

# 다중 홉 무선 네트워크에서 종단 간 신뢰성 통신을 위한 평판 기반의 협력적 라우팅 기법

김태훈<sup>†</sup>, 탁성우<sup>††</sup>

## 요 약

다중 홉 무선 네트워크에서는 일부 중계 단말이 악의적인 목적으로 비협력적이거나 이기적인 행동을 하면 네트워크의 성능이 저하되는 문제점이 발생한다. 무선 단말간의 협력적인 동작을 가정한 기존의 애드혹 라우팅 기법에서는 악의적으로 행동하는 이기적인 무선 단말에 의해 발생하는 성능 감소 문제를 해결할 수 없다. 이에 본 논문에서는 다중 홉 무선 네트워크의 성능을 향상시킬 수 있는 평판 기반의 협력적 애드혹 라우팅 프로토콜인 CARE (Cooperative Ad hoc routing protocol based REputation) 기법을 제안하였다. 제안한 CARE 기법은 홉 대 홉 기반의 패킷 포워딩 과정에서 악의적으로 행동하거나 무단으로 라우팅 경로에서 이탈하는 이기적인 무선 단말을 우회하도록 라우팅 경로를 설정하는 네트워크 계층간의 수평적 상호 작용을 제공한다. 그리고 CARE 기법은 수직적 상호 작용을 기반으로 하여 MAC 계층으로부터 획득한 무선 채널의 상황 정보를 반영하여 라우팅 경로의 품질 향상시키며, 네트워크 계층에서 획득한 무선 단말의 평판 정보를 전송 계층에 반영하여 TCP의 성능 향상을 제공한다. CARE 기법의 성능을 평가한 결과, 단말의 빈번한 이동과 악의적인 단말이 존재하는 다중 홉 무선 네트워크 환경에서 패킷 전송의 낮은 실패율과 패킷의 평균 전송 시간의 향상을 제공함과 동시에 종단간 무선 단말의 향상된 TCP 성능을 확인하였다

## A Reputation based Cooperative Routing Scheme for End-to-End Reliable Communications in Multi-hop Wireless Networks

Taehoon Kim<sup>†</sup>, Sungwoo Tak<sup>††</sup>

## ABSTRACT

If a certain relay node in multi-hop wireless networks might become a malicious node that does not cooperate with other nodes or a selfish node, network throughput will be dramatically decreased. Most of existing ad hoc routing protocols assuming that the nodes will fully cooperate with other nodes do not resolve the problem of network performance degradation due to malicious and selfish nodes. This paper presents the CARE (Cooperative Ad hoc routing protocol based REputation) scheme incorporating the reputation management that can achieve a multi-hop wireless network with high throughput performance. The proposed scheme provides the horizontal cross-layer approach which can identify misbehaving malicious, selfish nodes dropped out of the hop-by-hop based packet processing in the network and then set up an optimal packet routing path that will detour misbehaving nodes. And the vertical cross-layer approach contained in the CARE scheme attempts to improve the quality of routing paths by exploiting the quality of link information received from the MAC layer. Besides, it provides high TCP throughput by exploiting the reputation values of nodes acquired from the network layer into the transport layer. A case study on experiments and simulations shows that the CARE scheme incorporating vertical and horizontal cross-layer approaches yields better performance in terms of the low rate of packet loss, fast average packet delivery time, and high TCP throughput between end-to-end nodes.

**Key words:** Multi-hop Wireless Networks(다중 홉 무선 네트워크), Routing Protocol(라우팅 프로토콜), TCP(Transmission Control Protocol)

※ 교신저자(Corresponding Author) : 탁성우, 주소 : 부산시 금정구 장전2동(609-735), 전화 : 051)510-2387, FAX : 051)515-2208, E-mail : swtak@pusan.ac.kr  
접수일 : 2009년 3월 27일, 수정일 : 2009년 6월 5일  
완료일 : 2009년 8월 11일

<sup>†</sup> 준회원, 부산대학교 컴퓨터공학과  
(E-mail : ninkthb@hotmail.com)

<sup>††</sup> 종신회원, 부산대학교 정보컴퓨터공학부 부교수

※ 이 논문은 부산대학교 자유과제 학술연구비(2년)에 의하여 연구되었음.

## 1. 서 론

다중 홉 무선 네트워크(Multi-hop Wireless Networks)는 이동 무선 단말간의 종단간 통신을 지원하는 별도의 기간망 지원 없이 무선 이동 단말들이 자발적인 상호 협력에 의하여 구성된다. 이러한 네트워크 환경에서 무선 단말의 네트워크 계층에서는 애드혹 라우팅 프로토콜을 사용하여 무선 단말의 이동성에 따른 끊임없는 종단간 연결을 제공해야 한다. 대표적인 애드혹 라우팅 프로토콜에는 DSR (Dynamic Source Routing) [1]과 AODV (Ad hoc On demand Distance Vector) 라우팅 기법 [2]이 있다. DSR과 AODV 라우팅 기법을 포함한 기존의 애드혹 라우팅 기법은 모든 무선 단말이 패킷의 라우팅과 포워딩 과정에서 상호 협력적으로 동작하는 것을 가정하고 있다. 그러나 다중 홉 무선 네트워크를 구성하고 있는 무선 단말 중 일부가 악의적인 목적으로 다른 무선 단말에게 비협력적이거나 이기적인 행동을 하면 네트워크의 성능은 저하된다 [3]. 이와 같은 단말의 악의적이고 이기적인 무선 단말의 행동으로 인한 패킷의 손실은 종단간 전송 계층에서 동작되는 TCP (Transmission Control Protocol)의 성능에도 영향을 미친다. 소스 단말의 TCP는 악의적인 중계 단말로 인하여 발생된 패킷 손실을 네트워크 혼잡에 따른 패킷 손실로 인식하여 TCP 혼잡 윈도우 (Congestion Window)의 크기를 줄인다. 이러한 현상이 네트워크 내의 각 무선 단말에게 발생하면 결국엔 전체 네트워크의 성능이 현저히 감소되는 문제가 발생하게 된다.

한편, 다중 무선 홉 네트워크 환경은 유선 네트워크보다 비트 에러율이 높으며 무선 단말의 이동에 따른 네트워크 환경이 계속 변하기 때문에, 이러한 네트워크 환경을 고려하여 무선 네트워크의 성능을 향상시킬 수 있는 기법을 애드혹 라우팅 프로토콜은 제공할 수 있어야 한다. 그러나, 기존의 애드혹 라우팅 프로토콜인 DSR과 AODV 라우팅 기법은 하위 계층인 MAC 계층 (Medium Access Control Layer)과 상위 계층인 TCP 간의 수직적 상호 작용을 고려하지 않고 네트워크 계층에서 독립적으로 수행하기 때문에 동적으로 변하는 무선 네트워크 환경에 빠르게 대응할 수 없다.

이에 본 논문에서는 평판 기반의 협력적 애드혹

라우팅 프로토콜인 CARE (Cooperative Ad hoc routing protocol based REputation) 기법을 제안하였다. 제안 기법은 무선 단말간 신뢰성있는 통신을 지원하기 위한 수평적 상호 작용(Horizontal Cross Layer)과 다중 홉 무선 네트워크의 성능을 향상시키기 위한 수직적 상호 작용(Vertical Cross Layer)으로 구성된다. CARE 라우팅 기법의 평판 기반 수평적 상호 작용은 각 무선 단말이 이웃 단말의 패킷 라우팅 및 포워딩 행동에 대한 신뢰도(Trustworthiness)를 계산한 후에 낮은 신뢰도 값을 가진 악의적인 무선 단말을 다중 홉 무선 네트워크에서 고립시킨다. CARE 라우팅 기법의 수직적 상호 작용은 무선 채널의 상태를 고려하여 채널의 품질이 우수한 링크를 라우팅 경로에 포함시켜 동적으로 변하는 무선 네트워크의 환경 변화에 적응하도록 한다. 그리고 네트워크 계층과 상위 전송 계층인 TCP간의 수직적 상호 작용 측면에서는 각 무선 단말이 획득한 평판 정보를 반영한 TCP 혼잡 제어 기법을 사용하여 악의적인 단말에 의한 TCP 성능 저하 문제를 해결한다.

본 논문의 구성은 다음과 같다. 2장에서는 다중 홉 무선 네트워크에서의 애드혹 라우팅 프로토콜과 관련된 기존 연구와 평판 관리 기법, 그리고 TCP 혼잡 제어 기법에 대한 기존 연구를 기술한다. 3장에서는 CARE 라우팅 기법에서의 평판 기반 수평적 상호 작용에 대한 동작과 무선 채널 상태 및 TCP의 상호 의존성을 고려한 수직적 상호 작용에 대한 동작 방식을 기술한다. 그리고 4장에서는 CARE 라우팅 기법의 성능에 대한 실험을 수행하고 분석하였다. 마지막으로 5장에서는 결론을 기술하였다.

## 2. 관련 연구

본 논문에서는 다중 홉 무선 네트워크에서 악의적인 단말에 의해 발생하는 3가지 형태의 문제점을 각각 NF (No Forwarding), FR (Free Riding), FF (False Feedback)로 정의하였다. NF는 소스 단말과 목적지 단말간에 설정된 라우팅 경로상에 위치한 중계 단말이 소스 단말의 패킷을 중계하지 않고 버리는 악의적인 단말의 행위이다. FR은 라우팅 경로 설정에 참여한 이기적인 단말이 다른 단말에서 보낸 패킷을 포워딩 하지 않고 자신의 패킷만 보내는 행위이다. FF는 악의적인 행동을 하는 무선 단말에게 좋은

평가를 주거나 협력적인 무선 단말에게 나쁜 평가를 주는 행위이다.

이러한 문제점과 연관된 기존의 연구로는 패킷 송수신에 대한 가격 결정 정책(Pricing Policy) 기반의 다중 홉 무선 네트워크 플랫폼과 평판 기반의 다중 홉 무선 네트워크 플랫폼이 있다. 패킷 송수신에 대한 가격 결정 기법으로는 PPM (Packet Purse Model) 및 PTM (Packet Trade Model) 기법 [4], MFEF (Microeconomic Framework for Enabling Forwarding) 기법 [5], 그리고 Sprite 기법 [6]이 있다. 그리고 대표적인 평판 기법으로는 CORE (Collaborative Reputation) 기법 [7]과 CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks) 기법 [8]이 있다.

가격 결정 기법은 기본적으로 패킷을 송수신하는데 필요한 가상 통화(Virtual Currency)의 비용을 책정한 후에 중계 단말이 패킷의 라우팅 및 포워딩을 정상적으로 처리하면 참조논문 [4]에서 도입한 Nugget과 같은 가상 통화의 양을 증가시킨다. 그리고 각 단말은 패킷을 정상적으로 송수신하는데 가상 통화를 지불해야 하며, 가상 통화의 양이 많을수록 패킷 송수신의 기회가 증가한다. 이러한 가격 결정 정책은 다중 홉 무선 네트워크에 있는 각 단말이 패킷의 라우팅 및 포워딩을 담당하는 중계 단말로 참여할 것을 독려하여 NF 문제를 해결함과 동시에 네트워크의 성능을 증가시키고자 한다. 그러나 적절한 패킷 송수신의 가상 통화 비용을 결정하기가 어려우며 가상 통화의 양을 공평하게 결정 및 분배와 관리를 하는 중앙 시스템이 있어야 함과 동시에 이러한 중앙 시스템의 배치문제를 해결하기가 어려운 단점이 있다.

CORE 기반의 평판 기법은 단말 간의 다중 홉 무선 네트워크에서 중계 단말이 자신의 패킷만을 송신하고 이웃 단말로부터 전달 받은 패킷은 버리는 이기적이고 악의적인 행동을 막고자 제안하였다. 그리고 CONFIDANT 기법은 악의적으로 행동하는 단말을 격리시킬 수 있는 평판 기법을 DSR 라우팅 기능에 포함시켜 제안하였다. 그러나 CORE와 CONFIDANT는 상대 단말에 대하여 거짓 평가를 수행하는 악의적인 단말의 FF 문제를 고려하지 않았다. 참조 논문 [9] 역시 DSR 라우팅 기능에 평판 기법을 포함시켜 제공한다. 참조 논문 [10]에 의하면 이러한 기법들은 패킷

을 버리는 악의적인 단말이 라우팅 경로에 참가할 수 있기에 악의적인 단말을 네트워크로부터 격리시킬 수가 없다는 문제점이 있다. 이에 본 논문에서 제안하는 CARE 기법은 네트워크의 성능을 향상시키기 위하여 NF, FR, FF 문제를 모두 고려하는 평판 기반의 수평적 협력 방식을 사용한다.

한편 네트워크 계층의 입장에서 하위 계층인 MAC 계층과 상위 계층인 TCP 계층간의 수직적 상호 작용에 대하여 살펴보면 다음과 같다. 먼저 참조 논문 [11-13]에서 기술한 바와 같이 채널의 품질이 계속 변화하는 무선 네트워크의 성능을 향상시키기 위해서는 MAC 계층과 다른 계층간의 의존성이 있는 정보 교환을 통하여 네트워크 성능을 향상시킬 수 있음을 기술하였다. 본 논문에서는 MAC 계층으로부터 획득한 무선 채널 정보를 CARE 라우팅 기법에 반영하였다.

한편, TCP가 다중 홉 무선 네트워크에서 동작할 때 발생할 수 있는 문제점을 살펴보면 다음과 같다. 먼저, 유선 네트워크의 환경을 고려하여 설계된 TCP는 악의적인 중계 단말의 동작으로 인한 패킷 손실은 네트워크의 혼잡에 의하여 발생된 것이라고 판단하여 TCP의 혼잡 윈도우 크기를 줄인다 [14-15]. 이는 네트워크의 성능 감소를 유발시킨다. 그리고 동적으로 변하는 무선 채널의 환경과 무선 단말의 잦은 이동으로 인한 라우팅 경로의 잦은 결손이 발생한다. 만약 라우팅 경로의 재설정 시간이 소스 단말의 TCP에서 설정되어 있는 RTO (Retransmission Time-Out) 값보다 길어지면, 소스 단말의 TCP는 혼잡 윈도우 크기를 초기화한 후에 패킷을 재전송하게 되어 TCP의 성능이 감소하게 된다.

또한, 무선 네트워크에서 고려되는 라우팅 경로의 특성으로는 라우팅 경로의 길이와 비대칭적인 단방향 링크(Asymmetric Uni-directional Link)의 동작이다. 라우팅 경로의 길이가 길어질수록 라우팅 경로의 결손 확률이 높아져 패킷 손실이 발생할 가능성이 커지고 이로 인하여 소스 단말의 TCP 혼잡 윈도우 크기가 감소하게 되어 네트워크의 성능이 저하될 수 있다. 이러한 문제점과 연관된 기존의 연구로는 TCP-F (TCP-Feedback) [16], TCP-ELFN (TCP-Explicit Link Failure Notification) [17], 그리고 ATCP (Ad-hoc TCP) [18] 기법이 있다. 그러나 이러한 기법에는 기존의 TCP 기법을 수정하기 때문에

기존 TCP간의 호환성 문제가 존재한다.

본 논문에서 제안한 CARE 기법은 네트워크 계층에서 획득한 무선 단말의 평판 정보를 반영하여 전송 계층을 담당하는 TCP의 성능을 향상시켜 수직적 상호 작용의 효율성을 지원한다.

### 3. CARE (Cooperative Ad-hoc routing protocol based REputation) 라우팅 기법

#### 3.1 CARE 라우팅 기법의 구조

그림 1은 본 논문에서 제안하는 CARE 라우팅 기법의 구조를 보여준다. CARE 라우팅 기법에서 수평적 상호 작용은 라우팅 경로 탐색 단계, 데이터 포워딩 단계, 그리고 평판 정보 관리 단계로 구성된다. 그리고 CARE 라우팅 기법에서 수직적 상호 작용은 다중 홉 무선 네트워크 환경을 라우팅 경로 탐색에 적용하는 단계와 평판 정보 관리 단계에서 획득한 평판 정보를 TCP 혼잡 제어 기법에 적용하는 단계로 구성된다.

그림 1에서 보는 바와 같이 CARE 라우팅 기법의 수직적 상호 작용을 살펴보면 다음과 같다. 다중 홉 무선 네트워크의 MAC 계층 정보를 기반으로 소스 단말과 목적지 단말간에 생성 가능한 다수의 라우팅 경로 중에서 가상 링크의 품질이 가장 좋은 라우팅 경로를 선택한다. 그리고 무선 단말의 이동이나 무선 채널의 품질 변화 때문에 라우팅 경로의 품질이 저하 되면 기존의 라우팅 경로가 손실되기 전에 새로운 라우팅 경로를 확보한다. 또한 이웃 단말에게 패킷을 중계하지 않는 악의적인 단말에 의해 발생된 패킷 손실은 TCP의 성능을 감소시킬 수 있다. 이러한 문제를 해결하기 위하여 소스 단말은 평판 정보 관리 단계에서 획득한 다른 무선 단말의 평판 정보를 자신의 TCP 혼잡 제어 기법에 적용시켜 TCP 전송률을

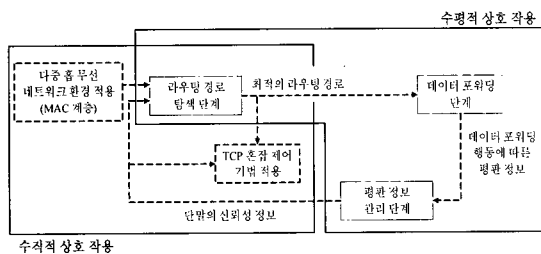


그림 1. CARE 라우팅 기법의 구조

제어한다.

#### 3.2 CARE 라우팅 기법의 수평적 상호 작용

이 절에서는 CARE 라우팅의 수평적 협력 기법에 대하여 설명한다. 먼저 수평적 협력 기법에서 사용하는 용어와 기호를 정의한다. CARE 라우팅의 수평적 협력 기법에서 각 단말은 이웃 단말이 악의적으로 행동하는지 판단하기 위하여 평판 정보를 사용하여 신뢰도를 계산한다. 평판 정보는 직접적 평판 정보와 간접적 평판 정보로 구분된다. 그림 2는 CARE 라우팅의 수평적 상호 작용에서 각 단말이 이웃 단말의 직접적 평판 정보와 간접적 평판 정보를 획득하는 과정이다. 그림 2에서는 단말 A가 단말 I에게 데이터를 전송하기 위한 라우팅 경로(LLID<sub>1</sub>로 표기)와 단말 G가 단말 C에게 데이터를 전송하기 위한 라우팅 경로(LLID<sub>2</sub>로 표기)가 설정되어 있다고 가정한다. 그림 2의 단계 (1)에서와 같이 직접적 평판 정보는 각 단말이 이웃 단말의 포워딩 행동을 직접 관찰한 결과이다. 무선 네트워크 환경에서 각 단말은 이웃 단말이 전송한 패킷을 수신할 수 있기 때문에 다중 홉 단말이 전송한 패킷의 유효성을 검사할 수 있다. 간접적 평판 정보는 그림 2의 단계 (2)에서와 같이 이웃 단말의 포워딩 행동을 직접 관찰한 단말로부터 받은 평판 정보이다.

각 단말은 직접 및 간접 평판 정보를 기반으로 이웃 단말의 신뢰도를 계산한다. CARE 라우팅의 수평적 상호 작용에서는 두 가지 신뢰도 정보인 STT (Short-Term Trustworthiness)와 LTT (Long-Term Trustworthiness)를 사용한다. STT는 각 단말의 악의적인 행동을 판단하는 기준으로 짧은 시간 동안 각 단말의 포워딩 행동을 계산한 값이다. 다중 홉 무선 네트워크 환경에서는 단말의 행동이 시간에 따라

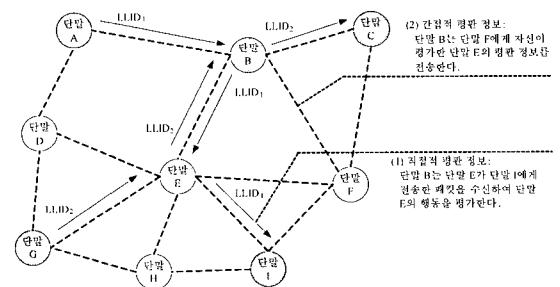


그림 2. CARE 라우팅 기법에서 평판 정보를 획득하는 과정

표 1. CARE 라우팅의 수평적 상호 작용에서 사용되는 인자

기 호	설 명	기 호	설 명
$NA$	다중 홉 네트워크에 있는 이동 단말의 집합	$N$	네트워크에 있는 이동 단말의 집합
$t_0$	시스템의 초기 시작 시각	$t_n$	인접 단말이 번째 패킷을 포워딩한 시점
$Neighbor(A)$	무선 단말 A의 이웃 단말 집합	$RM_{A,B}(t_n)$	시각 $t_n$ 에서 단말 A가 단말 B를 평가한 평판 값
$CGR_{A,B}(t_n, t_{n+1})$	시각 $t_n$ 부터 시각 $t_{n+1}$ 까지 단말 A가 단말 B를 평가한 좋은 평판 값의 합	$CBR_{A,B}(t_n, t_{n+1})$	시각 $t_n$ 부터 시각 $t_{n+1}$ 까지 단말 A가 단말 B를 평가한 나쁜 평판 값의 합
$CGR_{A,B}^{short-term}(t_n)$	시각 $(t_n - TN_{short-term})$ 부터 시각 $t_n$ 까지 단말 A가 단말 B를 평가한 좋은 평판 값의 합	$CBR_{A,B}^{short-term}(t_n)$	시각 $(t_n - TN_{short-term})$ 부터 시각 $t_{n+1}$ 까지 단말 A가 단말 B를 평가한 나쁜 평판 값의 합
$STT_{A,B}(t_n)$	시각 $t_n$ 에서 단말 A가 단말 B를 평가한 STT 값	$LTT_{A,B}(t_n)$	시각 $t_n$ 에서 단말 A가 단말 B를 평가한 LTT 값

일시적으로 악의적 혹은 협력적으로 변할 수 있기 때문에 CARE 라우팅의 수평적 협력 기법에서는 각 단말이 행동한 포워딩 결과에 따라 각 단말의 STT를 평가한다. 4장의 실험에서 사용한 STT의 평가 주기 값( $TN_{short-term}$ )은 60초로 설정하였다. LTT는 각 단말이 초기에서 현재 시점까지 행동한 포워딩 결과를 평가한 값으로 각 단말의 장기간 신뢰성에 대한 평판 정보를 나타낸다.

CARE 라우팅의 수평적 상호 작용에 사용되는 공식 (1)부터 (6)에 사용되는 인자는 표 1과 같다. 표 1에서 단말 B가 협력적으로 행동하면  $RM_{A,B}(t_n)=1$ 이고, 단말 B가 악의적으로 행동하면  $RM_{A,B}(t_n)=-1$ 이다.

CARE 라우팅의 수평적 상호 작용에 대한 절차는 그림 3과 같다. 먼저, 단말 A는 단말 B에게 패킷을 전송한다 (그림 3의 단계 (1)). 중계 단말 B는 수신한

패킷을 이웃 중계 단말 C에게 전송한다. 이 때 단말 A도 중계 단말 B가 전송한 패킷을 수신할 수 있기 때문에 단말 B의 포워딩 행동을 평가하여 중계 단말 B의 평판 정보를 계산한다. 만약 단말 B가 단말 A로부터 받은 패킷을 전송하지 않거나 조작하여 전송하면 단말 A는 단말 B를 악의적인 단말로 판단하여 나쁜 평가를 부여하며, 그렇지 않은 경우에는 좋은 평가를 부여한다 (그림 3의 단계 (2)). 그리고 단말 A는 단말 B의 평판 정보인  $CGR_{A,B}(t_0, t_n)$ ,  $CBR_{A,B}(t_0, t_n)$ ,  $CGR_{A,B}^{short-term}(t_n)$ ,  $CBR_{A,B}^{short-term}(t_n)$ ,  $STT_{A,B}(t_n)$ , 그리고  $LTT_{A,B}(t_n)$ 을 수정한다 (그림 3의 단계 (3)).  $t_0$ 는 시스템의 초기 시작 시간이고  $t_n$ 은 현재 시각을 나타낸다. 그리고  $t_{n-1}$ 은  $t_n$  직전에 평판 정보를 수정한 시각이다.  $CGR_{A,B}(t_0, t_n)$ 과  $CBR_{A,B}(t_0, t_n)$  및  $LTT_{A,B}(t_n)$ 은 수식 (1), 및 수식 (2), 그리고 수식 (3)과 같이 계산된다.

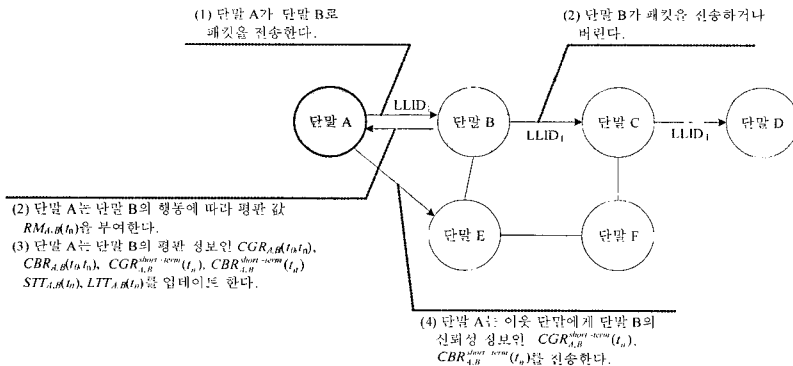


그림 3. CARE 라우팅의 평판 관리 기법

$$CGR_{A,B}(t_0, t_n) = CGR_{A,B}(t_0, t_{n-1}) + RM_{A,B}(t_n) \quad (1)$$

(단,  $RM_{A,B}(t_n) = 1$ )

$$CBR_{A,B}(t_0, t_n) = CBR_{A,B}(t_0, t_{n-1}) + RM_{A,B}(t_n) \quad (2)$$

(단,  $RM_{A,B}(t_n) = -1$ )

$$LTT_{A,B}(t_n) = \max(0, \frac{CGR_{A,B}(t_0, t_n) - |CBR_{A,B}(t_0, t_n)|}{CGR_{A,B}(t_0, t_n) + |CBR_{A,B}(t_0, t_n)}) \quad (3)$$

$CGR_{A,B}^{short-term}(t_n)$ 과  $CBR_{A,B}^{short-term}(t_n)$ 는  $STT_{A,B}(t_n)$ 를 계산하기 위하여 사용되는 값으로 각각 수식 (4) 및 수식 (5)와 같이 계산된다.

$$CGR_{A,B}^{short-term}(t_n) = \begin{cases} \text{if } RM_{A,B}(t_n) = -1 \\ CBR_{A,B}(t_n - TN_{short-term}, t_{n-1}) \\ + \sum_{i \in Neighbor(A)} LTT_{A,i}(t_n) CGR_{i,B}^{short-term}(t_n) \quad (4-1) \\ \text{if } RM_{A,B}(t_{n-1}) = -1 \text{ and } RM_{A,B}(t_n) = 1 \\ CBR_{A,B}(t_n - TN_{short-term}, t_{n-1}) \\ + \sum_{i \in Neighbor(A)} LTT_{A,i}(t_n) CGR_{i,B}^{short-term-term}(t_n) + RM_{A,B}(t_n) \quad (4-2) \\ \text{if } RM_{A,B}(t_{n-1}) = 1 \text{ and } RM_{A,B}(t_n) = 1 \\ CBR_{A,B}(t_n - TN_{short-term}, t_{n-1}) \\ + \sum_{i \in Neighbor(A)} LTT_{A,i}(t_n) CGR_{i,B}^{short-term}(t_n) + \alpha RM_{A,B}(t_n) \quad (4-3) \end{cases}$$

$$CBR_{A,B}^{short-term}(t_n) = \begin{cases} \text{if } RM_{A,B}(t_n) = -1 \\ CBR_{A,B}(t_n - TN_{short-term}, t_{n-1}) \\ + \sum_{i \in Neighbor(A)} LTT_{A,i}(t_n) CBR_{i,B}^{short-term}(t_n) \quad (5-1) \\ \text{if } RM_{A,B}(t_{n-1}) = -1 \text{ and } RM_{A,B}(t_n) = 1 \\ CBR_{A,B}(t_n - TN_{short-term}, t_{n-1}) \\ + \sum_{i \in Neighbor(A)} LTT_{A,i}(t_n) CBR_{i,B}^{short-term}(t_n) + RM_{A,B}(t_n) \quad (5-2) \\ \text{if } RM_{A,B}(t_{n-1}) = 1 \text{ and } RM_{A,B}(t_n) = 1 \\ CBR_{A,B}(t_n - TN_{short-term}, t_{n-1}) \\ + \sum_{i \in Neighbor(A)} LTT_{A,i}(t_n) CBR_{i,B}^{short-term}(t_n) + \alpha RM_{A,B}(t_n) \quad (5-3) \end{cases}$$

수식 (4-1) 및 (4-2), (4-3), 그리고 수식 (5-1) 및 (5-2), (5-3)은 최근  $TN_{short-term}$  동안 단말 A가 단말 B를 평가한 직접 평판 정보 값의 합이다. 수식 (4-1)부터 수식(5-3)의 첫 번째 항은  $t_{n-1}$ 까지의 평판정보를 의미하며, 둘째 항은 현재 시각  $t_n$ 의 평판정보이다. 수식 (4-3)과 수식 (5-3)에서 보는 바와 같이 단말 A는 지난 두 번의 평가 값이 연속으로 동일하면  $\alpha$ 배 만큼의 가중치를 단말 B의 평판 값에 부여한다. 이는 연속된 두 번의 평가 결과가 동일한 값이면 평가의 결과를 신뢰할 수 있기 때문이다. 본 논문에서는  $\alpha$ 의 값을 1.25로 지정하여 실험을 수행하였다. 수

식 (4-2)와 수식 (5-2)의 우변의 둘째 항은 단말 A의 이웃 단말이 단말 B의 포워딩 행동을 평가한 간접 평판 정보 값의 합이다. 간접 평판 정보는 직접 평판 정보와 달리 다른 단말들이 평가하여 전달한 평판 정보이기 때문에 거짓 단말에 의해 조작될 수 있다. 따라서 수식 (4-1)부터 수식 (5-3)까지 간접 평판 정보를 알려준 단말의 신뢰도 값인 LTT 값이 포함되어 있다. STT가  $TN_{short-term}$  동안의 평판 정보만을 이용하는 것과는 달리 LTT는 각 단말이 수행한 전체 포워딩 결과를 기반으로 계산되었기 때문에 악의적인 단말이 일시적으로 협력적인 행동을 하더라도 낮은 값을 가지게 된다. 따라서 악의적인 단말이 알려준 거짓 간접 평판 정보가  $CGR_{A,B}^{short-term}(t_n)$ 과  $CBR_{A,B}^{short-term}(t_n)$ 에 미치는 영향은 미미하다. 마지막으로 악의적인 단말을 우회하는 라우팅 경로 설정을 위해 사용되는  $STT_{A,B}(t_n)$ 는 수식 (4)와 수식 (5)를 이용하여 수식 (6)과 같이 계산된다. 수식 (1)부터 수식 (6)에 의해 평판 정보 업데이트가 완료되면 단말 A는 이웃 단말에게 간접 평판 정보인  $CGR_{A,B}^{short-term}(t_n)$ 와  $CBR_{A,B}^{short-term}(t_n)$  값을 전송한다 (그림 3의 단계 (4)).

$$STT_{A,B}(t_n) = \max(0, \frac{CGR_{A,B}^{short-term}(t_n) - |CBR_{A,B}^{short-term}(t_n)|}{CGR_{A,B}^{short-term}(t_n) + |CBR_{A,B}^{short-term}(t_n)|}) \quad (6)$$

다음은 CARE 라우팅의 수평적 상호 작용에서 라우팅 경로 탐색 단계에 대하여 기술하기로 한다. 먼저 그림 4는 CARE 라우팅 경로 탐색 단계에서 사용되는 CARE 라우팅 메시지의 형식이다. 1 바이트의 TYPE 필드는 라우팅 메시지의 타입을 구별한다. TYPE 필드가 0이면 라우팅 경로 탐색 요청 메시지인 CARE-REQ (CARE routing REQuest) 메시지이며, 1이면 라우팅 경로 탐색 응답 메시지인 CARE-REP (CARE routing REPlY) 메시지이다. 1 바이트의 LEN (LENgth) 필드는 메시지의 길이를 4 바이트 단위로 나타낸 값이다. 그리고 1 바이트의 TTL (Time-To-Live) 필드는 메시지가 중계 가능한 홉수이다. 1 바이트의 HOP 필드는 메시지가 지나온

TYPE 1 바이트	LEN 1 바이트	TTL 1 바이트	HOP 1 바이트	QoS 1 바이트	STToL 4 바이트	LLID 8 바이트	SN 4 바이트	SIP 4 바이트	DIP 4 바이트
---------------	--------------	--------------	--------------	--------------	----------------	---------------	-------------	--------------	--------------

그림 4. CARE 라우팅 메시지 형식

홉 수를 나타낸다. 1 바이트의 QoL (Quality of Logical link) 필드는 메시지가 지나온 라우팅 경로의 링크 채널 품질을 나타내는 값이다. 4 바이트의 STToL (Short-Term Trustworthiness of Logical link) 필드는 라우팅 메시지가 지나온 라우팅 경로의 신뢰도를 나타낸다. 8 바이트의 LLID 필드는 논리적인 가상 링크의 식별자를 나타낸다. 4 바이트의 SN (Sequence Number) 필드는 CARE 라우팅 메시지의 시퀀스이다. SIP (Source IP) 필드와 DIP (Destination IP) 필드는 메시지를 생성한 소스 단말과 목적지 단말의 IP 주소를 나타낸다.

라우팅 경로가 저장되는 논리적 링크 정보 테이블(LLIT, Logical Link Information Table)의 구조는 그림 5와 같다. 4 바이트의 DIP 필드는 그림 4에서 기술한 LLID로 구별되는 라우팅 경로에 존재하는 목적지 단말의 IP 주소를 나타낸다. 6 바이트의 NH\_MAC (Next Hop Medium Access Control) 필드는 LLID로 구별되는 라우팅 경로를 구성하고 있는 이웃 무선 단말의 MAC 주소이다. 1 바이트의 LLHop 필드는 그림 4의 DIP 필드가 나타내는 목적지 단말까지 패킷이

도착하는데 필요한 홉 수이다. 그리고 1 바이트의 QoL 필드는 논리적인 가상 링크 경로의 통신 채널 품질을 나타낸다. 4 바이트의 STToL 필드는 설정된 라우팅 경로의 신뢰도를 나타낸다. 4 바이트의 LLAge (Logical Link Age) 필드는 설정된 라우팅 경로의 유효 기간으로, 초기 설정 값은 5초이다. LLAge 필드 값은 매초마다 감소되며, 0이 되면 해당 논리적 링크 정보 테이블에서 삭제된다.

그림 6과 그림 7은 그림 3의 네트워크에서 소스 단말 A가 목적지 단말 D로 패킷을 전송하는데 요구되는 CARE 라우팅의 동작 과정을 보여준다. 그림 6에서  $IP_x$ 와  $MAC_x$ 는 각각 단말 X의 IP 주소와 MAC 주소를 나타낸다. 그리고 단말 A가 전송하는 CARE-REQ 메시지의 LLID 값은  $LLID_0$ 이며, 단말 D가 단말 A에게 전송하는 CARE-REP 메시지의 LLID 값은  $LLID_1$ 이다. 먼저, 단말 A가 CARE-REQ 메시지를 생성하여 이웃 단말로 전송한다(그림 6의 과정 (1)). CARE-REQ 메시지를 수신한 중계 단말 B와 중계 단말 E는 그림 6의 (A)와 같이 논리적 링크 정보 테이블을 구성한다. 중계 단말 B와 중계 단말

DIP 4 바이트	LLID 8 바이트	SN 4 바이트	NH_MAC 6 바이트	LLHop 1 바이트	QoL 1 바이트	STToL 4 바이트	LLAge 4 바이트
...	...	...	...	...	...	...	...

그림 5. 논리적 링크 정보 테이블의 구조

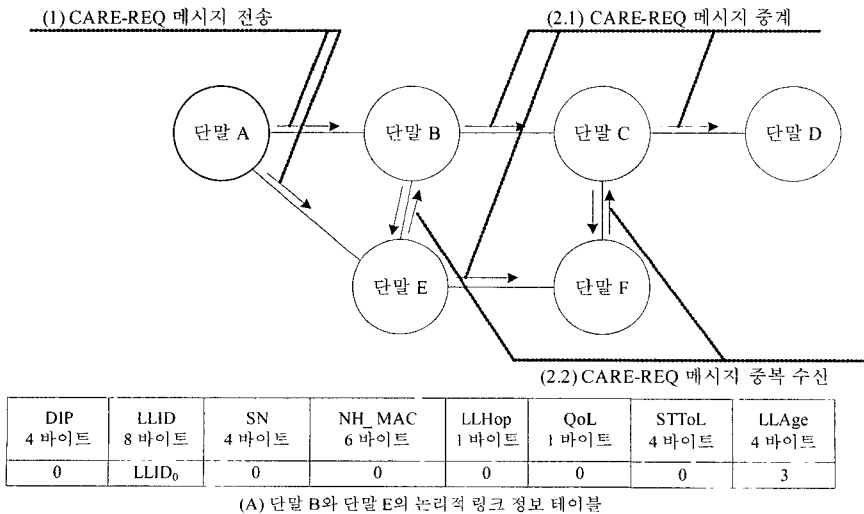


그림 6. CARE-REQ 메시지 처리 과정에 대한 예

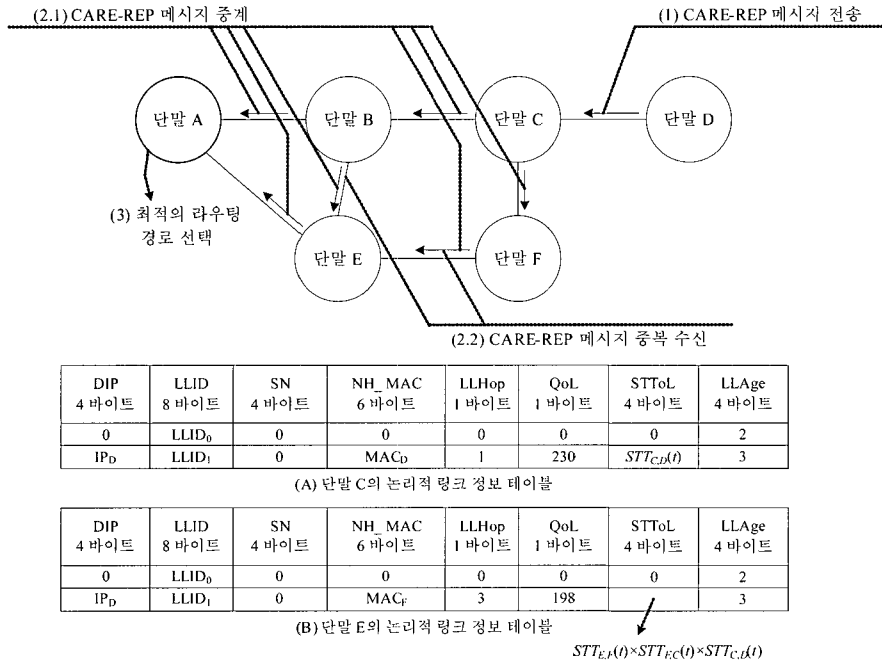


그림 7. CARE-REP 메시지 처리 과정에 대한 예

E는 자신이 목적지 단말이 아니기 때문에 다시 이웃 단말로 재전송한다. 이 때 중계 단말 B와 중계 단말 E는 서로 이웃하고 있기 때문에 CARE-REQ 메시지를 중복 수신하지만 논리적 링크 정보 테이블을 참조하여 중복 수신임을 확인하여 메시지를 버린다. 이러한 과정은 CARE-REQ 메시지의 TTL 필드가 0이 되거나 CARE-REQ 메시지가 목적지 단말에 도착할 때까지 반복된다.

CARE-REQ 메시지를 받은 목적지 단말 D는 CARE-REP 메시지를 생성하고 이웃 중계 단말 C에게 전송한다(그림 7의 과정 (1)). 중계 단말 C는 그림 7의 (A)와 같은 논리적 링크 정보 테이블을 구성한다. 따라서 중계 단말 C는 LLID 필드 값이 LLID<sub>1</sub>인 패킷을 중계 단말 D의 MAC 주소인 MAC<sub>D</sub>로 전송해야 함을 알 수 있다. 또한 중계 단말 C는 목적지 단말 D까지의 홉 수와 링크 품질 그리고 링크 신뢰도를 알 수 있다. 중계 단말 C는 CARE-REP 메시지의 목적지 단말 A가 아니기 때문에 수신한 CARE-REP 메시지를 이웃 중계 단말인 중계 단말 B와 중계 단말 F에게 전송한다(그림 7의 과정 (2)). 중계 단말 B는 소스 단말 A와 중계 단말 E에게 전송하며, 중계 단말 E는 중계 단말 F로부터 중복 CARE-REP 메시지를

수신한다. 그림 7에서는 중계 단말 F로부터 받은 CARE-REP 메시지의 링크 품질과 신뢰도가 높다고 가정하여 그림 7의 (B)와 같이 논리적 링크 정보 테이블을 구성하였다. 또한 소스 단말 A도 중계 단말 B와 중계 단말 E로부터 중복된 CARE-REP 메시지를 수신하므로 채널 품질과 신뢰도, 그리고 홉 수를 기반으로 한 최적의 라우팅 경로를 결정한다(그림 7의 과정 (3)).

### 3.3 CARE 라우팅 기법의 수직적 상호 작용

CARE 라우팅의 수직적 상호 작용은 MAC 계층 정보를 반영한 라우팅 경로 관리 기법과 CARE 라우팅에서 얻은 각 단말의 신뢰성 정보를 반영한 TCP 혼잡 제어 기법으로 구성된다. 먼저 CARE 라우팅 기법은 CARE 라우팅 메시지 및 논리적 링크 정보 테이블의 QoL 필드를 이용하여 우수한 무선 채널 품질을 가진 하위 링크 계층으로 구성된 라우팅 경로를 생성한다. 또한 CARE 라우팅 기법은 단말의 이동이나 무선 채널의 품질이 변하여 라우팅 경로의 품질이 저하되면, 기존의 라우팅 경로가 손실되기 전에 새로운 라우팅 경로를 설정한다. 이를 위하여 각 단말은 패킷 전송 과정에서 매 홉의 채널 품질을 측정



하고 최소값을 QoL 필드에 저장한다. 패킷을 수신한 목적지 단말은 QoL 필드 값이  $QoL_{Min}$  보다 작으면 단말의 이동 혹은 무선 채널의 품질이 변하여 설정된 라우팅 경로가 손실될 가능성이 높은 것으로 판단한다. 그리고 새로운 라우팅 경로를 설정하기 위하여 CARE-REP 메시지를 소스 단말에게 전송한다. 본 논문의 실험에서 사용한  $QoL_{Min}$  값은 50이다.

CARE 라우팅의 수직적 상호 작용에서는 TCP-FARE (Fast REcovery based on trustworthiness) 와 TCP-RARE (Rate Adaptive congestion control based on REputation)를 제안하였다. TCP-FARE는 TCP의 Fast Recovery 기법을 확장하여 패킷 손실 전의 혼잡 윈도우 값까지 빠르게 혼잡 윈도우를 증가시키는 기법으로 수식 (7)과 같이 TCP 혼잡 윈도우의 증가량을 결정한다. 표 2는 TCP의 Fast Recovery 기법을 확장한 TCP-FARE의 알고리즘이다.

$$\Delta CWnd = \frac{1}{2} \max(CWnd - sstresh, (CWnd - sstresh) \times (1 - STToL)) \quad (7)$$

TCP-FARE는 악의적인 단말에 의해 패킷 손실이 발생하면 라우팅 경로의 신뢰도에 따라 빠르게 혼잡 윈도우를 회복하는 방법이다. 반면 TCP-RARE는 라우팅 경로의 신뢰도에 따라 패킷의 전송률을 조절하여 악의적인 단말에 의해 패킷 손실이 발생하는 확률

을 줄이는 방법이다. 라우팅 경로의 신뢰도가 낮으면 악의적인 단말에 의해 패킷이 손실될 확률이 크므로 패킷 전송률을 줄여야 한다. 라우팅 경로의 신뢰도에 따른 전송률을 계산하는 TCP-RARE의 알고리즘은 다음과 같다. 먼저 CARE 라우팅에 의해 생성된 라우팅 경로가  $K$ 개의 다른 단말로 구성되 단있다고 가정한다.  $p_i$  ( $1 < i < K$ )는 각 단말이 악의적으로 행동할 확률을 나타낸다. 따라서 설정된 라우팅 경로를 통해 패킷이 성공적으로 목적지 단말까지 전송될 확률  $p_s$ 는 수식 (8)과 같다. 이 때, 각 단말이 악의적으로 행동할 확률  $p_i$ 는 알려져 있지 않으므로  $p_s$ 도 알 수 없다. 이에 본 논문에서는 각 단말이 악의적으로 행동할 확률  $p_i$ 를 단말의 평판 값으로 사용한다. 따라서 앞서 설명한 CARE-REP 알고리즘에 의하여 각 라우팅 경로  $p_s$ 는 논리적 링크 테이블에 저장된  $STToL$  필드 값과 같다.

$$p_s = (1 - p_1)(1 - p_2) \dots (1 - p_K) = \prod_{i=1}^K (1 - p_i) \approx STToL \quad (8)$$

제  $STToL$  필드 값을 기반으로 TCP 전송률에 사용되는 기호는 다음과 같다.  $W(t)$ 와  $R(t)$ 는 각각 시각  $t$ 에서 TCP 혼잡 윈도우 크기와 RTT (Round Trip Time) 값이다.  $X(t)$ 는 시각  $t$ 에서 TCP의 전송률이다. 참고문헌[19] 에서와 같이  $X(t) = W(t)/R(t)$ 을

표 2. TCP-FARE의 혼잡 윈도우 관리 기법

1	<b>TCP ACK 수신</b>
	<i>CWnd</i> : TCP 혼잡 윈도우
	<i>MSS</i> : 최대 세그먼트 크기
	<i>ssresh</i> : TCP Slow Start 임계값
	<i>STToL</i> : 해당 TCP 연결의 라우팅 경로 신뢰도
	<i>Dup(ACK)</i> : 수신한 TCP ACK의 중복 수신 횟수
	<i>AdvertisedWin(ACK)</i> : 수신한 TCP ACK의 Window Size 필드 값
	<i>SendBytes</i> : 소스 단말이 수신 단말로 전송한 데이터 중 ACK를 수신하지 못한 데이터 량
2	if <i>Dup(ACK)</i> = 3 then
3	<i>ssresh</i> ← 0.5 × <i>CWnd</i>
4	retransmit the lost segment
5	<i>CWnd</i> ← <i>ssresh</i> + 3 × <i>MSS</i> (참조논문 [4]에 의하여)
6	else if <i>Dup(ACK)</i> > 3 then
7	<i>CWnd</i> ← <i>CWnd</i> + Δ <i>CWnd</i> (수식 (7)에 의하여)
8	if ( <i>CWnd</i> > <i>SendBytes</i> ) and ( <i>AdvertisedWin(ACK)</i> > 0) then
9	transmit a segment
10	endif
11	else if <i>Dup(ACK)</i> = 0 then
12	<i>CWnd</i> ← <i>ssresh</i>
13	endif
14	end

가정한다.  $N(t)$ 는 시각  $t$ 에서 손실된 패킷의 수로  $\lambda(t)$ 의 분포를 가진다. 참고문헌[20]에서 접근한 것과 유사하게  $N(t)$ 는  $W(t)$ 와는 서로 독립이라고 가정하였다 이는 패킷이 손실된 이유가 TCP 혼잡 윈도우 크기의 변화량보다는 악의적인 단말에 의한 라우팅 경로의 재설정으로 인한 것이라고 가정하였기 때문이다. 따라서 TCP 혼잡 윈도우의 크기의 변화량  $dW(t)$ 는 수식 (9)와 같이 계산된다. 수식 (9)의 첫 번째 항은 RTT 마다 1씩 증가하는 TCP 혼잡 윈도우의 산술적 증가(Additional Increment)를 나타내며 두 번째 항은 매 패킷 손실이 발생할 때 마다 TCP 혼잡 윈도우를 절반으로 감소시키는 배수적 감소(Multiplicative Decrease)를 나타낸다. 수식 (9)의 양변에 평균화 취하면, 수식 (10)을 유도할 수 있다.

$$dW(t) = \frac{1}{R(t)}dt - \frac{W(t)}{2}dN(t) \quad (9)$$

$$\frac{d\bar{W}}{dt} = \frac{1}{R} - \frac{\bar{W}}{2} \frac{E[dN(t)]}{dt} = \frac{1}{R} - \frac{\bar{W}}{2} \lambda(t) \quad (10)$$

수식 (10)의  $\lambda(t)$ 는 패킷 손실 수에 대한 분포이므로 전송한 패킷의 수와 라우팅 경로에서 패킷이 손실될 확률을 곱하여 얻을 수 있다. 따라서  $\lambda(t)$ 는 수식 (11)와 같이 계산할 수 있다. TCP-RARE에서는 ACK가 도착할 때마다 수식 (12)과 같이 TCP 전송률을 계산하여 패킷을 전송한다. 수식 (12)에서 보는 바와 같이 TCP 전송률은 혼잡 윈도우의 크기와 RTT, 그리고 라우팅 경로의 신뢰도인 크기와 R값에 의해 조절된다. 크기와 R값이 크면 수식 (12)의 두 번째 항의 값이 작아지므로 전송률은 커지고, 크기와 R값이 작으면 전송률은 작아진다. 따라서 악의적인 단말이 패킷을 버려 라우팅 경로의 신뢰도가 감소하면 해당 경로로 전송하는 데이터적인 단말도 낮아져서 악의적인 단말로 인한 패킷의 손실의 횟수 및 TCP 전송률의 감소 현상을 줄일 수 있다.

$$\lambda(t) = X(t) \times (1 - p_s) \approx X(t) \times (1 - STToL) \quad (11)$$

$$\frac{d\bar{W}}{dt} = \frac{1}{R} - \frac{\bar{W}}{2} \frac{E[dN(t)]}{dt} = \frac{1}{R} - \frac{\bar{W}}{2} \lambda(t) \quad (12)$$

#### 4. 성능분석 및 비교평가

본 논문에서 제안한 CARE 라우팅 기법의 성능을

측정하는데 사용된 실험 및 시뮬레이션 환경은 다음과 같다. NS-2 시뮬레이터 기반으로 수행되는 시뮬레이션 환경은 1000m × 500m에 임의적으로 50개의 단말을 배포하였다. 각 단말은 100m의 전송거리를 가지는 전방향성(Omni-directional) 안테나를 사용한다. 각 단말의 이동은 RWP (Random-Way Point) 모델을 사용하여 구현하였으며 연속된 이동 중간에는 5초 또는 10초의 정지 시간을 주었다. 이 장에서는 먼저 라우팅 프로토콜의 성능 비교 척도인 패킷 손실률, 종단간 패킷 전송 지연 시간, 그리고 네트워크 성능(Throughput)을 분석하였다. 그림 8은 무선 단말이 이동하는 다중 홉 무선 네트워크 환경에서 제안한 CARE 라우팅 기법과 기존 AODV와 DSR 라우팅 기법을 적용한 경우에 발생하는 패킷 전송의 실패율을 보여준다. 패킷 전송의 실패율을 측정하기 위하여 각 무선 단말은 설정된 라우팅 경로에 따라 목적지 단말에게 Echo Request를 담당하는 ICMP (Internet Control Management Protocol) 메시지를 10ms 단위로 보내고, 목적지 단말에서는 Echo Reply를 담당하는 ICMP 메시지를 소스 단말에게 전송한다. 이를 수신한 소스 단말은 송수신한 ICMP 메시지의 응답 횟수를 측정하여 패킷 전송의 실패율을 측정한다. 그리고 시뮬레이션 환경에서는 단말의 수를 고려하여 10kbps부터 100Kbps까지 10 단계로 변화시켰다.

이에 대한 실험과 성능 분석을 한 결과, 그림 8과 같이 DSR 라우팅에서 패킷 전송의 실패율이 가장 높게 나타났으며, 다음으로 AODV 및 CARE 라우팅 기법 순으로 나타났다. DSR 라우팅 기법이 다른 라우팅 기법들에 비하여 패킷 전송 실패율이 높은 이유는 다음과 같다. DSR 라우팅에서 각각의 무선 단말은 설정한 라우팅 경로 정보를 캐쉬 테이블에 저장하

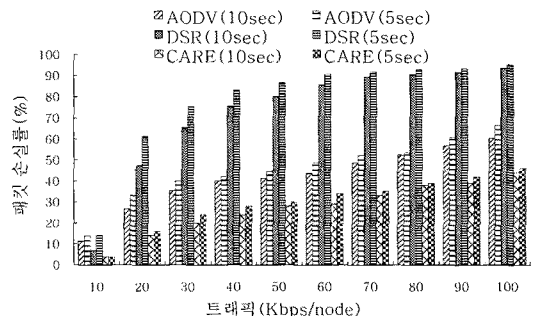


그림 8. 무선 단말의 정지 시간이 각각 5초 및 10초인 경우의 패킷 손실률

고 이를 기반으로 하여 패킷을 전달한다. 따라서 중계 무선 단말이 이동하여 기존에 설정된 라우팅 경로가 더 이상 유효하지 않음에도 불구하고 이동한 중계 무선 단말로 패킷을 포워딩하는 무선 단말은 자신의 캐쉬 정보에 저장되어 있는 기존의 라우팅 경로를 따라 패킷을 전송하기 때문에 패킷의 손실 가능성이 매우 높다. 한편, AODV 라우팅은 주기적인 Hello 메시지를 교환하여 라우팅 경로의 유효성을 점검한다. 따라서 DSR 라우팅에 비하여 낮은 패킷 전송의 실패율을 제공할 수 있다. CARE 라우팅 기법은 수직적 협력 기법을 통해 하위 물리 및 데이터 링크 계층의 정보를 참조하여 라우팅 재설정 과정의 동적으로 수행한다. 따라서 무선 단말의 이동으로 인하여 전파 세기의 신호가 작아지면 MAC 계층에서 획득한 링크 품질 값을 기반으로 새로운 라우팅 경로를 형성하는 과정을 수행한다. 즉 AODV나 DSR은 라우팅 경로가 손실된 후에 라우팅 경로를 재설정하지만 CARE 라우팅 기법은 라우팅 경로가 손실되기 전에 재설정한다. 그리고 채널의 품질에 기반을 두어 좋은 라우팅 경로를 선택하기 때문에 패킷 전송의 실패율이 DSR과 AODV 라우팅보다 낮다. 또한 무선 단말의 이동이 자주 일어날수록 패킷 전송의 실패율이 증가함을 보여준다. 이는 무선 단말의 이동으로 인하여 라우팅 경로의 유효한 시간이 짧아지기 때문이다.

그림 9는 무선 단말의 이동에 따른 AODV와 DSR, 그리고 CARE 라우팅에서 패킷의 평균 전송 지연 시간을 보여준다. 실험 환경은 그림 8에서 적용한 실험 환경과 동일하다. 그림 8의 패킷 손실율에 대한 영향

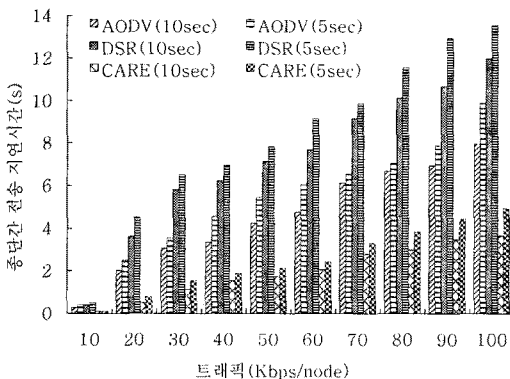


그림 9. 무선 단말의 정지 시간이 각각 5초 및 10초인 경우의 중단간 평균 패킷 전송 지연 시간

으로 DSR의 패킷의 평균 패킷 전송 지연시간이 가장 크게 나타났으며, 다음으로 AODV와 CARE 라우팅 순으로 평균 패킷 전송 지연시간이 작게 나타났다. 패킷 손실율이 증가하면 패킷 재전송이 빈번하게 발생하게 되어 패킷 전송 지연시간이 길어짐과 동시에 무선 단말 간의 채널 간섭 현상이 증가되어 평균 패킷 전송 지연 시간이 길어지게 된다.

본 논문에서 제안한 수평적 상호 작용의 성능에 대한 분석 내용은 다음과 같다. 수평적 상호 작용은 NF, FR, FF 와 같은 악의적인 단말의 행동을 고려하기 때문에 실험 환경을 다시 정의하였다. 먼저 50개의 단말 중에서 임의적으로 몇몇의 악의적인 단말을 선택한다. 실험에서는 0개에서부터 45개까지 10단계로 변화시켰다. 선택된 악의적인 단말은 0.3의 확률로 수신한 패킷을 버린다. 실험 시간은 총 20,000초이며 각 단말은 임의로 선택된 목적지 단말로 10Kbps의 CBR (Constant Bit Rate) 트래픽을 전송한다. 먼저 제안한 수평적 상호 작용에서 각 단말의 STT 값과 LTT 값의 변화를 확인하기 위하여 악의적인 단말이 30%를 차지하는 다중 홉 무선 네트워크 환경에서 CARE 라우팅 기법을 적용하였을 때, 시간에 따른 STT 값과 LTT 값을 측정하였다. 이 시뮬레이션에서 50개의 각 단말은 단말 A, 단말 B, ..., 순으로 명명한다.

표 3은 10번의 패킷 전송 처리 결과를 통해 얻어진 단말 A가 이웃 단말을 평가한 STT 값과 LTT 값이다. 그리고 표 4는 단말 A의 이웃 단말들이 단말 A가 전송한 패킷을 처리한 결과를 보여준다. 표 3에서 중계 단말  $i$ 는 단말 A로부터 받은 패킷을 중계하는 단말로서 실험에서는 단말 B, 단말 C 그리고 단말 D가 있으며, 단말 C는 악의적으로 행동하는 단말이다. 61번째 트랜잭션에서 단말 B는 단말 A로부터 받은 패킷을 다음 홉인 단말 C로 전송하였으므로 단말 A는 단말 B를 협력적으로 행동하는 단말로 판단하여 평균 값인  $RM_{A,B}(t_{61})$ 을 1로 할당하였다. 그리고 수식 (1), (3), (4), (6)에 의하여 각각  $CGR_{A,B}(t_w, t_{61})$ ,  $LTT_{A,B}(t_{61})$ ,  $CGR_{A,B}^{short-term}(t_{61})$ , 그리고  $STT_{A,B}(t_{61})$  값을 갱신한다. 특히 62번째 트랜잭션에서 단말 B는 61번째 트랜잭션에 이어 연속적으로 단말 A로부터 받은 패킷을 협력적으로 행동하여 다음 홉의 이웃 단말로 전송하였으므로 값은  $RM_{A,B}(t_{62})$ 의 1.25배로부터 계산된다. 또한 62번째 트랜잭션에서 단말 C의

표 3. 단말 A가 이웃 단말을 평가한 신뢰도 정보 (단말 C는 악의적인 단말)

트랜잭션 (중계 단말 i)	평판					STT			LTT		
	$RM_{A,i}$	$CGR_{A,i}^{short-term}$	$CCGR_{A,i}^{short-term}$	$CGR_{A,i}(t_0, t_n)$	$CBR_{A,i}(t_0, t_n)$	$STT_{A,B}$	$STT_{A,C}$	$STT_{A,D}$	$LTT_{A,B}$	$LTT_{A,C}$	$LTT_{A,D}$
61 (B)	1	18.5	3	18	3	0.720	0.56	0.695	0.714	0.619	0.684
62 (B)	1	19.75	3	19	3	0.736	0.51	0.704	0.727	0.619	0.684
63 (C)	-1	17.2	5.19	17	5	0.750	0.53	0.704	0.727	0.545	0.684
64 (D)	1	18.32	3	17	3	0.750	0.55	0.718	0.727	0.545	0.7
65 (D)	1	20.3	3	18	3	0.762	0.55	0.742	0.727	0.545	0.714
66 (C)	-1	17.93	6.44	17	6	0.769	0.47	0.742	0.727	0.478	0.714
67 (B)	-1	23.49	4	19	4	0.709	0.47	0.747	0.652	0.478	0.714
68 (C)	-1	17.93	7.69	17	7	0.709	0.39	0.754	0.652	0.417	0.714
69 (B)	1	23.49	4	20	4	0.709	0.36	0.754	0.667	0.417	0.714
70 (D)	1	22.68	3.41	19	3	0.720	0.38	0.738	0.667	0.417	0.727

표 4. 단말 A의 이웃 단말들이 패킷을 처리한 결과

트랜잭션	단말 B,C,D 간의 패킷 처리 및 평판 정보
61	트랜잭션 B1 [B→C:-1], 트랜잭션 C1 [C→D: 1]
62	트랜잭션 C2 [C→B: 1], 트랜잭션 B2 [B→D: 1], 트랜잭션 D1 [D→C:-1]
63	트랜잭션 B3 [B→C: 1]
64	트랜잭션 B4 [B→D: 1], 트랜잭션 C3 [C→B: 1], 트랜잭션 D2 [D→B: 1]
65	트랜잭션 D3 [D→B: 1]
66	트랜잭션 C4 [C→B: 1], 트랜잭션 C5 [C→D: 1]
67	트랜잭션 B5 [B→D: 1]
68	트랜잭션 B6 [B→C:-1]
69	트랜잭션 C6 [C→B: 1], 트랜잭션 C7 [C→D:-1], 트랜잭션 D3 [D→B: 1], 트랜잭션 D4 [D→C: 1]
70	트랜잭션 C8 [C→D: 1], 트랜잭션 D5 [D→C:-1]

STT 값인  $STT_{A,C}(t_{62})$ 가 0.51로 감소하였는데, 이는 표 4의 트랜잭션 B1에 의해 단말 B가 단말 A에게 단말 C의 간접 평판 정보를 전송하였기 때문이다.

협력적으로 행동하는 일반 단말과 악의적인 단말의 평균 STT 및 평균 LTT 값의 변화는 그림 10과 같다. 그림 10을 보면 초기에는 모든 단말의 STT 및 LTT 값이 각각 0.5와 1을 가진다. 시뮬레이션 초기에는 아직 충분한 평판 정보를 획득하지 못하였기 때문에 STT 및 LTT의 평균값이 크게 변하지만 약 60초 이후에는 일반 단말의 신뢰도 값이 악의적인 단말보다 큼을 확인할 수 있다.

따라서 CARE 라우팅의 수평적 협력 기법을 통해 일반 단말은 악의적인 단말을 우회하는 기법을 통해 일반 단말은 악의적인 단말을 우회하는 라우팅 경로를 선택하여 악의적인 단말로 인한 패킷 손실이 발생

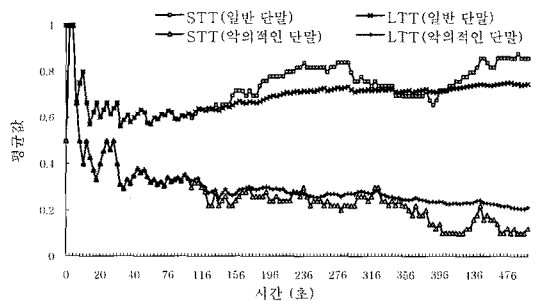


그림 10. 시간에 따른 일반 단말과 악의적인 단말의 STT 및 LTT 값의 변화

하는 NF 문제를 해결할 수 있다. 그리고 각 단말은 STT 값이 작은 이웃 단말의 CARE-REQ 패킷을 중계하지 않는다. 이는 이웃 단말의 패킷은 중계하지 않고 자신이 전송하는 패킷만 이웃 단말에 의해 전송

되는 문제인 FR 문제를 해결한다. 한편 악의적인 단말의 STT 값이 감소하여 네트워크에서 고립된 후 협력적으로 행동하면, 다시 이웃 단말에 의해 네트워크 서비스를 받을 수 있어야 한다. 이를 위해 CARE 라우팅의 수평적 협력 기법은 수식 (3)과 수식 (6)에서 설명한 바와 같이 STT 값을 최근  $TN_{short term}$  동안의 평판 정보만으로 계산하여 악의적인 단말의 STT 값을 다시 회복할 수 있도록 한다. 그 결과, 그림 10과 같이 STT 값은 시간에 따라 증가 또는 감소하지만 LTT 값의 변화량은 매우 적다. 이는 LTT 값은 STT 값과 달리 모든 평판 정보로부터 계산되기 때문이다.

그림 11은 이동 단말의 정지시간이 10초일 때, 악의적인 단말의 수에 따른 AODV, DSR 그리고 CARE 라우팅 기법의 패킷 손실률을 비교한 그림이다. 본 논문에서는 제안한 수평적 상호 작용 (Horizontal Cross Layer, 그림 11과 그림 12에서 HCL로 표기)의 성능을 평가하기 위하여 HCL을 적용하기 전후의 CARE 라우팅에 대한 패킷 손실률을 측정하였으며, 또한 AODV와 DSR 라우팅 기법에도 HCL을 적용하

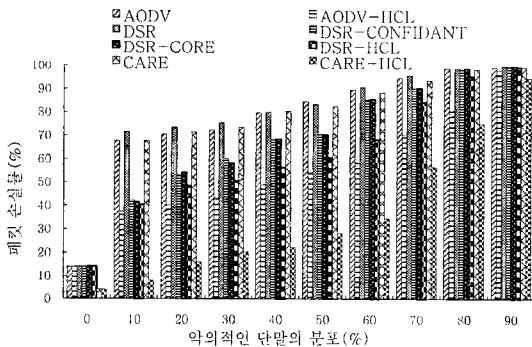


그림 11. 악의적인 단말의 분포에 따른 패킷 손실률

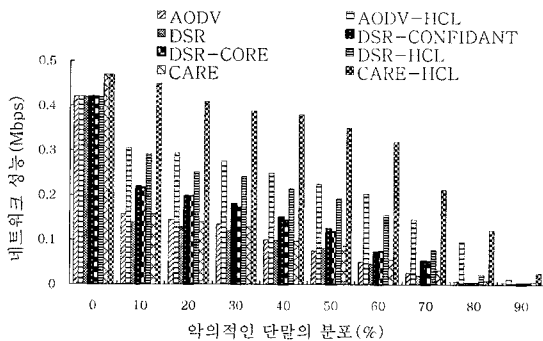


그림 12. 악의적인 단말의 분포에 따른 네트워크 성능

여 실험을 하였다. 또한 기존의 기법인 CONFIDANT와 CORE를 DSR 라우팅에 적용하였다.

그림 11과 같이 악의적인 단말의 수가 증가할수록 패킷 손실률은 크게 감소하였다. 그러나 수평적 상호 작용을 적용한 후에는 패킷 손실률이 수평적 상호 작용을 적용하기 전보다 크게 감소되는 것을 확인할 수 있다. 이는 수평적 상호 작용에 의해 패킷이 손실될 확률이 적은 신뢰도가 높은 라우팅 경로를 선택하기 때문이다. 특히 CARE 라우팅 기법이 AODV와 DSR에 비하여 더 낮은 패킷 손실률을 보여주었는데, 이는 CARE 라우팅 기법의 수평적 상호 작용 때문에 설정된 경로의 신뢰도와 채널 품질이 일정 값 이상보다 적을 경우 즉시 다른 경로를 탐색하여 우수한 새로운 라우팅 경로를 설정하기 때문이다. 또한 2장에서 살펴본 바와 같이 CONFIDANT 기법과 CORE 기법은 거짓 평가를 수행하는 악의적인 단말의 FF 문제를 고려하지 않아 수평적 상호 작용을 지원하지 않는 CARE 라우팅 기법보다 성능이 감소되는 것을 확인할 수 있었다.

그림 13은 거짓된 평판 정보를 전송하는 단말의 악의적인 FF 행동이 있는 경우에 CARE 라우팅 기법의 성능을 평가하기 위하여 거짓 단말의 수에 따른 악의적인 단말의 검출률을 따로 분석하였다. 거짓 평판 정보를 이웃 단말에게 전송하면 악의적인 단말이 협력적으로 행동하는 일반 단말로 잘못 판단되거나 일반 단말이 악의적인 단말로 판단하게 하는 FF 문제를 발생시킨다. CARE 라우팅 기법은 거짓 단말의 수가 전체 단말의 30%인 경우에 약 250초 내에서 모든 악의적인 단말을 거의 검출하였다. 그림 14는 CARE 라우팅 기법의 수직적 상호 작용에서 TCP-

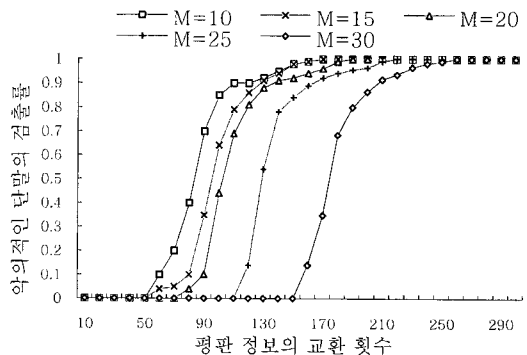


그림 13. 거짓 단말의 분포에 악의적인 단말의 검출률

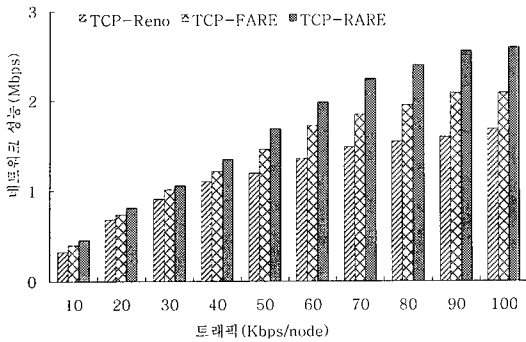


그림 14. CARE 라우팅 기법과 TCP간의 수직적 상호 작용에 대한 성능

RARE 및 TCP-FARE의 성능을 TCP-Reno와 비교한 그림이다. 그림 14의 시뮬레이션 환경은 악의적인 단말이 전체 단말의 30%인 경우이며, 시뮬레이션 환경은 앞서 수행하였던 그림 11과 동일하다. TCP-Reno는 악의적인 단말에 의한 패킷 손실을 무선 네트워크 혼잡 상태로 인식하기 때문에 혼잡 상태에서 벗어나기 위하여 TCP 혼잡 윈도우의 크기를 절반으로 줄여 네트워크에 유입되는 데이터 량을 감소시킨다. 반면, TCP-FARE는 라우팅 경로의 신뢰도를 기반으로 악의적인 단말로 인한 패킷 손실을 암묵적으로 탐지하여 TCP 혼잡 윈도우를 패킷 손실 전의 값까지 빠르게 회복한다. 따라서 TCP-FARE의 성능이 TCP-Reno에 비하여 우수함을 그림 14에서 확인할 수 있다. TCP-RARE는 TCP-FARE와 달리 악의적인 단말에 의한 패킷 손실 횟수를 최소화하기 위하여 TCP 전송률을 네트워크 상태에 따라 동적으로 변화한다. 특히 각 단말의 트래픽이 30Kbps일 때, 600초 동안 악의적인 단말에 의한 패킷 손실 횟수가 TCP-Reno, TCP-FARE, 그리고 TCP-RARE인 경우에 각각 2715, 2684, 그리고 1611이다. 따라서 TCP-RARE는 불필요한 TCP 혼잡 윈도우의 감소를 최소화하여 TCP-Reno와 TCP-FARE에 비하여 더 성능이 우수함을 그림 14를 통해 확인하였다.

### 5. 결 론

본 논문에서는 다중 홉 무선 네트워크의 성능을 향상시키기 위하여 하위 계층인 MAC 계층과 상위 계층인 전송 계층의 TCP간의 수직적 상호 작용과 네트워크 계층 간의 수평적 상호 작용을 제공하는

CARE 라우팅 기법을 제안하였다. CARE 라우팅 기법의 수평적 상호 작용에서는 패킷의 포워딩 과정에서 악의적으로 행동하거나 무단으로 라우팅 경로에서 이탈하는 이기적인 무선 단말을 우회하도록 라우팅 경로를 설정한다. CARE 라우팅 기법의 수직적 상호 작용에서는 MAC 계층으로부터 획득한 무선 채널의 상황 정보를 반영하여 네트워크 계층에서 구성되는 라우팅 경로의 품질 향상에 반영하고, 또한 네트워크 계층에서 획득한 단말의 평판 정보를 전송 계층인 TCP의 혼잡 제어 기법에 반영하여 TCP의 성능을 향상시킨다. 시뮬레이션을 통해 제안한 CARE 라우팅 기법의 성능을 평가한 결과, CARE 라우팅 기법은 무선 단말의 빈번한 이동에도 불구하고 종단간 패킷 전송률, 종단간 패킷 전송 지연 시간, 그리고 네트워크 성능이 우수함을 확인할 수 있었다. 또한 다중 홉 무선 네트워크 내에 악의적인 단말이 있더라도 CARE 라우팅의 수평적 및 수직적 상호 작용을 통하여 패킷 전송의 낮은 실패율과 패킷의 평균 전송 시간을 향상시키고 동시에 라우팅 경로의 신뢰도가 반영된 TCP-FARE와 TCP-RARE를 사용하여 TCP의 성능을 향상시킬 수 있음을 확인하였다.

### 참 고 문 헌

- [1] D. Johnson, D. Maltz, and Y. Hu, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," IETF RFC 4728, Feb. 2007.
- [2] C. Perkins, E. Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF RFC3561, July. 2003.
- [3] P. Dewan, P. Dasgupta, and A. Bhattacharya, "On using reputations in ad hoc networks to conter malicious nodes," Proc. of the 10th International Conference on Parallel and Distributed Systems, pp. 665-672 July. 2004.
- [4] L. Buttyan and J.P. Hubaux, "Enforcing service availability in mobile ad hoc WANS," Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing, pp. 87-96, Aug. 2000.
- [5] O. Ileri, S.C. Mau, and N. Mandayan, "Pricing

- for enabling forwarding in self-configuring ad hoc networks," *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 1, pp. 151-162, Jan. 2005.
- [6] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks," Proc. of IEEE INFOCOM 2003, pp. 1987-1997, Mar. 2003.
- [7] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Proc. of the 6th IFIP Conference on Communications and Multimedia Security, pp. 107-121, Sep. 2002.
- [8] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of Nodes - Fairness in Dynamic Ad-hoc Network," Proc. of the 3rd IEEE/ACM Symposium on Mobile Ad Hoc Network and Computing, pp. 226-236, Jun. 2002.
- [9] Y. Rebahi, V. Mujica-V, and D. Sisalem, "A reputation-based trust mechanism for ad hoc networks," Proc. of the 10th IEEE Symposium on Computers and Communications, pp. 37-42, Jun. 2005.
- [10] S. Buchegger, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Communication Magazine*, Vol. 43, No. 7, pp. 101-107, July. 2005.
- [11] B. Kim, Y. Fang, T.F. Wong, and Y. Kwon, "Throughput enhancement through dynamic fragmentation in wireless LANs," *IEEE Transaction on Vehicular Technology*, Vol. 54, No. 4, pp. 1415-1425, July. 2005.
- [12] S. Shakkottai, T.S. Rappaport, and P.C. Karlsson, "Cross-layer design for wireless networks," *IEEE Communication Magazine*, Vol. 41, No. 10, pp. 112-119, Oct. 2003.
- [13] V. Srivastava and M. Motani, "Cross-layer design: a survey and the road ahead," *IEEE Communication Magazine*, Vol. 43, No. 12, pp. 112-119, Dec. 2005.
- [14] F. Kevin and S. Floyd, "Simulation-based comparisons of Tahoe, Reno, and SACK TCP," *ACM SIGCOMM Computer Communication Review*, Vol. 26, No. 3, pp. 5-21, July. 1996.
- [15] M. Allman, V. Paxson, and W. Stevens, "TCP congestion control," IETF RFC 2581, Apr. 1999.
- [16] K. Chandran, S. Raghunathan, S. Venkatesan, and R. Prakash, "A feedback based scheme for improving TCP performance in ad hoc wireless networks," *IEEE Personal Communications Magazine*, Vol. 8, No. 1, pp. 34-39, Feb. 2001.
- [17] G. Holland and N. Vaidya, "Analysis of TCP performance over mobile ad hoc networks," Proc. of ACM MOBICOM 1999, pp. 219-230, Aug. 1999.
- [18] J. Liu and S. Singh, "ATCP: TCP for mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, Vol. 19, No. 7, pp. 1300-1315, July. 2001.
- [19] M. Mathis, J. Semke, and J. Mahdavi, "The Macroscopic behavior of the TCP congestion avoidance algorithm," *ACM Computer Communications Review*, Vol. 27, No. 3, July. 1997.
- [20] V. Misra, W. Gong, and D. Towsley, "Fluid-based analysis of a network of AQM routers supporting TCP flows with an application to RED," Proceedings of ACM SIGCOMM, Aug. 2000.



김 태 훈

2006년 2월 부산대학교 정보컴퓨터공학부 공학사  
2008년 2월 부산대학교 컴퓨터공학과 공학석사  
2008년 3월~현재 부산대학교 컴퓨터공학과 박사과정

관심분야 : 무선 네트워크, P2P, 위치인식



탁 성 우

1995년 2월 부산대학교 컴퓨터공학과 공학사  
1997년 2월 부산대학교 컴퓨터공학과 공학석사  
2003년 12월 미국 미주리주립대 Computer Science박사  
2004년 South Dakota State

Univ. 조교수

2004년~현재 부산대학교 정보컴퓨터공학부 부교수  
2004년~현재 부산대학교 컴퓨터 및 정보통신 연구소 겸  
임 연구원

관심분야 : 유무선 네트워크, SoC설계, 실시간 시스템,  
위치인식