



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0027663
(43) 공개일자 2019년03월15일

(51) 국제특허분류(Int. Cl.)
H04W 28/02 (2009.01) H04W 28/26 (2009.01)
H04W 74/02 (2009.01) H04W 88/06 (2009.01)
(52) CPC특허분류
H04W 28/0268 (2013.01)
H04W 28/26 (2013.01)
(21) 출원번호 10-2017-0114726
(22) 출원일자 2017년09월07일
심사청구일자 2017년09월07일
기술이전 희망 : 기술양도

(71) 출원인
울산대학교 산학협력단
울산광역시 남구 대학로 93(무거동)
상명대학교산학협력단
서울특별시 종로구 홍지문2길 20 (홍지동, 상명대학교)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김유라
울산광역시 남구 대학로 93, 8호관 427호 (무거동, 울산대학교)
배윤한
서울특별시 종로구 홍지문2길 20, 종합관 M414호 (홍지동, 상명대학교)
(뒷면에 계속)
(74) 대리인
김중선, 이형석

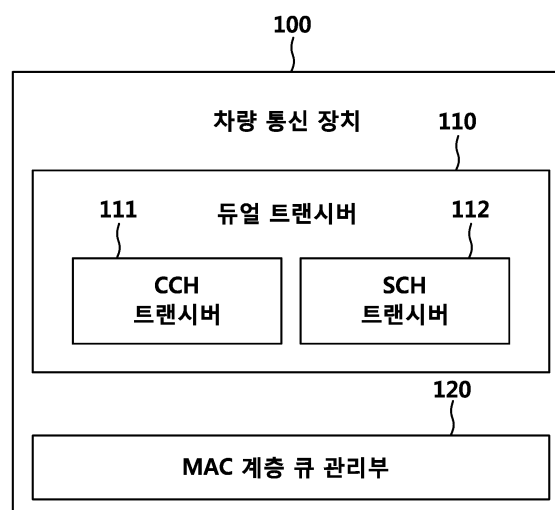
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 차량 환경용 무선 접속을 위한 차량 통신 방법 및 장치

(57) 요약

본 발명은 차량 환경용 무선 접속을 위한 차량 통신 방법 및 장치에 관한 것으로서, 본 발명의 실시 예들은 듀얼 트랜시버를 이용하여 제어 채널과 서비스 채널을 동시에 사용하고, 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 안전 패킷 및 서비스 채널 예약용 패킷을 전송하고 서비스 채널 예약을 통해 비-경쟁 예약기반으로 데이터 파일을 송수신함으로써, 안전 패킷에 대한 서비스 품질의 요구 사항(예컨대, 100ms 이내의 지연과 최소 98%의 성공적인 전달 확률)을 충족시킬 수 있는, 차량 환경용 무선 접속을 위한 차량 통신 방법 및 장치를 제공한다.

대표도 - 도5



(52) CPC특허분류

H04W 74/02 (2013.01)

H04W 88/06 (2013.01)

(72) 발명자

최봉대

서울특별시 동대문구 천장산로9가길 7 (이문동)

업무소속

서울특별시 은평구 불광로 122-10, 3202동 502호
(불광동, 북한산현대힐스테이트)

이 발명을 지원한 국가연구개발사업

과제고유번호 1345247609

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 이공학개인지초연구지원

연구과제명 무선 통신망 설계 및 성능분석에 필요한 대기행렬이론 개발과 응용

기 여 율 25/100

주관기관 울산대학교

연구기간 2016.05.01 ~ 2017.04.30

이 발명을 지원한 국가연구개발사업

과제고유번호 1345254183

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 이공학개인지초연구지원

연구과제명 에너지 하베스팅 무선인지 네트워크의 성능 분석 및 최적화를 위한 대기행렬모형 개발

기 여 율 30/100

주관기관 상명대학교

연구기간 2016.11.01 ~ 2017.10.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1711019441

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 신진연구자지원

연구과제명 IEEE 1609.4/802.11p WAVE 시스템에서 MAC 프로토콜의 성능 분석

기 여 율 40/100

주관기관 성균관대학교

연구기간 2014.05.01 ~ 2015.04.30

이 발명을 지원한 국가연구개발사업

과제고유번호 1345264011

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 개인기초연구(교육부)

연구과제명 차량네트워크의 연결성 분석을 위한 수학적 프레임워크 개발

기 여 율 5/100

주관기관 울산대학교

연구기간 2017.06.01 ~ 2018.02.28

명세서

청구범위

청구항 1

차량 통신 장치에 의해 수행되는 차량 환경용 무선 접속을 위한 차량 통신 방법에 있어서,
경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 안전 패킷(Safety packet)을 송수신하는 단계;
경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 서비스 채널 예약용 패킷(Request for service packet)을 전송하여 서비스 채널을 예약하는 단계; 및
상기 예약된 서비스 채널을 통해 비-경쟁 예약기반으로 데이터 파일(Data file)을 송수신하는 단계;
를 포함하는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 2

제1항에 있어서,
상기 안전 패킷을 송수신하는 단계는,
상기 전송된 안전 패킷에 대한 응답(Acknowledge) 메시지의 수신 여부에 따라 상기 전송된 안전 패킷에 대한 전송 여부를 확인하고, 상기 응답 메시지를 수신한 경우 상기 전송된 안전 패킷의 전송 성공으로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 3

제2항에 있어서,
상기 안전 패킷을 송수신하는 단계는,
상기 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 상기 안전 패킷을 재전송하고, 재전송 제한에 도달하면 상기 전송된 안전 패킷의 전송 실패로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 4

제1항에 있어서,
상기 서비스 채널을 예약하는 단계는,
상기 전송된 서비스 채널 예약용 패킷에 대한 응답 메시지의 수신 여부에 따라 서비스 채널에 대한 예약 여부를 확인하고, 상기 응답 메시지를 수신한 경우 노변 장치로부터 서비스 채널을 할당받고 서비스 채널의 예약 성공으로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 5

제4항에 있어서,
상기 서비스 채널을 예약하는 단계는,
상기 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 상기 서비스 채널 예약용 패킷을 재전송하고, 재전송 제한에 도달하면 서비스 채널의 예약 실패로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 6

제1항에 있어서,
상기 데이터 파일을 송수신하는 단계는,

상기 서비스 채널을 예약하는 단계에서 서비스 채널에 대한 예약 여부에 따라 서비스 채널에 대한 할당 여부를 확인하고, 상기 서비스 채널이 예약된 경우 예약된 서비스 채널을 통해 전송 기회 동안 데이터 파일을 송수신하는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 7

제6항에 있어서,

상기 데이터 파일을 송수신하는 단계는,

상기 서비스 채널의 예약이 실패한 경우, 데이터 파일의 송수신 실패로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 8

제1항에 있어서,

상기 안전 패킷 및 상기 서비스 채널 예약용 패킷은 각각 제1 및 제2 액세스 카테고리 큐에 할당되고, 상기 제1 액세스 카테고리는 상기 제2 액세스 카테고리 큐보다 높은 우선 순위를 가지는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 9

제8항에 있어서,

상기 제1 및 제2 액세스 카테고리 큐는,

상기 제어 채널에서 서로 경쟁하는 차량 환경용 무선 접속을 위한 차량 통신 방법.

청구항 10

입력된 안전 패킷 및 서비스 채널 예약용 패킷을 경쟁 기반의 제어 채널에 대응되는 제1 큐에 할당하고, 입력된 데이터 파일을 비-경쟁 예약 기반의 서비스 채널에 대응되는 제2 큐에 할당하는 MAC 계층 큐 관리부;

경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 안전 패킷을 송수신하고, 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 서비스 채널 예약용 패킷을 전송하여 서비스 채널을 예약하는 제1 트랜시버; 및

상기 예약된 서비스 채널을 통해 비-경쟁 예약기반으로 데이터 파일을 송수신하는 제2 트랜시버;

를 포함하는 차량 환경용 무선 접속을 위한 차량 통신 장치.

청구항 11

제10항에 있어서,

상기 제1 트랜시버는,

상기 전송된 안전 패킷에 대한 응답(Acknowledge) 메시지의 수신 여부에 따라 상기 전송된 안전 패킷에 대한 전송 여부를 확인하고, 상기 응답 메시지를 수신한 경우 상기 전송된 안전 패킷의 전송 성공으로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 장치.

청구항 12

제11항에 있어서,

상기 제1 트랜시버는,

상기 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 상기 안전 패킷을 재전송하고, 재전송 제한에 도달하면 상기 전송된 안전 패킷의 전송 실패로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 장치.

청구항 13

제10항에 있어서,

상기 제1 트랜시버는,

상기 전송된 서비스 채널 예약용 패킷에 대한 응답 메시지의 수신 여부에 따라 서비스 채널에 대한 예약 여부를 확인하고, 상기 응답 메시지를 수신한 경우 노변 장치로부터 서비스 채널을 할당받고 서비스 채널의 예약 성공으로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 장치.

청구항 14

제13항에 있어서,

상기 제1 트랜시버는,

상기 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 상기 서비스 채널 예약용 패킷을 재전송하고, 재전송 제한에 도달하면 서비스 채널의 예약 실패로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 장치.

청구항 15

제10항에 있어서,

상기 제2 트랜시버는,

상기 서비스 채널을 예약하는 단계에서 서비스 채널에 대한 예약 여부에 따라 서비스 채널에 대한 할당 여부를 확인하고, 상기 서비스 채널이 예약된 경우 예약된 서비스 채널을 통해 전송 기회 동안 데이터 파일을 송수신하는 차량 환경용 무선 접속을 위한 차량 통신 장치.

청구항 16

제15항에 있어서,

상기 제2 트랜시버는,

상기 서비스 채널의 예약이 실패한 경우, 데이터 파일의 송수신 실패로 확인하는 차량 환경용 무선 접속을 위한 차량 통신 장치.

청구항 17

제10항에 있어서,

상기 안전 패킷 및 상기 서비스 채널 예약용 패킷은 각각 제1 및 제2 액세스 카테고리 큐에 할당되고, 상기 제1 액세스 카테고리는 상기 제2 액세스 카테고리 큐보다 높은 우선 순위를 가지는 차량 환경용 무선 접속을 위한 차량 통신 장치.

청구항 18

제17항에 있어서,

상기 제1 및 제2 액세스 카테고리 큐는,

상기 제어 채널에서 서로 경쟁하는 차량 환경용 무선 접속을 위한 차량 통신 장치.

발명의 설명

기술 분야

본 발명은 차량 환경용 무선 접속을 위한 차량 통신 방법 및 장치에 관한 것으로서, 더욱 상세하게는 안전 패킷에 대한 서비스 품질의 요구 사항(예컨대, 100ms 이내의 지연과 최소 98%의 성공적인 전달 확률)을 충족시킬 수 있는, 차량 환경용 무선 접속을 위한 차량 통신 방법 및 장치에 관한 것이다.

[0001]

배경 기술

- [0002] 최근, 차량 환경용 무선 접속(WAVE, wireless access in vehicular environments)에 관한 연구에 대한 요구가 학문 분야뿐만 아니라 산업 분야에서도 발생하고 있다. WAVE의 목적은 자동차 통신 장비 및 도로인프라와 함께 전자통신 기술을 사용함으로써, 차량 충돌로 인한 대량 사상자 비용을 줄이면서 운전자에게 안락함과 효율적인 여행을 보장하는 상업 및 엔터테인먼트 서비스를 추가로 제공하는 것이다. 안전 애플리케이션은 차량 간의 비상 패킷 및 상태 패킷 교환을 통해 운전자가 사고를 피할 수 있도록 도와준다. 한편, 인터넷 액세스 및 전자지도 업데이트와 같은 비-안전 애플리케이션은 편의성을 제공한다. WAVE는 최근 업계에서 활발히 개발되고 있는 자율 주행 자동차의 핵심인프라가 될 것이다.
- [0003] ITS(Intelligent Transportation Systems)는 교통운송체계의 안정성과 효율성을 높이고 교통사고 및 도로 혼잡을 감소시킨다. ITS는 운전자의 편안함을 증진시킨다.
- [0004] ITS를 위한 국제 표준 기술을 살펴보면 다음과 같다.
- [0005] IEEE 워킹 그룹은 차량 네트워크에 대한 새로운 통신 표준으로서 차량 환경용 무선 접속(WAVE)이라고 하는 IEEE 802.11p 및 IEEE 1609 표준 제품군을 도입했다. 또한, 유럽 통신 표준 협회에서 운영하는 지능형 교통 시스템의 기술위원회(ETSI TC-ITS)도 유사한 표준인 ITS-G5를 도입했다.
- [0006] WAVE 장치에는 차량 단말기(OBU, on-board unit)와 노변 장치(RSU, roadside unit)의 두 가지 유형이 있다. OBU는 차량에 탑재된 통신 장비이다. RSU는 유선인프라 네트워크에 연결되어 있으며 도로의 고정된 위치에 있다. IEEE 802.11p 및 IEEE 1609.4 표준은 OBU들 간의 V2V(vehicle-to-vehicle) 통신과 OBU 및 RSU 간의 V2I(vehicle-to-infrastructure) 통신을 위한 매체 액세스 제어(MAC) 및 물리 계층(PHY) 프로토콜에 대해 기술하고 있다. IEEE 802.11p는 단일 채널 동작을 위한 MAC 계층을 지정하고, IEEE 1609.4는 다중 채널 동작을 위한 MAC 계층을 지정한다. IEEE 802.11p 및 IEEE 1609.4 표준의 MAC 프로토콜은 채널 라우팅 및 채널 선택기로 구성된 채널 조정 기능을 추가하여 IEEE 802.11e EDCA(enhanced distributed channel access)를 준수한다.
- [0007] 도 1은 IEEE의 WAVE 장비 및 네트워크 구성도를 나타낸 도면이다.
- [0008] WAVE 장비는 도 1과 같이 OBU(on-board unit)와 RSU(roadside unit)로 구분된다. OBU는 차량에 장착된 무선 통신 장비이며 RSU는 도로에 고정되어 유선 인프라 망과 통신을 담당한다. OBU들 사이의 통신을 V2V(vehicle-to-vehicle) 통신이라고 하며, OBU와 RSU 사이의 통신을 V2I(vehicle-to-infrastructure) 통신이라고 한다.
- [0009] IEEE WAVE의 서비스 카테고리에는 안전 애플리케이션(Safety applications) 및 비-안전 애플리케이션(Non-safety applications)이 포함된다. 안전 애플리케이션은 운전자가 사고를 피할 수 있도록 도와준다. 비-안전 애플리케이션은 인터넷 액세스 및 전자지도 업데이트 등 운전자를 위한 편의성을 제공한다.
- [0010] IEEE WAVE의 서비스품질(QoS, Quality of Service)에 대한 요구사항은 다음과 같다.
- [0011] 안전 애플리케이션은 지연(delay) $\leq 100\text{msec}$ 인 조건 및 성공적인 전달 확률(successful delivery probability) $\geq 98\%$ 인 조건을 가진다. 비-안전 애플리케이션은 RSU의 커버리지 내에서 대용량 데이터 파일의 전송이 완료되는 조건을 가진다.
- [0012] 도 2는 WAVE 시스템의 다중 채널 동작을 나타낸 도면이다.
- [0013] 다중 채널 동작과 관련된 표준을 살펴보면 다음과 같다.
- [0014] IEEE 802.11p / IEEE 1609.4는 V2V 및 V2I 통신을 위한 MAC 프로토콜을 지정하고 있다. IEEE 802.11p는 단일 채널 동작을 위한 MAC 프로토콜을 지정하고, IEEE 1609.4는 다중 채널 동작을 위한 MAC 프로토콜을 지정한다.
- [0015] 다중 채널 동작의 경우, 5.850GHz ~ 5.925GHz 주파수 대역에서의 75MHz 대역폭은 도 2와 같이 7개의 10MHz 주파수 채널로 분할된다. 이러한 7개의 채널 중 하나는 제어 채널(CCH)로 지정되고 다른 6개 채널은 서비스 채널(SCH)로 사용된다.
- [0016] 도 3은 싱글 라디오를 위한 채널 동작을 나타낸 도면이다.
- [0017] OBU에는 한 번에 하나의 무선 채널에서만 작동하는 단일 라디오 장치, 또는 제어 채널과 서비스 채널에서 동시에 작동하는 듀얼 라디오 장치가 장착 될 수 있다. 모든 차량이 안전 패킷을 청취할 수 있는 단일 라디오 장치로 MAC 프로토콜을 작동하려면, 채널 시간을 CCH 간격(CCHI)과 SCH 간격(SCHI)으로 구성된 고정 길이 100ms의 동기화 간격으로 분할해야 하며, 둘 다 기본값은 50ms(도 3 참조)이다. 단일 라디오 장치를 가진 OBU는 한 번에

하나의 채널을 통해서만 패킷을 전송할 수 있기 때문에, CCH와 SCH 간의 연속적인 전환이 50ms마다 이루어져야 한다. CCHI 동안 모든 OBU 라디오는 안전 패킷의 송수신을 위해 CCH로 조정된다. SCHI 동안 모든 OBU 라디오는 비-안전 메시지의 송수신을 위해 6개의 SCH 중 1개의 SCH에 맞춰 조정된다.

- [0018] 단일 라디오 장치의 단점은 CCHI 동안 SCH를 사용할 수 없다는 것이며 그 결과 SCH 대역폭의 절반이 낭비된다. 사용 가능한 전송 대역폭을 절반으로 줄이면 안전 애플리케이션에 대한 QoS 요구 사항을 만족시키지 못한다는 것이 연구 결과로 보고되었다. 다중 라디오 장치의 비용 문제로 인해, 현재 IEEE 1609.4 WAVE에서는 OBU에 단일 라디오 장치가 장착되어 있다고 가정한다. 그러나 미래에는 무선 기술의 진보로 인해 라디오 비용이 급격히 떨어지며 듀얼 라디오 장치에 대한 고려가 가능해질 것이다. IEEE 1609.4는 표준의 서두에서 다중 라디오 장치의 채택 가능성에 관해 언급하고 있다. 또한, ITS-G5는 각 OBU가 두 개의 라디오를 가진 것으로 고려한다.

선행기술문헌

특허문헌

- [0019] (특허문헌 0001) 한국 등록특허공보 제10-1690157호 (2016년12월21일 등록)

발명의 내용

해결하려는 과제

- [0020] 본 발명의 실시 예들은 듀얼 트랜시버를 이용하여 제어 채널과 서비스 채널을 동시에 사용하고, 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 안전 패킷 및 서비스 채널 예약용 패킷을 전송하고 서비스 채널 예약을 통해 비-경쟁 예약기반으로 데이터 파일을 송수신함으로써, 안전 패킷에 대한 서비스 품질의 요구 사항(예컨대, 100ms 이내의 지연과 최소 98%의 성공적인 전달 확률)을 충족시킬 수 있는, 차량 환경용 무선 접속을 위한 차량 통신 방법 및 장치를 제공하고자 한다.

과제의 해결 수단

- [0021] 본 발명의 제1 측면에 따르면, 차량 통신 장치에 의해 수행되는 차량 환경용 무선 접속을 위한 차량 통신 방법에 있어서, 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 안전 패킷(Safety packet)을 송수신하는 단계; 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 서비스 채널 예약용 패킷(Request for service packet)을 전송하여 서비스 채널을 예약하는 단계; 및 상기 예약된 서비스 채널을 통해 비-경쟁 예약기반으로 데이터 파일(Data file)을 송수신하는 단계;를 포함하는 차량 환경용 무선 접속을 위한 차량 통신 방법이 제공될 수 있다.
- [0022] 상기 안전 패킷을 송수신하는 단계는, 상기 전송된 안전 패킷에 대한 응답(Acknowledge) 메시지의 수신 여부에 따라 상기 전송된 안전 패킷에 대한 전송 여부를 확인하고, 상기 응답 메시지를 수신한 경우 상기 전송된 안전 패킷의 전송 성공으로 확인할 수 있다.
- [0023] 상기 안전 패킷을 송수신하는 단계는, 상기 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 상기 안전 패킷을 재전송하고, 재전송 제한에 도달하면 상기 전송된 안전 패킷의 전송 실패로 확인할 수 있다.
- [0024] 상기 서비스 채널을 예약하는 단계는, 상기 전송된 서비스 채널 예약용 패킷에 대한 응답 메시지의 수신 여부에 따라 서비스 채널에 대한 예약 여부를 확인하고, 상기 응답 메시지를 수신한 경우 노변 장치로부터 서비스 채널을 할당받고 서비스 채널의 예약 성공으로 확인할 수 있다.
- [0025] 상기 서비스 채널을 예약하는 단계는, 상기 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 상기 서비스 채널 예약용 패킷을 재전송하고, 재전송 제한에 도달하면 서비스 채널의 예약 실패로 확인할 수 있다.
- [0026] 상기 데이터 파일을 송수신하는 단계는, 상기 서비스 채널을 예약하는 단계에서 서비스 채널에 대한 예약 여부에 따라 서비스 채널에 대한 할당 여부를 확인하고, 상기 서비스 채널이 예약된 경우 예약된 서비스 채널을 통해 전송 기회 동안 데이터 파일을 송수신할 수 있다.
- [0027] 상기 데이터 파일을 송수신하는 단계는, 상기 서비스 채널의 예약이 실패한 경우, 데이터 파일의 송수신 실패로 확인할 수 있다.

- [0028] 상기 안전 패킷 및 상기 서비스 채널 예약용 패킷은 각각 제1 및 제2 액세스 카테고리 큐에 할당되고, 상기 제1 액세스 카테고리는 상기 제2 액세스 카테고리 큐보다 높은 우선 순위를 가질 수 있다.
- [0029] 상기 제1 및 제2 액세스 카테고리 큐는, 상기 제어 채널에서 서로 경쟁할 수 있다.
- [0030] 한편, 본 발명의 제2 측면에 따르면, 입력된 안전 패킷 및 서비스 채널 예약용 패킷을 경쟁 기반의 제어 채널에 대응되는 제1 큐에 할당하고, 입력된 데이터 파일을 비-경쟁 예약 기반의 서비스 채널에 대응되는 제2 큐에 할당하는 MAC 계층 큐 관리부; 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 안전 패킷을 송수신하고, 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 서비스 채널 예약용 패킷을 전송하여 서비스 채널을 예약하는 제1 트랜시버; 및 상기 예약된 서비스 채널을 통해 비-경쟁 예약기반으로 데이터 파일을 송수신하는 제2 트랜시버;를 포함하는 차량 환경용 무선 접속을 위한 차량 통신 장치가 제공될 수 있다.
- [0031] 상기 제1 트랜시버는, 상기 전송된 안전 패킷에 대한 응답(Acknowledge) 메시지의 수신 여부에 따라 상기 전송된 안전 패킷에 대한 전송 여부를 확인하고, 상기 응답 메시지를 수신한 경우 상기 전송된 안전 패킷의 전송 성공으로 확인할 수 있다.
- [0032] 상기 제1 트랜시버는, 상기 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 상기 안전 패킷을 재전송하고, 재전송 제한에 도달하면 상기 전송된 안전 패킷의 전송 실패로 확인할 수 있다.
- [0033] 상기 제1 트랜시버는, 상기 전송된 서비스 채널 예약용 패킷에 대한 응답 메시지의 수신 여부에 따라 서비스 채널에 대한 예약 여부를 확인하고, 상기 응답 메시지를 수신한 경우 노변 장치로부터 서비스 채널을 할당받고 서비스 채널의 예약 성공으로 확인할 수 있다.
- [0034] 상기 제1 트랜시버는, 상기 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 상기 서비스 채널 예약용 패킷을 재전송하고, 재전송 제한에 도달하면 서비스 채널의 예약 실패로 확인할 수 있다.
- [0035] 상기 제2 트랜시버는, 상기 서비스 채널을 예약하는 단계에서 서비스 채널에 대한 예약 여부에 따라 서비스 채널에 대한 할당 여부를 확인하고, 상기 서비스 채널이 예약된 경우 예약된 서비스 채널을 통해 전송 기회 동안 데이터 파일을 송수신할 수 있다.
- [0036] 상기 제2 트랜시버는, 상기 서비스 채널의 예약이 실패한 경우, 데이터 파일의 송수신 실패로 확인할 수 있다.
- [0037] 상기 안전 패킷 및 상기 서비스 채널 예약용 패킷은 각각 제1 및 제2 액세스 카테고리 큐에 할당되고, 상기 제1 액세스 카테고리는 상기 제2 액세스 카테고리 큐보다 높은 우선 순위를 가질 수 있다.
- [0038] 상기 제1 및 제2 액세스 카테고리 큐는, 상기 제어 채널에서 서로 경쟁할 수 있다.

발명의 효과

- [0039] 본 발명의 실시 예들은 듀얼 트랜시버를 이용하여 제어 채널과 서비스 채널을 동시에 사용하고, 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 안전 패킷 및 서비스 채널 예약용 패킷을 전송하고 서비스 채널 예약을 통해 비-경쟁 예약기반으로 데이터 파일을 송수신함으로써, 안전 패킷에 대한 서비스 품질의 요구 사항(예컨대, 100ms 이내의 지연과 최소 98%의 성공적인 전달 확률)을 충족시킬 수 있다.
- [0040] 본 발명의 실시 예들은 항상 CCH를 모니터링하여 안전 메시지를 송수신할 수 있으며, 복수의 SCH 중에서 노변 장치가 지정해준 SCH를 통하여 비-안전 메시지를 동시에 송수신할 수 있다.
- [0041] 본 발명의 실시 예들은 제어 채널과 서비스 채널 간의 스위칭이 필요하지 않으며, 채널 스펙트럼의 전체 포텐셜을 이용할 수 있다.
- [0042] 본 발명의 실시 예들은 노변 장치가 송신자에게 안전 패킷의 수신 확인을 허용하여 송신자가 충돌 발생 시 안전 패킷을 재전송함으로써, 브로드캐스팅된 패킷의 신뢰성을 향상시킬 수 있다.
- [0043] 본 발명의 실시 예들은 송신자가 충돌 시(즉, ACK 메시지 미수신 시) 안전 패킷을 재전송함으로써, 안전 패킷의 전송성공확률을 높일 수 있다. 예컨대, 본 발명의 실시 예들은 차량 수가 150 개에 도달하더라도 98% 이상의 성공적인 전달 확률로 100ms 이내에 안전 패킷을 전달할 수 있다.
- [0044] 본 발명의 실시 예들은 액세스 지연에 대한 이점 외에도 차량 수가 적은 희박한 환경에서 CCH를 보다 효율적으로 활용할 수 있다.

도면의 간단한 설명

- [0045] 도 1은 IEEE의 WAVE 장비 및 네트워크 구성도를 나타낸 도면이다.
- 도 2는 WAVE 시스템의 다중 채널 동작을 나타낸 도면이다.
- 도 3은 싱글 라디오를 위한 채널 동작을 나타낸 도면이다.
- 도 4는 본 발명의 실시 예에 따른 차량 통신 장치가 적용되는 시스템 구성을 나타낸 도면이다.
- 도 5는 본 발명의 실시 예에 따른 차량 환경용 무선 접속을 위한 차량 통신 장치의 구성도이다.
- 도 6 및 도 7은 본 발명의 실시 예에 따른 듀얼 트랜시버를 이용한 채널 동작을 나타낸 도면이다.
- 도 8은 본 발명의 실시 예에 따른 차량 통신 장치의 MAC 계층 큐 관리부를 나타낸 도면이다.
- 도 9는 본 발명의 실시 예에 따른 차량 통신 방법에서 제어 채널 및 서비스 채널에서의 각 패킷의 동작을 나타낸 도면이다.
- 도 10은 본 발명의 실시 예에 따른 차량 통신 방법에서 안전 패킷의 전송 흐름도를 나타낸 도면이다.
- 도 11은 본 발명의 실시 예에 따른 차량 통신 방법에서 RFS 패킷의 전송 흐름도를 나타낸 도면이다.
- 도 12는 본 발명의 실시 예에 따른 차량 통신 방법에서 데이터 파일의 송/수신 흐름도를 나타낸 도면이다.
- 도 13은 본 발명의 실시 예에 따른 안전 패킷의 성능 분석에 필요한 마르코프 체인을 나타낸 도면이다.
- 도 14는 본 발명의 실시 예에 따른 RFS 패킷의 성능 분석에 필요한 마르코프 체인을 나타낸 도면이다.
- 도 15는 본 발명의 실시 예에 따른 안전 패킷의 접속 지연의 확률 분포를 나타낸 도면이다.
- 도 16은 본 발명의 실시 예에 따른 안전 패킷의 성공적인 전달 확률을 나타낸 도면이다.
- 도 17은 본 발명의 실시 예에 따른 RFS 패킷의 성공적인 전달 확률을 나타낸 도면이다.
- 도 18은 본 발명의 실시 예에 따른 안전 패킷의 성공적인 전달 확률의 비교 결과를 나타낸 도면이다.
- 도 19 및 도 20은 본 발명의 실시 예에 따른 비-안전 패킷의 성공적인 전달 확률 및 평균 액세스 지연의 비교 결과를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0046] 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 설명한다. 본 발명에 따른 동작 및 작용을 이해하는 데 필요한 부분을 중심으로 상세히 설명한다. 본 발명의 실시 예를 설명하면서, 본 발명이 속하는 기술 분야에 익히 알려졌고 본 발명과 직접적으로 관련이 없는 기술 내용에 대해서는 설명을 생략한다. 이는 불필요한 설명을 생략함으로써 본 발명의 요지를 흐리지 않고 더욱 명확히 전달하기 위함이다.
- [0047] 또한, 본 발명의 구성 요소를 설명하는 데 있어서, 동일한 명칭의 구성 요소에 대하여 도면에 따라 다른 참조부호를 부여할 수도 있으며, 서로 다른 도면임에도 동일한 참조부호를 부여할 수도 있다. 그러나 이와 같은 경우라 하더라도 해당 구성 요소가 실시 예에 따라 서로 다른 기능을 갖는다는 것을 의미하거나, 서로 다른 실시 예에서 동일한 기능을 갖는다는 것을 의미하는 것은 아니며, 각각의 구성 요소의 기능은 해당 실시 예에서의 각각의 구성 요소에 대한 설명에 기초하여 판단하여야 할 것이다.
- [0048] 도 4는 본 발명의 실시 예에 따른 차량 통신 장치가 적용되는 시스템 구성을 나타낸 도면이다.
- [0049] 우선, 본 발명의 실시 예에 따른 차량 통신 장치가 적용되는 시스템 구성에서의 주요 가정을 살펴보기로 한다. 첫째, 다중채널환경이 고려된다. 둘째, 각 OBU에는 듀얼 라디오를 가진 듀얼 트랜시버(dual transceivers)가 장착되어 있다. 셋째, RSU와 같은 통신인프라가 도로에 설치되어 있다.
- [0050] 안전 패킷에 대한 QoS 요구 사항(즉, 100ms 이내의 지연과 최소 98%의 성공적인 전달 확률)을 충족시키기 위해, 본 발명의 주요 가정을 구체적으로 살펴보면 다음과 같다.
- [0051] 모든 OBU에는 듀얼 라디오 장치가 장착되어 있다고 가정한다. 따라서, CCH와 SCH 간의 채널 스위칭은 필요하지 않으며, 채널 스펙트럼의 전체 포텐셜이 이용될 수 있다.

- [0052] 대부분의 비-안전 애플리케이션은 차량과 RSU 간에 데이터 전송을 수반한다. 따라서, RSU와 같은 인프라가 도로에 설치되어 있다고 가정하고 안전 및 비-안전 애플리케이션을 모두 지원하는 MAC 프로토콜을 고려한다. 하나의 RSU에 의해 커버되는 통신 영역인 WAVE 기본 서비스 세트(WBSS, WAVE basic service set)가 고려된다.
- [0053] 안전 패킷은 이웃 차량으로 브로드캐스트되고, 브로드캐스트된 패킷은 일반적으로 응답되지 않는다. 그 결과, 송신자는 실패한 전송을 감지할 수 없으며, 재전송을 위한 이진 백 오프 메커니즘을 사용할 수 없다. 이는 특히 충돌이 심한 차량 밀집 지역에 WAVE 성능 저하를 야기하고, 충돌 경고 장치에 심각한 신뢰성 문제를 초래한다. 모든 OBU는 RSU의 커버리지 내에 있기 때문에, RSU는 OBU로부터 브로드캐스팅된 패킷을 수신할 수 있다. 따라서, 브로드캐스팅된 패킷의 신뢰성을 향상시키기 위해, RSU만이 송신자에게 안전 패킷의 수신 확인을 허용하여 송신자가 충돌 발생 시 안전 패킷을 재전송할 수 있다고 가정한다. 안전 애플리케이션을 지원하기 위해서는 비상 패킷에 대한 다중 홉 브로드캐스트가 요구된다. 본 발명에서, 비상 패킷을 수신한 RSU는 이웃 RSU와 통신하여 비상 패킷을 전달할 수 있다. 그런 다음 이웃 RSU는 전달된 비상 패킷을 자신의 커버리지 내에 있는 차량에 브로드캐스팅한다.
- [0054] 도 5는 본 발명의 실시 예에 따른 차량 환경용 무선 접속을 위한 차량 통신 장치의 구성도이다.
- [0055] 도 5에 도시된 바와 같이, 본 발명의 실시 예에 따른 차량 환경용 무선 접속을 위한 차량 통신 장치(100)는 MAC 계층 큐 관리부(120), 제1 트랜시버(111) 및 제2 트랜시버(112)를 포함한다.
- [0056] 본 발명의 실시 예에 적용되는 듀얼 라디오 장치는 WAVE에서 장기적인 솔루션으로 사용될 것으로 예상되며, 듀얼 라디오 장치를 장착한 차량은 CCH를 통해 안전 메시지를 지속적으로 모니터링할 수 있다. 그러나 이러한 장점에도 불구하고, 듀얼 라디오 장치를 사용하는 WAVE MAC 프로토콜에 대한 연구는 거의 이루어지지 않았다. 본 발명은 듀얼 라디오 장치를 사용하여 WAVE의 안전 및 비-안전 애플리케이션을 모두 지원하는 MAC 프로토콜에 관한 것이다.
- [0057] 듀얼 라디오 장치는 동시에 두 개의 채널을 통해 패킷을 송수신할 수 있다. 듀얼 라디오 중 하나의 라디오(즉, CCH 라디오)는 CCH에 사용되고, 다른 라디오(즉, SCH 라디오)는 지정된 SCH에서 데이터 파일의 동시 교환을 위해 사용된다. 따라서 듀얼 라디오 장치를 사용하면 단일 라디오 장치 사용시 발생하는 비효율적인 채널 이용 문제를 해결하는 데 도움이 된다.
- [0058] 본 발명의 MAC 프로토콜로서, CCH상에서는 경쟁 기반 EDCA 방식을 사용하여 안전 패킷 및 서비스 채널 예약용(RFS, request for service) 패킷을 각각 높은 우선 순위 및 낮은 우선 순위로 전송한다. 반면, SCH상에서는 예약을 통한 비-경쟁 방식을 사용하여 정보 및 상업용 데이터 파일과 같은 비-안전 애플리케이션을 서비스한다.
- [0059] 상기 MAC 프로토콜에 대해, 본 발명은 수학적 분석 모델을 제안하고 주요 성능 지표인 안전 패킷과 RFS 패킷의 성공적인 전달 확률 및 지연을 평가한다. 본 발명의 수학적 분석 모델에서, M/M/K/K/N 큐잉 모델에 기반한 근사화 방법을 제시하고, 안전 패킷 및 RFS 패킷을 위한 두 개의 상호 작용하는 마르코프 체인을 구성한다.
- [0060] 본 발명의 실시 예에 따른 MAC 프로토콜의 성능은 수치 연구 및 시뮬레이션을 통해 검증된다. 수치 결과는 안전 패킷에 대한 QoS 요구 사항이 충족됨을 나타낸다. 즉, 차량 수가 150 개에 도달하더라도 98% 이상의 성공적인 전달 확률로 100ms 이내에 안전 패킷을 전달할 수 있다. 또한 본 발명의 비-경쟁 예약 기반 기법은 경쟁 기반의 랜덤 선택 기법보다 비-안전 패킷의 접근 지연 측면에서 우수한 성능을 보여준다.
- [0061] 이하, IEEE 802.11p / 1609.4 WAVE에서 CCH상의 경쟁 기반 EDCA와 SCH의 예약으로 구성된 본 발명의 MAC 프로토콜을 설명한다. 안전 패킷 및 RFS 패킷을 각각 설명하기로 한다.
- [0062] CCH는 안전 관련 메시지를 제공하고 제어 패킷을 교환하기 위한 공개 채널이다. 안전 패킷은 상태 패킷과 비상 패킷으로 구성된다. 상태 패킷은 위치, 방향, 속도 및 가속도와 같은 차량의 상태에 관한 정보를 포함하며, 모든 차량은 100ms마다 이웃 차량에게 상태 패킷을 브로드캐스트한다. 비상 패킷은 급정거나 자동차 사고와 같은 예기치 않은 사건 발생 시 생성되고, 대형 사고를 예방하기 위해 다른 운전자에게 사고 상황에 대한 사전 정보를 제공한다.
- [0063] SCH는 차량의 사용자가 데이터 파일을 업로드 또는 다운로드하려고 할 때, 데이터 파일의 전송에 사용된다. SCH에 접근하기 위한 두 가지 방법이 있다. 즉, 두 가지 방법은 (i) 예약 기반 방식, (ii) 랜덤 선택 방식이다. 즉 (i) 각 OBU가 예약된 SCH에 접근하도록 CCH에서 예약한다. (ii) 각 OBU가 랜덤하게 SCH를 선택하고, 동일한 SCH를 선택한 OBU들은 SCH에 접근하기 위해 서로 경쟁한다. 도 18, 도 19 및 도 20에서 이 두 가지 방법의 성능을 비교한다. 본 발명에서는 다음과 같은 예약 기반 방식을 사용한다. 데이터 파일을 업로드 또는 다운로드하기 위

해 먼저 SCH를 예약한다. 예약 후, 할당된 SCH를 통해 데이터 파일을 송수신한다. SCH를 예약하기 위해, OBU는 경쟁 방식의 EDCA를 이용하여 CCH상에서 RSU에게 RFS 패킷을 전송한다. RFS 패킷이 성공적으로 전송되었고 사용 가능한 SCH가 있으면, RSU는 OBU에게 SCH 한 개를 할당한다.

- [0064] 본 발명에서는 WAVE의 안전 및 비-안전 애플리케이션을 모두 지원하는 MAC 프로토콜을 고려한다. 애플리케이션 유형에 따라 QoS 요구 사항이 결정된다. 안전 애플리케이션의 경우, 100ms 미만의 매우 짧은 지연과 98% 이상의 높은 성공적인 전달 확률을 QoS 요구 사항으로 갖는다. 왜냐하면, 안전 메시지가 손실(또는 장기 지연)되면 차량이 위험에 관한 경고 메시지를 제공받지 못하여 심각한 사고로 이어질 수 있기 때문이다. 비-안전 애플리케이션의 경우, RSU 커버리지 내에서 서비스가 완료될 수 있도록 대용량 데이터 파일의 전송 시간이 짧아야 한다. 왜냐하면, 빠른 차량 이동성과 좁은 범위의 RSU 커버리지로 인해 차량이 짧은 시간 내에 RSU 커버리지를 통과하기 때문이다.
- [0065] 이하, 도 5의 본 발명의 실시 예에 따른 차량 환경용 무선 접속을 위한 차량 통신 장치(100)의 각 구성요소들의 구체적인 구성 및 동작을 설명한다.
- [0066] MAC 계층 큐 관리부(120)는 입력된 안전 패킷 및 서비스 채널 예약용 패킷을 경쟁 기반의 제어 채널에 대응되는 제1 큐에 할당하고, 입력된 데이터 파일을 비-경쟁 예약 기반의 서비스 채널에 대응되는 제2 큐에 할당한다.
- [0067] 제1 트랜시버(111)는 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 안전 패킷을 송수신하고, 경쟁 기반의 분산 채널 접근 방식에 따라 제어 채널을 통해 서비스 채널 예약용 패킷을 전송하여 서비스 채널을 예약한다. 여기서, 제1 트랜시버(111)는, 전송된 안전 패킷에 대한 응답(Acknowledge) 메시지의 수신 여부에 따라 그 전송된 안전 패킷에 대한 전송 여부를 확인하고, 응답 메시지를 수신한 경우 그 전송된 안전 패킷의 전송 성공으로 확인한다. 제1 트랜시버(111)는, 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 안전 패킷을 재전송하고, 재전송 제한에 도달하면 그 전송된 안전 패킷의 전송 실패로 확인한다. 제1 트랜시버(111)는, 전송된 서비스 채널 예약용 패킷에 대한 응답 메시지의 수신 여부에 따라 서비스 채널에 대한 예약 여부를 확인하고, 응답 메시지를 수신한 경우 노변 장치로부터 서비스 채널을 할당받고 서비스 채널의 예약 성공으로 확인한다. 제1 트랜시버(111)는, 응답 메시지를 미수신한 경우, 재전송 제한에 도달하지 않으면 서비스 채널 예약용 패킷을 재전송하고, 재전송 제한에 도달하면 서비스 채널의 예약 실패로 확인한다.
- [0068] 제2 트랜시버(112)는 제1 트랜시버(111)를 통해 예약된 서비스 채널을 통해 비-경쟁 예약기반으로 데이터 파일을 송수신한다. 여기서, 제2 트랜시버(112)는, 서비스 채널을 예약하는 단계에서 서비스 채널에 대한 예약 여부에 따라 서비스 채널에 대한 할당 여부를 확인하고, 서비스 채널이 예약된 경우 예약된 서비스 채널을 통해 전송 기회 동안 데이터 파일을 송수신한다. 제2 트랜시버(112)는, 서비스 채널의 예약이 실패한 경우, 데이터 파일의 송수신 실패로 확인한다.
- [0069] 상기 안전 패킷 및 서비스 채널 예약용 패킷은 각각 제1 및 제2 액세스 카테고리 큐에 할당되고, 상기 제1 액세스 카테고리는 상기 제2 액세스 카테고리 큐보다 높은 우선 순위를 가진다. 제1 및 제2 액세스 카테고리 큐는, 제어 채널에서 서로 경쟁한다.
- [0070] 도 6 및 도 7은 본 발명의 실시 예에 따른 듀얼 트랜시버를 이용한 채널 동작을 나타낸 도면이다.
- [0071] 본 발명은 ITS 서비스의 안전 애플리케이션 및 비-안전 애플리케이션의 서비스품질 요구사항을 모두 만족하는 IEEE 802.11p / 1609.4 WAVE MAC 프로토콜에 관한 것이다.
- [0072] 도 6과 같이, 차량 통신 장치(100)는 듀얼 트랜시버(110)를 이용하여 제어 채널 및 서비스 채널을 동시에 사용한다. 본 발명의 실시 예에 따른 차량 통신 장치(100)는 듀얼 트랜시버(110)가 장착되어 CCH와 SCH를 동시에 사용할 수 있다. 제1 트랜시버(111)(Transceiver 1) 즉, CCH 트랜시버(111)는 항상 CCH를 모니터링하여 안전 메시지를 송수신할 수 있다. 또한, 제2 트랜시버(112) 즉, SCH 트랜시버(112)는 6개의 SCH중에서 RSU가 지정해준 SCH를 통하여 비-안전 메시지를 송수신할 수 있다.
- [0073] 본 발명의 실시 예에 따른 MAC 프로토콜에는 CCH 접속 방법과 SCH 접속 방법이 있다. CCH 접속은 경쟁 기반의 EDCA 방법이 이용되고, SCH 접속은 비경쟁 기반의 예약 방법이 이용된다.
- [0074] 또한, RSU가 ACK 메시지를 전송하는 방식도 이용된다. RSU는 WBSS 내의 OBU가 브로드캐스트한 안전 패킷을 성공적으로 수신하면 송신자에게 대표로 ACK 메시지를 전송한다. 따라서 송신자는 충돌 시(즉, ACK 메시지 미수신 시) 안전 패킷을 재전송할 수 있다. 이로써, 안전 패킷의 성공적인 전달 확률을 높일 수 있다. IEEE의 WAVE는 안전 애플리케이션의 서비스 품질에 대한 요구사항으로 100ms 이내의 지연과 최소 98%의 성공적인 전달 확률을

요구하고 있다.

- [0075] 본 발명의 실시 예에 따른 차량 통신 장치(100)는 CCH와 SCH를 동시에 사용할 수 있다. CCH에서는 안전 메시지 전송과 비-안전 메시지 전송 예약을 수행한다. 안전 패킷과 RFS 패킷이 CCH에서 EDCA 프로토콜을 따라 서로 경쟁한다. CCH는 비 동기화 되어 있다. SCH에서는 CCH에서 RFS 패킷을 사용하여 예약한 결과에 따라 비-안전 메시지를 송수신한다. 즉, 비경쟁 방식이다.
- [0076] 도 8은 본 발명의 실시 예에 따른 차량 통신 장치(100)의 MAC 계층 큐 관리부(120)를 나타낸 도면이다.
- [0077] 각 차량 통신 장치(100)에서 발생하는 트래픽은 안전 패킷, RFS 패킷 및 데이터 파일로 구분된다.
- [0078] 안전 패킷(Safety packet)은 IEEE WAVE의 안전 애플리케이션과 관련된 패킷이다. 예컨대, 상태 패킷(status packet) 및 긴급 패킷(emergency packet)이 포함된다.
- [0079] 서비스 채널 예약용 패킷(RFS packet)은 하기의 데이터 파일 전송 시 필요한 SCH를 예약하는데 사용되는 패킷이다.
- [0080] 데이터 파일(Data file)은 IEEE WAVE의 비-안전 애플리케이션(non-safety application)과 관련된 패킷이다. 예컨대, 인터넷 접속(Internet access) 및 전자-지도 업데이트(electronic-map update)가 포함된다.
- [0081] 트래픽 종류에 따른 채널 사용과 접속(Access) 방법이 하기의 [표 1]과 같이 나타난다.

표 1

채널 종류	CCH	SCH
트래픽 종류	안전 패킷, RFS 패킷	데이터 파일
접속 방법	EDCA (경쟁 방식)	예약 (비 경쟁 방식)

- [0084] 본 발명의 실시 예에 따른 차량 통신 장치(100)는 1개의 제어 채널에 경쟁 기반(contention-based) EDCA(enhanced distributed channel access) 방법을 이용하여 접속(access)하고, 나머지 6개의 서비스 채널에 비-경쟁 예약(contention-free reservation) 방법을 이용하여 접속한다.
- [0085] 제어 채널을 통해 전송되는 패킷의 종류에는 안전 패킷과 RFS 패킷이 있다.
- [0086] 서비스 채널을 통해 전송되는 패킷의 종류에는 맵 다운로드 및 상업 광고와 같은 비-안전 애플리케이션과 관련된 패킷이 있다.
- [0087] 제어 채널 접속 방법은 안전 패킷을 높은 우선 순위인 AC₁(Access Category 1)로 분류하고, RFS 패킷을 낮은 우선 순위인 AC₂(Access Category 2)로 분류하여 경쟁 기반 EDCA로 제어 채널을 접속한다.
- [0088] 서비스 채널 접속 방법은 비-안전 애플리케이션을 사용할 때마다 제어 채널로 RFS 패킷을 전송하여 서비스 채널을 예약하여 사용한다. 즉, 비-경쟁 예약 방법이 이용된다.
- [0089] CCH 상의 EDCA에서 액세스 카테고리 1(AC[1])과 액세스 카테고리 2(AC[2])를 살펴보면, 각 OBU는 CCH에서 전송되는 트래픽을 두 종류의 액세스 카테고리 1로 구분한다. AC[1]은 높은 우선 순위(high priority)를 가지고, AC[2]는 낮은 우선 순위(low priority)를 가진다. 안전 패킷은 AC[1]에 해당하며, RFS 패킷은 AC[2]에 해당한다. 여기서, EDCA 파라미터는 $AIFS[1] \leq AIFS[2]$, $CW_{min}[1] \leq CW_{min}[2]$ 및 $CW_{max}[1] \leq CW_{max}[2]$ 를 만족하도록 설정한다.
- [0090] 도 9는 본 발명의 실시 예에 따른 차량 통신 방법에서 제어 채널 및 서비스 채널에서의 각 패킷의 동작을 나타낸 도면이다.
- [0091] CCH 상으로 RFS 패킷이 성공적으로 전달되면 SIFS가 경과된 후 ACK 패킷이 전달된다. 이때 도 9의 예시에서 SCH1, SCH2, SCH3 및 SCH6은 사용 중이므로 가용한 유휴 SCH는 SCH4 및 SCH5 이다. ACK 패킷에는 SCH4를 사용하여 TXOP 동안 데이터 파일을 송/수신할 수 있다는 정보를 포함하여 상기 RFS 패킷을 성공적으로 전송한 OBU에 게 전달된다. 상기 OBU는 SCH 라디오를 SCH4로 맞추어 상기 TXOP 동안 데이터 파일을 송/수신한다. ACK 패킷이 전송된 후 비어있지 않은 AC[1] 및 AC[2]는 각각 AIFS[1] 및 AIFS[2] 기간 동안 대기한 후 백 오프 절차를 재개

한다. AC[1] 백 오프 카운터 값이 0에 도달한 OBU는 안전 패킷을 CCH 상으로 전송한다. 이 때 도 9의 예시에서 다른 OBU의 AC[2] 백 오프 카운터 값도 0에 도달하여 RFS 패킷이 CCH 상으로 전송되었다. 따라서 두 패킷은 서로 충돌하게 된다.

- [0092] 비어있지 않은 모든 AC[1]은 충돌을 감지한 후 AIFS[1] 동안 대기한 후 백 오프 절차를 재개한다. 비어있지 않은 모든 AC[2] 역시 충돌을 감지한 후 AIFS[2] 동안 대기한 후 백 오프 절차를 재개한다. AC[1] 백 오프 카운터 값이 0에 도달한 OBU는 안전 패킷을 CCH 상으로 전송한다. 이 때 도 9의 예시에서 모든 AC[2]가 AIFS[2] 동안 대기 중이므로 상기 OBU는 안전 패킷을 성공적으로 전달한다.
- [0093] 이후 AC[2] 백 오프 카운터 값이 0에 도달한 OBU는 RFS 패킷을 CCH 상으로 전송한다. 상기 RFS 패킷은 성공적으로 전달되어 SIFS가 경과된 후 ACK 패킷이 전달된다. 이때 도 9의 예시에서 SCH1, SCH2, SCH4 및 SCH6은 사용 중이므로 가용한 유휴 SCH는 SCH3 및 SCH5이다. ACK 패킷에는 SCH5를 사용하여 TXOP 동안 데이터를 송/수신할 수 있다는 정보를 포함하여 상기 RFS 패킷을 전송한 OBU에게 전달된다. 상기 OBU는 SCH 라디오를 SCH5로 맞추어 상기 TXOP 동안 데이터를 송/수신한다.
- [0094] 도 10은 본 발명의 실시 예에 따른 차량 통신 방법에서 안전 패킷의 전송 흐름도를 나타낸 도면이다.
- [0095] 차량 통신 장치(100)는 전송할 안전 패킷이 있는지를 확인한다(S101).
- [0096] 상기 확인 결과(S101), 전송할 안전 패킷이 있으면, 차량 통신 장치(100)는 EDCA를 이용하여 안전 패킷의 전송을 시도한다(S102). 반면, 상기 확인 결과(S101), 전송할 안전 패킷이 없으면, 차량 통신 장치(100)는 안전 패킷이 있는지를 확인하는 S101 과정을 다시 수행한다.
- [0097] 그리고 차량 통신 장치(100)는 ACK 메시지가 수신되는지를 확인한다(S103).
- [0098] 상기 확인 결과(S103), ACK 메시지가 수신되면, 차량 통신 장치(100)는 안전 패킷의 전송성공으로 판단한다(S104).
- [0099] 한편, 상기 확인 결과(S103), ACK 메시지가 수신되지 않으면, 차량 통신 장치(100)는 재전송 제한에 도달하는지를 확인한다(S105).
- [0100] 상기 확인 결과(S105), 재전송 제한에 도달하지 않으면, 차량 통신 장치(100)는 EDCA를 이용하여 안전 패킷의 전송을 시도하는 S102 과정부터 수행한다.
- [0101] 반면, 상기 확인 결과(S105), 재전송 제한에 도달하면, 차량 통신 장치(100)는 안전 패킷의 전송실패로 판단한다(S106).
- [0102] 도 11은 본 발명의 실시 예에 따른 차량 통신 방법에서 RFS 패킷의 전송 흐름도를 나타낸 도면이다.
- [0103] 차량 통신 장치(100)는 전송할 RFS 패킷이 있는지를 확인한다(S201).
- [0104] 상기 확인 결과(S201), 전송할 RFS 패킷이 있으면, 차량 통신 장치(100)는 EDCA를 이용하여 RFS 패킷의 전송을 시도한다(S202). 반면, 상기 확인 결과(S201), 전송할 RFS 패킷이 없으면, 차량 통신 장치(100)는 RFS 패킷이 있는지를 확인하는 S201 과정을 다시 수행한다.
- [0105] 그리고 차량 통신 장치(100)는 ACK 메시지가 수신되는지를 확인한다(S203).
- [0106] 상기 확인 결과(S203), ACK 메시지가 수신되면, 차량 통신 장치(100)는 RSU로부터 SCH를 할당받았는지를 확인한다(S204).
- [0107] 상기 확인 결과(S204), RSU로부터 SCH를 할당받으면, 차량 통신 장치(100)는 RFS 패킷의 전송성공으로 판단한다(S205). 반면, 상기 확인 결과(S204), RSU로부터 SCH를 할당받지 않으면, 차량 통신 장치(100)는 RFS 패킷의 전송실패로 판단한다(S207).
- [0108] 한편, 상기 확인 결과(S203), ACK 메시지가 수신되지 않으면, 차량 통신 장치(100)는 재전송 제한에 도달하는지를 확인한다(S206).
- [0109] 상기 확인 결과(S206), 재전송 제한에 도달하지 않으면, 차량 통신 장치(100)는 EDCA를 이용하여 RFS 패킷의 전송을 시도하는 S202 과정부터 수행한다.
- [0110] 반면, 상기 확인 결과(S206), 재전송 제한에 도달하면, 차량 통신 장치(100)는 RFS 패킷의 전송실패로 판단한다(S207).

- [0111] 도 12는 본 발명의 실시 예에 따른 차량 통신 방법에서 데이터 파일의 송/수신 흐름도를 나타낸 도면이다.
- [0112] 차량 통신 장치(100)는 전송하거나 받고 싶은 데이터 파일이 있는지를 확인한다(S301).
- [0113] 상기 확인 결과(S301), 전송하거나 받고 싶은 데이터 파일이 있으면, 차량 통신 장치(100)는 RFS 패킷을 생성하고 그 생성된 RFS 패킷을 이용하여 SCH를 예약한다(S302). 반면, 상기 확인 결과(S301), 전송하거나 받고 싶은 데이터 파일이 없으면, 차량 통신 장치(100)는 데이터 파일이 있는지를 확인하는 S301 과정을 다시 수행한다.
- [0114] 그리고 차량 통신 장치(100)는 SCH의 예약이 성공인지를 확인한다(S303).
- [0115] 상기 확인 결과(S303), SCH의 예약이 성공하면, 차량 통신 장치(100)는 예약한 SCH를 통해 전송 기회(TXOP) 동안 데이터 파일을 송/수신한다(S304).
- [0116] 그리고 차량 통신 장치(100)는 데이터 파일의 송/수신성공으로 판단한다(S305).
- [0117] 한편, 상기 확인 결과(S303), SCH의 예약이 성공하지 않으면, 차량 통신 장치(100)는 데이터 파일의 송/수신 실패로 판단한다(S306).
- [0119] 한편, 본 발명의 실시 예에 따른 차량 통신 방법은 CCH에 대한 EDCA와 SCH에 대한 예약으로 구성된 MAC 프로토콜에 관한 것이다.
- [0120] 이하, IEEE 802.11p / 1609.4 WAVE에서 CCH상의 경쟁 기반 EDCA와 SCH의 예약으로 구성된 본 발명의 실시 예에 따른 MAC 프로토콜에 대해 자세히 설명한다.
- [0121] 액세스 카테고리 1(AC_1) 및 액세스 카테고리 2(AC_2)를 살펴보기로 한다. 2개의 액세스 카테고리 AC_1 큐 및 AC_2 큐는 각각 안전 패킷 및 RFS 패킷을 저장하기 위해 각 OBU의 MAC 계층에 존재한다. AC_1 큐 및 AC_2 큐는 CCH 상에서 서비스된다.
- [0122] 상태 패킷은 100ms마다 생성되며, 비상 패킷은 이벤트 구동 발생으로 생성된다. 상태 패킷 및 비상 패킷은 안전 패킷에 해당한다. 안전 패킷이 생성되면 AC_1 큐에 저장된다. 새로 생성된 안전 패킷이 가장 최신의 정보를 가지고 있기 때문에, 오래된 안전 패킷은 새로 생성된 안전 패킷으로 대체된다. 즉, 안전 패킷이 새로 생성될 때 AC_1 큐에서의 이전 안전 패킷이 전송되지 않은 경우, 이전 패킷은 오래되어 새롭게 생성된 패킷으로 대체된다. 따라서 각 OBU는 AC_1 큐에 항상 0개 또는 1개의 안전 패킷을 가지고 있으며, 차량에 전송되는 안전 패킷은 항상 최신 정보를 가지고 있다. RFS 패킷은 차량의 사용자가 데이터 파일을 업로드 또는 다운로드하려고 시도할 때마다 생성된다. 생성된 RFS 패킷은 SCH를 예약하기 위해 AC_2 큐에 저장된다. 데이터 파일은 RFS 패킷의 핸드 셰이크 협상 후에 할당 받은 SCH 상에서 송수신된다.
- [0123] 한편, 백 오프 절차없이 첫 번째 패킷을 전송하는 경우를 살펴보기로 한다.
- [0124] 비어있는 AC_i 큐에 도착한 첫 번째 패킷은 CCH가 DIFS 기간 동안 유향 상태로 감지되면 백 오프 절차없이 즉시 전송된다. CCH가 DIFS 기간 동안 사용 중으로 감지되면, AC_i 는 감지를 중지하고 매체의 사용이 끝날 때까지 대기한다. 대기 후 AC_i 는 패킷 전송을 위해 백 오프 절차를 수행한다. 반면, 비어있지 않은 AC_i 큐에 도착한 패킷은 백 오프 절차를 거쳐 전송되어야 한다.
- [0125] CCH 액세스 프로토콜을 살펴보기로 한다. 안전 패킷 및 RFS 패킷이 CCH에 액세스하는 방식을 설명한다. RFS 패킷 대비 안전 패킷에 높은 우선 순위를 주기 위해, IEEE 802.11e 표준의 EDCA 메커니즘을 채택한다. EDCA는 AIFS(arbitration inter frame space) 및 CW(contention window) 크기와 같은 채널 액세스 파라미터 값들을 각 AC 별로 다르게 설정함으로써 우선 순위 패킷에 대한 차별화된 액세스를 제공한다. 사고를 피하기 위해 안전 패킷에 높은 우선 순위가 부여되고, 반면 RFS 패킷은 낮은 우선 순위가 부여된다. 이에 따라 본 발명에서는 액세스 카테고리 AC_1 및 AC_2 에 대한 채널 액세스 파라미터 값들을 하기와 같이 설정한다.
- [0126] $AC_i (i = 1, 2)$ 에 대한 AIFS 값을 $AIFS_i$ 라 하자. AC_2 대비 AC_1 에 높은 우선 순위를 부여하기 위해

$AIFS_1 \leq AIFS_2$ 를 만족하도록 $AIFS_i$ 를 설정한다. AC_i 는 패킷(즉, AC_1 내의 안전 패킷 또는 AC_2 내의 RFS 패킷)을 전송하기 전에 먼저 $AIFS_i$ 기간 동안 연속적으로 CCH를 감지한다. $AIFS_i$ 기간 동안 CCH가 유휴 상태임을 감지하면, AC_i 는 패킷을 전송한다. 그렇지 않으면(즉, CCH가 사용 중임을 감지하면), AC_i 는 $[0, CW_{min,i} - 1]$ 범위에서 백 오프 카운터 값을 랜덤하게 선택하여, CCH가 사용 중으로 감지된 후 즉시 백 오프 절차를 수행한다. 여기서 $CW_{min,i}$ 는 AC_i 에 대한 최소 CW 크기를 나타낸다. AC_2 대비 AC_1 에 높은 우선 순위를 부여하기 위해 $CW_{min,1} < CW_{min,2}$ 를 만족하도록 $CW_{min,i}$ 를 설정한다. AC_i 는 CCH가 유휴 상태임을 감지할 때마다 백 오프 카운터 값을 감소시키고, CCH가 사용 중임을 감지하면 백 오프 카운터 값을 고정시킨다. 백 오프 카운터 값이 0에 도달하면 AC_i 는 패킷을 전송한다.

[0127] 각 OBU가 안전 패킷 및 RFS 패킷을 생성하고 여러 차량이 단일 RSU의 커버리지 내에 있기 때문에, 다수의 AC_1 과 AC_2 가 CCH에서 서로 경쟁하고 있다. 하나의 OBU에 있는 AC_1 백 오프 카운터와 AC_2 백 오프 카운터가 동시에 0에 도달하면 내부 충돌(internal collision)이 발생한다. 내부 충돌을 피하기 위해 우선 순위가 높은 AC_1 은 안전 패킷을 전송하는 반면, 우선 순위가 낮은 AC_2 는 충돌 발생으로 간주하고 CW 크기를 두 배로 늘려 CCH 액세스에 대한 백 오프 절차를 재개한다. 따라서 AC_1 패킷은 다른 OBU들의 AC_1 패킷 및 AC_2 패킷과 충돌할 수 있다. 반면 AC_2 패킷은 다른 OBU들의 AC_1 패킷 및 AC_2 패킷, 또는 자체 OBU의 AC_1 패킷과 충돌할 수 있다. 충돌이 발생할 때마다, 각 AC_i 는 최대 값 $CW_{max,i}$ 까지 CW 크기를 두 배로 늘린다. AC_i 의 최대 백 오프 단계가 m_i 인 경우 $CW_{max,i}$ 는 아래와 같이 결정된다.

[0129]
$$CW_{max,i} = 2^{m_i} CW_{min,i}$$

[0130] 상기 최대 CW 크기는 재전송 제한 $m_i + f_i$ ($f_i \in \{0, 1, \dots, \infty\}$)까지 유지된다. 그러므로 AC_i 에 대한 k 번째 CW 크기는 다음과 같이 주어진다.

[0132]
$$W_k^i = \begin{cases} 2^k CW_{min,i} & 0 \leq r \leq m_i \\ CW_{max,i} & m_i < r \leq m_i + f_i \end{cases}$$

[0133] 재전송 제한 $m_i + f_i$ 에 도달할 때까지 성공적으로 전송되지 못한 패킷은 AC_i 에서 폐기된다. 본 발명의 분석에서는 $f_1 = \infty$ 및 $f_2 < \infty$ 로 설정하였다. 그러나, 본 발명의 분석은 일반적인 경우로 쉽게 확장될 수 있다.

[0134] 안전 서비스를 위해, 모든 OBU는 CCH에서 안전 패킷을 브로드캐스트한다. 안전 패킷에 대한 QoS 요구 사항인 최소 98%의 성공적인 전달 확률을 보장하기 위해, RSU는 WBSS 내의 OBU가 브로드캐스트한 안전 패킷을 성공적으로 수신하면 송신자에게 대표로 ACK 메시지를 전송한다. 따라서 송신자는 충돌된 패킷이 있는 경우 재전송 할 수 있다.

[0135] 한편, SCH 액세스 프로토콜을 살펴보기로 한다. OBU가 SCH에서 데이터 파일을 송수신하는 방식을 설명한다. 데이터 파일을 업로드/다운로드하고자 하는 OBU는 앞서 설명한 경쟁 기반 EDCA 방식에 따라 먼저 RFS 패킷을 CCH를 통해 RSU로 전송해야 한다. RFS 패킷을 성공적으로 수신한 후, RSU는 현재의 SCH 가용도에 기초하여 서비스

요청을 수락 또는 거절한다. 적어도 하나의 사용 가능한 유휴 SCH가 있다면, 서비스 요청이 수락되고 RSU는 서비스를 요청한 OBU에게 ACK 패킷을 보낸다. ACK 패킷은 사용할 SCH ID와 전송 기회(TXOP)에 대한 정보를 포함한다. 전송 기회란 OBU가 데이터 파일을 독점적으로 송수신할 수 있는 시간 간격을 뜻한다. OBU는 CCH상에서 경쟁 기반 EDCA에 따라 RSU와 성공적인 핸드 셰이크 후, SCH 라디오를 지정된 SCH로 전환한 다음 TXOP 동안 전체 데이터 파일을 한 번에 송/수신하는데 사용한다. RSU가 RFS 패킷을 성공적으로 수신했지만 그 순간에 사용 가능한 유휴 SCH가 없다면, 서비스 요청이 거절되고 RSU는 서비스를 요청한 OBU에게 NAK 패킷을 전송한다. 그러면 OBU는 데이터 파일 송/수신을 포기하고 RFS 패킷을 폐기한다.

[0136] 한편, 본 발명의 수학적 분석 모델 및 기법에 대해서 살펴보기로 한다.

[0137] 본 발명의 분석 기법은 임베디드 이산 시간 마르코프 체인을 이용하여 태그된 AC_i 의 확률적 변화를 모델링하는 것이다. 네트워크에 N 개의 차량과 K 개의 서비스 채널($K = 1, 2, \dots, 6$)이 있다고 하자. 각 OBU는 안전 패킷 및 RFS 패킷을 생성한다. 따라서 N 개의 AC_1 큐와 N 개의 AC_2 큐는 CCH에서 서로 경쟁한다. 본 발명의 분석 모델에 사용되는 주요 가정은 다음과 같다. 실제적인 상황을 반영하기 위해 불포화 조건(즉, 큐가 비어있는 경우도 있음)을 다룬다. 안전 패킷은 모수가 λ_1 인 포아송 과정에 따라 생성된다. 또한 OBU는 데이터 파일의 송/수신이 완료될 때까지 새로운 RFS 패킷을 생성하지 않으며, RFS 패킷은 데이터 파일의 송/수신이 완료된 후, 기댓값이 $1/\lambda_2$ 인 지수 분포를 따라 생성된다. 데이터 파일의 크기는 기댓값이 $E[L_{data}]$ 인 기하 분포를 따른다. 분석의 용이성을 위해 $AIFS_1 = AIFS_2 = DIFS$ 로 설정한다.

[0138] 본 발명의 분석 모델에서 시간 축은 슬롯으로 이산화되며 각 슬롯은 (i) 길이가 σ 인 기본 백 오프 슬롯, (ii) 길이가 $T_{s,1} = T_{safety} + SIFS + T_{ACK} + DIFS$ 인 AC_1 패킷의 성공적인 전송 슬롯, (iii) 길이가 $T_{s,2} = T_{RFS} + SIFS + T_{ACK} + DIFS$ 인 AC_2 패킷의 성공적인 전송 슬롯, (iv) 길이가 $T_{c,1} = T_{safety} + EIFS$ 인 AC_1 패킷만으로 인한 충돌 슬롯, (v) 길이가 $T_{c,2} = T_{RFS} + EIFS$ 인 AC_2 패킷만으로 인한 충돌 슬롯으로 분류될 수 있다. 본 발명에서는 슬롯의 경계를 임베디드 포인트로 설정한다. 두 개의 임의의 연속된 임베디드 포인트 사이의 구간을 일반 슬롯이라고 한다. 분석의 용이성을 위해 관계대로 $T^* \triangleq T_{s,1} = T_{s,2} = T_{c,1} = T_{c,2}$ 라 가정한다. 따라서 일반 슬롯은 길이가 σ 인 유휴 슬롯이거나 아니면 길이가 T^* 인 사용중인 슬롯이 된다.

[0139] 본 발명의 분석에 사용되는 주요 파라미터는 전송 확률 및 조건부 충돌 확률이다. 전송 확률 $\tau_i(i = 1, 2)$ 는 AC_i 가 일반 슬롯에서 패킷 전송을 시도할 확률을 나타낸다. 조건부 충돌 확률 $p_i(i = 1, 2)$ 는 AC_i 가 패킷 전송을 시도한다는 가정하에, 전송된 AC_i 패킷이 충돌을 겪을 확률을 나타낸다. 전송 확률 τ_i 및 조건부 충돌 확률 p_i 는 채널 상태 및 백 오프 이력에 관계없이 일정하다고 가정된다. 상기 파라미터를 찾기 위해 비양키(Bianchi)형 마르코프 체인(Markov chain)과 갱신 보상 과정이 주로 사용된다. 본 발명에서는 비양키형 마르코프 체인 방법을 이용한다.

[0140] 도 13은 본 발명의 실시 예에 따른 안전 패킷의 성능 분석에 필요한 마르코프 체인을 나타낸 도면이다.

[0141] 안전 패킷의 성능 분석을 살펴보기로 한다. AC_1 큐에서 안전 패킷의 지연 및 성공적인 전달 확률을 분석한다. 이를 위해 임의의 AC_1 을 태그된 AC_1 로 간주하고, 각 임베디드 포인트에서 태그된 AC_1 의 확률적 변화를 관찰한다.

[0142] 태그된 AC_1 에 대한 마르코프 체인 모델링을 살펴보기로 한다. $X_1(t)$ 를 t 번째($t = 1, 2, \dots$) 임베디드 포인트

트에서 태그된 AC₁의 상태를 나타내는 확률 변수라 하자. 태그된 AC₁은 (i) 백 오프 상태, (ii) 유티 상태, (iii) 캐리어 감지 상태 중 하나의 상태를 취할 수 있다. AC₁이 t 번째 슬롯 동안 백 오프 절차를 수행하는 경우, AC₁은 t 번째 임베디드 포인트에서 백 오프 상태가 된다. 백 오프 상태는 다음과 같이 표시된다.

$$X_1(t) = (k, j)$$

여기서 $k = 0, 1, \dots, m_1$ 및 $j = 0, 1, \dots, W_k^1 - 1$ 은 태그된 AC₁의 백 오프 단계와 백 오프 카운터 값을 각각 나타내고 $W_k^1 = 2^k CW_{\min,1}$ 이다. 태그된 AC₁은 자신의 큐가 비어있는 경우 유티 상태가 된다. 유티 상태는 다음과 같이 표시된다.

$$X_1(t) = \text{idle}$$

대체가 아닌 안전 패킷은 태그된 AC₁이 유티 상태일 때 생성되거나 또는 이전 안전 패킷이 성공적으로 전송되는 동안만 생성될 수 있다. 유티 상태인 태그된 AC₁에서 안전 패킷이 생성될 때 CCH가 사용 중이 지 않으면, 태그된 AC₁은 CCH가 사용 중으로 감지될 때까지 AIFS₁ 기간 동안 CCH를 감지한다. 상기 캐리어 감지 상태는 다음과 같이 표시된다.

$$X_1(t) = (-1, d), \quad d = 0, 1, \dots, D$$

여기서 $D \triangleq AIFS_1/\sigma$ 는 AIFS₁ 을 유티 슬롯 단위로 환산한 값이며, $X_1(t) = (-1, d)$ 는 태그된 AC₁이 $(D - d)\sigma$ 기간 전부터 t 번째 임베디드 포인트까지 줄곧 CCH가 유티 상태였음을 감지하는 것을 나타낸다.

임베디드 프로세스 $\{X_1(t)\}_{t=1}^{\infty}$ 는 이산 시간 마르코프 체인을 형성하며, 도 13에 도시된 천이 다이어그램을 갖는다. 도 13에 도시된 천이 확률은 각각 다음과 같이 계산된다. 표기법을 간소화하기 위해 아래의 기호를 사용한다.

$$p(y|x) \triangleq P(X_1(t+1) = y \mid X_1(t) = x)$$

본 발명은 우선 $0 \leq k \leq m_1$ 및 $1 \leq j \leq W_k^1 - 1$ 인 k, j 에 대해 $X_1(t) = (k, j)$ 인 경우를 고려한다. 이 경우 AC₁은 다음 임베디드 포인트에서 백 오프 카운터 값을 1 씩 감소시킨다. 따라서 상태 $X_1(t) = (k, j)$ 로부터의 천이 확률은 다음과 같다.

$$p(k, j-1|k, j) = 1$$

이후, 백 오프 카운터 값이 0에 도달하면(즉, $X_1(t) = (k, 0)$), 태그된 AC₁은 안전 패킷을 전송한다. 안전 패킷이 전송되는 동안 태그된 AC₁에서 다른 안전 패킷이 새로 생성될 확률을 p_{arr} 라 하면 다음과 같이 계산된

다.

$$p_{arr} = 1 - e^{-\lambda_1 T^*}$$

그러면, 상태 $X_1(t) = (k, 0)$ 으로부터의 천이 확률은 $0 \leq k < m_1$ 에 대해 다음의 [수학식 1]과 같이 구해진다.

수학식 1

$$p(y|k, 0) = \begin{cases} (1 - p_1)(1 - p_{arr}) & y = \text{idle} \\ (1 - p_1)p_{arr}/W_0^1 & y = (0, j), 0 \leq j \leq W_0^1 - 1 \\ p_1/W_{k+1}^1 & y = (k+1, j), 0 \leq j \leq W_{k+1}^1 - 1 \end{cases}$$

여기서 p_1 은 하기의 [수학식2]에 의해 주어진 조건부 충돌 확률이다.

수학식 2

$$p_1 = 1 - (1 - \tau_1)^{N-1}(1 - \tau_2)^{N-1}$$

만약 $k = m_1$ 이면 천이 확률은 다음의 [수학식 3]과 같다.

수학식 3

$$p(y|k, 0) = \begin{cases} (1 - p_1)(1 - p_{arr}) & y = \text{idle} \\ (1 - p_1)p_{arr}/W_0^1 & y = (0, j), 0 \leq j \leq W_0^1 - 1 \\ p_1/W_m^1 & y = (m_1, j), 0 \leq j \leq W_{m_1}^1 - 1 \end{cases}$$

여기서 [수학식 1]과 [수학식 3]의 첫 번째와 두 번째 항은 AC_1 이 안전 패킷을 성공적으로 전송하는 사건을 나타낸다. 첫 번째 항은 안전 패킷이 성공적으로 전송되는 동안 태그된 AC_1 에서 다른 안전 패킷이 새로 생성되지 않는 경우를 표현한다(따라서 AC_1 은 유힬 상태로 천이된다). 두 번째 항은 안전 패킷이 성공적으로 전송되는 동안 태그된 AC_1 에서 다른 안전 패킷이 새로 생성되는 경우를 표현한다(따라서 AC_1 은 백 오프 단계가 0인 백 오프 상태로 천이된다). t 번째 슬롯에서 전송된 안전 패킷에 충돌이 발생하면, AC_1 은 [수학식 1] 및 [수학식 3]의 마지막 항에 반영되는 백 오프 절차를 반복한다.

다음으로, $X_1(t) = \text{idle}$ 인 경우를 고려하자. 이러한 조건하에 t 번째 슬롯이 유힬 슬롯이며, t 번째 슬롯 동안 태그된 AC_1 에서 안전 패킷이 생성될 확률을 α_1 로 정의하자. 반면 t 번째 슬롯이 사용중인 슬롯이며, t 번

제 슬롯 동안 태그된 AC₁에서 안전 패킷이 생성될 확률을 α_2 로 정의하자. 모수가 λ_1 인 포아송 과정에 따라 안전 패킷이 생성되는 경우, 상기 확률 α_1 , α_2 는 하기의 [수학식 4] 및 [수학식 5]와 같이 계산된다.

수학식 4

$$\alpha_1 = P_{idle}^1(1 - e^{-\lambda_1 \sigma})$$

수학식 5

$$\alpha_2 = (1 - P_{idle}^1)(1 - e^{-\lambda_1 T^*})$$

여기서 P_{idle}^1 은 태그된 AC₁이 안전 패킷을 전송하는 상태가 아니라는 가정하에 유휴 슬롯을 관찰할 조건부 확률을 나타내며 하기의 [수학식 6]에 의해 주어진다.

수학식 6

$$P_{idle}^1 = (1 - \tau_1)^{N-1}(1 - \tau_2)^N$$

따라서 상태 $X_1(t) = idle$ 로부터의 천이 확률은 다음과 같다.

$$p(y|idle) = \begin{cases} \alpha_1 & y = (-1, D) \\ \alpha_2/W_0^1 & y = (0, j), 0 \leq j \leq W_0^1 - 1 \\ 1 - \alpha_1 - \alpha_2 & y = idle \end{cases}$$

여기서 첫 번째와 두 번째 항은 t 번째 슬롯 동안 태그된 AC₁에서 안전 패킷이 생성되는 사건을 나타낸다. t 번째 슬롯 동안 안전 패킷이 생성되지 않으면 AC₁은 유휴 상태로 유지된다.

본 발명은 마지막으로 $X_1(t) = (-1, d)$ 인 경우를 고려한다. 먼저 $1 \leq d \leq D$ 인 경우를 살펴보자. t 번째 슬롯이 유휴 상태이면 태그된 AC₁은 CCH를 계속 감지한다. t 번째 슬롯이 유휴 상태가 아니면 태그된 AC₁은 CCH 감지를 중지하고 백 오프 단계가 0인 백 오프 상태로 천이한다. 따라서 $1 \leq d \leq D$ 인 상태 $X_1(t) = (-1, d)$ 로부터의 천이 확률은 다음과 같다.

$$p(y|-1, d) = \begin{cases} P_{idle}^1 & y = (-1, d-1) \\ (1 - P_{idle}^1)/W_0^1 & y = (0, j), 0 \leq j \leq W_0^1 - 1 \end{cases}$$

$d = 0$ 인 경우를 살펴보자. $X_1(t) = (-1, 0)$ 이면 AC_1 은 t 번째 슬롯 동안 안전 패킷을 전송한다. 이 경우 AC_1 은 $t+1$ 번째 임베디드 포인트에서 유향 상태로 천이되거나 백 오프 단계가 0인 백 오프 상태로 천이된다. 유향 상태로 천이되기 위해서는 t 번째 슬롯 동안 안전 패킷이 성공적으로 전송되어야 하며 패킷 전송 중에 다른 안전 패킷이 새로 생성되지 않아야 한다. 따라서 상태 $X_1(t) = (-1, 0)$ 으로부터의 천이 확률은 다음과 같다.

$$p(y|-1, 0) = \begin{cases} (1 - p_1)(1 - p_{arr}) & y = \text{idle} \\ (p_1 + (1 - p_1)p_{arr})/W_0^1 & y = (0, j), 0 \leq j \leq W_0^1 - 1 \end{cases}$$

한편, 마르코프 체인 $\{X_1(t)\}_{t=1}^{\infty}$ 의 정상 상태 확률을 살펴보기로 한다. 정상 상태 확률을 나타내기 위해 아래의 [수학식 7]의 기호를 사용한다.

수학식 7

$$\begin{aligned} \pi_{idle} &\triangleq \lim_{t \rightarrow \infty} P(X_1(t) = \text{idle}) \\ \pi_{(-1, d)} &\triangleq \lim_{t \rightarrow \infty} P(X_1(t) = (-1, d)) \\ \pi_{(k, j)} &\triangleq \lim_{t \rightarrow \infty} P(X_1(t) = (k, j)) \end{aligned}$$

여기서, $d = 0, 1, \dots, D$, $k = 0, 1, \dots, m_1$, $j = 0, 1, \dots, W_k^1 - 1$ 이다. 정상 상태 확률을 구하기 위해, 도 13에 도시된 천이 다이어그램을 기반으로 하는 균형 방정식을 이용한다. 균형 방정식의 근본적인 원리는, 마르코프 체인 $\{X_1(t)\}_{t=1}^{\infty}$ 의 상태 공간 S의 임의의 부분 집합 E에 대해 하기의 [수학식 8]이 성립된다는 것이다.

수학식 8

$$\sum_{j \in E^c} \sum_{i \in E} \pi_i p(j|i) = \sum_{l \in E} \sum_{k \in E^c} \pi_k p(l|k)$$

[수학식 8]에 적절한 부분 집합 E를 적용함으로써, 정상 상태 확률 $\pi_{(-1, d)}$ 및 $\pi_{(k, j)}$ 를 다음의 [수학식 9] 및 [수학식 10]과 같이 π_{idle} 의 상수배로 나타낼 수 있다.

수학식 9

[0197] $\pi_{(-1,d)} = c_{(-1,d)} \pi_{\text{idle}}$

수학식 10

[0199] $\pi_{(k,j)} = c_{(k,j)} \pi_{\text{idle}}$

[0200] 여기서, 상수 $c_{(-1,d)}$ 및 $c_{(k,j)}$ 는 다음과 같이 주어진다.

[0202] $c_{(-1,d)} = \alpha_1 (P_{\text{idle}}^1)^{D-d}$

[0203]
$$c_{(k,j)} = \begin{cases} \left(\frac{\alpha_1 + \alpha_2}{1 - p_{\text{arr}}} - \alpha_1 (P_{\text{idle}}^1)^D (1 - p_1) \right) \frac{(W_k^1 - j)(p_1)^k}{W_k^1}, & k \neq m_1 \\ \left(\frac{\alpha_1 + \alpha_2}{1 - p_{\text{arr}}} - \alpha_1 (P_{\text{idle}}^1)^D (1 - p_1) \right) \frac{(W_k^1 - j)(p_1)^k}{W_k^1(1 - p_1)}, & k = m_1 \end{cases}$$

[0204] 확률 π_{idle} 은 하기의 정규화 조건을 이용하여 구할 수 있다.

[0206] $\pi_{\text{idle}} + \sum_{d=0}^D \pi_{(-1,d)} + \sum_{k=0}^{m_1} \sum_{j=0}^{W_k^1-1} \pi_{(k,j)} = 1$

[0207] 그 결과는 다음과 같다.

[0209]
$$\pi_{\text{idle}} = \frac{1}{1 + \sum_{d=0}^D c_{(-1,d)} + \sum_{k=0}^{m_1} \sum_{j=0}^{W_k^1-1} c_{(k,j)}}$$

[0210] 이제 마르코프 체인 $\{X_1(t)\}_{t=1}^{\infty}$ 의 정상 분포를 이용하여 전송 확률 τ_1 를 다음의 [수학식 11]과 같이 표현할 수 있다.

수학식 11

[0212]
$$\tau_1 = \pi_{(-1,0)} + \sum_{k=0}^{m_1} \pi_{(k,0)} = \frac{c_{(-1,0)} + \sum_{k=0}^{m_1} c_{(k,0)}}{1 + \sum_{d=0}^D c_{(-1,d)} + \sum_{k=0}^{m_1} \sum_{j=0}^{W_k^1-1} c_{(k,j)}}$$

[0213] 시스템 파라미터 값이 주어지면, [수학식 11]은 두 개의 미지수 τ_1 과 τ_2 의 함수가 된다. 특히, 상수 α_1 , α_2 , P_{idle}^1 및 p_1 은 각각 [수학식 2], [수학식 4], [수학식 5], [수학식 6]에 보인 바와 같이 미지수

τ_1 과 τ_2 를 포함한다. τ_1 과 τ_2 를 구하려면, 관계식 1개가 더 필요하며, 이것은 RFS 패킷의 성능 분석을 통해 유도된다([수학식 26] 참조).

[0215] 한편, 안전 패킷의 지연 및 성공적인 전달 확률에 대해서 설명하기로 한다.

[0216] 안전 패킷의 지연을 S_1 로 표시하자. S_1 은 안전 패킷이 생성된 순간부터 안전 패킷이 성공적으로 전송 완료된 시점까지의 경과 시간으로 정의된다. 전술한 바와 같이, 대체가 아닌 안전 패킷은 태그된 AC₁이 유희 상태일 때 생성되거나 또는 이전 안전 패킷이 성공적으로 전송되는 동안만 생성될 수 있다. 따라서 지연 S_1 은 하기의 $S_{1,a}$, $S_{1,b}$, $S_{1,c}$ 및 $S_{1,d}$ 중 하나에 해당된다.

[0217] $S_{1,a}$ 을 살펴보면, 안전 패킷이 유희 상태에서 생성되고 연속적으로 $d = D$ 에서 $d = 1$ 까지의 캐리어 감지 상태 $(-1, d)$ 를 통과한다는 가정하에, 상기 안전 패킷이 상태 $(-1, 0)$ 에서 전송되는 경우 지연을 나타낸다(이때 성공적으로 또는 충돌이 발생한 전송을 모두 포함한다).

[0218] $S_{1,b}$ 을 살펴보면, 안전 패킷이 유희 상태에서 생성되고 $d = D$ 에서 $d \leq 1$ 까지의 캐리어 감지 상태 $(-1, d)$ 를 통과하지만 상태 $(-1, 0)$ 에 도달하지 않는다는 가정하에, 상기 안전 패킷이 상태 $(0, 0)$ 에서 전송되는 경우 지연을 나타낸다(이때 성공적으로 또는 충돌이 발생한 전송을 모두 포함한다).

[0219] $S_{1,c}$ 을 살펴보면, 안전 패킷이 유희 상태에서 생성되고 어떤 캐리어 감지 상태도 거치지 않는다는 가정하에, 상기 안전 패킷이 상태 $(0, 0)$ 에서 전송되는 경우 지연을 나타낸다(이때 성공적으로 또는 충돌이 발생한 전송을 모두 포함한다).

[0220] $S_{1,d}$ 을 살펴보면, 안전 패킷이 이전의 안전 패킷이 성공적으로 전송되는 동안 생성되었다는 가정하에, 상기 안전 패킷이 상태 $(0, 0)$ 에서 전송되는 경우 지연을 나타낸다(이때 성공적으로 또는 충돌이 발생한 전송을 모두 포함한다).

[0221] 다음으로, $S_{1,a}$, $S_{1,b}$, $S_{1,c}$ 및 $S_{1,d}$ 에 대한 표현식을 도출한다. 달리 언급되지 않는 한, 지연과 관련된 모든 측정 항목은 유희 슬롯 단위로 표시된다. AC₁의 n 번째 백 오프 단계에서 소비된 지연을 B_n^1 이라 하자. B_n^1 의 확률 생성 함수(PGF)는 다음의 [수학식 12]와 같다.

수학식 12

$$E[z^{B_n^1}] = \frac{1}{w_n^1} \{z^0 + \sum_{v=1}^{w_n^1-1} (P_{\text{idle}}^1 z + (1 - P_{\text{idle}}^1) z^T)^v\}$$

[0224] 여기서 $T \triangleq T^*/\sigma$ 는 안전 패킷의 전송 시간을 나타낸다. B_n^1 을 이용하여 $S_{1,a}$ 를 다음의 [수학식 13]과 같이 표현할 수 있다.

수학식 13

$$S_{1,a} = \begin{cases} D + T, & \text{w.p. } (1 - p_1) \\ D + T + \sum_{n=0}^k (B_{\min\{n, m_1\}}^1 + T), & \text{w.p. } (p_1)^{k+1}(1 - p_1) \end{cases}$$

여기서, $k = 0, 1, 2, \dots$ 이다. [수학식 13]의 첫 번째 항은 안전 패킷이 상태 $(-1, 0)$ 에서 성공적으로 전송되는 경우를 나타낸다. 그렇지 않은 경우, [수학식 13]의 두 번째 항에서 표현된 바와 같이, 안전 패킷은 성공적으로 전송될 때까지 $k + 1$ 회($k = 0, 1, \dots$) 재전송된다.

캐리어 감지가 상태 $(-1, 0)$ 까지 지속되지 않는다는 가정하에, 캐리어 감지 상태에서 소비된 지연을 A_1 이라 하자. A_1 의 PGF는 다음과 같다.

$$E[z^{A_1}] = \frac{1}{1 - (P_{\text{idle}}^1)^D} \sum_{m=1}^D (P_{\text{idle}}^1)^{m-1} (1 - P_{\text{idle}}^1) z^{m-1+T}$$

A_1 을 이용하여 $S_{1,b}$ 를 다음의 [수학식 14]와 같이 표현할 수 있다.

수학식 14

$$S_{1,b} = A_1 + \sum_{n=0}^k (B_{\min\{n, m_1\}}^1 + T) \quad \text{w.p. } (p_1)^k(1 - p_1)$$

여기서 $k = 0, 1, \dots$ 은 안전 패킷이 성공적으로 전송될 때까지의 총 재전송 횟수를 나타낸다. 위와 마찬가지로 $S_{1,c}$ 를 다음의 [수학식 15]와 같이 표현할 수 있다.

수학식 15

$$S_{1,c} = \sum_{n=0}^k (B_{\min\{n, m_1\}}^1 + T) \quad \text{w.p. } (p_1)^k(1 - p_1)$$

여기서, $k = 0, 1, \dots$ 이다. 안전 패킷이 이전 안전 패킷의 성공적인 전송 기간 중에 생성되면, AC_1 은 캐리어 감지 상태를 거치지 않고 백 오프 상태로 진입한다. 따라서, $S_{1,d}$ 는 다음의 [수학식 16]과 같이 $S_{1,c}$ 와 동일한 분포를 가진다.

수학식 16

$$S_{1,d} = \sum_{n=0}^k (B_{\min\{n,m_1\}}^1 + T) \quad \text{w. p. } (p_1)^k(1-p_1)$$

여기서, $k = 0, 1, \dots$ 이다. [수학식 13], [수학식 14], [수학식 15] 및 [수학식 16]을 각각 이용하면 $S_{1,a}$, $S_{1,b}$, $S_{1,c}$ 및 $S_{1,d}$ 의 PGF를 구할 수 있다. S_1 의 PGF는 다음과 같이 유도된다.

$$E[z^{S_1}] = \omega_1^a E[z^{S_{1,a}}] + \omega_1^b E[z^{S_{1,b}}] + \omega_1^c E[z^{S_{1,c}}] + \omega_1^d E[z^{S_{1,d}}]$$

여기서, ω_1^a , ω_1^b , ω_1^c 및 ω_1^d 는 다음과 같다.

$$\omega_1^a = \frac{\pi_{\text{idle}} \alpha_1 (P_{\text{idle}}^1)^D}{\pi_{\text{idle}}(\alpha_1 + \alpha_2) + \tau_1(1-p_1)(1-e^{-\lambda_1 T^*})}$$

$$\omega_1^b = \frac{\pi_{\text{idle}} \alpha_1 (1-(P_{\text{idle}}^1)^D)}{\pi_{\text{idle}}(\alpha_1 + \alpha_2) + \tau_1(1-p_1)(1-e^{-\lambda_1 T^*})}$$

$$\omega_1^c = \frac{\pi_{\text{idle}} \alpha_2}{\pi_{\text{idle}}(\alpha_1 + \alpha_2) + \tau_1(1-p_1)(1-e^{-\lambda_1 T^*})}$$

$$\omega_1^d = \frac{\tau_1(1-p_1)(1-e^{-\lambda_1 T^*})}{\pi_{\text{idle}}(\alpha_1 + \alpha_2) + \tau_1(1-p_1)(1-e^{-\lambda_1 T^*})}$$

최종적으로 지연 S_1 의 확률 분포 함수는 PGF $E[z^{S_1}]$ 로부터 구할 수 있다.

각 안전 패킷은 전달 마감 기한 $L (= 100\text{ms})$ 이내에 이웃 차량에게 전송되어야 한다. AC_1 에 대한 재전송 제한을 ∞ 로 설정 했으므로, 안전 패킷은 전달 마감 기한이 만료되기 전에 전달되면 성공적으로 전달된 것으로 간주된다. 따라서 안전 패킷의 성공적인 전달 확률 P_{succ}^1 은 S_1 의 확률 분포로부터 다음과 같이 구해진다.

$$P_{\text{succ}}^1 = P(S_1 < L)$$

도 14는 본 발명의 실시 예에 따른 RFS 패킷의 성능 분석에 필요한 마르코프 체인을 나타낸 도면이다.

RFS 패킷의 성능 분석을 살펴보기로 한다. AC_2 큐에서 RFS 패킷의 지연 및 성공적인 전달 확률을 분석한다. 이를 위해 임의의 AC_2 를 태그된 AC_2 로 간주하고, 각 임베디드 포인트에서 태그된 AC_2 의 확률적 변화를 관찰한다. RFS 패킷의 성능 분석 방법은 안전 패킷의 성능 분석 방법과 유사하다. 따라서 여기서는 차이점만 강조하여 단순화하여 설명하기로 한다.

태그된 AC_2 에 대한 마르코프 체인 모델링을 살펴보기로 한다.

$X_2(t)$ 를 t 번째 임베디드 포인트에서 태그된 AC_2 의 상태를 나타내는 확률 변수라 하자. 태그된 AC_2 는 (i) 백 오프 상태, (ii) SCH 상으로 데이터 파일을 전송하는 상태, (iii) 유휴 상태, (iv) 캐리어 감지 상태 중 하나의

상태를 취할 수 있다. 태그된 AC₂가 백 오프 상태이면 하기와 같이 표시된다.

$$X_2(t) = (k, j)$$

여기서 $k = 0, 1, \dots, m_2 + f_2$, $j = 0, 1, \dots, W_k^2 - 1$ 및 $W_k^2 = 2^{\min(k, m_2)} CW_{\min, 2}$ 이다. 태그된 AC₂가 RFS 패킷을 성공적으로 전송하고 사용 가능한 SCH가 있으면, 그 중 하나의 SCH를 할당받는다. 태그된 AC₂는 할당된 SCH를 통해 데이터 파일을 송수신한다. 이 경우, $X_2(t)$ 는 하기와 같이 표시된다.

$$X_2(t) = tx$$

태그된 AC₂는 자신의 큐가 비어있는 경우 유헴 상태가 된다. 유헴 상태는 다음과 같이 표시된다.

$$X_2(t) = \text{idle}$$

RFS 패킷은 태그된 AC₂가 유헴 상태일 때만 생성될 수 있다. RFS 패킷이 생성될 때 CCH가 사용 중이 지 않으면, AC₂는 캐리어 감지 상태가 되며 다음과 같이 표시된다.

$$X_2(t) = (-1, d), \quad d = 0, 1, \dots, D$$

임베디드 프로세스 $\{X_2(t)\}_{t=1}^{\infty}$ 는 이산 시간 마르코프 체인을 형성하며, 도 14에 도시된 천이 다이어그램을 갖는다. 도 14에 도시된 천이 확률은 각각 다음과 같이 계산된다. 표기법을 간소화하기 위해 아래의 기호를 사용한다.

$$p(y|x) \triangleq P(X_2(t+1) = y | X_2(t) = x)$$

먼저, 백 오프 상태 $X_2(t) = (k, j)$ (단, $0 \leq k \leq m_2 + f_2$ 및 $1 \leq j \leq W_k^2 - 1$) 로부터의 천이 확률은 다음과 같다.

$$p(k, j-1 | k, j) = 1$$

백 오프 카운터 값이 0에 도달하면(즉, $X_2(t) = (k, 0)$), 태그된 AC₂는 RFS 패킷을 전송한다. 태그된 AC₂가 RFS 패킷을 성공적으로 전송한 직후 모든 K 개의 SCH가 사용중일 확률을 p_{full} 이라 하자. 그러면, 상태 $X_2(t) = (k, 0)$ 으로부터의 천이 확률은 $0 \leq k < m_2 + f_2$ 에 대해 다음의 [수학식 17]과 같이 유도된다.

수학식 17

$$p(y|k, 0) = \begin{cases} (1-p_2)(1-p_{full}) & y = tx \\ (1-p_2)p_{full} & y = idle \\ p_2/W_{k+1}^2 & y = (k+1, j), 0 \leq j \leq W_{k+1}^2 - 1 \end{cases}$$

여기서 p_2 는 하기의 [수학식 18]에 의해 주어진 조건부 충돌 확률이다.

수학식 18

$$p_2 = 1 - (1 - \tau_1)^N (1 - \tau_2)^{N-1}$$

만약 $k = m_2 + f_2$ 이면 천이 확률은 다음의 [수학식 19]와 같다.

수학식 19

$$p(y|k, 0) = \begin{cases} (1-p_2)(1-p_{full}) & y = tx \\ (1-p_2)p_{full} + p_2 & y = idle \end{cases}$$

여기서, [수학식 17] 및 [수학식 19]의 첫 번째 항은 RFS 패킷의 성공적인 전송 후에 SCH가 태그된 AC₂에 할당되는 사건을 나타낸다. [수학식 17] 및 [수학식 19]의 두 번째 항은 태그된 AC₂가 RFS 패킷을 폐기하는 사건을 나타낸다. 이러한 사건은 RFS 패킷이 성공적으로 전송된 직후 K 개의 모든 SCH가 사용 중이거나, RFS 패킷이 충돌된 후 재전송 제한에 도달한 경우($k = m_2 + f_2$ 인 경우 가능) 발생한다. RFS 패킷에 충돌이 발생하였으나 재전송 제한에 도달하지 않은 경우, AC₂는 [수학식 17]의 마지막 항에 반영되는 백 오프 절차를 반복한다.

다음으로, $X_2(t) = tx$ 인 경우(즉, 태그된 AC₂가 t 번째 임베디드 포인트에서 SCH상으로 데이터 파일을 전송하는 상태)를 고려하자. 태그된 AC₂의 파일 전송이 $t+1$ 번째 임베디드 포인트까지 계속될 확률을 p_{tx} 라 하자. 데이터 파일의 크기가 기댓값이 $E[L_{data}]$ 인 기하 분포를 따르면, 파일 전송 시간은 기댓값이 $(1-q)^{-1} = E[L_{data}]/(R\sigma)$ 인 기하 분포를 따르게 된다. 여기서 R 은 데이터 속도이다. 따라서, 확률 p_{tx} 는 하기의 [수학식 20]과 같다.

수학식 20

$$p_{tx} = qP_{idle}^2 + q^T(1 - P_{idle}^2)$$

[0288] 여기서 P_{idle}^2 은 태그된 AC₂가 RFS 패킷을 전송하는 상태가 아니라는 가정하에 유헤 슬롯을 관찰할 조건부 확률을 나타내며 하기의 [수학식 21]에 의해 주어진다.

[0289]

수학식 21

$$P_{idle}^2 = (1 - \tau_1)^N (1 - \tau_2)^{N-1}$$

[0290]

[0291] 따라서 상태 $X_2(t) = tx$ 로부터의 천이 확률은 다음과 같다.

$$p(y|tx) = \begin{cases} p_{tx} & y = tx \\ 1 - p_{tx} & y = idle \end{cases}$$

[0293]

[0294] $X_2(t) = idle$ 이라고 가정하자. 이러한 조건하에 t 번째 슬롯이 유헤 슬롯이며, t 번째 슬롯 동안 태그된 AC₂에서 RFS 패킷이 생성될 확률을 β_1 로 정의하자. 반면 t 번째 슬롯이 사용중인 슬롯이며, t 번째 슬롯 동안 태그된 AC₂에서 RFS 패킷이 생성될 확률을 β_2 로 정의하자. 모수가 λ_2 인 포아송 과정에 따라 데이터 파일이 생성되는 경우, 상기 확률 β_1 및 β_2 는 다음의 [수학식 22] 및 [수학식 23]과 같이 계산된다.

수학식 22

$$\beta_1 = P_{idle}^2 (1 - e^{-\lambda_2 \sigma})$$

[0296]

수학식 23

$$\beta_2 = (1 - P_{idle}^2)(1 - e^{-\lambda_2 T^*})$$

[0298]

[0299] 상태 $X_2(t) = idle$ 로부터의 천이 확률은 AC₁의 천이 확률에서 $\alpha_1, \alpha_2, W_0^1$ 를 각각 β_1, β_2, W_0^2 로 대체함으로써 아래와 같이 구할 수 있다. 유사성 때문에 자세한 설명은 생략한다.

$$p(y|idle) = \begin{cases} \beta_1 & y = (-1, D) \\ \beta_2 / W_0^2 & y = (0, j), 0 \leq j \leq W_0^2 - 1 \\ 1 - \beta_1 - \beta_2 & y = idle \end{cases}$$

[0301]

[0302] $1 \leq d \leq D$ 인 상태 $X_2(t) = (-1, d)$ 로부터의 천이 확률은 다음과 같다.

$$p(y|-1, d) = \begin{cases} P_{\text{idle}}^2 & y = (-1, d-1) \\ (1 - P_{\text{idle}}^2)/W_0^2 & y = (0, j), 0 \leq j \leq W_0^2 - 1 \end{cases}$$

$X_2(t) = (-1, 0)$ 일 때, 태그된 AC₂는 $0 \leq k < m_2 + f_2$ 인 상태 $X_2(t) = (k, 0)$ 과 같은 방식으로 동작한다. 그러므로 [수학식 17]을 적용함으로써 상태 $X_2(t) = (-1, 0)$ 으로부터의 천이 확률이 다음과 같이 구해진다.

$$p(y|-1, 0) = \begin{cases} (1 - p_2)(1 - p_{\text{full}}) & y = \text{tx} \\ (1 - p_2)p_{\text{full}} & y = \text{idle} \\ p_2/W_0^2 & y = (0, j), 0 \leq j \leq W_0^2 - 1 \end{cases}$$

한편, p_{full} 을 구하는 과정을 살펴보면 다음과 같다.

p_{full} 에 대한 정확한 공식은 네트워크 내의 모든 AC₂들의 상태를 추적하는 $2N$ -차원 마르코프 체인을 사용하여 도출할 수 있다. 그러나, 이 기법은 큰 값을 가지는 N 에 대해 계산 복잡성을 수반한다. 복잡성 문제를 피하기 위해, N 개의 유한 소스를 갖는 M/M/K/K/N 큐잉 모델에 기반하여 p_{full} 에 대한 근사 공식을 제시한다. Engset 모델로 알려진 M/M/K/K/N 시스템은 K 개의 서버와 N 개의 유한 소스로 구성된다. 모든 K 개의 서버가 사용 중인 경우, 도착 고객은 시스템에 진입하지 못하고 지수 분포를 따르는 랜덤 시간 후에 재진입을 시도한다. 도착 고객이 K 개의 서버가 모두 사용 중인 것을 발견할 확률(즉, Engset 손실 공식)은 다음의 [수학식 24]와 같다.

수학식 24

$$\frac{1}{\sum_{i=0}^K \binom{N-1}{i} \left(\frac{\lambda}{\mu}\right)^i} \binom{N-1}{K} \left(\frac{\lambda}{\mu}\right)^K$$

여기서 λ 와 μ 는 각각 Engset 모델에서 소스의 도착률과 서버의 서비스율을 나타낸다.

본 발명은 Engset 모델에서 K 개의 서버와 N 개의 유한 소스를 각각 K 개의 SCH와 N 개의 AC₂로 간주한다. 또한 도착 간격 및 서비스 시간과 비교할 때, 백 오프 절차에서의 경쟁 시간은 무시할 정도로 작기 때문에 0으로 근사한다. 그러면, 각 RFS 패킷은 모수가 λ_2 인 포아송 과정에 따라 AC₂에서 생성되기 때문에 $\lambda = \lambda_2$ 가 된다. 또한, SCH상의 파일 전송 시간은 기댓값이 $E[L_{\text{data}}]/R$ 인 기하 분포를 따르기 때문에 $\mu = R/E[L_{\text{data}}]$ 가 된다. 따라서 [수학식 24]의 Engset 손실 공식으로부터 하기와 같이 p_{full} 에 대한 근사 공식이 구해진다.

$$p_{\text{full}} \approx \frac{1}{\sum_{i=0}^K \binom{N-1}{i} \left(\frac{\lambda_2 R}{E[L_{\text{data}}]}\right)^i} \binom{N-1}{K} \left(\frac{\lambda_2 R}{E[L_{\text{data}}]}\right)^K$$

수치 연구와 시뮬레이션을 사용하여 근사의 정확성을 검증한다(도 15 참조).

한편, 정상 상태 확률에 대해서 살펴보기로 한다. 다음의 [수학식 25]와 같이 표시된 마르코프 체인 $\{X_2(t)\}_{t=1}^{\infty}$ 의 정상 상태 확률을 구한다.

수학식 25

$$\begin{aligned} \chi_{\text{idle}} &\triangleq \lim_{t \rightarrow \infty} P(X_2(t) = \text{idle}) \\ \chi_{(-1,d)} &\triangleq \lim_{t \rightarrow \infty} P(X_2(t) = (-1, d)) \\ \chi_{(k,j)} &\triangleq \lim_{t \rightarrow \infty} P(X_2(t) = (k, j)) \\ \chi_{\text{tx}} &\triangleq \lim_{t \rightarrow \infty} P(X_2(t) = \text{tx}) \end{aligned}$$

여기서, $d = 0, 1, \dots, D$, $k = 0, 1, \dots, m_2 + f_2$, $j = 0, 1, \dots, W_k^2 - 1$ 이다. 균형 방정식 [수학식 8]에 적절한 부분 집합 E를 적용함으로써, 정상 분포 $\chi_{(-1,d)}$, $\chi_{(k,j)}$, χ_{tx} 각각을 다음과 같이 χ_{idle} 의 상수배로 나타낼 수 있다.

$$\chi_{(-1,d)} = \xi_{(-1,d)} \chi_{\text{idle}}$$

$$\chi_{(k,j)} = \xi_{(k,j)} \chi_{\text{idle}}$$

$$\chi_{\text{tx}} = \xi_{\text{tx}} \chi_{\text{idle}}$$

여기서, 상수 $\xi_{(-1,d)}$, $\xi_{(k,j)}$ 및 ξ_{tx} 는 다음과 같이 주어진다.

$$\xi_{(-1,d)} = \beta_1 (P_{\text{idle}}^2)^{D-d}$$

$$\xi_{(k,j)} = (\beta_1 + \beta_2 - \beta_1 (P_{\text{idle}}^2)^D (1 - p_2)) \left(1 - \frac{j}{W_k^2}\right) (p_2)^k$$

$$\xi_{\text{tx}} = \frac{1-p_{\text{full}}}{1-p_{\text{tx}}} ((\beta_1 + \beta_2)(1 - (p_2)^{m_2+f_2+1}) + \beta_1 (P_{\text{idle}}^2)^D (1 - (p_2)^{m_2+f_2+1}))$$

확률 χ_{idle} 은 하기의 정규화 조건을 이용하여 구할 수 있다.

$$\chi_{\text{idle}} + \sum_{d=0}^D \chi_{(-1,d)} + \sum_{k=0}^{m_2+f_2} \sum_{j=0}^{W_k^2-1} \chi_{(k,j)} + \chi_{\text{tx}} = 1$$

그 결과는 다음과 같다.

$$\chi_{\text{idle}} = \frac{1}{1 + \sum_{d=0}^D \xi_{(-1,d)} + \sum_{k=0}^{m_2+f_2} \sum_{j=0}^{W_k^2-1} \xi_{(k,j)} + \xi_{\text{tx}}}$$

이제 마르코프 체인 $\{X_2(t)\}_{t=1}^{\infty}$ 의 정상 상태 확률을 이용하여 전송 확률 τ_2 를 다음의 [수학식 26]과 같이 표현할 수 있다.

수학식 26

$$\tau_2 = \chi_{(-1,0)} + \sum_{k=0}^{m_2+f_2} \chi_{(k,0)} = \frac{\xi_{(-1,0)} + \sum_{k=0}^{m_2+f_2} \xi_{(k,0)}}{1 + \sum_{d=0}^D \xi_{(-1,d)} + \sum_{k=0}^{m_2+f_2} \sum_{j=0}^{W_k^2-1} \xi_{(k,j)} + \xi_{\text{tx}}}$$

시스템 파라미터 값이 주어지면, [수학식 26]은 두 개의 미지수 τ_1 과 τ_2 의 함수가 된다. 특히, 상수 β_1 , β_2 , P_{idle}^2 , p_2 및 p_{tx} 는 각각 [수학식 22], [수학식 23], [수학식 21], [수학식 18], [수학식 20]에 보인 바와 같이 미지수 τ_1 과 τ_2 를 포함한다. [수학식 11]과 [수학식 26]을 연립하여 풀면 τ_1 과 τ_2 를 구할 수 있다.

한편, RFS 패킷의 지연 및 성공적인 전달 확률에 대해서 살펴보기로 한다.

RFS 패킷의 지연을 S_2 로 표시하자. S_2 는 태그된 AC₂가 RFS 패킷을 생성한 순간부터 SCH를 할당받거나(즉, RFS 패킷이 성공적으로 전달됨), RFS 패킷을 폐기하는(재전송 제한 또는 SCH의 비가용성으로 인해) 시점까지의 경과 시간으로 정의된다. 따라서 지연 S_2 는 하기의 $S_{2,a}$, $S_{2,b}$ 및 $S_{1,c}$ 중 하나에 해당된다.

$S_{2,a}$ 는 연속적으로 $d = D$ 에서 $d = 1$ 까지의 캐리어 감지 상태 $(-1, d)$ 를 거친 후, 상태 $(-1, 0)$ 에서 전송되는 RFS 패킷의 지연을 나타낸다.

$S_{2,b}$ 는 $d = D$ 에서 $d \leq 1$ 까지의 캐리어 감지 상태 $(-1, d)$ 를 거친 후(그러나 상태 $(-1, 0)$ 에 도달하지 않음) 상태 $(0, 0)$ 에서 전송되는 RFS 패킷의 지연을 나타낸다.

$S_{2,c}$ 는 어떤 캐리어 감지 상태를 거치지 않고, 상태 $(0, 0)$ 에서 전송되는 RFS 패킷의 지연을 나타낸다.

$S_{2,a}$, $S_{2,b}$ 및 $S_{2,c}$ 의 표현식은 각각 [수학식 27], [수학식 28] 및 [수학식 29]와 같다.

수학식 27

$$S_{2,a} = \begin{cases} D + T & \text{w.p. } (1 - p_2) \\ D + T + \sum_{n=0}^k (B_{\min\{n,m_2\}}^2 + T) & \text{w.p. } (p_2)^{k+1}(1 - p_2), \quad 0 \leq k \\ D + T + \sum_{n=0}^{m_2+f_2} (B_{\min\{n,m_2\}}^2 + T) & \text{w.p. } (p_2)^{m_2+f_2+1} \end{cases}$$

수학식 28

$$S_{2,b} = \begin{cases} A_2 + \sum_{n=0}^k (B_{\min\{n,m_2\}}^2 + T) & \text{w.p. } (p_2)^k(1 - p_2), \quad 0 \leq k < m_2 \\ A_2 + \sum_{n=0}^{m_2+f_2} (B_{\min\{n,m_2\}}^2 + T) & \text{w.p. } (p_2)^{m_2+f_2} \end{cases}$$

수학식 29

$$S_{2,c} = \begin{cases} \sum_{n=0}^k (B_{\min\{n,m_2\}}^2 + T) & \text{w.p. } (p_2)^k(1 - p_2), \quad 0 \leq k < m_2 + f_2 \\ \sum_{n=0}^{m_2+f_2} (B_{\min\{n,m_2\}}^2 + T) & \text{w.p. } (p_2)^{m_2+f_2} \end{cases}$$

여기서, B_n^2 는 AC₂의 n 번째 백 오프 단계에서 소비된 지연이고 B_n^2 의 PGF는 하기와 같이 주어진다.

$$E[z^{B_n^2}] = \frac{1}{W_n^2} \{z^0 + \sum_{v=1}^{W_n^2-1} (P_{\text{idle}}^2 z + (1 - P_{\text{idle}}^2) z^T)^v\}$$

또한 A_2 는 캐리어 감지가 상태 $(-1, 0)$ 까지 지속되지 않는다는 가정하에, 캐리어 감지 상태에서 소비된 지연을 나타내고, A_2 의 PGF는 하기와 같다.

$$E[z^{A_2}] = \frac{1}{1 - (P_{\text{idle}}^2)^D} \sum_{m=1}^D (P_{\text{idle}}^2)^{m-1} (1 - P_{\text{idle}}^2) z^{m-1+T}$$

[수학식 27], [수학식 28] 및 [수학식 29]를 각각 이용하면 $S_{2,a}$, $S_{2,b}$ 및 $S_{2,c}$ 의 PGF를 구할 수 있다. S_2 의 PGF는 다음과 같이 주어진다.

$$E[z^{S_2}] = \omega_2^a E[z^{S_{2,a}}] + \omega_2^b E[z^{S_{2,b}}] + \omega_2^c E[z^{S_{2,c}}]$$

[0364] 여기서, ω_2^a , ω_2^b 및 ω_2^c 는 다음과 같다.

$$[0366] \quad \omega_2^a = \frac{\beta_1}{\beta_1 + \beta_2} (P_{\text{idle}}^2)^D$$

$$[0367] \quad \omega_2^b = \frac{\beta_1}{\beta_1 + \beta_2} (1 - (P_{\text{idle}}^2)^D)$$

$$[0368] \quad \omega_2^c = \frac{\beta_2}{\beta_1 + \beta_2}$$

[0369] 최종적으로 지연 S_2 의 확률 분포 함수는 PGF $E[z^{S_2}]$ 로부터 구할 수 있다.

[0370] RFS 패킷은 성공적으로 전달되거나 폐기된다. RFS 패킷이 성공적으로 전달되기 위해서는 RFS 패킷의 성공적인 전송 후에 SCH가 AC₂에 할당되어야 한다. RFS 패킷이 성공적으로 전송되었지만 가용한 SCH가 없는 경우, 본 발명은 RFS 패킷을 폐기하므로 실패한 전달로 간주한다. 따라서 앞에서 언급된 세 가지 가능한 경우를 고려하여 다음과 같이 RFS 패킷의 성공적인 전달 확률을 얻을 수 있다.

$$[0372] \quad P_{\text{succ}}^2 = \omega_2^a((p_2)^0 + (p_2)^1 + \dots + (p_2)^{m_2+f_2+1})(1-p_2)(1-p_{\text{full}})$$

$$[0373] \quad + \omega_2^b((p_2)^0 + (p_2)^1 + \dots + (p_2)^{m_2+f_2})(1-p_2)(1-p_{\text{full}})$$

$$[0374] \quad + \omega_2^c((p_2)^0 + (p_2)^1 + \dots + (p_2)^{m_2+f_2})(1-p_2)(1-p_{\text{full}})$$

$$[0375] \quad = (1-p_{\text{full}})(\omega_2^a(1 - (p_2)^{m_2+f_2+2}) + (\omega_2^b + \omega_2^c)(1 - (p_2)^{m_2+f_2+1}))$$

[0377] 한편, 분석의 정확성을 검증하고 본 발명의 MAC 프로토콜 성능을 평가하기 위해 수치 결과와 시뮬레이션 결과를 비교한다. 시뮬레이션 설정 및 파라미터에 대해서 살펴보기로 한다.

[0378] 본 발명은 매트랩(Matlab)을 사용하여 이벤트 드리븐 방식의 시뮬레이터를 개발했으며 시뮬레이션 결과를 얻기 위해 몬테카를로 시뮬레이션을 수행했다. 노드 밀도가 미치는 영향을 조사하기 위해 차량 수를 50부터 200까지 변화시키고, 페이딩 및 음영이 없는 이상적인 무선 채널을 가정한다. 따라서 패킷은 긴 액세스 지연(안전 패킷의 경우), 충돌 또는 SCH의 비가용성(RFS 패킷의 경우)과 같은 MAC 계층 문제로 인해 손실된다. 시뮬레이션은 60분 동안 실행되었으며, 정상 상태 결과를 획득하기 위해 처음 1분 동안의 시뮬레이션 결과는 제외했다. 랜덤 시드를 사용하여 1000개의 시뮬레이션을 실행하고, 결과값에 대해 산술평균을 계산했다.

[0379] 본 발명에서는 IEEE 802.11p 표준에 정의된 EDCA 파라미터를 채택한다([표 2] 참조). 상태 패킷은 100ms마다 생성되고 비상 패킷은 안전 패킷에 포함되므로, 안전 패킷이 평균적으로 50ms마다 발생한다고 가정한다. 표준에 따르면 데이터 속도는 최대 27Mbps까지 지원되며 기본값은 6Mbps이므로 수치 연구를 위해 $R = 6\text{Mbps}$ 로 설정한다. [표 2]에 제시된 바와 같이 본 발명은 RFS 패킷 대비 안전 패킷에 더 높은 우선 순위를 부여하기 위해 $m_1 < m_2$ 및 $CW_{\min,1} < CW_{\min,2}$ 를 만족시키는 백 오프 파라미터 m_i , $CW_{\min,i}$ 를 선택한다. 각 파라미터 세트에 대해 Matlab을 사용하여 [수학식 11]과 [수학식 26]을 연립하여 풀고, 안전 패킷 및 RFS 패킷의 지연 분포와 성공적인 전달 확률을 구한다.

표 2

파라미터	값
λ_1	20 packets/sec
λ_2	0.003 packets/sec
f_2	3
m_1	4
m_2	5
$CW_{min,1}$	64
$CW_{min,2}$	128
$E[L_{status}]$	120 Bytes
$E[L_{RFS}]$	120 Bytes
$E[L_{data}]$	5 MBytes
K	1, 2, 4, 6
R	6 Mbps
σ	12 μ_{sec}
DIFS	36 μ_{sec}
SIFS	32 μ_{sec}
T_{ACK}	64 μ_{sec}

[0383] 도 15는 본 발명의 실시 예에 따른 안전 패킷의 접속 지연의 확률 분포를 나타낸 도면이다.

[0384] 도 15에 도시된 바와 같이, MAC 프로토콜 성능 중에서 안전 패킷의 접속 지연(access delay) S_1 의 확률분포 $P(S_1 \leq t)$ (K : 서비스 채널의 수, N : 차량의 수)가 나타나 있다. 즉, $P(S_1 \leq t)$, $t \geq 0$ 와 같다. 차량 수가 $N = 50, N = 100, N = 150, N = 200$ 이고 $K = 6$ 인 경우, 도 15는 안전 패킷의 액세스 지연 분포에 관한 분석 결과와 시뮬레이션 결과를 보여준다. 도 15에 사용된 백 오프 파라미터는 $(m_1, m_2) = (4, 5)$ 및 $(CW_{min,1}, CW_{min,2}) = (64, 128)$ 이다. 성능 검증을 위해 개발한 수학적 모델의 정확성을 살펴보기로 한다. 이를 위해, 먼저 분석 결과와 시뮬레이션 결과를 비교하여 수학적 분석의 정확성을 검증한다. 도 15에서 시뮬레이션(Simulation)은 몬테카를로 컴퓨터 시뮬레이션 결과를 나타내며, 분석(Analysis)은 수학적 모델을 이용하여 유도한 이론적 결과를 나타낸다. 도 15에 도시된 결과를 살펴보면, 시뮬레이션 결과와 분석 결과가 일치한다. 즉, 개발한 수학적 모델의 정확성이 확인된다.

[0385] 안전 패킷의 지연은 QoS 요구 사항에 따라 100ms보다 짧아야 하므로, 100ms보다 긴 액세스 지연을 갖는 안전 패킷은 손실된 것으로 간주된다. 즉, 안전 패킷의 성공적인 전달 확률 P_{succ}^1 은 하기와 같이 주어진다.

[0387]
$$P_{succ}^1 = P(S_1 < 100 \text{ msec})$$

[0388] 도 15에 도시된 바와 같이 차량의 수 N 이 커질수록 안전 패킷의 액세스 지연은 길어진다. 또한, 도 15는 $N = 50, N = 100$ 인 경우, 안전 패킷의 액세스 지연이 거의 100% 성공적인 전달 확률과 함께 각각 5ms,

10ms 미만인 것을 나타낸다. 한편, 도 15에서 $N = 150, N = 200$ 인 경우 $P(S_1 \leq 100 \text{ msec})$ 의 값을 정확히 알기 어렵기 때문에, 도 16을 제공하여 $N = 150, N = 200$ 인 경우 각각 $P(S_1 \leq 100 \text{ msec}) \simeq 0.99$ 및 $P(S_1 \leq 100 \text{ msec}) \simeq 0.89$ 임을 확인한다. 상기 결과는 차량의 수가 150을 초과하지 않으면 안전 서비스에 대한 QoS 요구 사항(즉, 100ms 이내의 지연과 최소 98%의 성공적인 전달 확률)이 충족됨을 나타낸다.

[0389] 도 16은 본 발명의 실시 예에 따른 안전 패킷의 성공적인 전달 확률을 나타낸 도면이다.

[0390] 안전 패킷을 100ms 이내에 성공적으로 전달할 확률(K : 서비스 채널의 수)이 도 16에 나타나 있다. 본 발명의 실시 예에 따른 차량 통신 방법의 효과에 대해서 살펴보기로 한다. 안전 패킷의 성능 검증과 관련하여, 도 16은 안전 패킷을 100ms 이내에 전달할 확률을 보여준다. 즉, 성공적인 전달 확률이 나타나 있다. 차량 수가 150대에 도달하더라도 성공적인 전달 확률이 98% 이상이 된다. 즉, 제안한 MAC 프로토콜은 안전 패킷에 대한 QoS 요구 사항을 만족시킨다. 도 16에서, 성공적인 전달 확률은 K 값에 의해 거의 영향을 받지 않는다. 이 결과는 RSU와 예약 협상 시점에서 K 개의 모든 SCH가 사용 중인 경우 RFS 패킷이 폐기되기 때문에 발생한다.

[0391] 도 17은 본 발명의 실시 예에 따른 RFS 패킷의 성공적인 전달 확률을 나타낸 도면이다.

[0392] 도 17에는 RFS 패킷의 성공적인 전달 확률 P_{succ}^2 이 나타나 있다. 본 발명은 도 17에서 AC_2 패킷의 성능을 보여준다. 도 17의 왼쪽 도면은 $K = 1, K = 2, K = 4$ 및 $K = 6$ 에 대해 차량의 수 N 이 50에서 200까지 변화될 때, RFS 패킷의 성공적인 전달 확률 P_{succ}^2 를 나타낸다. 성공적인 전달 확률은 사용 가능한 SCH의 수에 크게 영향을 받는다는 것을 알 수 있다. 특히, 도 17의 오른쪽 도면은 RFS 패킷의 성공적인 전달 확률이 $K = 6$ 일 때 $N \leq 150$ 에 대해 92% 이상임을 보여준다. 또한 도 17의 오른쪽 도면은 분석 결과가 시뮬레이션 결과와 잘 일치 함을 보여 주며, P_{full} 에 대한 근사가 정확함을 나타낸다.

[0393] 한편, 성능 비교를 살펴보기로 한다. 본 발명의 MAC 프로토콜에서는 SCH에 접근하기 위해 예약 기반(reservation-based) 방식이 사용되므로 각 OBU는 비-경쟁 방식으로 예약된 SCH에 접근할 수 있다. 성능 비교를 위해, 비-경쟁 방식과 반대되는 개념인 경쟁 기반 방법을 고려한다. 경쟁 기반 방법으로서 랜덤 선택 기법을 생각하고 본 발명의 MAC 프로토콜과 성능을 비교한다. 랜덤 선택 기법은 다음과 같이 동작한다. 비-안전 패킷을 전송하기 위해 각 OBU는 임의로 SCH 중 하나를 선택한다. 그런 다음 선택한 SCH에 접근하기 위해 각 OBU는 동일한 SCH를 선택한 다른 OBU들과 IEEE 802.11 DCF에 따라 경쟁한다. 반면, 안전 패킷을 전송하기 위해 각 OBU는 IEEE 802.11 DCF에 따라 경쟁하여 CCH에 접근한다. 본 발명의 프로토콜과 같이, RSU는 브로드캐스트된 안전 패킷에 대해 ACK 메시지를 보낸다. 달리 언급하지 않는 한, [표 2]의 파라미터를 사용한다.

[0394] 도 18은 본 발명의 실시 예에 따른 안전 패킷의 성공적인 전달 확률의 비교 결과를 나타낸 도면이다.

[0395] 도 18에는 $K = 6$ 및 $R \in \{6, 12, 18, 24\}$ Mbps인 경우 안전 패킷의 성공적인 전달 확률 P_{succ}^1 의 비교 결과가 나타나 있다. 본 발명의 MAC 프로토콜과 랜덤 선택 기법은 안전 패킷의 성공적인 전달 확률에 대해 거의 동일한 성능을 보인다. 본 발명의 MAC 프로토콜에서는 CCH가 안전 패킷 및 RFS 패킷에 의해 공유되는 반면, 랜덤 선택 기법에서는 CCH가 안전 패킷에 의해서만 사용된다. 그럼에도 불구하고 상기와 같이 동일한 성능을 보이는 이유는, 안전 패킷이 높은 우선 순위를 가지며 RFS 패킷이 안전 패킷에 비해 드물게 생성되기 때문이다.

[0396] 도 19 및 도 20은 본 발명의 실시 예에 따른 비-안전 패킷의 성공적인 전달 확률 및 평균 액세스 지연의 비교 결과를 나타낸 도면이다.

[0397] 도 19 및 도 20에는 $K = 6$ 및 $R \in \{6, 12, 18, 24\}$ Mbps인 경우 비-안전 패킷의 성공적인 전달 확률 P_{succ}^2 와 평균 액세스 지연 $E[S_2]$ 의 비교 결과가 각각 나타나 있다. $R = 6$ Mbps인 경우, 랜덤 선택 기법

은 본 발명의 MAC 프로토콜보다 높은 성공적인 전달 확률을 보인다. 그러나 평균 액세스 지연과 관련하여, 본 발명의 MAC 프로토콜은 랜덤 선택 기법보다 우수한 성능을 보인다. $R \in \{12, 18, 24\}$ Mbps인 경우, 본 발명의 MAC 프로토콜과 랜덤 선택 기법은 $N \leq 150$ 에 대해 99% 이상의 성공적인 전달 확률을 달성한다. 액세스 지연과 관련하여, 본 발명의 MAC 프로토콜은 랜덤 선택 기법보다 우수한 성능을 보인다. 액세스 지연에 대한 이점 외에도, 본 발명의 MAC 프로토콜은 차량이 적은 희박한 도로 환경에서 CCH의 보다 효율적인 활용을 제공할 수 있다.

[0399]

이상에서 설명한 실시 예들은 그 일 예로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시 예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

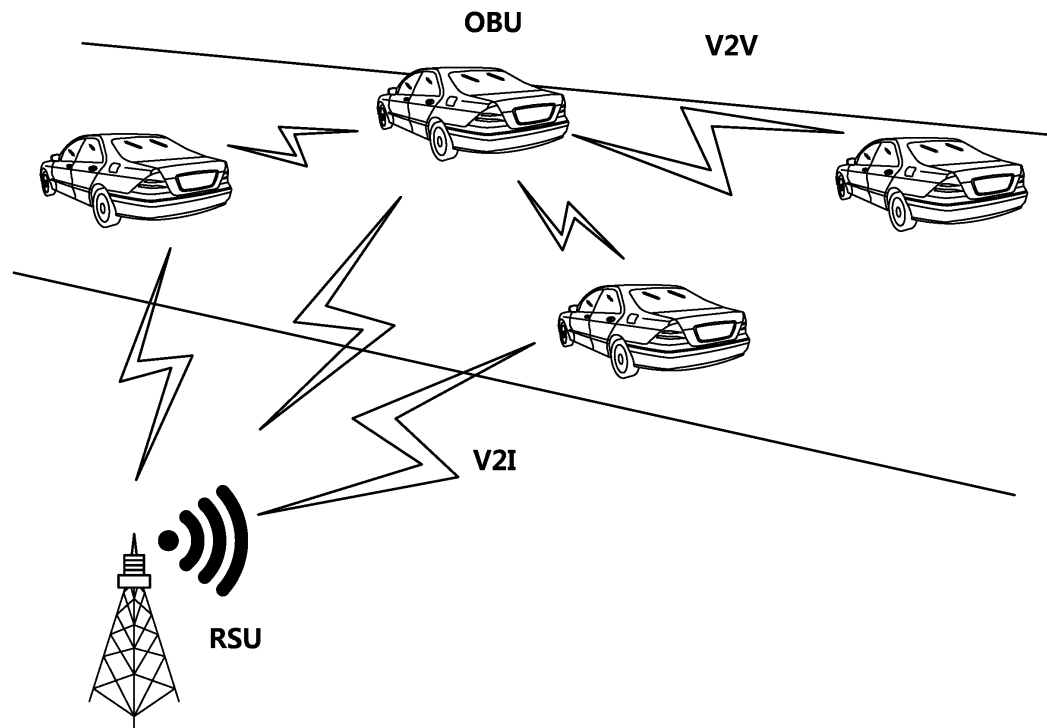
부호의 설명

[0400]

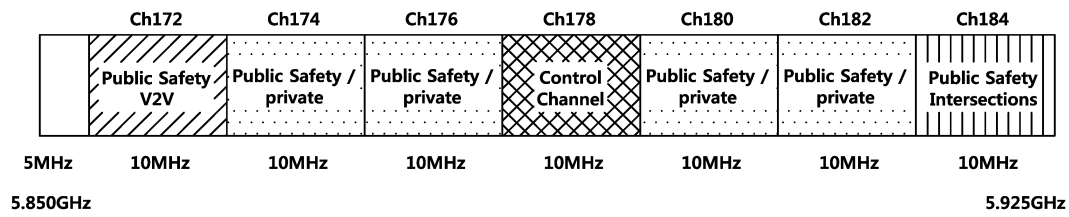
- 100: 차량 통신 장치
- 110: 듀얼 트랜시버
- 111: CCH 트랜시버
- 112: SCH 트랜시버
- 120: MAC 계층 큐 관리부

도면

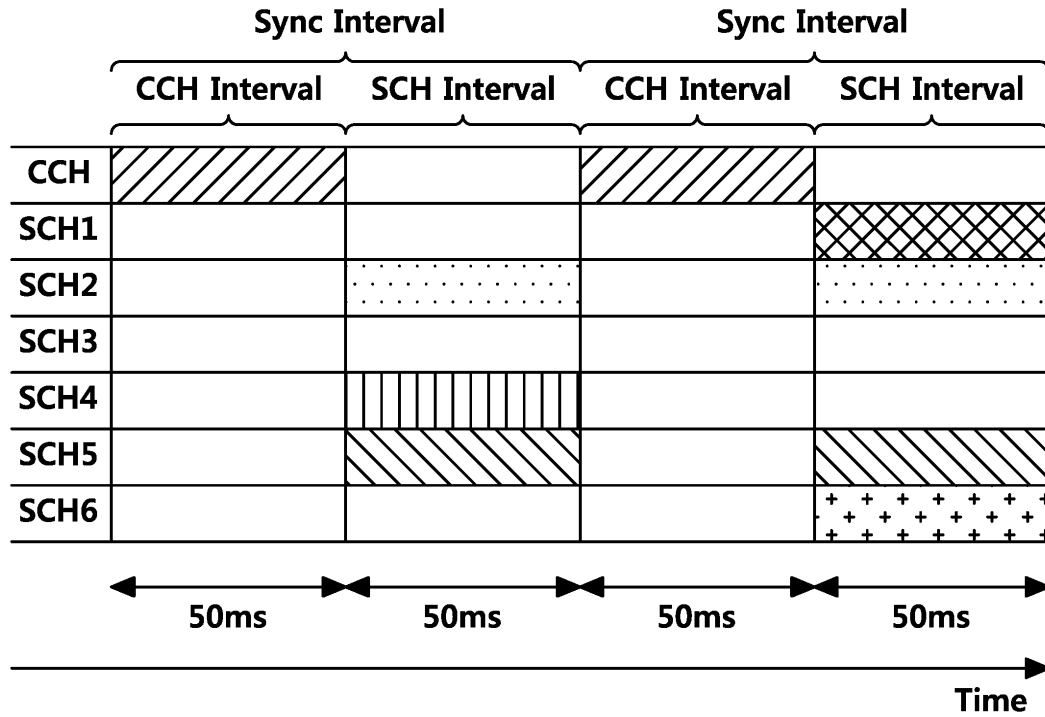
도면1



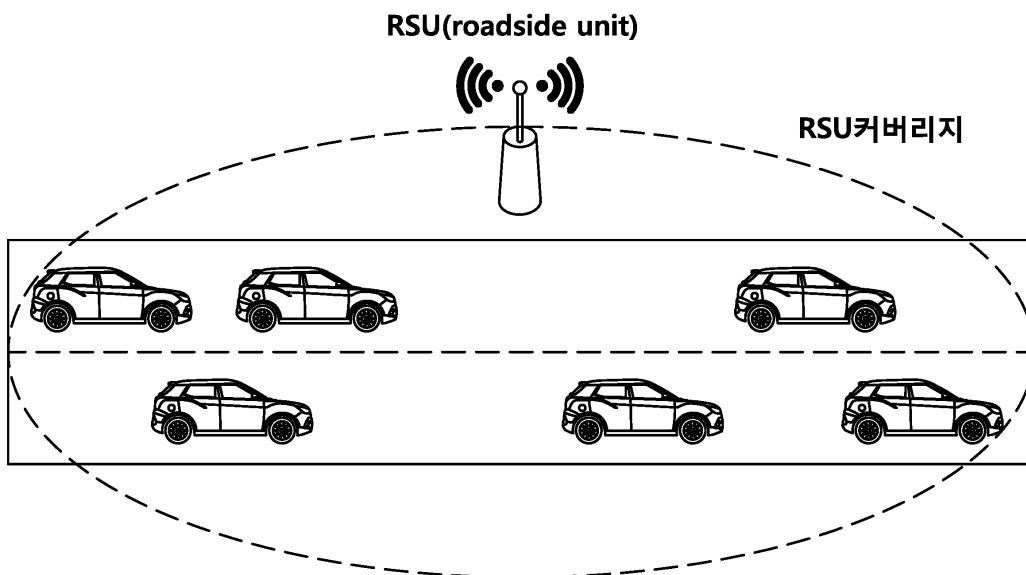
도면2



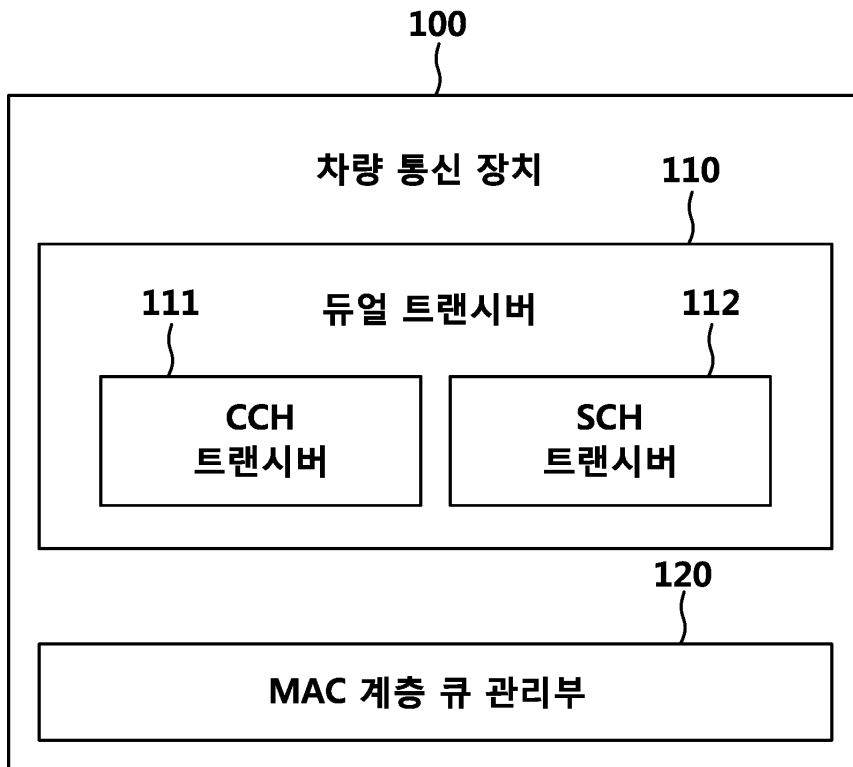
도면3



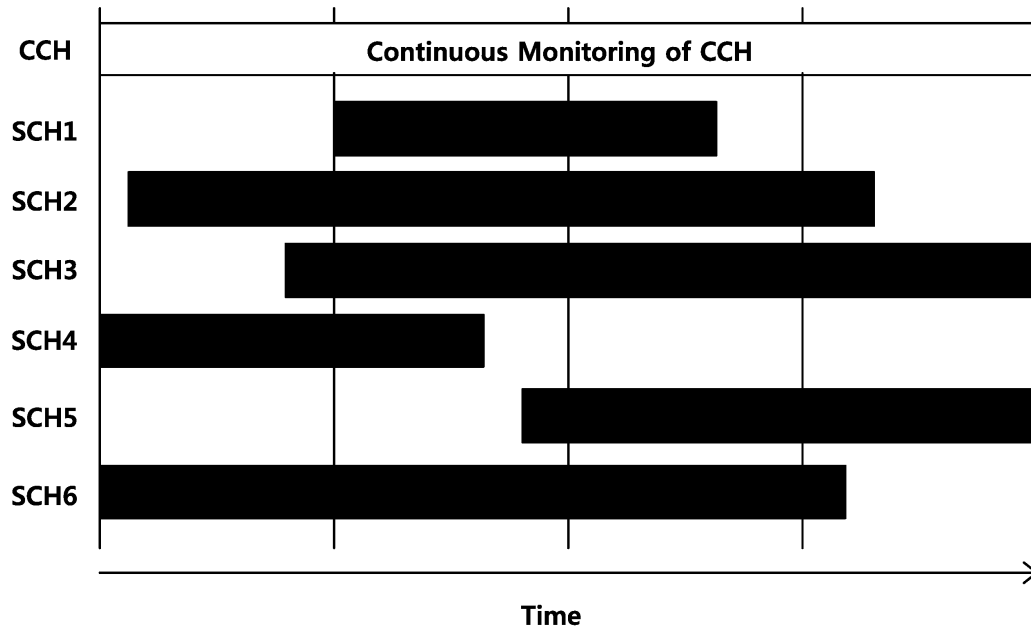
도면4



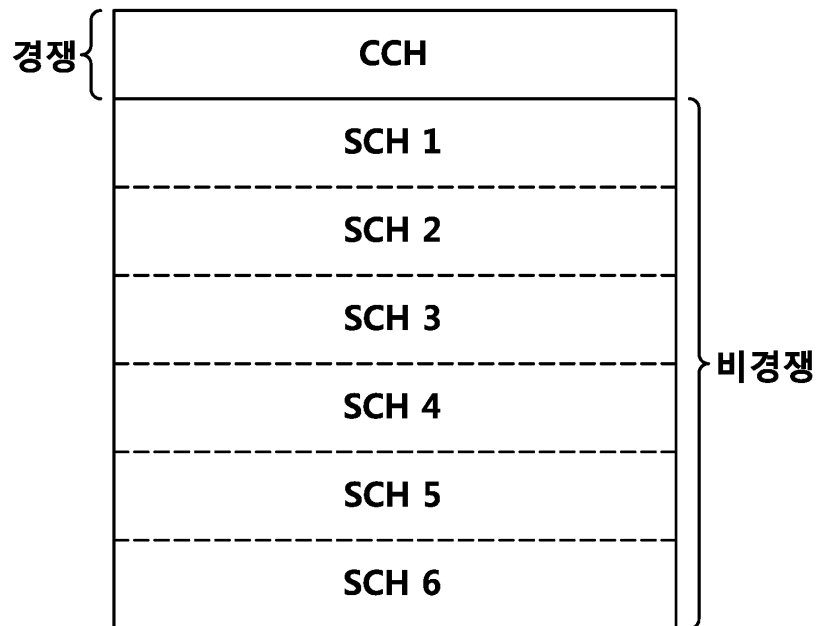
도면5



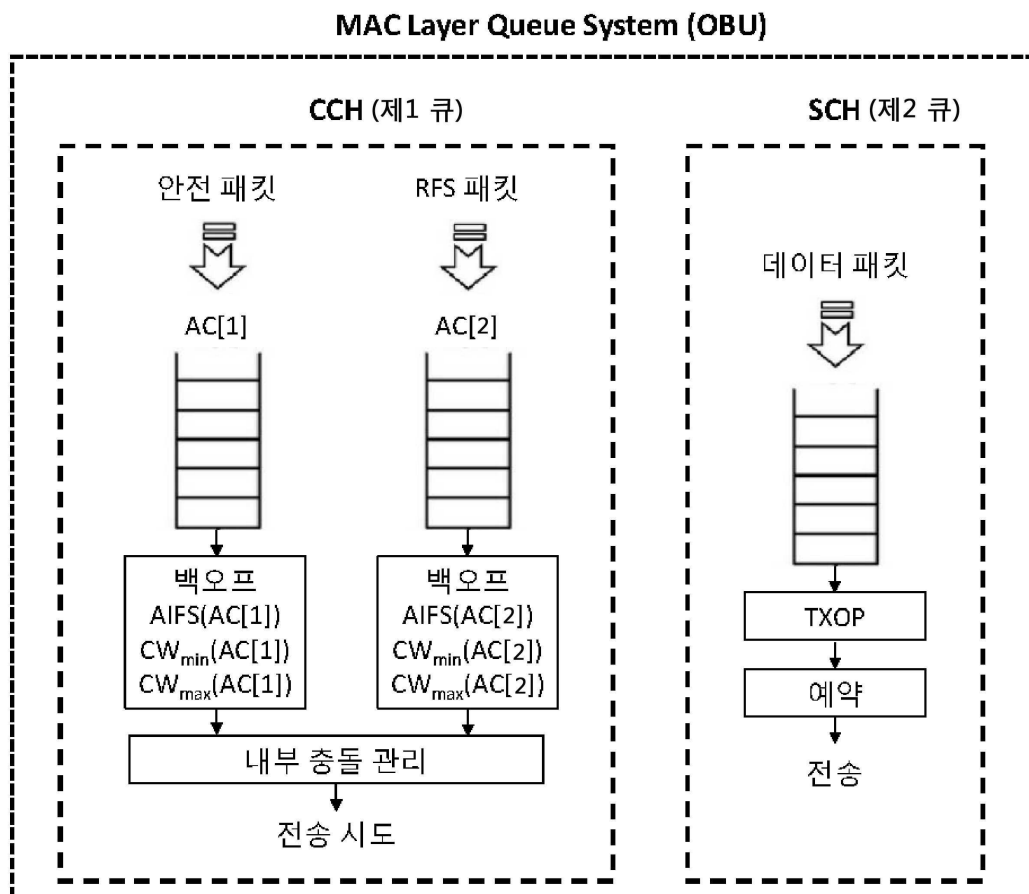
도면6



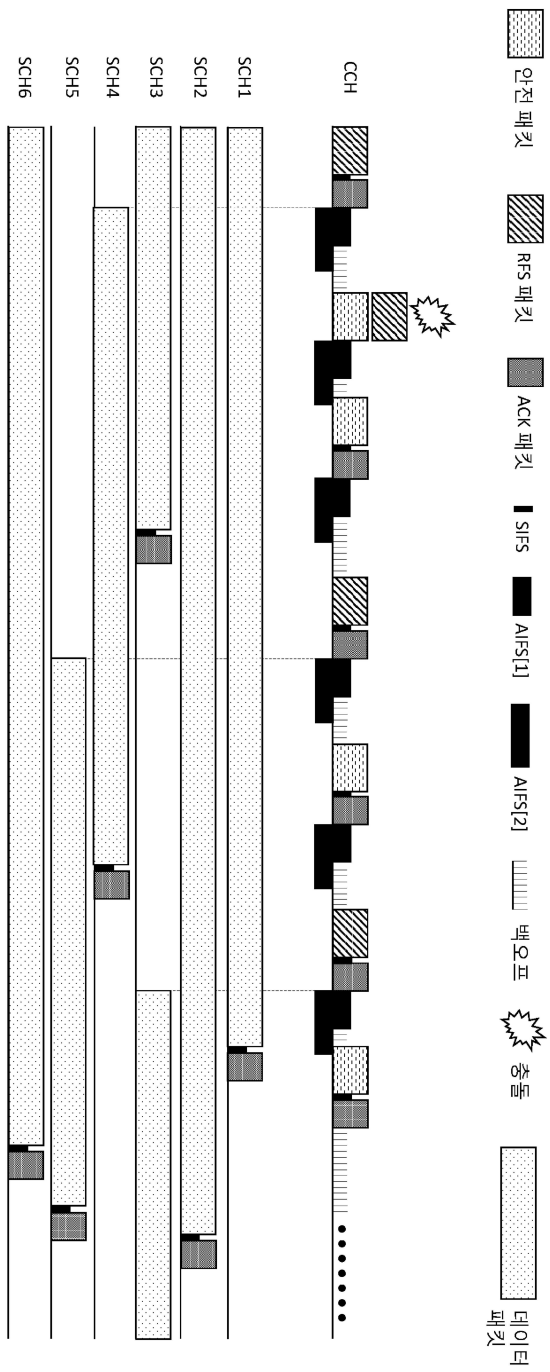
도면7



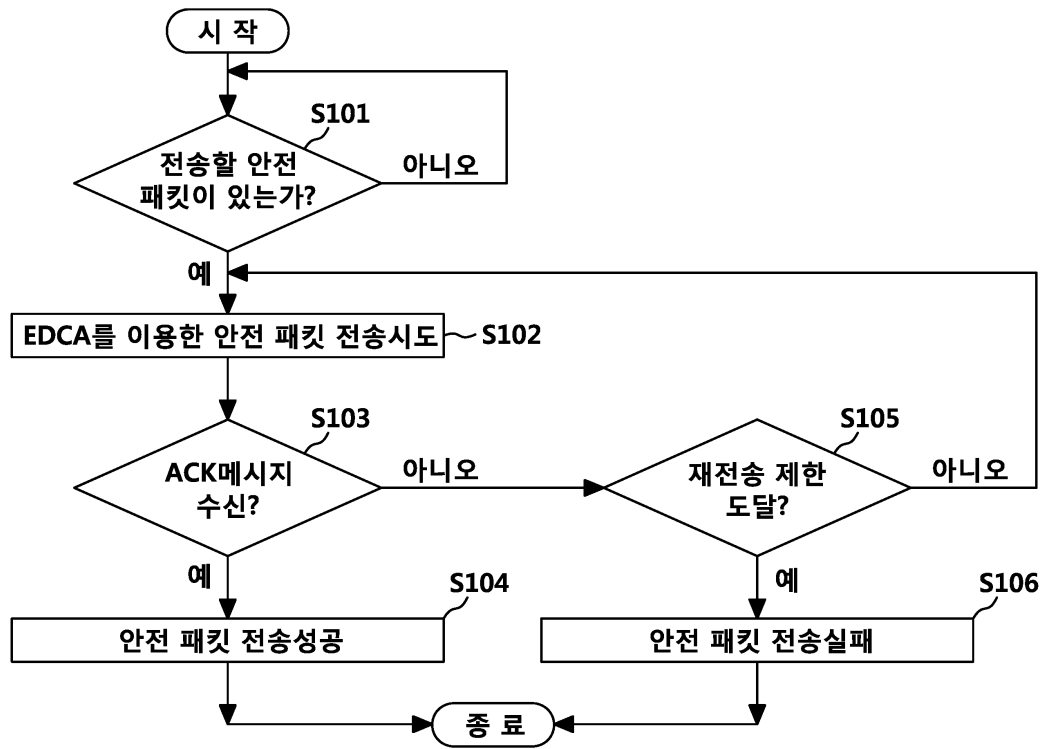
도면8



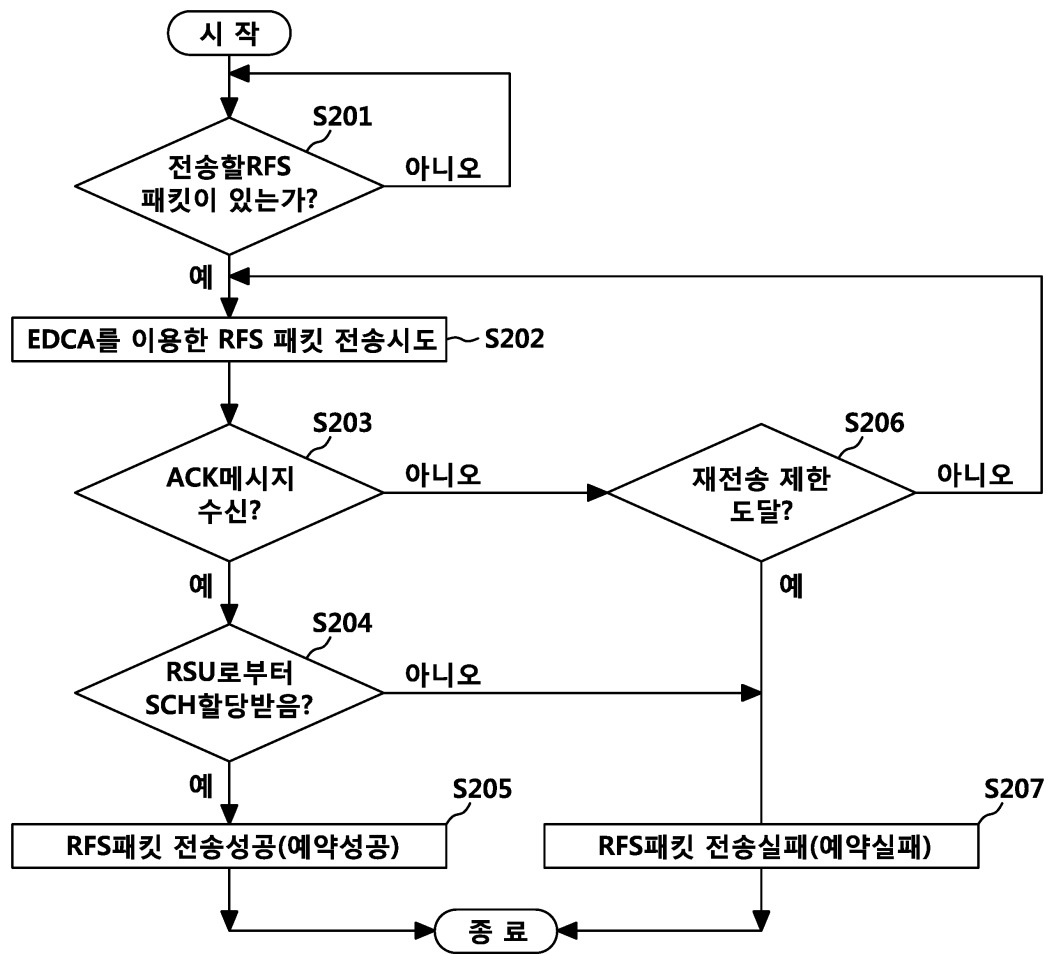
도면9



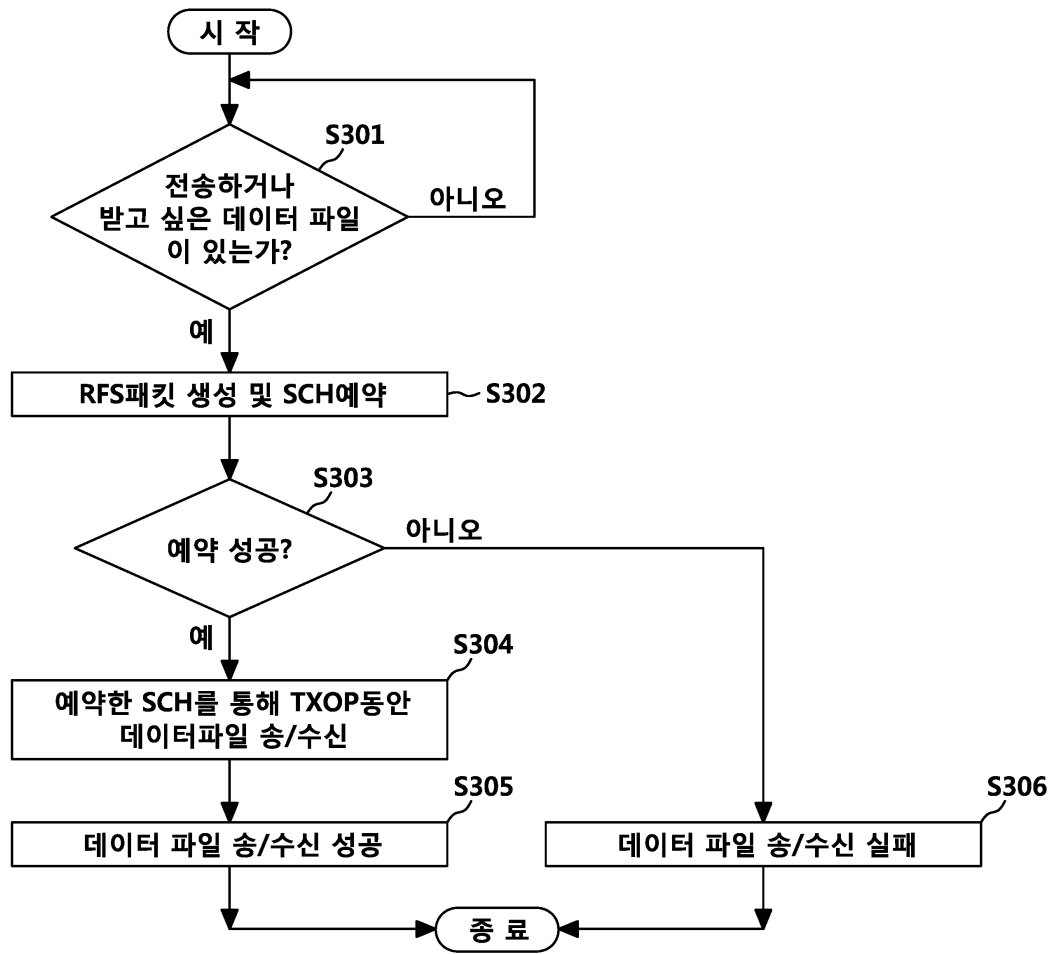
도면10



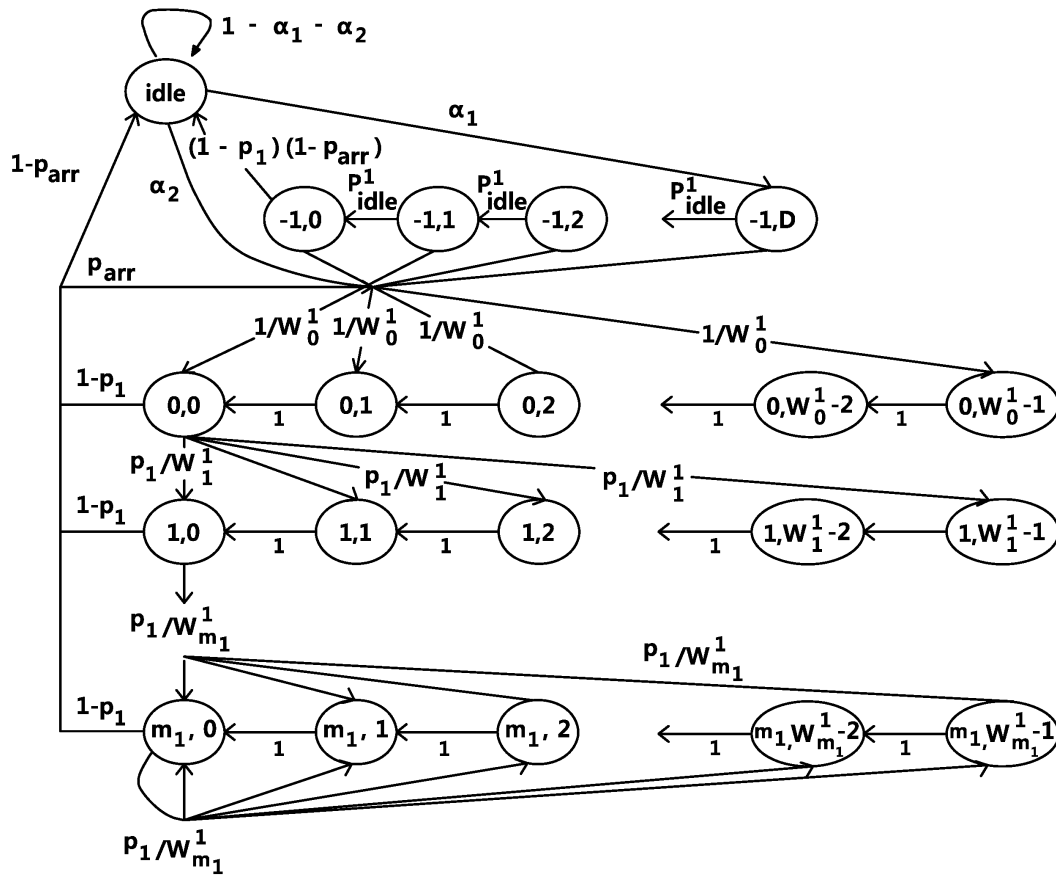
도면11



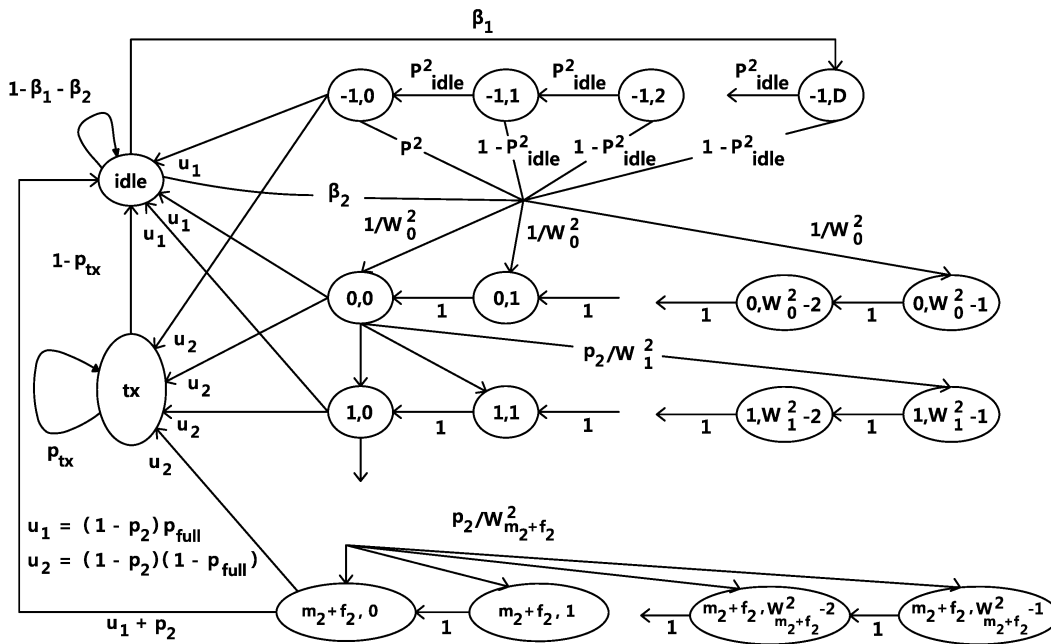
도면12



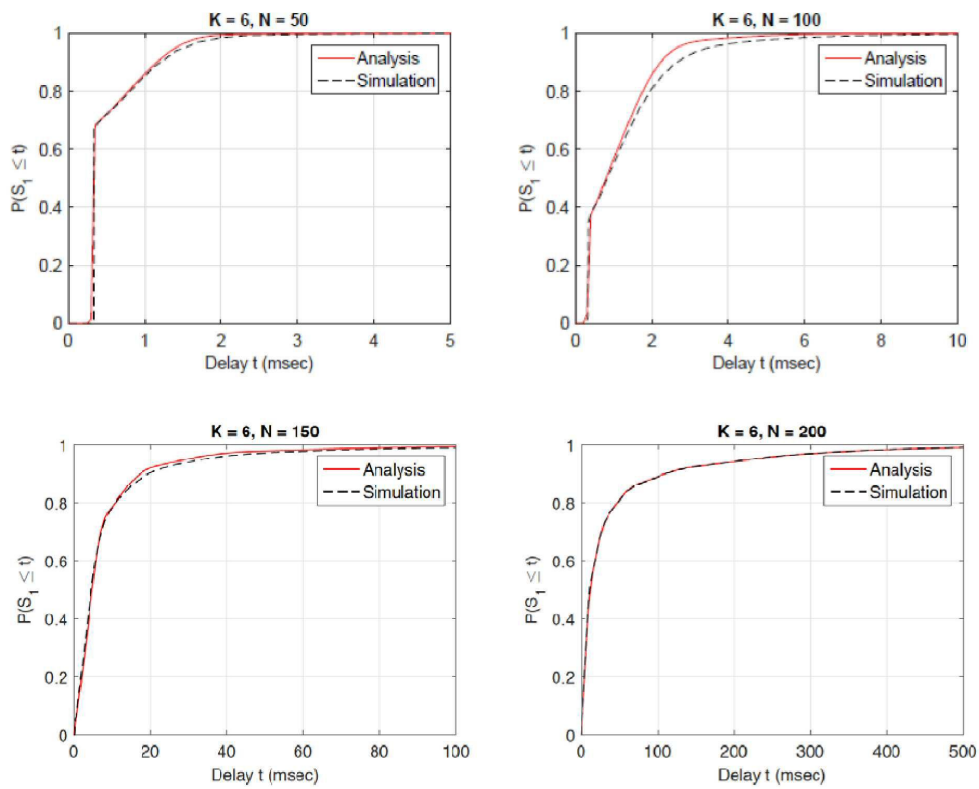
도면13



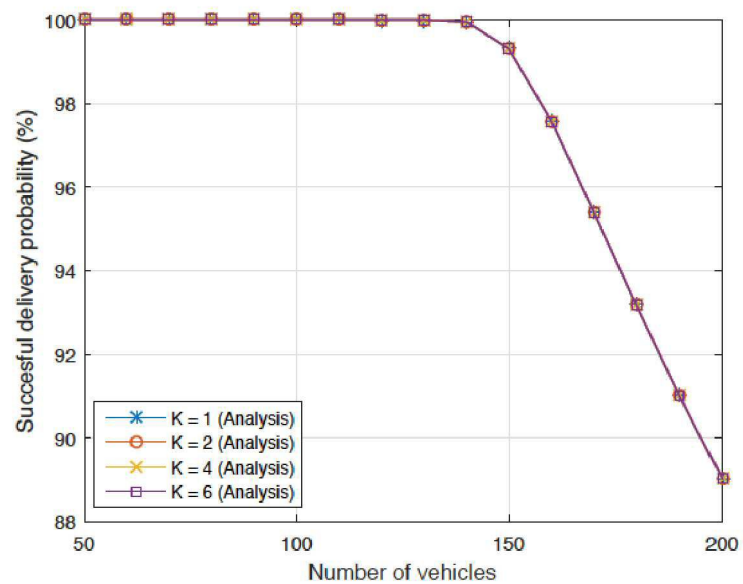
도면14



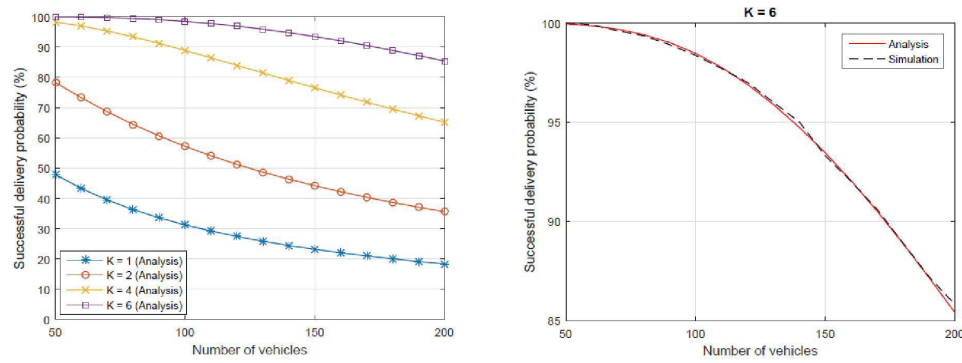
도면15



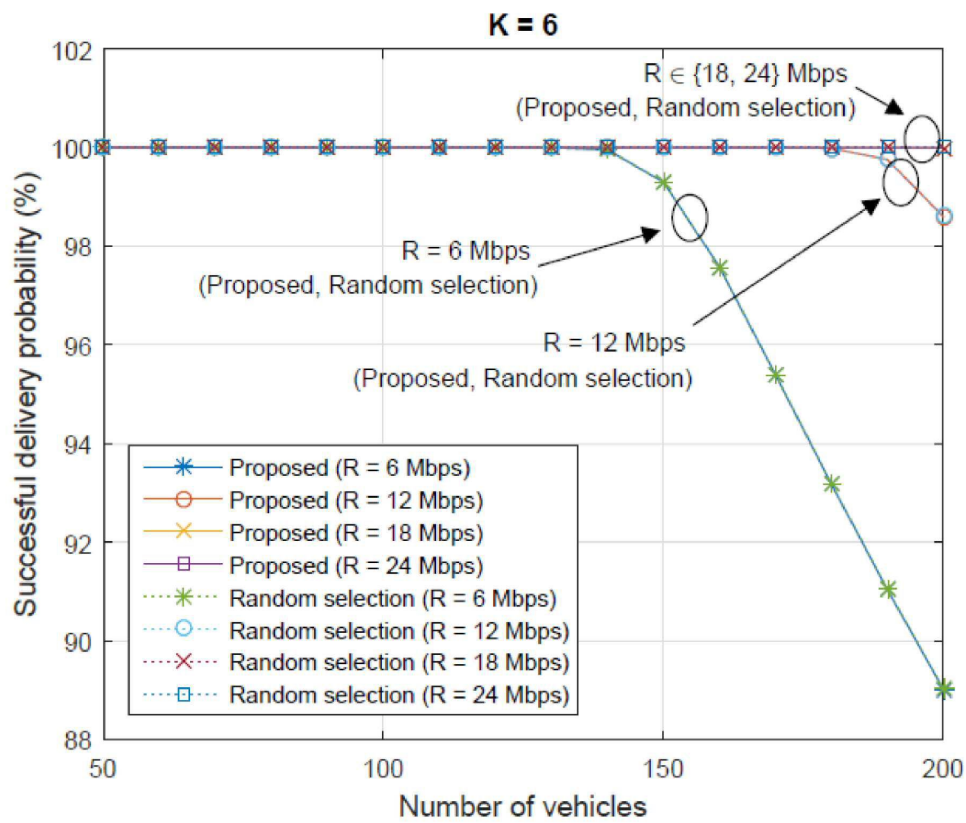
도면16



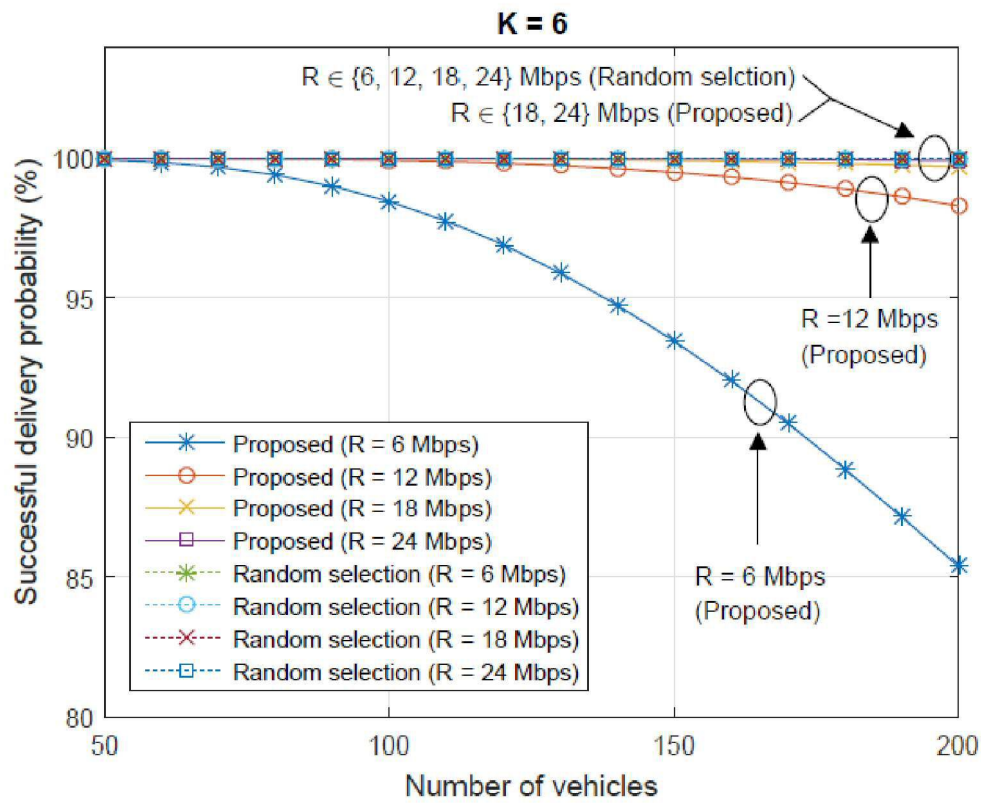
도면17



도면18



도면19



도면20

