Journal of the Korean Institute of Industrial Engineers
Vol. 34, No. 2, pp. 246-254, June 2008.

Infrastructure Mode IEEE 802.11 무선랜 시스템에서 효율적인 은닉 단말 발견 방법을 통한 MAC 성능 개선

최 우 용†

동아대학교 산업경영공학과

MAC Performance Enhancement by Efficient Hidden Node Detection in Infrastructure Mode IEEE 802.11 Wireless LANs

Woo-Yong Choi

Dept. of Industrial and Management Systems Engineering, Dong-A University, Busan 604-714, Korea

In this paper, a new efficient hidden node detection method is proposed to decide whether the RTS/CTS mechanism is necessary to resolve the hidden node problem for the data transmission of each node in infrastructure mode IEEE 802.11 wireless LANs. The nodes, for which the RTS/CTS mechanism is found to be not necessary by the hidden node detection method, can transmit their data frames without performing the RTS/CTS exchange. Only the nodes, for which the RTS/CTS mechanism is found to be necessary by the hidden node detection method, perform the RTS/CTS exchange before their data frame transmissions.

Keywords: Wireless LAN, Hidden Node Problem, RTS/CTS, MAC

1. 서 론

현재 전 세계적으로 설치되고 있는 무선랜 시스템은 사용자의 이동성을 제공하지 못하는 기존의 유선랜 시스템의 한계를 극복하기 위하여 개발되었다. 무선랜 시스템은 AP (Access Point)가 존재하여 다른 무선랜이나 인터넷과 같은 외부망과의 연결이 가능한 infrastructure mode와 외부망과의 연결이 불가능한 ad hoc mode를 모두 지원할 수 있다. 이러한 무선랜 시스템은 기존의 유선랜 시스템에 비하여 사용자의 이동성을 보장하는 장점을 가지는 반면 유선랜 시스템에서는 존재하지 않는 은닉 단말 문제 (hidden node problem)를 가지는데 무선랜 시스템의 성능을 저하시키는 중요한 요인으로 지적되고 있다(Sobrinho, Haan and Brazio, 2005; Tobagi and Kleinrock, 1975; Xu, Gerla and Bae, 2002).

Infrastructure mode 무선랜에서 은닉 단말 문제는 Choi and Lee (2006)에서 설명되어 있듯이 무선랜에서 어떤 단말 A가 AP로 데이터를 전송하고 있을 때 단말 A의 데이터 전송 신호를 물리적으로 감지하지 못하는 다른 단말 B가 AP로 데이터를 전송하는 경우 발생하는데 이 경우 AP는 단말 A와 B로부터 데이터를 모두 제대로 받지 못하게 된다. 무선랜에서 발생하는 이러한 은닉 단말 문제를 해결하기 위하여 무선랜 관련 표준화 단체인 IEEE 802.11 WG (Working Group)에서는 RTS (Request to Send) 프레임과 CTS (Clear to Send) 프레임에 기초한 채널 예약 방식을 채택하였다(IEEE Std 802.11, 1999).

RTS 프레임과 CTS 프레임에 기초한 채널 예약 방식에 따르면 데이터를 전송하고자 하는 송신측 단말은 수신측 단말에 먼저 RTS 프레임을 보내고 RTS 프레임을 제대로 수신한 수신측 단말은 현재 다른 단말로부터의 채널 예약이 없을 경우 채널 예약을 승인하는 CTS 프레임을 송신측 단말에 보낸다. 이러한 RTS 프레임과 CTS 프레임은 관련된 송신측 단말과 수신측 단말 이외의 무선랜 내의 다른 단말도 수신하여 자신의 NAV (Network Allocation Vector) 값을 수정하게 되는데 NAV

† 연락저자 : 최우용, 부산광역시 사하구 하단2동 840번지 동아대학교 산업경영공학과, Fax : 051-200-7697, E-mail : wychoi77@dau.ac.kr
2007년 08월 접수; 2008년 01월 수정본 접수; 2008년 02월 게재 확정.

는 다른 단말의 채널 예약으로 인하여 앞으로 전송을 시도할 수 없는 잔여 시간을 의미한다. 따라서 RTS 프레임과 CTS 프레임을 성공적으로 교환한 송신측 단말과 수신측 단말 이외의 다른 단말은 무선랜 내에서 은닉 단말 문제로 인하여 비록 물리적으로 데이터 전송 신호를 제대로 감지하지 못한다 하더라도 데이터 전송 시도를 일정 시간 (하나의 데이터 프레임과 ACK 프레임의 전송에 필요한 시간) 이후로 미루게 됨으로써 은닉 단말 문제를 해결할 수 있다.

은닉 단말 문제는 모든 단말의 데이터 전송시에 항상 발생하는 것은 아니고 주로 무선랜의 서비스 영역의 가장자리에 위치한 단말이 데이터를 전송하고 있을 때 이러한 단말의 전송 신호를 서비스 영역의 가장자리에 위치한 일부의 다른 단말이 제대로 감지하지 못할 때 발생한다. 은닉 단말 문제가 발생하지 않는 데이터 전송시에 RTS 프레임과 CTS 프레임을 통하여 채널 예약을 하는 경우 불필요한 RTS 프레임과 CTS 프레임의 전송으로 인하여 무선랜의 MAC 성능이 저하될 수 있다. 이러한 불필요한 RTS 프레임과 CTS 프레임의 전송에 따른 문제점을 성공적으로 해결하기 위해서는 무선랜 내의 각 단말에 대하여 전송을 방해할 수 있는 다른 은닉 단말의 존재 여부를 판별하는 방법이 필요할 것이다. 이러한 은닉 단말 발견 방법에 따라서 무선랜 내에 다른 은닉 단말이 존재하는 단말의 경우 데이터 전송시에 RTS 프레임과 CTS 프레임의 전송을 통하여 채널 예약을 하도록 하고 다른 은닉 단말이 존재하지 않는 단말의 경우 데이터 전송시에 RTS 프레임과 CTS 프레임의 전송을 통하여 채널 예약을 하지 않도록 하면 불필요한 RTS 프레임과 CTS 프레임의 전송을 막음으로써 MAC 전송 효율이 향상될 수 있다.

Infrastructure mode 무선랜 내의 각 단말에 대하여 다른 은닉 단말의 존재 여부를 판별하는 은닉 단말 발견 방법에 대한 연구는 IEEE 802.11k draft 2.0 (2005), Kermani *et al*. (1997), Kristensen and Engelstad (2006A), Kristensen and Engelstad (2006B)에서 이루어져 왔다. 이러한 기존의 방법들은 대부분 무선랜 내의 각 단말이 현재 진행중인 다른 단말의 전송 신호를 제대로 수신하지 못하여 그 단말의 데이터 전송을 방해할 수 있는 은닉 단말이 될 수 있는지 없는지 판단하도록 하고 데이터 전송을 방해할 수 있는 다른 단말의 리스트를 각 단말이 관리하도록 하고 있다. 이를 좀 더 구체적으로 설명하면 다음과 같다. 일반적으로 무선랜 내에서 어떤 데이터 프레임을 성공적으로 전송하기 위한 프레임 전송 순서는 다음과 같다.

(RTS + CTS +) Data + ACK

데이터 프레임을 전송하기 전에 RTS 프레임과 CTS 프레임을 전송할 수도 있으나 RTS 프레임과 CTS 프레임의 전송 없이 바로 데이터 프레임을 전송할 수도 있다. 데이터 프레임을 전송한 후에는 데이터 프레임을 수신한 단말로부터 ACK 프레임이 전송되어야 한다. 예를 들어 이러한 프레임 전송 순서상에서 어떤 단말 C가 AP로부터 또 다른 단말 D에게 전송된 RTS 프레임을 제대로 수신하였으나 이에 대응되는 CTS 프레임을 단말 D로부터 제대로 수신할 수 없었다고 하자. 이는 단말 D가 CTS 프레임을 전송하였으나 단말 C가 단말 D의 전송 신호를 제대로 수신하지 못하여 단말 C가 단말 D의 전송을 방해할 수 있는 은닉 단말이 될 가능성을 내포한다. 이러한 현상이 반복된다면 단말 C가 단말 D의 전송을 방해할 수 있는 은닉 단말이라고 판단할 수 있을 것이다. 유사하게 단말 C가 AP로부터 단말 D에게 전송된 데이터 프레임을 제대로 수신하였으나 이에 대응되는 ACK 프레임을 단말 D로부터 제대로 수신할 수 없을 경우 단말 C가 단말 D의 전송을 방해할 수 있는 은닉 단말이라고 판단할 수 있을 것이다. 이와 같은 방법으로 각 단말은 데이터 전송을 방해할 수 있는 다른 단말의 리스트를 관리할 수 있으며 AP는 각 단말로부터 이러한 정보를 취합하여 각 단말에 대하여 전송을 방해할 수 있는 다른 은닉 단말의 존재 여부를 최종적으로 판단할 수 있을 것이다. 하지만 이러한 방법은 AP가 단말 D로 데이터를 전송한다는 가정을 가지고 있는데 만약 이러한 데이터 전송이 무선랜 내에 존재하지 않는다면 단말 D의 데이터 전송을 방해할 수 있는 은닉 단말을 제대로 발견할 수 없을 것이다. 그래서 Kristensen and Engelstad (2006A), Kristensen and Engelstad (2006B)는 은닉 단말을 발견하기 위한 목적의 트래픽을 무선랜 내에 부가적으로 생성하는 능동적인 은닉 단말 발견 방법을 제안하였다.

기존의 은닉 단말 발견 방법의 문제점은 다음과 같이 크게 두가지로 요약할 수 있다. 첫째, 기존의 은닉 단말 발견 방법은 모두 은닉 단말을 발견하기 위하여 단말간의 연결정보 (connectivity information)를 이용하고 있으나 Xu, Gerla and Bae (2002)에서 설명되어 있듯이 은닉 단말을 발견하기 위해서는 단말간의 연결정보를 기초로 하기보다 단말간의 전송파 감지정보 (carrier sensing information)를 이용하여야 한다. 일반적으로 단말간의 연결정보와 간섭정보 (interference information) 그리고 전송파 감지정보는 서로 다른데 이러한 정보간의 차이에 대한 자세한 설명은 Choi (2007), Xu, Gerla and Bae (2002), Zhou *et al*. (2005)에 있는데 기존의 은닉 단말 발견 방법은 모두 어떤 단말간의 해당 프레임에 대한 정상적인 전송 및 수신 여부로써 은닉 단말을 발견하는 것이기 때문에 방법의 구조상 단말간의 전송파 감지정보를 적용하기가 불가능하다. 둘째, 기존의 은닉 단말 발견 방법은 대부분 무선랜 내에 어떤 데이터 전송이 발생할 경우 이와 관련된 은닉 단말을 발견하는 수동적인 방법이다. 즉, 무선랜 내에 은닉 단말과 관련된 데이터 전송이 발생하지 않으면 은닉 단말을 발견할 수 없다. 이러한 수동적인 은닉 단말 발견 방법의 문제점을 개선하기 위해 Kristensen and Engelstad (2006A), Kristensen and Engelstad (2006B)이 제시한 능동적인 은닉 단말 발견 방법은 은닉 단말을 발견하기 위하여 지나치게 많은 트래픽을 무선랜 내에 발생시키는 문제점을 가진다.

본 논문에서는 기존의 은닉 단말 발견 방법의 문제점을 개

선하기 위하여 새로운 은닉 단말 발견 방법을 제안하고 제안한 은닉 단말 발견 방법에 기초하여 은닉 단말이 존재하는 단말은 데이터 전송시 RTS 프레임과 CTS 프레임에 기초한 채널 예약 방법을 사용하고 은닉 단말이 존재하지 않는 단말은 데이터 전송시 RTS 프레임과 CTS 프레임에 기초한 채널 예약 방법을 사용하지 않음으로써 MAC 전송 효율을 향상시키고자 한다. 무선랜 시스템에서는 PCF (Point Coordination Function) 프로토콜이 적용되는 CFP (Contention-Free Period)와 DCF (Distributed Coordination Function) 프로토콜이 적용되는 CP (Contention Period)가 반복적으로 나타나는데 본 논문에서 제안하는 은닉단말 발견 방법은 PCF 프로토콜이 적용되는 CFP에서 수행되는데 은닉 단말을 발견하기 위하여 별도의 부가적인 트래픽이 필요하지 않다. 그리고 은닉 단말을 발견하기 위하여 단말간의 전송파 감지정보를 사용하기 때문에 보다 정확히 은닉 단말을 발견할 수 있다.

2. 무선랜 시스템의 수퍼프레임 (Superframe) 구조

무선랜 시스템에서 실시간 트래픽에 대한 전송 서비스를 위해 개발된 PCF 프로토콜이 적용되는 구간인 CFP와 best effort 트래픽에 대한 전송 서비스를 위해 개발된 DCF 프로토콜이 적용되는 구간인 CP가 다음의 <Figure 1>과 같이 시간상에서 반복적으로 교대로 나타난다. 연속된 CFP와 CP를 합쳐서 수퍼프레임 혹은 CFP repetition interval이라고 한다.

일반 단말이 AP로부터의 폴링 없이 무선 채널을 통하여 데이터를 전송하기 위해서는 적어도 DIFS (DCF InterFrame Space) 동안 무선 채널이 idle한 상태이어야 하는 반면 AP는 DIFS 보다 작은 시간인 PIFS (PCF InterFrame Space) 동안만 무선 채널이 idle한 상태이면 데이터를 전송할 수 있다. 이러한 이유로 AP는 항상 무선 채널을 접근할 때 다른 일반 단말에 비하여 우선권을 가진다. <Figure 1>에서 CFP에서는 AP가 이러한 무선 채널 접근에 대한 우선권을 사용하여 채널의 사용에 대한 모든 제어를 중앙 집중적으로 관리하는 구간이다. 반면, CP에서는 AP가 이러한 무선 채널 접근에 대한 우선권을 포기하고 일반 단말과 같이 행동하는 구간이다. AP는 새로운 CFP가 시작되어야 하는 시점에 현재의 진행중인 트래픽이 종료된 후 새로운 CFP를 시작할 수 있다. 따라서 진행중인 트래픽의 전송에 많은 시간이 소요되는 경우 CFP가 예정된 시간보다 늦게 시작될 수도 있다.

3. 새로운 은닉 단말 발견 방법

3.1 단말간의 전송파 감지정보 수집방법

무선랜 내의 단말과 AP간의 association/reassociation/disassociation 과정을 통하여 AP는 무선랜 내의 N개의 단말의 리스트를 관리할 수 있다. 본 논문에서 제안하는 은닉 단말 발견 방법에서는 AP가 무선랜 내의 각 단말에 대하여 전송을 방해할 수 있는 은닉 단말을 발견하기 위하여 단말간의 전송파 감지정보를 사용한다. AP는 이러한 단말간의 전송파 감지정보를 <Figure 1>의 각 CFP에서 PCF 프로토콜을 사용하여 수집하여 각 단말에 대하여 은닉 단말의 존재 유무를 판단하고 은닉 단말의 존재 유무에 대한 판단 결과를 무선랜 내의 각 단말에 통보함으로써 각 단말이 각 CP에서 DCF 프로토콜을 사용하여 데이터를 전송할 때 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행할지 하지 않을지 판단하도록 한다. AP가 각 CFP에서 단말간의 전송파 감지정보를 수집하기 위하여 별도의 부가적인 트래픽이 발생하지 않으며 각 CFP에서 수집된 단말간의 새로운 전송파 감지정보를 사용하여 은닉 단말 존재 유무를 판단할 것이다. 따라서 각 단말은 각 CP에서 DCF 프로토콜을 사용하여 데이터를 전송할 때 직전의 CFP에서 AP가 수집한 단말간의 새로운 전송파 감지정보와 그 이전에 AP가 수집한 단말간의 전송파 감지정보를 바탕으로 이루어진 은닉 단말 존재 유무에 대한 판단 결과에 따라서 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행할지 하지 않을지 판단하게 된다. 각 CFP에서 AP가 무선랜 내의 N개의 단말간의 전송파 감지정보를 수집하는 방법을 다음 단락에서 설명한다.

단말 i는 현재의 상태에서 전송 신호를 감지할 수 있는 다른 단말의 MAC 주소의 집합, R_i를 관리해야 하고 AP는 각 단말로부터 전달된 전송파 감지정보를 바탕으로 N개의 단말의 전송파 감지정보, (R_1, R_2, ⋯, R_N)를 관리해야 한다. 각 CFP에서 AP는 자신의 무선랜 내의 단말간의 전송파 감지정보를 알기 위하여 단말 ID를 기준으로 각 단말을 순서대로 폴링한다. AP로부터 폴링 프레임을 전송 받은 단말 i는 과거 자신이 폴링 프레임을 수신한 시점부터 현재까지 데이터 프레임을 전송한 다

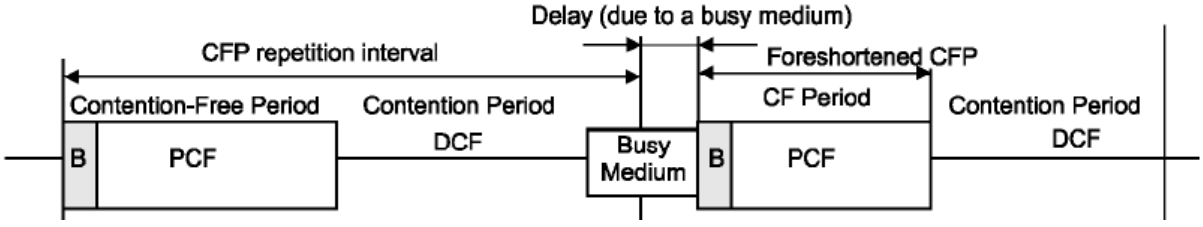

Figure 1. Superframe structure

Frame Cont.	Dur./ID	RA	TA	DA	Seq. Cont.	RC	Frame Body

Figure 2. Format of response frame

른 단말 중 MAC 주소가 R_i에 없고 전송 신호를 감지할 수 있는 해당되는 모든 단말의 MAC 주소를 R_i에 추가한다. 이 때, 단말 i는 해당되는 단말의 전송 신호의 감지 여부를 알기 위하여 수신 신호 강도를 PHY 계층에서 측정하여 전송파 감지결과를 busy 혹은 idle로 판정하여 MAC 계층에 알려주도록 한다. 전송파에 대해서 busy 혹은 idle로 판정하기 위한 자세한 방법은 IEEE Std 802.11 (1999)에 있다. 그리고 단말 i는 해당되는 단말의 MAC 주소를 단말의 데이터 전송 직전에 AP가 전송하는 폴링 프레임을 수신하여 폴링 프레임 내의 수신측 단말의 MAC 주소 필드로부터 알 수 있다. 이를 위하여 AP는 폴링 프레임을 전송할 때 자신의 무선랜 내에 있는 모든 단말이 폴링 프레임을 제대로 수신할 수 있도록 폴링 프레임을 방송해야 한다. 그리고 단말 i는 MAC 주소가 R_i에 있지만 이전의 3개의 폴링 프레임을 받기 직전의 시점부터 현재까지 전송 신호를 감지할 수 없는 단말이 있다면 해당되는 모든 단말의 MAC 주소를 R_i에서 삭제한다. 그리고 단말 i는 이러한 R_i에 추가 혹은 삭제되는 단말의 MAC 주소를 AP로 전송하는 데이터 프레임에 piggyback하여 AP에 알려준다. 만약 폴링 받은 시점에 단말 i가 전송할 데이터 프레임이 없으면 null 프레임을 전송하고 R_i에 추가 혹은 삭제되는 단말의 MAC 주소는 null 프레임에 piggyback한다. 새로운 단말이 무선랜에 association을 통하여 들어오는 경우 그 단말의 R_i는 처음에 공집합으로 시작한다. 각 단말이 자신과 다른 단말간의 전송파 감지정보의 변화 즉, R_i에 추가 혹은 삭제되는 단말의 MAC 주소를 AP에 알려주기 위하여 폴링 프레임에 대한 응답 프레임의 구성을 <Figure 2>와 같이 변경하여야 한다.

<Figure 2>에서 R_C는 R_i에 추가 혹은 삭제되는 단말의 MAC 주소의 집합을 의미한다. 그 이외의 다른 필드의 정의는 IEEE Std 802.11 (1999)와 동일하다.

이러한 방법을 이용하면 단말간의 전송파 감지정보가 대칭적이라고 가정하고 (즉, 단말 i가 단말 j의 전송 신호를 감지할 수 있으면 단말 j가 단말 i의 전송 신호를 감지할 수 있다고 가정함) 단말과 AP간에 전송에러가 발생하지 않는 경우 AP는 한번의 폴링 주기만으로 각 단말에 대하여 전송 신호를 감지할 수 있는 다른 단말의 MAC 주소를 모두 수집할 수 있다. 각 단말은 AP로부터 폴링 받은 시점에서 폴링 주기 내에서 이전에 전송한 단말과 자신간의 전송파 감지정보를 AP에 보고하기 때문에 단말간의 전송파 감지정보가 대칭적인 경우 한번의 폴링 주기만으로 AP는 각 단말에 대하여 전송 신호를 감지할 수 있는 다른 단말의 MAC 주소를 모두 수집할 수 있다. 만약 AP가 폴링 프레임을 전송하였으나 전송에러로 인하여 AP가 이에 대한 응답 프레임을 해당되는 단말로부터 제대로 수신할 수 없는 경우 AP는 PCF 프로토콜의 전송에러 복구절차에 따라서 폴링 리스트상의 다음 단말을 순서대로 폴링하여 단말간의 전송파 감지정보를 계속적으로 수집한다. 따라서 AP와 단말간의 전송에러가 발생하는 경우 단말간의 전송파 감지정보를 수집하는데 한번의 폴링주기 이상의 시간이 소요될 수 있을 것이다. 이러한 이유로 각 단말은 전송 신호를 감지할 수 있는 다른 단말의 MAC 주소의 집합인 R_i에서 어떤 단말을 삭제하기 위해서 이전의 3개의 폴링 프레임을 받기 직전의 시점부터 현재까지의 전송 신호를 관찰하도록 하였다. 이는 R_i에서 어떤 단말을 삭제하기 위해서 적어도 과거 3번의 폴링주기를 관찰하도록 한 것이다. 이에 대한 자세한 이론적인 분석을 다음 세부 절에서 제시한다.

3.2 전송파 감지정보 수집을 위한 소요시간 분석

AP가 현재의 무선랜 내의 N개의 단말간의 전송파 감지정보를 획득하기 위하여 몇번의 폴링주기가 필요한지 분석하기 위하여 다음의 3가지 가정을 하고자 한다.

- AP와 단말간의 각 폴링 프레임과 각 응답 프레임의 전송시 전송이 성공할 확률을 다른 사건과 독립적으로 p라 한다.
- AP가 단말 i에 전송하는 폴링 프레임을 다른 단말 j가 성공적으로 수신하여 단말 i의 MAC 주소를 성공적으로 획득할 확률을 다른 사건과 독립적으로 p라 한다.
- 단말 i의 전송 신호를 단말 j가 감지할 수 있는 위치에 있는 경우 단말 i가 AP로 전송하는 응답 프레임에 대한 전송 신호를 단말 j가 성공적으로 감지하여 단말 i와 자신간의 전송파 감지정보를 성공적으로 획득할 확률을 다른 사건과 독립적으로 p라 한다.

전송 실패 혹은 신호 감지 실패 확률을 α라 할 경우 전송 성공 혹은 신호 감지 성공 확률 $p = 1 - \alpha$이다.

어떤 하나의 폴링주기 내에서 단말 j가 단말 i의 전송 신호를 감지할 수 있는 위치에 있는 경우 단말 i와 단말 j간의 전송파 감지정보를 단말 j가 성공적으로 획득하여 AP로 성공적으로 전달하기 위해서는 다음의 5가지 사건이 순차적으로 발생해야 한다. AP가 각 단말을 폴링주기 내에서 순차적으로 풀링할 때 단말 i를 단말 j보다 먼저 폴링한다고 가정한다.

- AP가 단말 i로 폴링 프레임을 성공적으로 전송한다.
- AP가 단말 i로 전송한 폴링 프레임을 단말 j가 성공적으로 수신하여 단말 i의 MAC 주소를 성공적으로 획득한다.

- 단말 i가 AP로 전송하는 응답 프레임에 대한 전송 신호를 단말 j가 성공적으로 감지한다.
- AP가 단말 j로 폴링 프레임을 성공적으로 전송한다.
- 단말 j가 AP로 자신과 다른 단말간의 전송파 감지정보를 piggyback하여 응답 프레임을 성공적으로 전송한다.

앞의 5가지 사건 중에서 처음 3가지 사건은 단말 j가 자신과 단말 i간의 전송파 감지정보를 성공적으로 획득하기 위하여 필요한 사건이며 나머지 2가지 사건은 단말 j가 AP로 자신과 다른 단말간의 전송파 감지정보를 성공적으로 전달하기 위하여 필요한 사건이다. 앞의 각 사건이 어떤 하나의 폴링주기 내에서 발생할 확률은 가정에 의하여 서로 독립적으로 p이다. 따라서 단말 j가 단말 i의 전송 신호를 감지할 수 있는 위치에 있는 경우 어떤 하나의 폴링주기 내에서 단말 i와 단말 j간의 전송파 감지정보를 단말 j가 성공적으로 획득할 확률은 p^3이며 단말 j가 AP로 자신과 다른 단말간의 전송파 감지정보를 성공적으로 전달할 확률은 p^2이다.

어떤 두개의 단말이 서로의 전송파를 감지할 수 있는 위치에 있는 경우 어떤 하나의 단말이 자신과 다른 단말의 전송파 감지정보를 한번의 폴링주기 내에서 성공적으로 획득할 확률은 p^3이며 이러한 단말간의 전송파 감지정보가 한번의 폴링주기 내에서 성공적으로 획득되어 AP에 전달될 확률은 p^5이다. 그리고 어떤 두개의 단말이 서로의 전송파를 감지할 수 있는 위치에 있는 경우 어떤 하나의 단말이 자신과 다른 단말의 전송파 감지정보를 일반적으로 M (≥ 1)번의 폴링주기 내에 성공적으로 획득할 확률, P_M과 AP가 이러한 단말간의 전송파 감지정보를 일반적으로 M번의 폴링주기 내에 성공적으로 수집할 확률, Q_M을 다음의 식으로 계산할 수 있다.

$$P_M = 1-(1-p^3)^M$$

$$Q_M = 1-(1-p^5)^M$$

전송 실패 혹은 신호 감지 실패 확률, α = 0.1%, 0.5%, 1%, 2%, 5%인 경우에 대해서 어떤 두개의 단말이 서로의 전송파를 감지할 수 있는 위치에 있는 경우 어떤 하나의 단말이 자신과 다른 단말의 전송파 감지정보를 일반적으로 M번의 폴링주기 내에 성공적으로 획득할 확률, P_M과 AP가 이러한 전송파 감지정보를 M번의 폴링주기 내에 성공적으로 수집할 확률, Q_M을 M = 1, 2, 3, 4, 5에 대하여 구한 계산결과는 다음의 <Table 1>, <Table 2>와 같다. (Eckhardt and Steenkiste (1999)에 따르면 인위적인 간섭이 없는 일반적인 경우에 해당하는 논문의 Office와 Walking 시나리오의 경우 전송실패 확률은 대략적으로 5%보다 작다).

<Table 1>, <Table 2>의 결과에서 알 수 있듯이 전송 실패 혹은 신호 감지 실패 확률이 2% 이하인 경우 어떤 두개의 단말이 서로의 전송파를 감지할 수 있는 위치에 있는 경우 어떤 하나의 단말은 3번의 폴링주기만으로 99.9% 이상의 자신과 다른 단말의 전송파 감지정보를 성공적으로 획득할 수 있으며 AP는 3번의 폴링주기만으로 99.9% 이상의 전송파 감지정보를 성공적으로 수집할 수 있다. 그리고 전송 실패 혹은 신호 감지 실패 확률이 5%인 경우에도 어떤 하나의 단말은 3번의 폴링주기만으로 99.7% 이상의 자신과 다른 단말의 전송파 감지정보를 성공적으로 획득할 수 있으며 AP는 3번의 폴링주기만으로 98.8% 이상의 전송파 감지정보를 성공적으로 수집할 수 있다. 따라서 3.1절에서 각 단말이 전송 신호를 감지할 수 있는 다른 단말의 MAC 주소의 집합인 R_i에서 어떤 단말을 삭제하기 위해서 적어도 과거 3번의 폴링주기를 관찰하도록 한 것은 적절하다고 할 수 있다.

Table 1. Numerical results of P_M

α	P_1	P_2	P_3	P_4	P_5
0.1%	0.9970	0.9999	0.9999	0.9999	0.9999
0.5%	0.9850	0.9998	0.9999	0.9999	0.9999
1%	0.9702	0.9991	0.9999	0.9999	0.9999
2%	0.9411	0.9965	0.9998	0.9999	0.9999
5%	0.8573	0.9796	0.9971	0.9996	0.9999

Table 2. Numerical results of Q_M

α	Q_1	Q_2	Q_3	Q_4	Q_5
0.1%	0.99501	0.99998	0.99999	0.99999	0.99999
0.5%	0.97525	0.99939	0.99998	0.99999	0.99999
1%	0.95099	0.99760	0.99988	0.99999	0.99999
2%	0.90392	0.99077	0.99911	0.99991	0.99999
5%	0.77378	0.94882	0.98842	0.99738	0.99941

3.3 은닉 단말 발견 방법

CFP에서 AP에 의해 수집된 N개의 단말간의 전송파 감지정보와 관련된 상수인 $H_{i,j}$ (i = 1, 2, ⋯, N, j = 1, 2, ⋯, N, i ≠ j)를 다음과 같이 정의하고자 한다.

- $H_{i,j}$: 단말 i의 전송 신호를 단말 j가 감지하지 못하는 경우에는 1의 값을 가지며 그렇지 않은 경우 0의 값을 가짐.

$H_{i,j}$ = 1이면 단말 j가 단말 i의 데이터 전송을 방해할 수 있는 은닉 단말이 됨을 의미하여 $H_{i,j}$ = 0이면 단말 j가 단말 i의 은닉 단말이 아님을 의미한다. 따라서 N개의 단말 중에서 자신의 데이터 전송을 방해할 수 있는 은닉 단말이 존재하지 않는 단

말의 집합 Z를 다음과 같이 구할 수 있다.

$$Z = \{i | H_{i,j} = 0, \text{ for all } j \neq I\} \quad (1)$$

AP는 각 CFP에서 단말간의 새로운 전송파 감지정보에 따라서 식 (1)의 집합 Z를 새로 구하고 만약 Z에 추가되거나 Z에서 삭제되는 단말이 있는 경우 이러한 변화를 CFP에서 해당되는 단말에 폴링 프레임을 전송할 때 piggyback하여 알려준다. 이를 위하여 폴링 프레임의 구성을 <Figure 3>과 같이 변경하여야 한다.

Frame Control	Duration / ID	RA	TA	ZC

Figure 3. Format of polling frame

<Figure 3>에서 Z_C는 폴링 프레임의 수신측 단말이 식 (1)의 집합 Z에 추가되거나 Z에서 삭제되는 경우 이를 알려주기 위한 것으로써 만약 폴링 프레임의 수신측 단말이 Z에 추가되는 경우 Z_C의 값은 1을 가지며 만약 폴링 프레임의 수신측 단말이 Z에서 삭제되는 경우 Z_C의 값은 0을 가진다. 초기의 Z는 공집합으로 시작한다.

CFP에서 각 단말은 AP로부터 폴링 프레임을 수신하여 자신이 식 (1)의 집합 Z에 포함되는지 포함되지 않는지 판단하여 만약 자신이 Z에 포함되면 다음 CP에서 데이터를 전송할 때 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행하지 않고 데이터 프레임을 전송하는 절차에 바로 들어가게 되며 만약 자신이 Z에 포함되지 않으면 다음 CP에서 데이터를 전송할 때 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 먼저 수행하고 나서 데이터 프레임을 전송하는 절차에 들어가게 된다.

본 논문에서 제안하는 은닉 단말 발견 방법은 기본적으로 AP에 연결된 모든 단말이 CF-Pollable하며 AP와의 association 과정을 통하여 polling list에 가입한다는 가정을 가지고 있다. 따라서 CP 뿐만 아니라 CFP가 존재하며 각 CFP에서 AP는 각 단말에 대하여 적어도 한번의 폴링 프레임을 전송하여 한번의 데이터를 전송할 권리를 부여하여야 한다. 만약 infrastructure mode 무선랜이 이러한 가정을 만족시키지 못하면 논문에서 제안하는 은닉 단말 발견 방법은 적용할 수 없으며 모든 단말에 RTS/CTS 방법을 사용하여 데이터를 전송하거나 다른 기존의 방법을 사용하여야 한다. 만약 infrastructure mode 무선랜이 앞의 가정을 만족시킬 경우 각 CFP에서 본 논문에서 제안하는 새로운 은닉 단말 발견 방법에 따른 추가적인 overhead는 매우 작다고 할 수 있다. 이는 각 단말이 자신과 다른 단말간의 전송파 감지정보를 AP에 전달하거나 AP가 각 단말이 식 (1)의 집합 Z에 속하는지 속하지 않는지에 대한 정보를 전달할 때 변화된 정보만을 전달하며 이러한 정보를 기존의 폴링 프레임 혹은 이에 대한 응답 프레임에 piggyback하여 전달하기 때문이다.

4. 성능 분석

<Figure 4>는 IEEE 802.11a 무선랜의 4가지 경우 (무선랜 내의 단말의 수 N = 5, 10, 20, 30)를 보여준다. <Figure 4>의 4가지 무선랜은 N개의 단말이 2차원 평면상의 원에서 랜덤하게 분포하도록 하여 유도되었다. Xu, Gerla and Bae (2002)의 내용을 참고하여 <Figure 4>에서 AP를 포함한 각 단말의 데이터 전송 및 수신 가능 범위는 400m로 가정하고 AP를 포함한 각 단말의 전송파 감지 범위는 670m로 가정한다. 그리고 <Figure 4>의 각 무선랜의 서비스 반경을 각 단말의 데이터 전송 및 수신 가능 범위와 동일하게 400m로 가정한다.

본 논문의 서론에서 설명한 대로 무선랜 내의 은닉 단말을 발견하기 위하여 IEEE 802.11k draft 2.0 (2005), Kermani *et al*. (1997), Kristensen and Engelstad (2006A), Kristensen and Engelstad (2006B)에서 제안된 기존의 방법들은 모두 어떤 단말이 다른 단말의 데이터 전송을 방해할 수 있는 은닉 단말이 되는지 되지 않는지 판단하기 위하여 단말간의 연결정보를 사용한다. 따라서 기존의 방법들은 어떤 단말 E의 데이터 전송 및 수신 가능 범위(400m) 내에 나머지 모든 단말이 존재하는 경우 단말 E의 데이터 전송을 방해할 수 있는 다른 은닉 단말이 존재하지 않는다고 판정하고 그렇지 않은 경우 단말 E의 데이터 전송을 방해할 수 있는 다른 은닉 단말이 존재한다고 판정한다. 반면 본 논문의 제 3장에서 제안된 방법은 어떤 단말이 다른 단말의 데이터 전송을 방해할 수 있는 은닉 단말이 되는지 되지 않는지 판단하기 위하여 단말간의 전송파 감지정보를 사용한다. 따라서 어떤 단말 E의 전송파 감지 범위(670m) 내에 나머지 모든 단말이 존재하는 경우 단말 E의 데이터 전송을 방해할 수 있는 다른 은닉 단말이 존재하지 않는다고 판정하고 그렇지 않은 경우 단말 E의 데이터 전송을 방해할 수 있는 다른 은닉 단말이 존재한다고 판정한다. 자신의 데이터 전송을 방해할 수 있는 다른 은닉 단말이 존재하지 않는 단말들은 데

Table 3. Derivation results of STAs that need the channel reservation

	Case a	Case b	Case c	Case d
proposed method	none	STAs 2, 7	STAs 2, 7, 10, 12, 13, 14, 15	STAs 2, 7, 10, 12, 13, 14, 15, 21, 22, 23, 24
existing methods	STAs 2, 3, 4, 5	STAs 2, 3, 4, 5, 6, 7, 9, 10	All STAs except STA 8	All STAs

이터를 전송할 때 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행하지 않고 데이터 프레임을 전송하는 절차에 바로 들어가게 되고 자신의 데이터 전송을 방해할 수 있는 다른 은닉 단말이 존재하는 단말들은 데이터를 전송할 때 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행하고 나서 데이터 프레임을 전송하는 절차에 들어가게 된다. 본 논문의 제 3장에서 제안된 방법과 기존의 방법을 사용할 경우 데이터를 전송할 때 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행할 필요가 있는 단말들을 도출하여 그 결과를 비교하면 <Table 3>과 같다.

<Table 3>의 결과에 따르면 본 논문에서 제안한 방법을 사용할 경우 은닉 단말에 의한 전송 방해를 방지하기 위하여 데이터 전송시 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행할 필요가 있는 단말의 수가 기존의 방법에 비하여 상당히 줄어든다. 따라서 본 논문에서 제안한 방법을 사용할 경우 은닉 단말 문제를 해결하기 위하여 필요한 RTS 프레임과 CTS 프레임의 전송을 줄임으로써 무선채널을 통한 데이터 전송 효율을 향상시킬 수 있다.

본 논문의 제 3장에서 제안된 은닉 단말 발견 방법에 의한 <Figure 4>의 IEEE 802.11a 무선랜의 MAC 프로토콜의 성능 향상을 컴퓨터 시뮬레이션을 통하여 보이고자 한다. 성능 분석을 위하여 사용된 시뮬레이터는 본 논문의 저자에 의하여 C 코드로 작성되었다. 시뮬레이션을 위해서 데이터 프레임의 길이의 분포가 필요한데 여기서는 참고 문헌에 있는 NLANR (National Laboratory for Applied Network Research)의 홈페이지에 있는 자료를 참고하여 데이터 프레임의 길이가 <Figure 5>

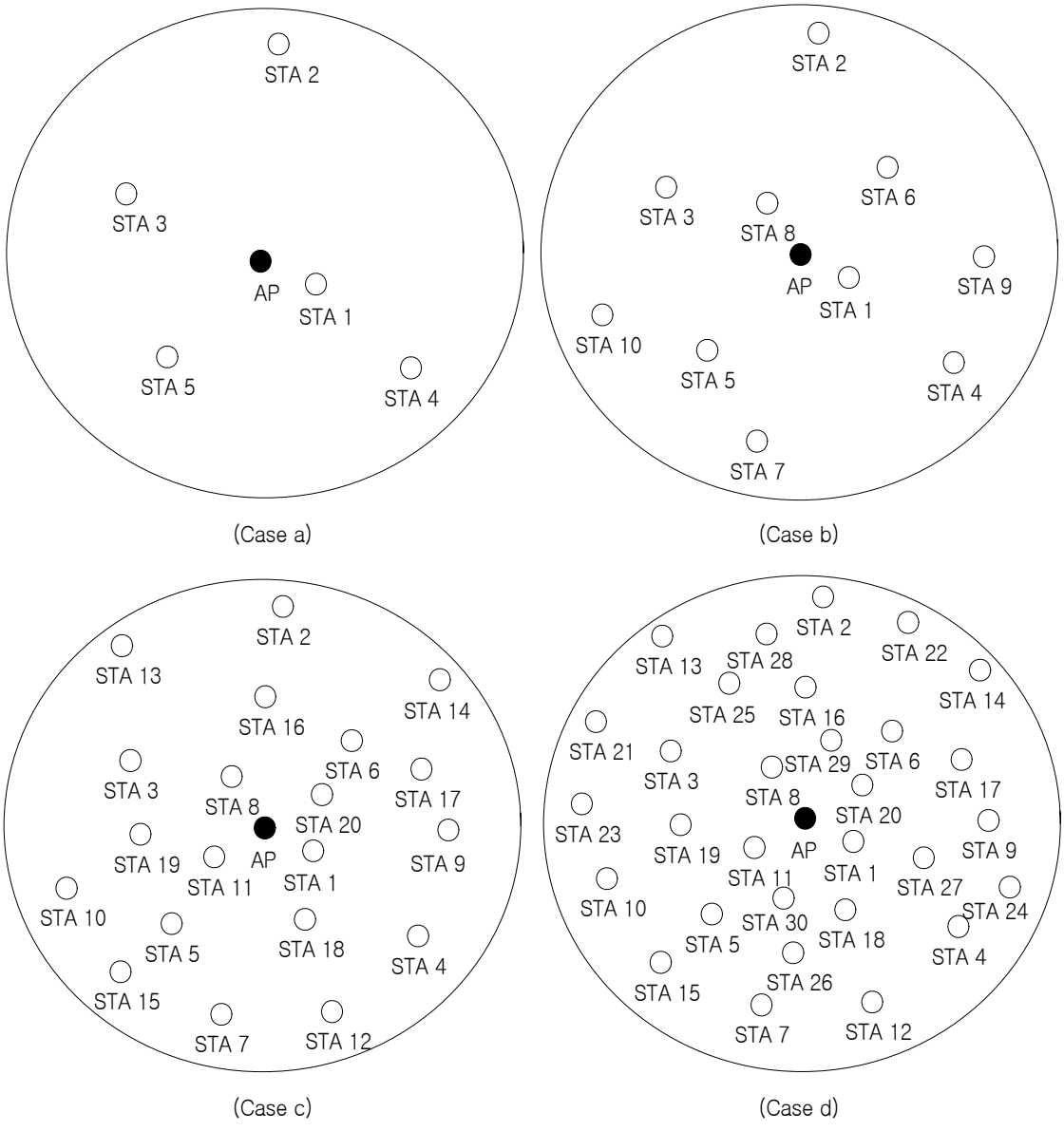

Figure 4. Four cases of IEEE 802.11a wireless LAN

의 확률 분포를 따른다고 한다. 즉, 각 단말에서 생성되는 각 데이터 프레임의 길이는 <Figure 5>의 확률 분포를 따르며 서로 독립이라고 가정한다.

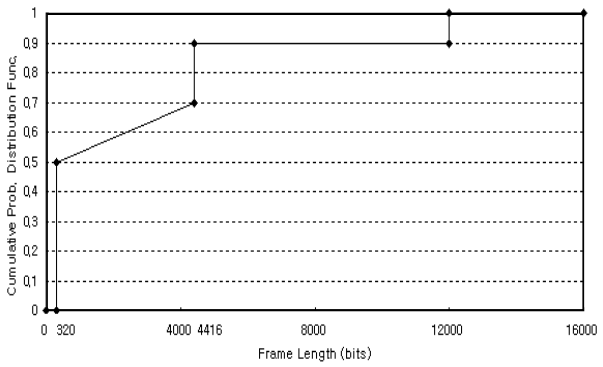

Figure 5. Data frame size distribution

또한 IEEE Std 802.11 (1999)의 MAC 프로토콜을 컴퓨터 시뮬레이션하기 위해서 다음의 parameter의 값이 필요하다.

- CWmin, CWmax (contention window의 최소값과 최대값)
- m (백오프의 최대 허용 단계)
- SIFS, PIFS, DIFS (Short InterFrame Space, PCF InterFrame Space, DCF InterFrame Space)
- L_{PHY} (PHY 계층의 헤더 전송 시간)
- L_{RTS}, L_{CTS} (RTS 프레임과 CTS 프레임의 전송 시간)
- L_{ACK} (ACK 프레임의 전송 시간)
- R (PHY 계층의 데이터 전송률)

<Table 4>는 IEEE Std 802.11a (1999)를 참고하여 IEEE 802.11a 무선랜의 앞의 parameter의 값을 나타낸 것이다. <Table 4>에서 L_{RTS}, L_{CTS}, L_{ACK}은 의무적으로 처리해야 하는 데이터 전송률 중 가장 큰 값으로 RTS, CTS, ACK 프레임을 전송할 때 소요되는 시간이며 PHY 계층의 헤더 전송 시간 (L_{PHY})도 포함되었다. IEEE 802.11a 무선랜에서 모든 단말이 의무적으로 처리해야 하는 데이터 전송률은 6Mbps, 12Mbps, 24Mbps이다. 따라서 RTS, CTS, ACK 프레임은 24Mbps의 전송률로 전송된다고 가정하였다. 그리고 전송 실패 확률은 5%로 가정하였다.

각 단말은 데이터 프레임을 전송한 후에 즉시 새로운 데이터 프레임을 전송하려고 계속적으로 시도한다고 가정한다. 그리고 각 수퍼프레임 시간은 20ms로 고정하고 CFP 시간은 고정되어 있지 않고 각 CFP에서 AP는 각 단말에 한번의 폴링 프레임 전송을 통하여 한번의 데이터를 전송할 기회를 부여하도록 한다. 분석의 편의상 <Figure 4>의 IEEE 802.11a 무선랜의 단말간 전송파 감지정보가 변하지 않는다고 가정한다. 그러나 단말간 전송파 감지정보가 변한다 하더라도 실제로는 전송파 감지정보의 변화에 해당하는 MAC 주소만 응답 프레임에 piggyback되어 전송되기 때문에 이로 인하여 발생하는 overhead는 작다고 할 수 있다. 예를 들어 초당 10개의 단말간 간섭정보가 변한다고 가정하자. 그러면 초당 10개의 MAC 주소가 응답 프레임에 piggyback되어 전송되어야 한다. 이로 인하여 필요한 전송률은 10 * 6 bytes / second = 480 bps이다. 이것은 IEEE 802.11a 무선랜의 전체 데이터 전송률인 54 Mbps에 비하여 매우 작다는 것을 알 수 있다.

Table 4. Values of parameters used for computer simulation

Parameters	Values
CWmin	15
CWmax	1023
m	7
SIFS	$16\mu s$
PIFS	$25\mu s$
DIFS	$34\mu s$
L_{PHY}	$24\mu s$
L_{RTS}	$31\mu s$
L_{CTS}	$29\mu s$
L_{ACK}	$29\mu s$
R	54Mbps

<Figure 6>은 <Table 4>의 parameter의 값을 사용하여 <Figure 4>의 4가지 IEEE 802.11a 무선랜에 대하여 구해진 컴퓨터 시뮬레이션 분석 결과로써 IEEE 802.11k draft 2.0 (2005), Kermani *et al.* (1997), Kristensen and Engelstad (2006A), Kristensen and Engelstad (2006B)의 기존의 은닉 단말 발견 방법과 본 논문의 3절에서 제안된 방법 그리고 모든 데이터 프레임의 전송시 RTS/CTS 방법을 사용하는 순수한 IEEE 802.11 scheme을 적용하여 구해진 MAC thorughput을 비교한 결과이다. <Figure 6>의 각 경우의 분석 결과는 10^6 타임 슬롯 동안 컴퓨터 시뮬레이션을 하여 얻어졌다. IEEE 802.11a 무선랜의 경우 하나의 타임 슬롯의 길이는 $9\mu s$이다. <Figure 6>의 MAC throughput은 CP 구간에서 DCF 프로토콜을 통하여 순수하게 MAC 데이터 프레임 내의 user payload를 성공적으로 전송하기 위하여 소요된 시간의 비율을 의미한다. 따라서 실제 IEEE 802.11a 무선랜의 MAC 계층에서 DCF 프로토콜을 통하여 사용되는 데이터 전송률은 54Mbps * 전체 시간에서 CP 구간이 차지하는 비율 * MAC throughput이다. 단말간의 연결정보를

이용하는 기존의 은닉 단말 발견 방법을 적용할 때 각 단말은 자신과 다른 단말간의 연결정보를 사용하여 자신이 데이터를 전송할 때 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행할 필요가 있는지 없는지 결정하도록 하였으며 자신과 다른 단말간의 연결정보를 획득하는데 부가적인 트래픽이 발생하지 않는다고 가정하였다. 특히, Kristensen and Engelstad (2006A), Kristensen and Engelstad (2006B)에서 제안된 능동적인 은닉 단말 발견 방법을 적용할 때 많은 부가적인 트래픽이 발생할 것으로 예상되는데 이러한 부가적인 트래픽에 의한 성능 저하는 무시하였다. 그럼에도 불구하고 본 논문의 3절에서 제안된 은닉 단말 발견 방법은 기존의 방법에 비하여 MAC throughput을 평균적으로 약 15% 증가시킨다는 것을 <Figure 6>의 분석 결과로부터 알 수 있었다. 그리고 은닉 단말 발견 방법을 적용하지 않는 순수한 IEEE 802.11 scheme과 비교하면 본 논문의 3절에서 제안된 은닉 단말 발견 방법은 기존의 방법에 비하여 MAC throughput을 평균적으로 약 16% 증가시킨다. <Figure 6>의 분석 결과로부터 기존의 은닉 단말 발견 방법과 본 논문의 제 3장에서 제안된 은닉 단말 발견 방법이 적용될 경우 모두 무선랜 내의 단말의 수가 커짐에 따라서 은닉 단말이 많아지고 MAC throughput이 작아지지만 본 논문에서 제안된 은닉 단말 발견 방법이 기존의 방법에 비하여 이러한 은닉 단말 문제를 훨씬 잘 해결한다고 할 수 있다.

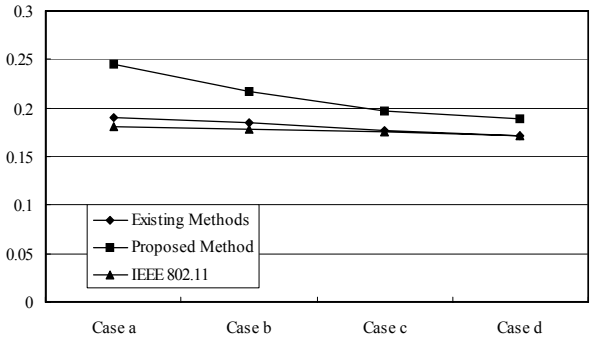

Figure 6. Numerical results of MAC throughput

5. 결 론

본 논문에서는 IEEE 802.11 무선랜에서 발생하는 은닉 단말 문제를 해결하기 위하여 은닉 단말을 발견하는 효율적인 방법을 제안하고 이를 MAC 프로토콜에 적용하여 무선랜의 MAC 성능을 향상시키는 방법을 제안하였다. 본 논문에서 제안된 은닉 단말 발견 방법은 단말간의 연결정보에 기초하는 기존의 방법의 문제점을 개선하여 은닉 단말에 의한 전송 방해를 방지하기 위하여 데이터 전송시 RTS 프레임과 CTS 프레임에 기초한 채널 예약을 수행할 필요가 있는 단말의 수를 줄인다.

참고 문헌

Choi, W.-Y. and Lee, S.-W. (2006), Optimal Polling Method for Improving PCF MAC Performance in IEEE 802.11 Wireless LANs, *Journal of Korean Institute of Industrial Engineers*, **32**(1), 1-8.

Choi, W.-Y. (2007), Efficient Polling Scheme for Multiple Direct Link Communication between STAs in Infrastructure Mode IEEE 802.11 Wireless LANs, *Journal of Korean Institute of Industrial Engineers*, **33**(2), 237-245.

Eckhardt, David A. and Steenkiste, Peter (1999), A Trace-Based Evaluation of Adaptive Error Correction for a Wireless Local Area Network, *Mobile Networks and Applications*, **4**, 273-287

IEEE Std 802.11 (1999), Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

IEEE Std 802.11a (1999), Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications : High Speed Physical Layer in the 5 GHz Band.

IEEE 802.11k draft 2.0 (2005), Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Radio Resource Measurement.

Kermani, P., McKay, D. N., Naghshineh, M., Novak, F. P. and Rezvani, B. (1997), Schemes to determine Presence of Hidden Terminals in Wireless Networks Environment and to Switch between Them, United States Patent 5661727.

Li, F. Y., Kristensen, A. and Engelstad, P. (2006A), Hidden Terminal Detection in 802.11-based Wireless Ad Hoc Networks, *Proc. IST Mobile & Wireless Communication Summit 2006*.

Li, F. Y., Kristensen, A. and Engelstad, P. (2006B), Passive and Active Hidden Terminal Detection in 802.11-based Ad Hoc Networks, *Proc. IEEE INFOCOM 2006*.

NLANR (National Laboratory for Applied Network Research) Internet Homepage, http://www.nlanr.net/NA/Learn/packetsizes.html

Sobrinho, J. L., Haan, R. and Brazio, J. M. (2005), Why RTS-CTS is not Your Ideal Wireless LAN Multiple Access Protocol, *IEEE WCNC 2005*, 81-87.

Tobagi, F. and Kleinrock, L. (1975), Packet Switching in Radio Channels: Part 2-The Hidden Node Problem in Carrier Sense Multiple Access Modes and the Busy Tone Solution, *IEEE Transactions on Communications*, **23**, 1417-1433.

Xu, K., Gerla, M. and Bae, Sang (2002), How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks, *Proc. IEEE GLOBECOM 2002*, 72-76.

Zhou, G., He, T., Stankovic, J. A. and Abdelzaher, T. (2005), RID : Radio Interference Detection in Wireless Sensor Networks, *Proc. INFOCOM 2005*, 891-901.