에 포워딩 서비스를 제공하는 노드는 너글렛(nuglet)[1]이라는 가상의 화폐로 보상을 받으며, 서비스를 받으려는 노드는 이 비용을 지불해야 한다. 다른 노드의 패킷을 포워딩한 노드들에게 너글렛이 지급되는 것은 PPM과 PTM에서 동일하나 이 비용을 최종적으로 누가 책임질 것인가는 두 모델에서 차이가 있는데, PPM에서는 전송 패킷의 송신자 노드가, PTM에서는 최종 목적지 노드가 지불하게 된다. 두 방법의 동작 방식을 살펴보면, 우선 PPM에서는 송신자 노드가 패킷을 전송할 때 너글렛을 패킷에 담아 전송하면 중간 노드들이 정해진 비용을 차감한 후 다음 노드로 포워딩한다. 너글렛이 부족하여 비용을 받을 수 없는 경우에는 중간 노드에서 패킷이 버려질 수 있으므로, 송신자 노드는 목적지까지의 거리를 고려하여 충분한 양의 너글렛을 담아야 한다. 이처럼 목적지까지의 경로와 거리를 알아야 한다는 제약 때문에 PPM은 DSR과 같은 송신자 경로 지정 방법과만 사용될 수 있다. 반면, PTM에서는 각각의 중간 노드가 이전 노드로부터 패킷을 사서 다음 노드에게 더 비싼 값에 파는 방식으로 패킷 전달이 이루어진다. 최종적으로는 목적지 노드가 모든 비용을 지불하는 방식이므로, 송신자 노드가 미리 경로를 파악하여 너글렛을 담을 필요가 없어서 다양한 경로 배정 방법과 함께 사용될 수 있다. 하지만, 송신자 노드가 패킷 전송에 대해 아무런 비용도 지불하지 않는 방식이므로, 서버에 과부하를 걸리게 할 목적으로 불필요한 데이타를 무한정 전송하는 Denial-of-Service(DoS) 공격의 대상이 될 수 있다. 그외에도 PPM과 PTM 방법의 공통적인 문제점이 있는데, 각 노드가 갖고 있는 너글렛의 유효성에 관한 문제이다. 너글렛 정보가 각각의 노드에 저장되므로, 각 노드는 이미 사용한 너글렛을 다시 사용하려 할 수도 있고 패킷 전송시 자신이 가져야 할 정당한 양보다 더 많은 너글렛을 차감할 수도 있다. 이를 위해 PPM/PTM 에서는 각 노드가 특수 칩(chip)이나 스마트 카드와 같은 손상 방지 보안 모듈(tamper resistant security module)을 가지고 있는 것으로 가정하고 있으나, 이런 가정이 PPM/PTM 방법이 널리 채택되지 못하는 주요 이유가 되고 있다.

Sprite(a simple, cheat-proof, credit-based system)[7]의 경우도 패킷을 포워딩한 노드에게 인센티브로 크레딧(credit)을 준다. PPM이나 PTM과 달리 손상 방지 하드웨어가 필요없는 대신 CCS(Credit Clearance Service)라고 하는 MANET 외부에 고정된 크레딧 관리 서버가 필요하다(그림 1 참조). Sprite 방식에서의 노드들은 패킷을 하나 받을 때마다 그에 해당하는 영수증(receipt)을 보관하고 있다가 시시때때로 제어 채널을 통해 CCS에게 전달한다. CCS는 이 영수증 내용에 기반하여 영수증 전송 노드의 직전 노드에게 패킷 전달의 대가로 크레딧을 지급하고, 대신 패킷 송신 노드에게서 크레딧을 받는다. 그런데, CCS가 중간 노드에게 지급하는 크레딧과 송신 노드에게서 차감하는 크레딧의 양이 항상 같은 것은 아니다. Sprite는 노드들이 모의하여 더 많은 크레딧을 받기 위해 CCS를 속이는 것을 막기 위해 기만 방지(cheat-proof) 알고리즘을 가지고 있는데, 이는 일단 송신자 노드에게서 중간 노드들에서 필요한 크레딧보다 더 많은 크레딧을 차감했다가 각 노드들의 영수증 내용이 일치하면 되돌려 주는 방식으로 동작한다. CCS를 속이려는 갖가지 시도에 대비하여 다양한 알고리즘을 갖고 있어서 어떠한 시도도 해당 노드들의 크레딧에 손실만을 줄뿐이므로 노드들은 정직하게 보고하게 된다. 그러나, Sprite는 포워딩하는 모든 메시지에 대한 영수증을 CCS에게 보고해야 하므로 규모가 큰 MANET의 경우 큰 오버헤드가 될 수 있고, 크레딧의 손실을 감수하면서까지 MANET에 해를 가하려는 악의적인 노드들에 대한 대응책이 없다. 또한, PPM/PTM과

1) 초기 연구에서는 너겟(nugget)이라는 이름이 사용되었으나 이후 너글렛(nuglet)으로 변경되었다.

마찬가지로 소스에서 목적지까지의 전체 경로에 대한 정보를 필요로 하므로, DSR과 같은 소스 경로 배정 프로토콜에서만 사용될 수 있다.

본 논문에서는 PIFA(Protocol-Independent Fairness Algorithm)를 제안한다. PIFA는 PPM/PTM이나 Sprite과 마찬가지로 크레딧 기반의 방법이기는 하지만 이전 방법들과는 달리 기본 라우팅 프로토콜의 종류와 무관하게 동작한다. 시뮬레이션을 수행한 결과, PIFA가 이기적인 노드들로 하여금 패킷 포워딩에 참여하게 효과적으로 유도함으로써 이기적인 노드들로 인해 네트워크 성능 저하가 발생하지 않도록 함을 알았다.

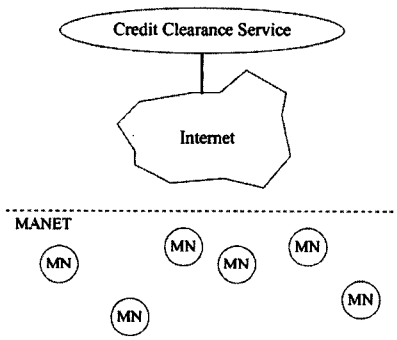


그림 1 Sprite의 구조

이 논문은 다음과 같이 구성된다. 2장에서는 PIFA의 동작에 대해서 설명하고, 3장에서는 성능 분석 결과를 보이며, 4장에서 결론을 맺는다.

2. PIFA(Protocol-Independent Fairness Algorithm)

지금까지는 한 MANET에 속한 노드들이 모두 단일 관리 기구에 의해서 관리되고 공통의 목표를 위해 협력한다고 가정해왔다. 그러나 최근에는 이기적인 노드들이 자신의 전력을 절약하기 위해서 다른 노드들의 패킷을 포워딩하지 않을 수도 있다는 문제가 제기되었다. 따라서 본 논문에서는 이기적인 노드들을 배제하거나 또는 이들이 패킷 포워딩에 자발적으로 참여하도록 하기 위한 크레딧 기반의 지불 기법을 제안한다. PPM/PTM [6]과 Sprite[7]는 소스에서 목적지로의 전체 경로 정보를 필요로 하기 때문에 DSR과 같은 소스 라우팅 프로토콜에서만 사용될 수 있는 반면, PIFA는 라우팅 프로토콜의 종류와 무관하게 사용될 수 있다.

2.1 제안된 알고리즘

PIFA를 사용하는 MANET 노드의 경우, 다른 노드들의 패킷을 포워딩함으로써 획득한 크레딧이 충분할 때만 패킷을 송신할 수 있다. PIFA는, 실제로 받게 되는 크레딧보다 더 많은 크레딧을 받기 위해 거짓 보고를 하는 단일의 악성(malicious) 노드를 검출하고 격리시킬 수 있다. 둘 이상의 노드가 공모(collusion)하지 않을 경우, PIFA는 여러 개의 악성 노드도 검출할 수 있다. PIFA에서는 노드들이 소스에서 목적지까지 전체 경로를 알고 있지 않아도 되며, 두 노드 간의 단일 홉 패킷 전송은 항상 성공한다고 가정한다.

PIFA에서는 CDB(Credit Database)를 관리하는 CM (Credit Manager)이라는 서버를 필요로 한다. MANET 노드들은 일정 주기 간격으로 CM에게 자신이 포워딩한 패킷 수를 보고한다. CM은 이들 정보가 신뢰할 수 있는 것인지 검증하고 신뢰할 수 있으면 이들 정보로부터 MANET의 현재 토폴로지를 유추해낸다. 에너지가 많은 노드나 또는 유선 네트워크에 연결되어 있는 AP (access point) 등이 CM이 될 수 있다.

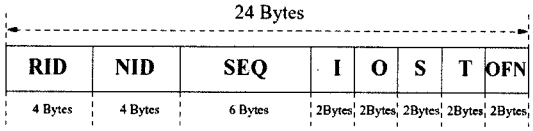


그림 2 CM으로의 보고 메시지 형식

그림 2는 MANET 노드가 자신의 이웃 노드 각각에 대해 CM에게 보내는 보고 메시지(report message)의 형식을 보인다. 각 필드의 의미는 다음과 같다:

- RID: 보고의 ID
- NID: 이웃 노드의 ID
- SEQ: 보고 메시지들을 동기화시키기 위한 현재 보고의 순서 번호
- I: 해당 이웃으로부터의 입력 패킷 수
- O: 해당 이웃으로의 출력 패킷 수
- S: 해당 이웃으로의 출력 패킷들 중에서 이 노드로부터 송신된 패킷 수
- T: 해당 이웃으로부터의 입력 패킷들 중에서 이 노드가 최종 목적지인 패킷 수
- OFN: 해당 이웃으로부터의 입력 패킷들 중에서 이 이웃이 송신한 패킷 수

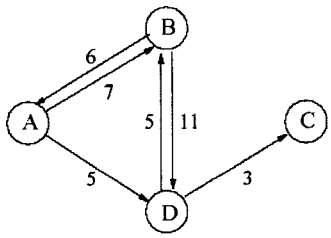
그림 3(a)는 CM으로의 보고 메시지들을 보여준다. 동일한 순서 번호를 갖는 보고 메시지들을 수집한 CM은 이들 보고의 신빙성 여부 검증을 위해 세 가지 검사를 수행한다. 첫 번째 검사는, 한 노드로부터의 출력 패킷 수가 상대방 노드로의 입력 패킷 수와 같아야 한다는 것이다. 예를 들어, 노드 n과 m이 서로 이웃이고 $Q_{n,m}$이 RID와 NID가 각각 n과 m인 메시지의 Q 필드인 경우 다음 조건을 만족해야 한다:

$$O_{n,m} = I_{m,n} \quad (1)$$

두 번째 검사는, F_n이 일정 주기 동안 노드 n이 포워

RID	NID	SEQ	I	O	S	T	OFN
A	B	128	6	7	7	2	2
A	D	128	0	5	1	0	0
B	A	128	7	6	2	3	7
B	D	128	5	11	7	1	3
C	D	128	3	0	0	3	2
D	A	128	5	0	0	4	1
D	B	128	11	5	3	9	7
D	C	128	0	3	2	0	0

(a) CM으로의 보고 메시지들



(b) (a)의 보고 메시지들로부터 계산된 토폴로지

그림 3 보고들로부터 현재 토폴로지의 계산 절차

딩한 패킷 수이고 A_n이 노드 n의 이웃 노드들의 집합인 경우, 다음 조건을 만족해야 한다는 것이다:

$$F_n = \sum_{m \in A_n} I_{n,m} - \sum_{m \in A_n} T_{n,m} = \sum_{m \in A_n} O_{n,m} - \sum_{m \in A_n} S_{n,m} \quad (2)$$

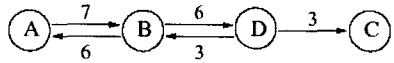
이 식은, 한 노드에서의 총 입력 패킷 수($\sum I$)와 총 종료(terminated) 패킷 수($\sum T$) 간의 차이가 포워딩 패킷 수와 같아야 하고, 또한 총 출력 패킷 수($\sum O$)와 총 송신 패킷 수($\sum S$) 간의 차이가 포워딩 패킷 수와 같아야 한다는 것이다. 노드 n은 F_n에 비례해서 CM으로부터 크레딧을 획득하며, $\sum S \times H_{avg}$(여기서 H_{avg}는 네트워크 내 임의의 두 노드 간의 평균 홉 수이다)만큼의 크레딧이 소모된다(실제로는 패킷이 목적지에 도달할 때까지의 경유 노드 수에 비례해서 크레딧이 소모되어야 하지만, AODV의 경우 전체 경로에 대한 정보가 없기 때문에 경로의 평균 홉 수를 기준으로 한다). 크레딧에 대한 정보는 CM에 의해서만 계산되고 저장된다. 만일 어떤 노드의 크레딧이 τ_c 값보다 작아지면, CM은 그 노드에게 다른 노드들의 패킷을 포워딩함으로써 크레딧을 획득하게끔 경고 메시지를 발송하고 이 노드를 블랙리스트에 등록하며, 블랙리스트에 대한 정보를 주기적으로 모든 MANET 노드들에게 전송한다. 크레딧이 τ_c보다 커질 때까지 이 경고 메시지는 주기적으로 발송되며, 블랙리스트에 있는 노드로부터 전송된 패킷은 다른 MANET 노드들에 의해서 포워딩되지 않는다. 블랙리스트 상의 노드는 크레딧이 τ_c 이상이 되어야만 블랙리스트에서 제외된다.

세 번째 검사는, S가 다음 홉 노드의 OFN과 동일해야 한다는 것이다. OFN의 목적은 악성 노드가 수식 (2)의 $\sum I$와 $\sum S$를 모두 변경함으로써 포워딩 패킷 수 F_n을 조작하지 못하도록 하기 위한 것이다. OFN은 해당 이웃 노드들로부터의 입력 패킷들 중에서 이들로부터 송신된 패킷의 수이다. 만일 어떤 한 주기에 보고된 정보들이 위의 세 가지 검사를 모두 통과하면, CM은 이들 보고로부터 그림 3(b)와 같은 토폴로지를 유추해낸다. 이 토폴로지는 노드 이동성으로 인해 실제 현재 토폴로지와 일치하지는 않지만 포워딩 패킷 수를 계산하는데 있어서는 문제가 되지 않는다. 이 토폴로지는 라우팅에 사용되는 것이 아니고 단지 노드들이 전송한 보고가 신빙성이 있는지 여부를 검사하는데 사용된다. 두 노드가 서로 상대로부터의 전송 범위에 현재 있는지 여부와 무관하게, 만일 이 주기 동안 이들 간에 교환된 패킷 수가 서로 일치하면, 이들 두 노드로부터의 보고는 위의 신빙성 검사를 통과하게 된다. 어떤 한 주기의 전반부에 그림 4(a)와 같이 노드가 분포되어 있었고 주기 후반부에는 노드들이 이동해서 그림 4(b)와 같이 분포된 경우, 현재 노드 위치와는 무관하게 그림 4(a)와 그림 4(b)를 합침으로써 그림 4(c)와 같은 토폴로지를 유추해낼 수 있다.

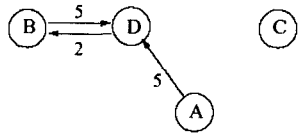
PIFA를 사용하는 MANET의 경우, 노드들은 자신의 패킷을 전송하기 위해서 크레딧이 필요하기 때문에 다른 노드들의 패킷을 고의로 포워딩하지 않을 수 없다. 초기에 CM은 일정량의 크레딧을 모든 노드들에게 할당해줌으로써 노드들이 패킷을 전송할 수 있도록 해준다.

2.2 악성 노드의 검출

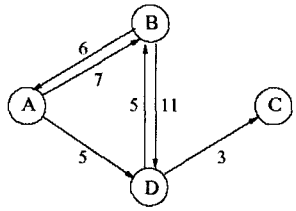
한 노드의 S가 다음 홉 노드의 OFN과 일치하지 않는 경우, 대부분의 경우 다음 홉 노드가 이전 노드의 포워딩 패킷 수를 속일 이유가 없기 때문에 CM은 OFN이 맞는다고 믿는다. 그러나 경우에 따라서는 네트워크에 혼동을 주기 위해서 다음 홉 노드가 거짓 정보를 고의로 보낼 수도 있다. 따라서 PIFA는 신빙성 검사를 통해 악성 노드를 검출해야 하며, 이를 위해 CM은 그림 5와 같은 불일치 보고 테이블(Inconsistency Record



(a) 주기 전반부의 토폴로지



(b) 주기 후반부의 토폴로지



(c) 통합된 토폴로지

그림 4 노드 이동성을 고려한 토폴로지 계산

Table; IRT)을 유지한다. 이 테이블에는 각 노드의 보고 조작 횟수가 기록되어 있으며, 여기서 $m_{i,j}$는 노드 i가 자신과 노드 j 간의 패킷 입출력 정보를 CM에게 거짓 보고한 횟수인 NAM(Numbers of Alleged Manipulation)에 해당한다. 가장 오른쪽 열은 각 노드의 총 NAM을 나타내며, 만일 이 값이 주어진 임계치 이상이 되면 이 노드는 네트워크에서 제외된다. 다른 노드들은 이 노드로부터의 패킷을 무시할 뿐만 아니라 이 노드가 자신의 패킷 전달을 하는 중간 노드로 사용되지 않도록 한다.

	a	b	c	d	···	Total
a	-	$m_{a,b}$	$m_{a,c}$	$m_{a,d}$	···	$\Sigma m_{a,i}$
b	$m_{b,a}$	-	$m_{b,c}$	$m_{b,d}$	···	$\Sigma m_{b,i}$
c	$m_{c,a}$	$m_{c,b}$	-	$m_{c,d}$	···	$\Sigma m_{c,i}$
d	$m_{d,a}$	$m_{d,b}$	$m_{d,c}$	-	···	$\Sigma m_{d,i}$
⋮	⋮	⋮	⋮	⋮	⋱	⋮

그림 5 불일치 보고 테이블(Inconsistency Record Table; IRT)

두 노드 a, b로부터의 보고가 일치하지 않는 경우 어느 노드가 거짓 보고를 했는지 알 수 없으며, 따라서 이들 두 노드의 NAM을 모두 1씩 증가시킨다:

$$m_{a,b} = m_{a,b} + 1$$
$$m_{b,a} = m_{b,a} + 1 \quad (3)$$

하지만 이때 피해를 보는 노드가 생길 수 있으며, 이 문제를 해결하기 위해서 PIFA에서는 a, b의 보고가 불일치하면 다른 노드들의 NAM 정보 중 a, b와 연관된 NAM 정보를 다음과 같이 반으로 줄인다:

$$m_{i,a} = \left| \frac{m_{i,a}}{2} \right|, \ \forall i \notin a, b$$
$$m_{i,b} = \left| \frac{m_{i,b}}{2} \right|, \ \forall i \notin a, b \quad (4)$$

No	Nodes
1	A-B
2	C-D
3	A-D
4	A-D
5	C-D
6	B-D

그림 6 불일치 보고 시나리오

No.1

	A	B	C	D	Total
A	-	1	0	0	1
B	1	-	0	0	1
C	0	0	-	0	0
D	0	0	0	-	0

No.2

	A	B	C	D	Total
A	-	1	0	0	1
B	1	-	0	0	1
C	0	0	-	1	1
D	0	0	1	-	1

No.3

	A	B	C	D	Total
A	-	1	0	1	2
B	0	-	0	0	0
C	0	0	-	0	0
D	1	0	1	-	2

No.4

	A	B	C	D	Total
A	-	1	0	2	3
B	0	-	0	0	0
C	0	0	-	0	0
D	2	0	1	-	3

No.5

	A	B	C	D	Total
A	-	1	0	1	2
B	0	-	0	0	0
C	0	0	-	1	1
D	2	0	2	-	4

No.6

	A	B	C	D	Total
A	-	0	0	0	0
B	0	-	0	1	1
C	0	0	-	0	0
D	2	1	2	-	5

그림 7 그림 6의 불일치 보고 시나리오에 대한 IRT의 변화

그림 4(c)의 토폴로지에서 그림 6과 같이 노드들의 보고가 일치하지 않는다고 가정하자. 노드 D가 포워딩 패킷 수를 거짓으로 보고한 악성 노드이며 NAM의 총합에 대한 임계치가 3인 경우, 불일치 보고에 대한 IRT 값의 변화가 그림 7에 나타나 있다. 1번째와 2번째 불일치 보고는 네 노드 각각의 NAM을 1 증가시킨다. 노드 A와 D의 보고가 불일치하는 3번째와 4번째의 경우 A와 D의 NAM을 1 증가시킬 뿐만 아니라 B와 C의 NAM이 A, D와 관련해서 예전에 증가되었었기 때문에 B와 C의 NAM을 반으로 감소시킨다. 노드 A와 D의 NAM이 임계치 3과 같기 때문에 A와 D는 네트워크에서 제외된다. 실제로는 노드 D가 거짓 보고를 했기 때문에 이 경우 A가 피해를 입게 되지만 5번째와 6번째 불일치가 발생하면 A는 피해 복구를 할 수 있게 된다.

3. 성능 평가

NS-2 시뮬레이터를 사용해서 PIFA의 성능을 평가했다. 시뮬레이션 환경은 1000m × 1000m 범위 내에 50개의 이동 노드가 있고 각 노드는 임의의 방향으로 최고 속도 20m/s로 이동한다. 수신 신호 세기가 거리 d에 대해 $1/d^4$인 two-ray ground reflection 모델을 사용했으며, 전송 범위와 채널 용량은 250m와 2Mbps로 각각 설정했다. MAC 프로토콜로 IEEE 802.11을 채택했으며, 유니캐스트 라우팅 프로토콜로 AODV를 사용했다. 소스와 목적지 노드 쌍은 임의로 선택되며, 각 소스는 1초마다 512 바이트 크기의 CBR 패킷을 2개 생성한다. 또한 보고 메시지는 1초마다 주기적으로 CM에게 전송된다. 초기 노드 에너지는 95Joule이며, 디폴트 NS-2 에너지 모델에 정의된 것처럼 패킷 1개를 송신 및 수신하는데 각각 0.660Joule과 0.395Joule을 소모한다. 초기 노드 크레딧은 10이며 총 시뮬레이션 시간은 1000초이고, 모든 성능 비교는 30번의 시뮬레이션에 대한 평균값을 기준으로 했다. 또한 여러 악성 노드들이 서로 공모하지 않는다고 가정했다.

그림 8은 이기적인 노드율에 따른 패킷 전송율을 보여준다. PIFA를 사용하는 경우, 이기적인 노드들은 크레딧이 필요할 때만 다른 노드들의 패킷을 포워딩한다. PIFA를 사용하지 않는 경우, 이기적인 노드들은 다른 노드들의 패킷을 포워딩하지 않는다. PIFA 사용 여부와 무관하게 이기적인 노드율이 증가하면 패킷 전송율이 감소한다. 그러나 PIFA를 사용하면 이기적인 노드율이 50%일 때조차도 패킷 전송율이 50% 이하로 떨어지지 않는다. 반면 PIFA를 사용하지 않으면 이기적인 노드율이 50%인 경우 전송율이 27.54%가 된다.

그림 9는 이기적인 노드율이 10% 또는 20%일 때의 시간의 흐름에 따른 패킷 전송율을 보여준다. PIFA를 사용하지 않는 경우, 시간이 지남에 따라 더 많은 이기적이지 않은 노드들이 에너지를 소모하게 됨에 따라 전송율이 급격히 감소한다. 반면, PIFA를 사용하는 경우, 다수의 이기적인 노드들이 초기 크레딧을 다 사용하고 거의 비슷한 시기에 패킷 포워딩에 참여하기 때문에 처음 어느 정도는 전송율이 증가하다가 그 이후에는 PIFA를 사용하지 않는 경우와 마찬가지로 전송율이 감소한다.

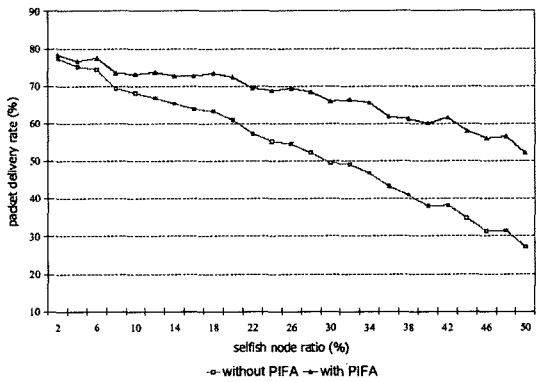


그림 8 이기적인 노드율에 따른 패킷 전송율

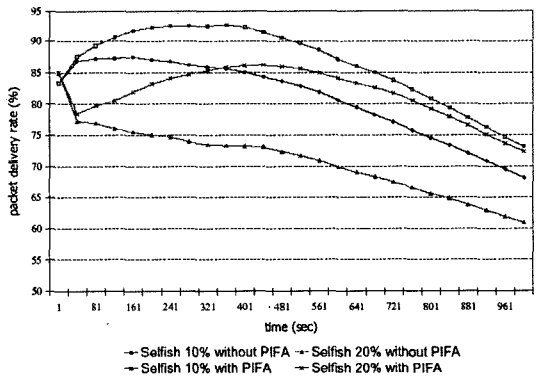


그림 9 시간의 변화에 따른 패킷 전송율의 변화

4. 결 론

본 논문에서는 이동 애드혹 네트워크에서 패킷 포워딩을 공평하게 하도록 하는 크레딧 지불 기법인 PIFA를 제안했다. PIFA에서는 이기적인 노드들이 자발적으로 다른 노드들의 패킷을 포워딩하게 함으로써 이동 장치들의 에너지가 공평하게 소모되도록 한다. PPM/PPT, Sprite와 같은 기존 크레딧 지불 기법들은 DSR과 같은 소스 라우팅 프로토콜에서만 사용될 수 있는 반면, 본 논문에서 제안한 PIFA는 라우팅 프로토콜의 종류와 무관하게 사용될 수 있다. 시뮬레이션을 통해 기반 유니캐

스트 라우팅 프로토콜로써 AODV를 사용하는 경우의 PIFA의 성능이 PIFA를 사용하지 않는 경우보다 패킷 전송율 측면에서 우수함을 보였다.

참 고 문 헌

[1] C. E. Perkins, E. M. Royer, and S. R. Das, "Ad hoc On-demand Distance Vector(AODV) Routing," IETF RFC 3561, July 2003.

[2] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet Draft, July 2004.

[3] H. Hassanein and A. Zhou, "Routing with Load Balancing in Wireless Ad Hoc Networks," ACM MSWiM, pp. 89-96, 2001.

[4] S.-J. Lee and M. Gerla, "Dynamic Load-Aware Routing in Ad Hoc Networks," IEEE ICC, pp. 3206-3210, 2001.

[5] Y. Yoo and S. Ahn, "A Simple Load-Balancing Approach in Cheat-Proof Ad-Hoc Networks," IEEE GLOBECOM, 2004.

[6] L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc Networks," ACM MobiHoc, pp. 87-96, 2000.

[7] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," IEEE INFOCOM, pp. 1987-1997, 2003.

안 상 현

1986년 서울대학교 컴퓨터공학과 졸업(학사). 1988년 서울대학교 대학원 컴퓨터공학과 졸업(석사). 1989년 9월~1993년 12월 University of Minnesota 컴퓨터학과(박사). 1988년 1월~1989년 8월 (주) 데이콤 연구원. 1994년 3월~1998년 2월 세종대학교 컴퓨터학과 교수. 1998년 3월~현재 서울시립대학교 컴퓨터과학부 교수. 관심분야는 애드혹 네트워크, 센서 네트워크, 홈 네트워크, 이동 통신, 라우팅 프로토콜 등

유 영 환

1996년 서울대학교 컴퓨터공학과 졸업(학사). 1998년 서울대학교 대학원 컴퓨터공학과 졸업(석사). 2004년 2월 서울대학교 전기컴퓨터공학부 졸업(박사). 2004년 4월~현재 Univ. of Cincinnati(Post-doc) 관심분야는 애드혹/센서 네트워크, 광통신, 인터넷

이 재 훈

1985년 한양대학교 전자공학과 졸업(학사). 1987년 한국과학기술원 전기및전자공학과 졸업(석사). 1995년 8월 한국과학기술원 전기및전자공학과 졸업(박사) 1987년 3월~1990년 4월 데이콤(연구원) 1990년 9월~1999년 2월 삼성전자 정보통신부문 선임연구원. 2000년 3월~2000년 12월 삼성전자 자문교수. 2000년 5월~현재 한국이더넷포럼 운영위원. 1999년 3월~현재 동국대학교 정보통신공학과 부교수. 관심분야는 초고속통신, 다중 액세스 프로토콜, 인터넷 프로토콜, 메트로 이더넷