(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 12/22 (2006.01)
H04L 9/32 (2006.01)
H04J 3/14 (2006.01)

(45) 공고일자 2007년01월25일
(11) 등록번호 10-0673825
(24) 등록일자 2007년01월18일

(21) 출원번호 10-2005-7002207
(22) 출원일자 2005년02월07일
심사청구일자 2005년02월07일
번역문 제출일자 2005년02월07일
(86) 국제출원번호 PCT/US2003/025065
국제출원일자 2003년08월11일
(65) 공개번호 10-2005-0052462
(43) 공개일자 2005년06월02일
(87) 국제공개번호 WO 2004/015540
국제공개일자 2004년02월19일

(30) 우선권주장 10/217,042 2002년08월12일 미국(US)

(73) 특허권자 해리스 코포레이션
미합중국 플로리다 32919 멜보른 웨스트 나사 블러바드 1025

(72) 발명자 빌하르쯔 토마스 제이
미합중국 32934 플로리다주 멜보른 폴로니우스 레인 2355

(74) 대리인 손은진

심사관 : 김병균

전체 청구항 수 : 총 6 항

(54) 침입 감지 특징이 있는 무선 근거리 또는 도시권 통신망및 이에 관한 방법

(57) 요약

무선 근거리 또는 도시권 통신망(10)은 매체 접근 층(MAC)을 이용하여 지국 상호간에 데이터를 전송하기 위한 복수의 지국들을 포함할 수 있으며, 여기서 개개의 지국들은 관련된 각각의 MAC 주소를 갖는다. 무선 통신망(10)은 또한 1개의 MAC 주소로부터의 프레임 검사 시퀀스(FCS) 에러들을 감지하기 위해 복수의 지국들 간의 전송을 감시함으로써, 그리고 한계값을 초과하는 MAC 주소에 대한 다수의 FCS 에러들을 감지하는 것에 기초하여 침입 경보를 발생함으로써 무선 통신망으로의 침입을 감지하기 위한 폴리싱 지국을 포함할 수 있다. 폴리싱 지국(13)은 또한 1개 이상의 실패한 MAC 주소의 인증들, 불법적인 통신망 할당 벡터(NAV) 값들, 및 기대하지 않은 경합 또는 무경합 동작에 기초하여 침입들을 감지한다.

대표도

도 1

특허청구의 범위

청구항 1.

각각의 MAC 주소를 가지며, 매체 접근 층(MAC)을 사용하여 상호간 데이터를 전송하는 복수의 지국들;과,

상기 복수의 지국들 간의 전송들을 감시함으로써, 해당 무선 통신망으로의 침입을 감지하는 폴리싱 지국;을 포함하는 무선 근거리 또는 도시권 통신망으로서,

상기 폴리싱 지국은,

(a) 1개의 MAC 주소로부터의 프레임 검사 시퀀스(FCS) 에러들;

(b) MAC 주소를 인증하는 데 실패한 시도들;

(c) 무선 통신망과 관련된 서비스 셋 ID들;

(d) 전송 데이터의 형성에 앞서 상기 복수의 지국들 간에 전송되며, 발송요청(RTS) 및 발송취소(CTS) 패킷들로부터 발생되는 데이터의 전송을 위해 지정된 지속시간을 지시하는 통신망 할당 벡터(NAV) 값으로서, 불법적인 NAV 값;

(e) 상기 복수의 지국들에 의한 무경합 주기(CFP) 외에서의 무경합 모드 동작; 및

(f) CFP 동안의 경합 모드 동작;

중 적어도 1개를 감지하고, 그런 다음에,

(ⅰ) 한계값을 초과하는 MAC 주소에 대한 FCS 에러들의 횟수의 감지;

(ii) MAC 주소를 인증하는 데 실패한 시도들의 한계값을 초과하는 횟수의 감지;

(iii) 무선 통신망의 서비스 셋 ID와 다르게 감지된 서비스 셋 ID들 중 1개;

(Ⅳ) 감지된 불법적인 NAV 값;

(ⅴ) CFP 동안의 경합 모드 동작의 감지; 및

(vi) CFP 외에서의 무경합 모드 동작의 감지;

중 적어도 1개를 기초로 하여, 침입 경보를 발생하는 것을 특징으로 하는 무선 근거리 또는 도시권 통신망.

청구항 2.

제 1 항에 있어서,

상기 복수의 지국들은 적어도 1개의 채널을 통하여 데이터 전송을 실시하며, 상기 폴리싱 지국은 더 나아가 상기 무선 근거리 또는 도시권 통신망내에 포함된 복수의 지국들 중의 적어도 하나의 지국으로부터 발생되지 않은 데이터 전송들을 상기 적어도 1개의 채널상에서 감지하고, 이러한 감지를 기초로 침입 경보를 발생하는 것을 특징으로 하는 무선 근거리 또는 도시권 통신망.

청구항 3.

제 1 항에 있어서,

상기 폴리싱 지국은 더 나아가 상기 복수의 지국들 중 적어도 1개의 지국에게 침입 경보를 전송하는 것을 특징으로 하는 무선 근거리 또는 도시권 통신망.

청구항 4.

복수의 지국들을 포함하는 무선 근거리 또는 도시권 통신망을 위한 침입 감지 방법으로서,

각각의 MAC 주소를 갖는 복수의 지국들 간에 데이터를 전송하는 단계;와,

상기 복수의 지국들간의 전송을 감시하는 단계;를 포함하며,

상기 복수의 지국들간의 전송을 감시하는 단계는,

(a) 1개의 MAC 주소로부터의 프레임 검사 시퀀스(FCS) 에러들;

(b) MAC 주소를 인증하는 데 실패한 시도들;

(c) 무선 통신망과 관련된 서비스 셋 ID들;

(e) 전송 데이터의 형성에 앞서 상기 복수의 지국들 간에 전송되며, 발송요청(RTS) 및 발송취소(CTS) 패킷들로부터 발생되는 데이터의 전송을 위해 지정된 지속시간을 지시하는 통신망 할당 벡터(NAV) 값으로서, 불법적인 NAV 값;

(e) 상기 복수의 지국들에 의한 무경합 주기(CFP) 외에서의 무경합 모드 동작; 및

(f) CFP 동안의 경합 모드 동작;

중 적어도 1개를 감지하기 위해 상기 복수의 지국들 간의 전송들을 감시하며, 그런 다음,

(i) 한계값을 초과하는 MAC 주소에 대한 FCS 에러들의 횟수의 감지;

(ii) MAC 주소를 인증하는 데 실패한 시도들의 한계값을 초과하는 횟수의 감지;

(iii) 무선 통신망의 서비스 셋 ID와 다르게 감지된 서비스 셋 ID들 중 1개;

(Ⅳ) 감지된 불법적인 NAV 값;

(v) CFP 동안의 경합 모드 동작의 감지; 및

(vi) CFP 외에서의 무경합 모드 동작의 감지;

중 적어도 1개를 기초로 하여, 침입 경보를 발생하는 것을 특징으로 하는 침입 감지방법.

청구항 5.

제 4 항에 있어서,

상기 복수의 지국들에 의해 적어도 1개의 채널을 통하여 데이터 전송을 실시하고, 상기 폴리싱 지국은 또한, 상기 무선 근거리 또는 도시권 통신망내에 포함된 복수의 지국들 중의 적어도 하나의 지국으로부터 발생되지 않은 데이터 전송들을 상기 적어도 1개의 채널상에서 감지하고, 이러한 감지를 기초로 침입 경보를 발생하는 것을 특징으로 하는 침입 감지방법.

청구항 6.

제 4 항에 있어서,

상기 폴리싱 지국은 상기 복수의 지국들 중 적어도 1개의 지국에게 침입 경보를 전송하는 것을 더 포함하는 것을 특징으로 하는 침입 감지방법.

명세서

기술분야

본 발명은 통신망 분야에 관한 것으로서, 더욱 상세하게는 무선 근거리 통신망 또는 도시권 통신망 및 이에 관련된 방법에 관한 것이다.

배경기술

무선통신망들은 과거 수년간 점진적인 발전을 경험하여 왔다. 2 개의 특별한 예가 무선 근거리 통신망(LAN), 그리고 무선 도시권 통신망(MAN:metropolitan area network)이다. 기본 서비스 셋(BBS)에서, 그러한 통신망들은 예를 들면, 라디오 주파수 신호를 매개로 하여 접근점 또는 기지국(즉,서버)과 교신하는 1개 이상의 무선 지국(예를 들어, 무선 통신망 인터페이스 카드(NIC)를 가진 랩탑)을 포함한다. 기지국은 예를 들면, 동기화와 동등화(coordination), 방송 패킷들의 발송, 그리고 무선 LAN/MAN과 전화통신망과 같은 유선 통신망 간의 교량의 제공과 같은 많은 기능들을 수행한다.

확장 서비스 셋(ESS)에서는, 복수의 기지국들이 통신망에 포함된다. 반면에, 어떤 무선 LAN/MAN에서는 기지국이 전혀 없을 수도 있으며, 단지 무선 지국들이 상호간의 P2P(peer to peer)통신에 관여한다. 이러한 위상기하(topology)는 독립적 기본 서비스 셋(IBSS)이라 불리고, IBSS에서는 전형적으로 무선 지국들 중 1개가, 결여된 기지국에 대한 프록시로 행동하도록 선택된다.

무선 LAN/MAN의 인기에 대한 가장 두드러진 이유는 아마도 그러한 통신망이 비교적 저렴하고, 유선 인프라의 구축이 불필요하다는 점에서 배치하기가 쉽다는 것이다. 그러나, 무선 LAN/MAN 장치들은 또한 유선 통신망들에는 없는 몇 가지 심각한 결점들을 갖고 있다. 예를 들면, 무선 LAN/MAN 장치들이 널리 보급되어 있기 때문에 그러한 장치들은 통신망에 침입하여 권한이 없는 지국(즉, 로우그(rogue) 지국)을 사용하여 통신망의 보안을 손상하려고 시도하는 장래의 해커들에게 쉽게 노출된다. 또한, 무선 LAN/MAN들은 상호간에 너무 가깝게 작동되므로, 특히 그것들이 공통 채널들을 공유한다면, 통신망들은 상호간을 침입하고 통신망 혼란을 야기한다.

무선 LAN/MAN내에서의 통신을 제어하기 위해 개발되어 온 더욱 두드러진 표준들 중의 하나는, 전기전자기술자협회 802 LAN/MAN 표준위원회의 것으로서 1999년의 "정보기술을 위한 IEEE 표준--원거리통신 및 정보 시스템--근거리 및 도시권 통신망--특정한 필요조건들--제 11부:무선 LAN 매체 접근 제어(MAC) 및 물리층(PHY) 상세"라 명명된 것인데, 이는 전체로서 본 명세서에 참조하여 포함되었다. 무선 통신 프로토콜을 제공할 뿐만 아니라, 802.11 표준은 또한 무선신호들을 도청으로부터 보호하기 위해 사용되는 유선 등가 프라이버시(WEP) 알고리즘을 정의한다. 더욱 특별하게는, WEP은 최초 전송된 메시지의 무결성(integrity)이 손상되지 않았음을 확실하게 하기 위한 무결성 검사 뿐만 아니라 지국 간에 전송되는 메시지의 암호화를 제공한다.

WEP 알고리즘이 통신망 보안의 얼마간의 수단을 제공하기는 하지만, 통신망으로의 잠재적인 침입들을 감지하거나 알려주지는 않는다. 단지 최근에야 그러한 침입 감지 시스템이 가능하게 되었다. 이러한 시스템들은 전형적으로, 침입 감지가 요구되는 지국에 설치되는 보안 감시 소프트웨어를 포함한다. 그러한 소프트웨어는 매체 접근 제어(MAC) 주소나 인터넷 프로토콜(IP) 주소를 감시하고 기록함으로써, 그리고 그것들을 권한 있는 통신망 지국들의 공지된 주소와 대조함으로써, 침입을 방지하는 시도가 가능하다. 더욱이 그러한 시스템들은 언제 WEP가 작동되지 않는지를 관찰할 수 있다.

와일드패킷(WildPackets) 주식회사의 침입방지시스템의 특별한 일 실시예는 에어로픽(AiroPeek)이라고 불린다. 에어로픽은 통신망에서 사용되는 ESS 및 BSS 동일성 증명들(ESSIDs, BSSIDs)에 기초한 권한 없는 로우그 지국들을 탐색한다. 즉, 통신망에서 사용되는 모든 권한 있는 BSSID 및 ESSID들의 목록이 생성된다. 그 후, 모든 권한 없는 지국들을 배제하

기 위하여 필터가 생성된다. 이 필터는 통상의 통신망 트래픽을 검색하여 포착함으로써, 그리고 ESSID 또는 BSSID와 일치하는 802.11 프레임의 데이터 오프셋을 결정함으로써 생성된다. 에어로픽은 또한 프레임 카운트를 기초로 트리거(trigger)되는 경보를 포함한다. 즉, 만약 프레임 카운트가 0을 넘어서면, 경보가 트리거된다(즉, 만약 어떤 프레임이라도 로우그 지국으로부터 감지되면, 경보가 트리거된다). 더욱이 에어로픽은 전자우편을 통하여 또는 시스템 외부로 다이얼을 돌리기 위해(예를 들어, 호출기로) 모뎀을 사용함으로써 경보의 통지를 제공할 수 있다.

상기 시스템에 의해 이루어진 진보에도 불구하고, 무선 LAN/MAN으로의 어떤 침입들은 그러한 시스템들에게 감지되지 않고 여전히 행해질 수 있다. 즉, 예를 들어 로우그 지국이 권한 있는 주소 및/또는 ID로의 접근이 이미 가능하다면, 상기 접근방식들은 로우그 지국의 통신망 침입을 감지하지 못할 수 있다.

발명의 상세한 설명

상술한 배경기술을 고려하여, 본 발명의 목적은 침입 감지 특징이 있는 무선 LAN/MAN 및 이에 관련된 방법을 제공하는 것이다.

본 발명에 따른 이러한, 그리고 다른 목적들, 특징들 및 장점들은 매체 접근(MAC) 층을 사용하여 상호간 데이터를 전송하기 위한 복수의 지국들을 포함하고, 여기서 개개의 지국들은 관련된 각각의 MAC 주소를 갖는 무선 근거리 또는 도시권 통신망에 의해 달성된다. 무선 통신망은 또한 무선 통신망으로의 침입을 감지하기 위한 폴리싱(policing) 지국을 포함한다. 이것은 MAC 주소로부터 프레임 검사 시퀀스(FCS) 에러들을 감지하는 복수의 지국들 간의 전송들을 감시함으로써, 그리고 한계값(threshold)을 초과하는 MAC 주소에 대한 다수의 FCS 에러들을 감지하는 것에 기초한 침입 경보를 발생함으로써 이루어질 수 있다.

더욱이, 폴리싱 지국은 MAC 주소를 인증하는 데 실패한 시도들을 감지하기 위하여 복수의 지국들 간의 전송들을 감시함으로써, 그리고 MAC 주소를 인증하는 데 실패한 다수의 시도들을 감지하는 것에 기초하여 침입 경보를 발생함으로써 무선 통신망으로의 침입을 감지할 수 있다. 더욱 상세하게는, 폴리싱 지국은 미리 결정된 주기 내에 MAC 주소를 인증하는 데 실패한 시도들의 횟수를 감지하는 것에 기초하여 침입 경보를 발생할 수 있다.

또한, 복수의 지국들은 상호간 데이터를 전송하기 전에 발송요청(RTS:request to send) 및 발송취소(CTS:clear to send) 패킷들을 전송할 수 있다. RTS 및 CTS 패킷들은 전형적으로 데이터 전송을 위해 지정된 지속시간을 지시하는 통신망 할당 벡터(NAV)를 포함한다. 이와 같이, 폴리싱 지국은 더 나아가 불법적인 NAV 값을 감지하기 위해 복수의 지국 간에 발송되는 RTS 및 CTS 패킷들을 감시함으로써 무선 통신망으로의 침입을 감지하고 이에 기초한 침입 경보를 발생할 수 있다.

복수의 지국들은 또한 무경합 주기(CFP:contention-free period) 동안에 단속적으로 무경합 모드에서 동작할 수 있다. 그리하여, 폴리싱 지국은 또한 CFP 외에서의 무경합 모드 동작을 감지(또는 반대로)하기 위해 복수의 지국들 간의 전송들을 감시함으로써 무선 통신망으로의 침입을 유익하게 감지하고 이에 기초한 침입 경보를 발생할 수 있다.

또한, 무선 통신망은 그와 관련된, 예를 들어 BSSID 및/또는 ESSID와 같은, 적어도 1개의 서비스 셋 ID를 가질 수 있다. 따라서, 폴리싱 지국은 더 나아가 그와 관련된 서비스 셋 ID들을 감지하기 위해 복수의 지국들 간의 전송들을 감시함으로써 무선 통신망으로의 침입들을 감지할 수 있다. 폴리싱 지국은 게다가 감지된 서비스 셋 ID들 중 1개가 무선통신망의 적어도 1개의 서비스 셋 ID와 다른 것을 기초로 침입 경보를 발생할 수 있다. 또한, 복수의 지국들은 적어도 1개의 채널을 통하여 데이터를 전송할 수 있고, 그리고 폴리싱 지국은 복수의 지국들 중 1개로부터 발생되지 않은 적어도 1개의 채널을 통한 전송을 감지하고 이에 기초한 침입 경보를 발생할 수 있다.

폴리싱 지국은 어떤 실시예들에서는 복수의 지국들 중 적어도 1개에게 침입 경보를 유익하게 전송할 수 있다. 이와 같이, 적당한 대응책들이 침입에 반응하기 위해 채택될 수 있다. 더 나아가, 폴리싱 지국은 1개 또는 그 이상의 기지국 및/또는 무선 지국을 포함할 수 있다.

본 발명의 침입 감지 방법의 관점은 복수의 지국들을 포함하는 무선 근거리 또는 도시권 통신망을 위한 것이다. 본 방법은 MAC 층을 사용하여 복수의 지국들 간에 데이터를 전송하는 것을 포함하고, 여기서 개개의 지국들은 관련된 각각의 MAC 주소를 가진다. 더욱이, MAC 주소로부터 FCS 에러들을 감지하기 위해 복수의 지국들 간의 전송이 감시될 수 있고, 그리고 MAC 주소에 대한 다수의 FCS 에러들이 한계값을 초과하는 것을 기초로 침입 경보가 발생된다.

또한, 본 방법은 MAC 주소들을 인증하는 데 실패한 시도들을 감지하기 위해 복수의 지국들 간의 전송들을 감시하는 것, 그리고 MAC 주소를 인증하는 데 실패한 다수의 시도들의 감지에 기초한 침입 경보를 발생하는 것을 역시 포함한다. 특히, 침입 경보는 미리 결정된 주기 내에 MAC 주소를 인증하는 데 실패한 다수의 시도들을 감지하는 것에 기초하여 발생될 수 있다.

더욱이, 본 방법은 데이터의 전송에 앞서 복수의 지국들 간의 RTS 및 CTS 패킷들을 전송하는 것을 포함할 수 있다. 상기 지목한 바와 같이, RTS 및 CTS 패킷들은 전형적으로, 데이터 전송을 위해 지정된 지속시간을 지시하는 NAV 값들을 포함한다. 더욱이, 복수의 지국들 간에 전송된 RTS 및 CTS 패킷들은 불법적인 NAV 값을 감지하기 위해 감시될 수 있으며, 그리고 감지된 불법적인 NAV 값에 기초하여 침입 경보가 발생된다.

복수의 지국들은 CFP 동안에 무경합 모드에서 단속적으로 동작할 수 있다. 그리하여, 본 방법은 또한 CFP 외에서의 무경합 모드 동작(또는 반대로)을 감지하기 위해 복수의 지국 간의 전송들을 감시하고 이에 기초한 침입 경보를 발생하는 것을 포함할 수 있다.

또한, 무선 통신망은 그와 관련된 적어도 1개의 서비스 셋 ID를 가질 수 있다. 따라서, 본 방법은 더 나아가 상호 연관된 서비스 셋 ID들을 감지하기 위해 복수의 지국들 간의 전송들을 감시하는 것, 그리고 감지된 서비스 셋 ID들 중 1개가 무선 통신망의 적어도 1개의 서비스 셋 ID와 다른 것을 기초로 침입 경보를 발생하는 것을 포함할 수 있다. 여기서 다시, 서비스 셋 ID들은 예를 들어 ESSID이거나 BSSID일 수 있다. 또한, 복수의 노드들은 적어도 1개의 채널을 통하여 데이터를 전송할 수 있다. 따라서 복수의 지국들 중 1개로부터 발생되지 않은 적어도 1개의 채널을 통한 전송이 감지되고, 이에 기초하여 침입 경보가 발생된다. 본 방법은 또한 복수의 지국들 중 적어도 1개에게 침입 경보를 전송하는 것을 포함할 수 있다.

실시예

이제 이하에서 본 발명은, 바람직한 본 발명의 실시예들을 나타낸 첨부 도면들을 참조하여 더욱 상세하게 설명될 것이다. 그러나, 본 발명은 다양한 다른 형태들로 실시될 수 있으며, 여기에 제시된 실시예들에만 한정되는 것으로 해석되지 않아야 한다. 오히려, 이러한 실시예들은 본 개시가 철저하고 완전하며, 그리고 해당 기술분야에서 통상의 지식을 가진 자에게 본 발명의 범위를 완전히 전달하기 위하여 제공된 것이다.

이하의 논의에서는, 같은 번호들은 처음부터 끝까지 같은 구성요소들을 나타낸다. 더욱이, 도 1 내지 도 10을 특히 언급하는 경우, 십의 자리가 다른 참조 번호들은 대체적인 실시예들에서 유사한 구성요소들을 지칭한다. 예를 들어, 도면 1내지 10에 도시된 무선 지국들 11, 21, 31, 41, 51, 61, 71, 81, 91, 및 101은 모두 유사한 구성요소들인 것 등이다. 그와 같이, 이러한 구성요소들은 부적당한 반복을 피하기 위해 처음 출현할 때에만 상세하게 설명될 수도 있지만, 뒤에 출현하는 구성요소들은 처음 설명된 것과 유사한 것으로 이해된다.

이제 도 1을 참조하면, 본 발명에 따른 무선 LAN/MAN(10)은 도식적으로 무선 지국(11) 및 기지국(또는 접근점, 12)을 포함한다. 도식적 명료함을 위해서 단지 1개의 무선 지국(11) 및 기지국(12)을 나타냈지만, 해당 기술분야에서 통상의 지식을 가진 자는 무선 통신망(10)내에 임의의 갯수의 무선 및/또는 기지국들이 포함될 수 있다는 것을 이해할 것이다.

무선 통신망(10)을 더 상세히 설명하기 전에, 무선 LAN/MAN 프로토콜에 관한 간략한 논의가 있어야 한다. 특히, 이하 논의는 설명의 명료화를 위해 802.11 표준을 사용하는 통신망 실시를 가정할 것이다. 그러나, 해당 기술분야에서 통상의 지식을 가진 자는 여기서 설명된 다수의 측면들 및 실시예들은 다른 적절한 무선 LAN/MAN 표준들(예를 들어, 블루투스, 등)과 함께 또한 사용될 수 있다는 것을 이해할 것이다.

802.11 표준은 데이터 전송을 위한 OSI 통신망 모델과 함께 사용하기 위한 것이고, 이것은 어떤 형태의 데이터가 다양한 프로토콜들을 사용하여 전송되는 7개의 층(layer)들을 포함한다. 이러한 층들은 애플리케이션 층, 프리젠테이션 층, 세션 층, 트랜스포트 층, 통신망 층, 데이터 링크 층, 및 물리 층을 포함한다. 데이터 링크 층은 매체 접근 제어(MAC) 및 논리 링크 제어 하위-층들을 더 포함한다.특히 무선 지국(11) 및 기지국(12)은 상호간 데이터를 송신하기 위해 MAC 층을, 특히 예를 들어, 상호 관련된 각각의 MAC 주소들을 사용한다. 물론, OSI 모델의 나머지 층들도 또한 데이터 송신을 위하여 사용될 수 있다. 더욱이, 데이터는 전형적으로 패킷으로 전송되고, 그리고 이하에서 설명되는 것처럼 다양한 패킷 형태들이 다른 형태의 메시지 데이터를 위해 사용된다.

본 발명에 따라, 무선 통신망(10)은 도식적으로 로우그 지국(14)에 의한 무선 통신망으로의 침입을 감지하기 위한 폴리싱 지국(13)을 포함한다. 일 예로서, 로우그 지국(14)은 무선 통신망의 해킹을 시도하는 장래의 해커에 의해 사용될 수 있고,

또는 그것은 단지 무선 통신망(10)과 너무 가깝게 작동하는 다른 무선 통신망으로부터의 노드일 수 있다. 폴리싱 지국(13)은 1개 이상의 무선 지국 또는 기지국을 포함할 수 있다. 본 실시예에서, 폴리싱 지국(13)은 MAC 주소로부터의 프레임 체크 시퀀스(FCS) 에러들을 감지하기 위해 지국들(11, 12) 간의 전송들을 감시한다. 주어진 MAC 주소에 대해 감지된 다수의 FCS 에러들이 한계값을 초과한다면, 폴리싱 지국(13)은 이에 기초한 침입 경보를 발생한다.

여기서 사용된 것처럼, "지국 간의 전송"이라는 말은 무선 통신망(10)의 동작 범위 내의 모든 전송뿐만 아니라, 지국들(11, 12) 중 1개로 또는 1개로부터의 직접적인 전송을 의미하려는 것이라는 점을 주목해야 한다. 다시 말하면, 폴리싱 지국(13)은, 특정적으로 통신망(10)의 지국으로 향하거나 그로부터 발생되었는지 여부에 관계없이 그것이 수신하는 다른 모든 전송들뿐만 아니라, 지국들(11, 12)로 향하거나 그로부터 발생되는 전송들을 감시할 수 있다.

상기 설명된 실시예(그리고, 이하 설명되는 것들)에서, 폴리싱 지국(13)은 유익하게 무선 통신망(10)의 지국들(11, 12)의 1개 이상에게 경보를 전송할 수 있다. 일 예로서, 폴리싱 지국(13)은 기지국(12)으로 직접 침입 경보를 전송할 수 있고, 그것이 다시 무선 통신망의 나머지 모든 지국들에게 통지할 수 있다. 대체적으로, 폴리싱 지국(13)이 모든 통신망 지국들에게 침입 경보를 방송할 수 있다. 둘 중 어느 경우에, 해당 기술분야에서 통상의 지식을 가진 자에 의해 이해되는 바와 같이, 권한 없는 침입에 응답하기 위해 적합한 대응책들이 취해질 수 있다. 그러한 대응책들은 본 발명의 범위를 넘는 것이고 따라서 여기서 논의되지는 않을 것이다.

이제 도 2로 전환하여, 무선 LAN/MAN(20)의 첫 번째 대체적인 실시예를 설명한다. 이 실시예에서, 폴리싱 지국(23)은 MAC 주소들을 인증하는 데 실패한 시도들을 감지하기 위하여 지국들(21, 22) 간의 전송을 감시함으로써 무선 통신망(20)으로의 침입을 감지한다. 특정한 MAC 주소를 인증하는 데 실패한 시도의 미리 결정되어 있는 임의의 횟수를 감지할 때, 폴리싱 노드(23)는 침입 경보를 발생할 것이다.

실패한 시도들의 임의의 횟수가 침입 경보를 발생하기 위한 한계값으로 사용될 수 있으나, 일반적으로 침입 경보의 발생없이 MAC 주소를 인증하려는 적어도 1개의 시도를 지국에게 허용하는 것이 바람직하다. 더욱이, 어떤 실시예들에서 폴리싱 지국(23)은 유익하게 감지된 실패 횟수가 미리 결정된 주기(예를 들어, 한 시간, 하루, 등) 안에 발생할 때만 침입 경보를 발생한다.

802.11 표준에 따라, 무선 LAN/MAN 내에서 상호간 교신하려는 2개의 지국들은 전형적으로 데이터 전송에 앞서 발송요청(RTS) 및 발송취소(CTS) 패킷들을 상호간 전송한다. 그 이유는 다른 전송들과의 충돌을 피하기 위한 것이다. 즉, 무선 LAN/MAN내의 많은 또는 나머지 모든 지국들은 공통된 채널로 교신하고 있을 수 있기 때문에, 지국들이 간섭 또는 통신망 혼란을 야기할 수 있는 동시 전송 중이 아님을 확실히 할 필요가 있다. 더욱이, RTS 및 CTS 패킷들은 전형적으로 데이터 전송을 위해 지정된 지속시간을 지시하는 통신망 할당 벡터(NAV)를 포함한다. 이 정보는 무선 LAN/MAN 안의 다른 모든 지국들에게 전송되고, 그 후 특정한 주기 동안에 전송이 중단될 것이다.

이제 도 3으로 전환하여, 무선 LAN/MAN(30)의 두 번째 대체적인 실시예를 설명한다. 여기서 폴리싱 지국(33)은 불법적인 NAV 값을 감지하기 위해 지국들(31, 32) 간 전송된 RTS 및 CTS 패킷들을 감시함으로써 무선 통신망으로의 침입들을 감지한다. 예를 들면, 무선 통신망(30)은 데이터 전송이 임의의 시간을 초과하지 않는 것과 같은 방식으로 실시될 수 있고, 이 시간은 통신망에 참여하는 모든 권한 있는 지국들에게 알려질 것이다. 따라서, 폴리싱 지국(33)이 할당된 시간 밖에서 NAV 값을 감지한다면, 이에 기초하여 침입 경보를 발생할 것이다.

802.11 표준의 다른 특징은 무선 LAN/MAN 내의 지국들이 경합 또는 무경합 모드에서 동작할 수 있다는 것이다. 즉, 경합 모드에서는 모든 지국들은 전송되는 각각의 데이터 패킷들을 위해 사용 중인 특정한 채널에의 접근을 위해 경합을 필요로 한다. 무경합 주기(CFP) 동안에, 매체의 사용은 기지국에 의해 제어되고, 따라서 채널 접근을 위해 지국들이 경합할 필요가 없어진다.

도 4에 도시된 무선 LAN/MAN(40)의 세 번째 실시예에 따라, 폴리싱 지국(43)은 CFP 외에서의 무경합 모드 동작을 감지하기 위해 지국들(41, 42) 간의 전송들을 감시함으로써 무선 통신망(40)으로의 침입들을 유익하게 감지할 수 있다. 이와 같이, 그러한 감지에 기초하여 침입 경보가 폴리싱 지국(43)에 의해 발생될 수 있다. 다시 말해, 모든 권한 있는 무선 지국들은 기지국(42)에 의해 언제 CFP가 설정되는지를 통지받기 때문에, CFP 외에서 무경합 모드로 동작하는 지국의 감지는 이 지국이 권한 있는 지국이 아니라는 것을 나타낸다. 물론, 이것은 또한 경합 모드동작이 CFP 동안에 감지되는 경우도 마찬가지이고, 그러한 실시예가 도 5에 도시되어 있다. 상기 CFP 침입 감지 접근방식 중 하나 또는 양자 모두가 주어진 1개의 응용예에서 실시될 수 있다는 것이 해당 기술분야에서 통상의 지식을 가진 자에 의해 이해될 것이다.

이제 도 6을 참조하여, 무선 LAN/MAN(60)의 다른 실시예를 설명한다. 여기서, 폴리싱 지국(63)은 권한 없는 주기 중의 전송들을 감지하기 위해 지국들(61, 62) 간의 전송들을 감시함으로써 무선 통신망(60)으로의 침입들을 감지한다. 즉, 무선 통신망(60)은 어떤 사용자라도 특정한 시간(예를 들어, 자정부터 오전 6시 까지) 중에는 통신망으로의 접근이 허락되지 않는 것과 같이 실시될 수 있다. 따라서, 이런 권한 없는 주기 내의 전송들을 감지하면, 폴리싱 지국(63)은 침입 경보를 유익하게 발생한다.

이제 부가적으로 도 7로 전환하여, 무선 LAN/MAN(70)의 또 다른 실시예를 설명한다. 이 실시예에서, 다양한 지국들(71, 72)이 상기 설명된 WEP 특징을 가능하도록 하고 따라서 그것들로부터 전송된 데이터 패킷들과 함께 무결성 검사값들을 발생하고 전송한다. 그리하여, 폴리싱 지국(73)은 각각의 데이터 패킷들과 일치하지 않는 무결성 검사 값들을 감지하기 위하여 지국들(71, 72) 간의 전송들을 감시함으로써 무선 통신망(70)으로의 침입들을 감지한다. 즉, 잘못된 키이 스트림이 메시지 암호문을 발생하기 위해 사용된다면, 또는 메시지가 로우그 지국(74)에 의해 변경되었다면, 무결성 검사값은 오류일 가능성이 매우 높을 것이다. 이처럼 해당 기술분야에서 통상의 지식을 가진 자에 의해 이해되는 바와 같이, 폴리싱 지국(73)은 그러한 잘못된 무결성 검사값이 감지될 때 침입 경보를 발생할 수 있다.

이제 본 발명에 따른 또 다른 무선 LAN/MAN(80)을 도 8을 참조하여 설명한다. 전형적으로, 상기 주목된 OSI 통신망 모델이 사용될 때, 각각의 MAC 시퀀스 번호가 발생되고 지국들(81, 82)로부터 개개의 데이터 패킷과 함께 전송된다. 즉, 개개의 연속적인 데이터 패킷과 함께 MAC 시퀀스 번호는 증가되며, 따라서 개개의 패킷은 그와 관련된 고유의 MAC 시퀀스 번호를 가진다. 이처럼, 폴리싱 지국(83)은 1개의 지국에 의한 비연속인 MAC 시퀀스 번호들의 사용을 감지하기 위해 지국들(81, 82) 간의 전송을 감시함으로써 무선통신망(80)으로의 침입들을 감지하고, 이에 기초하여 침입 경보를 발생할 수 있다.

이제 부가적으로 도 9로 전환하면, 무선 LAN/MAN(90)의 또 다른 실시예가 도시되어 있으며, 여기서 폴리싱 지국(93)은 미리 결정된 패킷 형태를 갖는 패킷들의 충돌을 감지하기 위해 지국들(91, 92) 간의 전송들을 감시함으로써 무선 통신망으로의 침입들을 감지한다. 특히, 미리 결정된 패킷 형태는 매니지먼트 프레임 패킷들(예를 들어, 인증, 연합, 및 비콘 패킷들), 컨트롤 프레임 패킷들(예를 들어, RTS 및 CTS 패킷들), 및/또는 데이터 프레임 패킷들을 포함한다. 폴리싱 지국(93)은 따라서 미리 결정된 패킷 형태 충돌의 한계 횟수를 감지하는 것에 기초한 침입 경보를 발생할 수 있다.

여기서 사용된 것처럼, "충돌"이란 상호간의 일정한 시간 이내의 전송들뿐만 아니라 동시적인 패킷들의 전송을 포함하는 의미이다. 즉, 어떤 형태의 패킷이 전송들 간의 시간 지연을 갖는다고 한다면(예를 들어, 몇 초 등), 2개의 그러한 패킷 형태들이 서로 너무 가깝게 전송된다면, 이것은 충돌이라 간주될 것이다. 일 예로서, 충돌의 한계 횟수는, 다른 한계값들이 역시 사용될 수 있을지라도, 예를 들면 약 3보다 클 수 있다. 더욱이, 한계 횟수는 문제되는 특정한 패킷 형태에 기초할 수 있으며, 즉, 다른 패킷 형태에 대해 한계 횟수가 다를 수 있다.

부가적으로, 한계 횟수는 미리 결정된 패킷 형태를 갖는 감시된 패킷의 총 갯수의 백분율에 기초할 수 있다. 예를 들면, 어떤 주기(예를 들어, 1시간) 동안에 전송된 패킷들의 어떤 백분율(예를 들어, 10% 보다 큰)이 충돌과 관계가 있다면, 침입 경보가 발생될 수 있다. 대체적으로, 감시된 패킷들의 총수 중에서 어떤 패킷들의 백분율(예를 들어, 10 중에서 3)이 충돌과 관계가 있다면, 같은 목적의 다른 적당한 한계 횟수들 및 방법들이 또한 사용될 수 있다.

이제 도 10을 참조하여, 무선 LAN/MAN(100)의 또 다른 실시예를 설명한다. 여기서, 폴리싱 지국(103)은 동일한 MAC 주소의 충돌들을 감지하기 위해 지국들(101, 102) 간의 전송들을 감시함으로써 무선 통신망으로의 침입을 감지한다. 즉, 복수의 터미널들이 서로 동시에 또는 비교적 가깝게 동일한 MAC 주소를 주장한다면, 에러가 발생했거나 지국들 중 1개가 로우그 지국(104)이다. 이처럼, 폴리싱 지국(103)은, 예를 들어 3보다 큰, 그런 충돌들의 한계 횟수를 감지하는 것에 기초하여 침입 경보를 발생한다. 여기서 다시, 다른 한계 횟수들이 또한 사용될 수 있으며, 상기 설명된 바와 같이 한계 횟수는 백분율에 기초할 수 있다.

이제 무선 통신망(10)을 위한 본 발명의 충돌감지 방법의 측면을 도 11을 참조하여 설명할 것이다. 블럭(110)에서 시작하여, 본 방법은 상기 주목된 바와 같이, 블럭(111)에서 MAC 층을 사용한 복수의 지국들(11, 12) 간의 데이터 전송을 포함한다. 블럭(112)에서 지국들(11, 12) 간의 전송들은 MAC 주소들 중 1개로부터의 FCS 에러들을 감지하기 위해 감시된다. 블럭(113)에서 그 MAC 주소에 대해 다수의 FCS 에러들이 한계값을 초과한다면, 블럭(114)에서 이에 기초하여 침입 경보가 발생되고, 따라서 본 방법을 종료(블럭(115))한다. 만약 그렇지 않으면, 도시된 바와 같이 계속하여 전송이 감시될 것이다.

이제 도 12를 참조하여 설명된 본 발명의 첫 번째 대체적인 방법의 측면에 따르면, 본 방법은 블럭(121)에서 지국들(21, 22) 간에 데이터를 전송하는 것으로 시작(블럭(120))되고, 상기 주목된 바와 같이 블럭(122)에서 MAC 주소들을 인증하는

데 실패한 시도들을 감지하기 위해 전송들을 감시한다. 블럭(123)에서 MAC 주소를 인증하는 데 실패한 다수의 시도들이 감지되면, 블럭(124)에서 침입 경보가 발생되고, 따라서 본 방법을 종결(블럭(125))한다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다.

이제 도 13을 참조하여 본 발명의 두 번째 대체적인 방법의 측면을 설명한다. 본 방법은 블럭(131)에서 지국들(31, 32) 간에 RTS 및 CTS 패킷들을 전송하는 것으로 시작(블럭(130))되고, 그 후 데이터를 전송한다. 상기 설명된 바와 같이, 블럭(132)에서 지국들(31, 32)간에 전송되는 RTS 및 CTS 패킷들은 그 안의 불법적인 NAV 값을 감지하기 위해 감시된다. 블럭(133)에서 불법적인 NAV 값이 감지되면, 블럭(134)에서 이에 기초하여 침입 경보가 발생되고, 따라서 본 방법을 종결(블럭(135))한다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다.

이제 도 14로 전환하여, 본 발명에 따른 세 번째 대체적인 방법의 측면을 설명한다. 본 방법은 블럭(141)에서 지국들(41, 42) 간에 데이터를 전송하는 것으로 시작(블럭(140))되고, 상기 설명된 바와 같이, 블럭(142)에서 CFP 외에서의 무경합 모드 동작을 감지하기 위해 전송들을 감시한다. 블럭(143)에서 그러한 동작이 CFP 외에서 감지되면, 블럭(144)에서 이에 기초하여 침입 경보가 발생되고, 따라서 본 방법을 종결(블럭(145))한다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다. CFP 동안에 경합 모드 동작이 감시되는 반대의 경우가 도 15에 도시되어 있다. 여기서 다시, 이러한 2 가지 방법 모두가 1개의 실시예에서 사용될 수 있으나, 항상 그렇게 해야 할 필요는 없다.

이제 본 발명의 4 번째 방법의 측면이 도 16을 참조하여 설명될 것이다. 본 방법은 블럭(161)에서 지국들(61, 62) 간에 데이터를 전송하는 것으로 시작(블럭(160))되고, 그리고 상기 설명된 바와 같이, 블럭(162)에서 권한 없는 주기 동안의 전송들을 감시한다. 블럭(163)에서 권한 없는 주기 동안에 전송들이 감지되면, 이에 기초하여 블럭(164)에서 침입 경보가 발생되고, 따라서 본 방법을 종결(블럭(165))한다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다.

이제 본 발명의 4 번째 방법의 측면이 도 17을 참조하여 설명될 것이다. 본 방법은 블럭(171)에서 지국들(71, 72) 간에 데이터를 전송하는 것으로 시작(블럭(170))되고, 그리고 상기 설명된 바와 같이, 블럭(172)에서 각각의 데이터 패킷과 일치하지 않는 무결성 검사값들을 감지하기 위해 전송들을 감시(172)한다. 이경우에, 블럭(174)에서 침입 경보가 발생되고, 따라서 본 방법을 종결(블럭(175))한다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다.

이제 도 18로 전환하여, 본 발명의 또 다른 방법의 측면을 설명한다. 본 방법은 블럭(181)에서 지국들(81, 82) 간에 데이터를 전송하는 것으로 시작(블럭(180))된다. 따라서 상기 설명된 바와 같이, 본 방법은 블럭(182)에서 1개의 지국에 의한 비연속적인 MAC 시퀀스 번호들의 사용을 감지하기 위해 전송들을 감시하는 것을 또한 포함한다. 블럭(183)에서 그러한 사용이 감지되면, 블럭(184)에서 침입 경보가 발생되고, 따라서 본 방법을 종결(블럭(185))한다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다.

부가적으로 도 19를 참조하면, 본 발명의 또 다른 방법의 측면은 블럭(191)에서 지국들(91, 92) 간에 데이터를 전송하는 것으로 시작(블럭(190))되고, 그리고 상기 주목된 바와 같이, 블럭(192)에서 미리 결정된 패킷 형태를 갖는 패킷들의 충돌을 감지하기 위해 전송들을 감시한다. 블럭(193)에서 미리 결정된 패킷 형태를 갖는 패킷들의 충돌에 대한 한계 횟수가 감지되면, 블럭(194)에서 침입 경보가 발생되고, 본 방법을 종결(블럭(195))한다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다.

이제 본 발명의 또 다른 침입 감지의 측면이 도 20을 참조하여 설명될 것이다. 본 방법은 지국들(101, 102) 간에 데이터를 전송하는 것으로 시작(블럭(200))되고, 그리고 상기 설명된 바와 같이, 블럭(202)에서 동일한 MAC 주소의 충돌들을 감지하기 위하여 전송들을 감시한다. 블럭(203)에서 동일한 MAC 주소의 충돌들에 대한 한계 횟수가 감지되면, 블럭(204)에서 침입 경보가 발생되고, 따라서 본 방법을 종결(블럭 205)한다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다.

이제 본 발명의 그 이상의 침입 감지의 측면들이 도 21을 참조하여 설명될 것이다. 상기 주목된 바와 같이, 무선 LAN/MAN은 전형적으로 IBSSD들, BSSID들, 및/또는 ESSIS들과 같은 1개 이상의 관련된 서비스 셋 ID들을 가진다. 도시된 바와 같이, 블럭(210)에서 시작하여 블럭(211)에서 데이터 전송이 지국들(11, 12) 간에 보내질 수 있으며, 블럭(212)에서 복수의 지국들 간의 전송들은 관련된 서비스 셋 ID들 및/또는 지정된 통신망 채널을 통해 권한 있는 지국으로부터 발생되지 않은 전송들을 감지하기 위해 감시된다.

이처럼, 블럭(213)에서 무선 통신망(10)의 권한 있는 서비스 셋 ID와 다른 서비스 셋 ID가 감지되고/감지되거나, 통신망 채널의 권한 없는 지국으로부터의 전송이 감지되면, 이에 기초하여 블럭(214)에서 침입 경보가 발생된다. 더욱이 상기 설명된 바와 같이, 블럭(215)에서 침입 경보는 통신망의 1개 이상의 지국으로, 또는 모뎀 등을 통하여 다른 소스로 유익하게 전송될 수 있다. 만약 그렇지 않으면, 도시된 바와 같이 침입의 감시가 계속될 것이다.

상기 설명된 방법의 측면들이 상기 설명된 1개 이상의 무선 통신망에서 모두 실시될 수 있다는 것이 해당 기술분야에서 통상의 지식을 가진 자에게 이해될 것이다. 또한, 본 발명의 부가적인 방법의 측면들은 상기 설명을 기초로 해당 기술분야에서 통상의 지식을 가진 자에게 명백할 것이므로 여기서 더 이상 언급되지는 않을 것이다.

상기 설명된 발명은 다양한 방식으로 실시될 수 있다는 것이 또한 이해될 것이다. 예를 들면, 폴리싱 지국(13)은 항상 무선 통신망(10)에 속하는 것은 아닌 1개 이상의 독립적으로 제공된 장치들에서 실시될 수도 있다. 대체적으로, 본 발명은 침입 감지가 요구되는 무선 LAN/MAN내에 존재하는 1개이상의 지국들에 설치되는 소프트웨어에서 실시될 수도 있다.

나아가, 본 발명의 상기 설명된 측면들 중 다수는 로우그 지국이 권한 있는 통신망 또는 MAC ID(예를 들어, CFP 외에서의 무경합 동작, 권한 없는 주기 동안의 전송 등)를 가지는 경우에도 무선 통신망 침입을 감지하기 위해 유익하게 사용될 수 있다. 더욱이, 상기 측면들의 1개 이상은 주어진 응용예에서 침입 감지의 바람직한 수준을 제공하기 위해 유익하게 사용될 수 있다. 본 발명의 그 이상의 장점은 본 발명이 기존의 침입 감지 시스템들, 특히 상부 OSI 통신망 층들의 침입에 중점을 둔 시스템들을 보완하기 위해 사용될 수 있다는 것이다.

산업상 이용 가능성

본 발명은 무선 통신망 분야에서, 특히 무선 근거리 또는 대도시 통신망 분야에서 향상된 보안특성을 가지는 무선 통신장치에 그리고 이에 관련된 방법의 형태로 산업상 유익하게 이용될 수 있다.

도면의 간단한 설명

도 1은 프레임 검사 시퀀스(FCS)에 기초한 침입 감지를 제공하기 위한, 본 발명에 따른 무선 LAN/MAN의 개략적인 블럭도이다.

도 2는 매체 접근 제어(MAC) 주소들의 실패한 인증들에 기초한 침입 감지를 제공하기 위한, 도 1의 무선 LAN/MAN의 다른 실시예를 보여주는 개략적인 블럭도이다.

도 3은 불법적인 통신망 할당 벡터(NAV)들에 기초한 침입 감지를 제공하기 위한, 도 1의 무선 LAN/MAN의 또 다른 실시예를 보여주는 개략적인 블럭도이다.

도 4 및 도 5는 각각, 무경합 주기(CFP) 외에서의 무경합 모드 동작에 기초한 침입 감지 및 CFP 동안의 경합 모드 동작에 기초한 침입 감지를 제공하기 위한, 도 1의 무선 LAN/MAN의 또 다른 실시예를 보여주는 개략적인 블럭도이다.

도 6은 권한 없는 주기 동안에 발생하는 전송들에 기초한 침입 감지를 제공하기 위한, 도 1의 무선 LAN/MAN의 또 다른 실시예를 보여주는 개략적인 블럭도이다.

도 7은 각각의 데이터 패킷들과 일치하지 않는 무결성 검사값(integrity check value)들의 감지에 기초한 침입 감지를 제공하기 위한, 도 1의 무선 LAN/MAN의 또 다른 실시예를 보여주는 개략적인 블럭도이다.

도 8은 지국에 의한 비연속적인 MAC 시퀀스 번호들의 사용 감지에 기초한 침입 감지를 제공하기 위한, 도 1의 무선 LAN/MAN의 또 다른 실시예를 보여주는 개략적인 블럭도이다.

도 9는 미리 결정된 패킷 형태를 갖는 패킷들의 충돌 감지에 기초한 침입 감지를 제공하기 위한, 도 1의 무선 LAN/MAN의 또 다른 실시예를 보여주는 개략적인 블럭도이다.

도 10은 동일한 MAC 주소의 충돌 감지에 기초한 침입 감지를 제공하기 위한, 도 1의 무선 LAN/MAN의 또 다른 실시예를 보여주는 개략적인 블럭도이다.

도 11은 본 발명에 따른, FCS 에러들의 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

도 12는 본 발명에 따른, MAC 주소들의 실패한 인증들의 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

도 13은 본 발명에 따른, 불법적인 통신망 할당 벡터(NAV) 값들의 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

도 14 및 도 15는 각각 본 발명에 따른, CFP 외에서의 무경합 모드 동작의 감지 및 CFP 동안의 경합 모드 동작의 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

도 16은 본 발명에 따른, 권한 없는 주기 동안에 발생하는 전송들의 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

도 17은 본 발명에 따른, 각각의 데이터 패킷들과 일치하지 않는 무결성 검사값들의 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

도 18은 본 발명에 따른, 지국에 의한 비연속적인 MAC 시퀀스 번호들의 사용 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

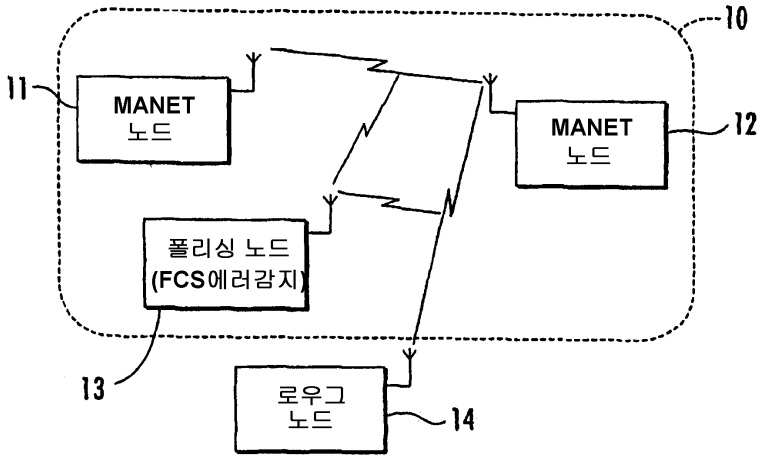
도 19는 본 발명에 따른, 미리 결정된 패킷 형태를 갖는 패킷들의 충돌 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

도 20은 본 발명에 따른, 동일한 MAC 주소의 충돌 감지에 기초한 침입 감지 방법을 보여주는 흐름도이다.

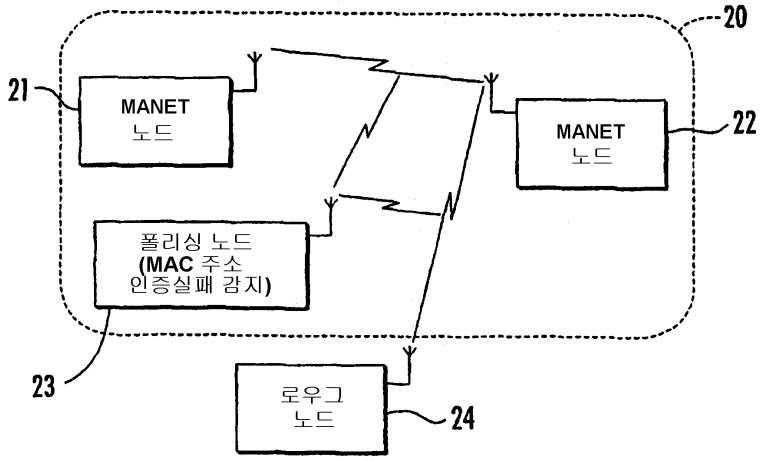
도 21은 본 발명의 침입 감지를 위한 부가적인 방법의 측면들을 보여주는 흐름도이다.

도면

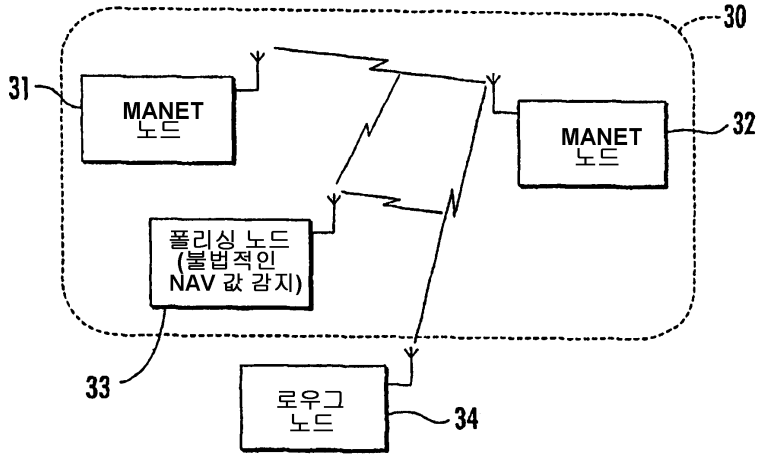
도면1



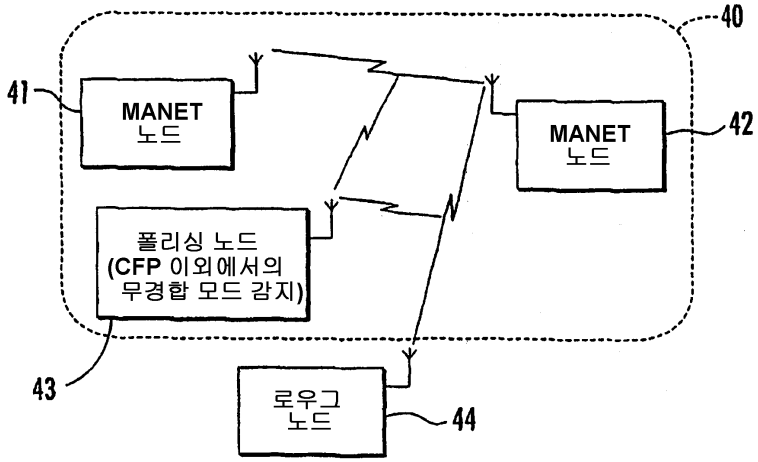
도면2


20
21
MANET
노드
MANET
노드
22
폴리싱 노드
(MAC 주소
인증실패 감지)
23
로우그
노드
24

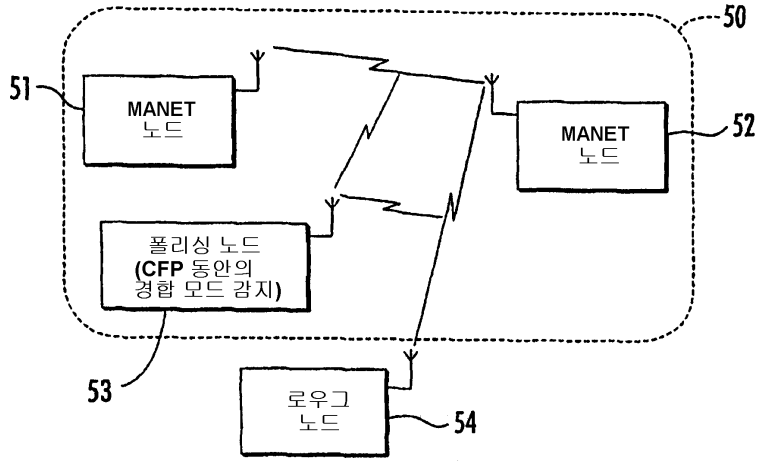
도면3


30
31
MANET
노드
MANET
노드
32
폴리싱 노드
(불법적인
NAV 값 감지)
33
로우그
노드
34

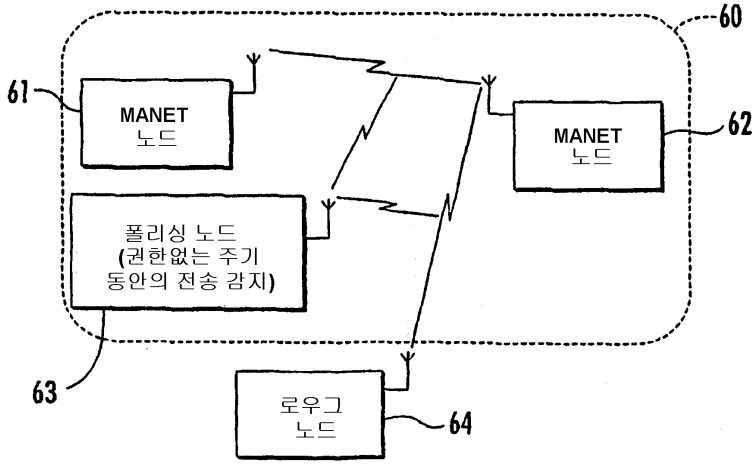
도면4


40
41
MANET
노드
MANET
노드
42
폴리싱 노드
(CFP 이외에서의
무경합 모드 감지)
43
로우그
노드
44

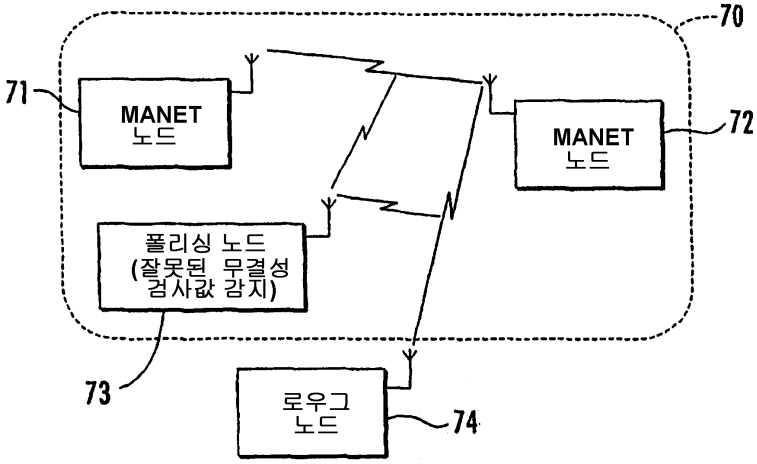
도면5


50
51
MANET
노드
MANET
노드
52
폴리싱 노드
(CFP 동안의
경합 모드 감지)
53
로우그
노드
54

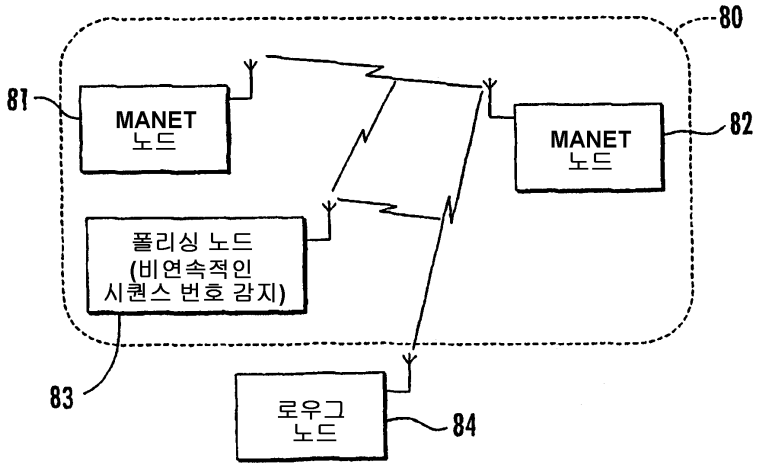
도면6


60
61
MANET
노드
MANET
노드
62
폴리싱 노드
(권한없는 주기
동안의 전송 감지)
63
로우그
노드
64

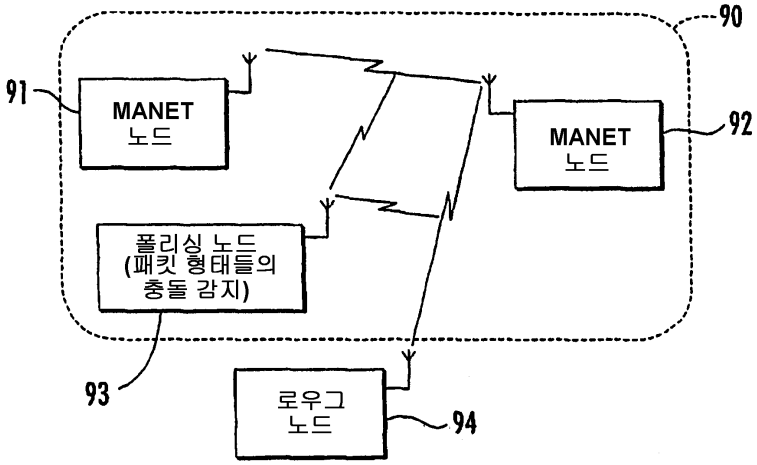
도면7


70
71
MANET
노드
MANET
노드
72
폴리싱 노드
(잘못된 무결성
검사값 감지)
73
로우그
노드
74

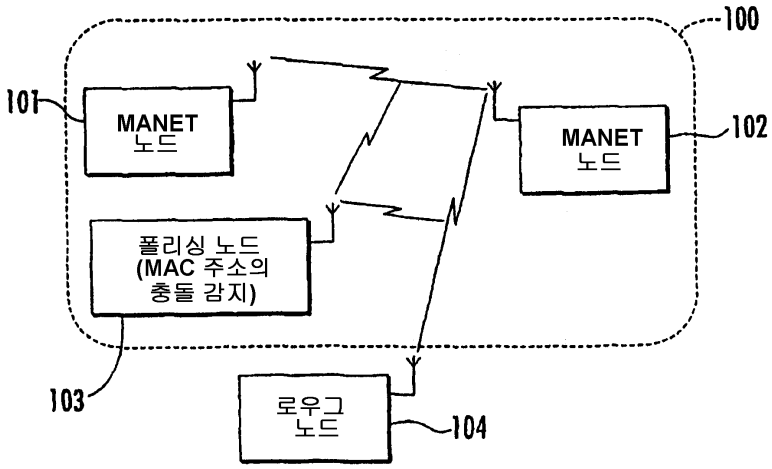
도면8


80
81
MANET
노드
82
MANET
노드
폴리싱 노드
(비연속적인
시퀀스 번호 감지)
83
로우그
노드
84

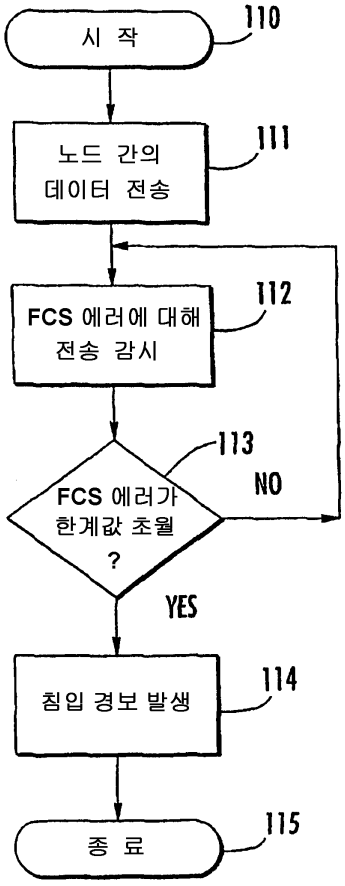
도면9


90
91
MANET
노드
92
MANET
노드
폴리싱 노드
(패킷 형태들의
충돌 감지)
93
로우그
노드
94

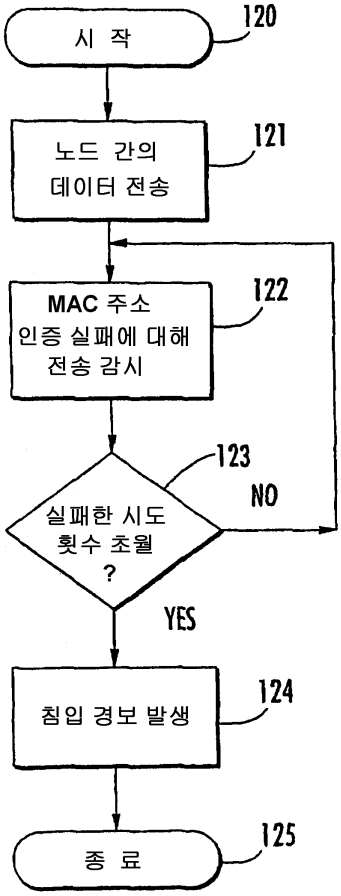
도면10


100
101
MANET
노드
102
MANET
노드
폴리싱 노드
(MAC 주소의
충돌 감지)
103
로우그
노드
104

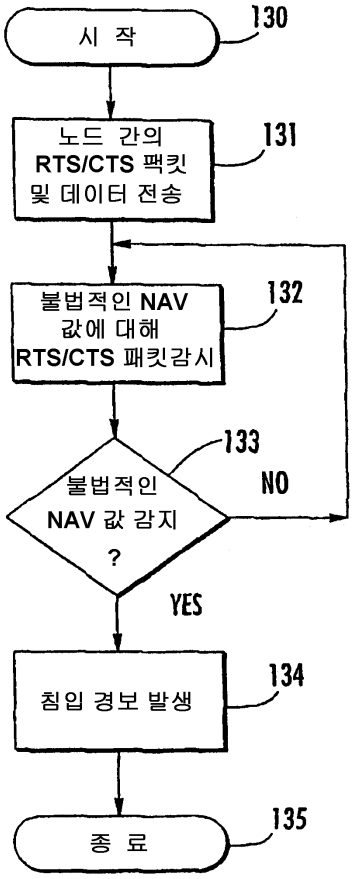
도면11


시 작
110
노드 간의
데이터 전송
111
FCS 에러에 대해
전송 감시
112
FCS 에러가
한계값 초월
?
113
NO
YES
침입 경보 발생
114
종 료
115

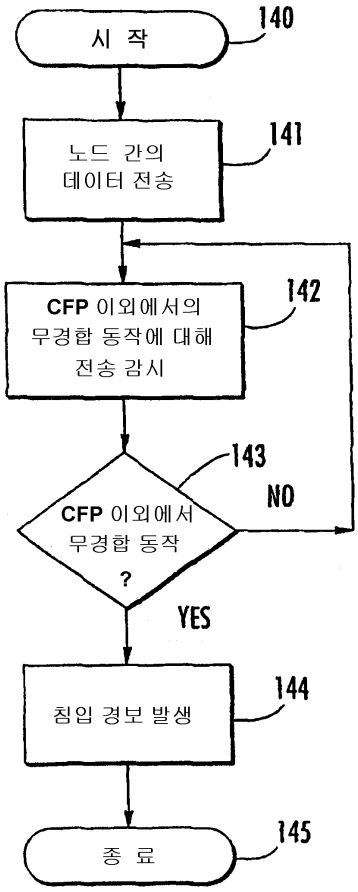
도면12


시 작
120
노드 간의
데이터 전송
121
MAC 주소
인증 실패에 대해
전송 감시
122
123
실패한 시도
횟수 초월
?
NO
YES
침입 경보 발생
124
종 료
125

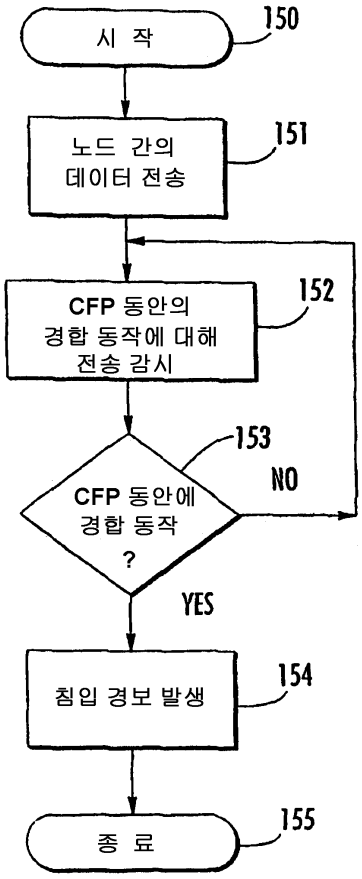
도면13


시 작
130
노드 간의
RTS/CTS 팩킷
및 데이터 전송
131
불법적인 NAV
값에 대해
RTS/CTS 패킷감시
132
불법적인
NAV 값 감지
?
133
NO
YES
침입 경보 발생
134
종 료
135

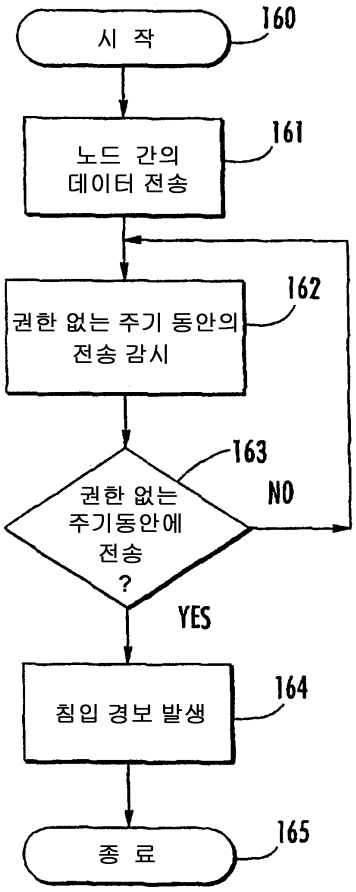
도면14


시 작
140
노드 간의
데이터 전송
141
CFP 이외에서의
무경합 동작에 대해
전송 감시
142
CFP 이외에서
무경합 동작
?
143
NO
YES
침입 경보 발생
144
종 료
145

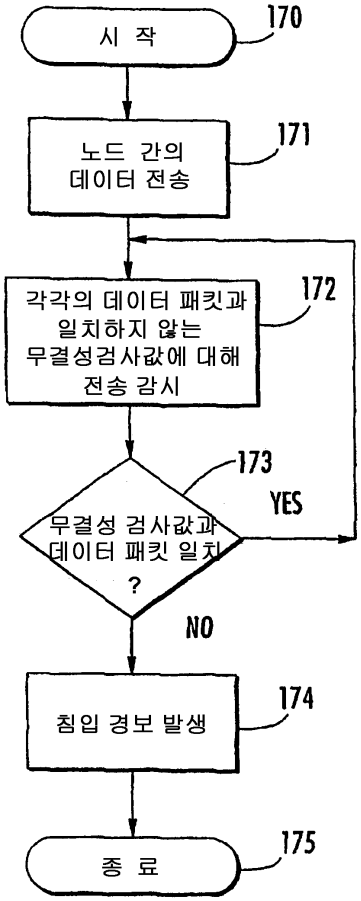
도면15


시 작
150
노드 간의
데이터 전송
151
CFP 동안의
경합 동작에 대해
전송 감시
152
CFP 동안에
경합 동작
?
153
NO
YES
침입 경보 발생
154
종 료
155

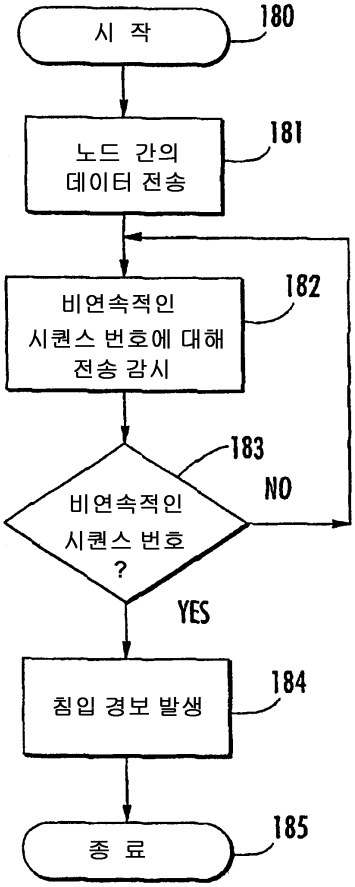
도면16


시 작
160
노드 간의
데이터 전송
161
권한 없는 주기 동안의
전송 감시
162
권한 없는
주기동안에
전송
?
163
NO
YES
침입 경보 발생
164
종 료
165

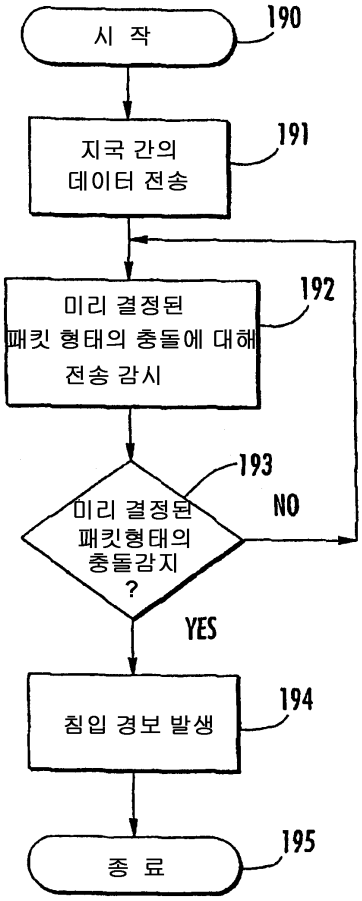
도면17


시 작
170
노드 간의
데이터 전송
171
각각의 데이터 패킷과
일치하지 않는
무결성검사값에 대해
전송 감시
172
무결성 검사값과
데이터 패킷 일치
?
173
YES
NO
침입 경보 발생
174
종 료
175

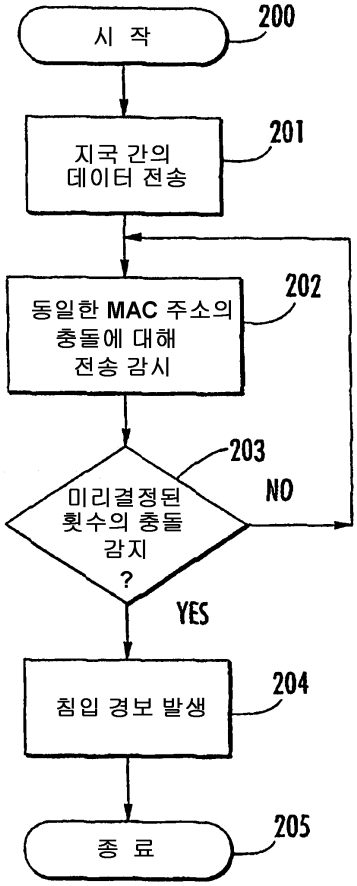
도면18


시 작
180
노드 간의
데이터 전송
181
비연속적인
시퀀스 번호에 대해
전송 감시
182
비연속적인
시퀀스 번호
?
183
NO
YES
침입 경보 발생
184
종 료
185

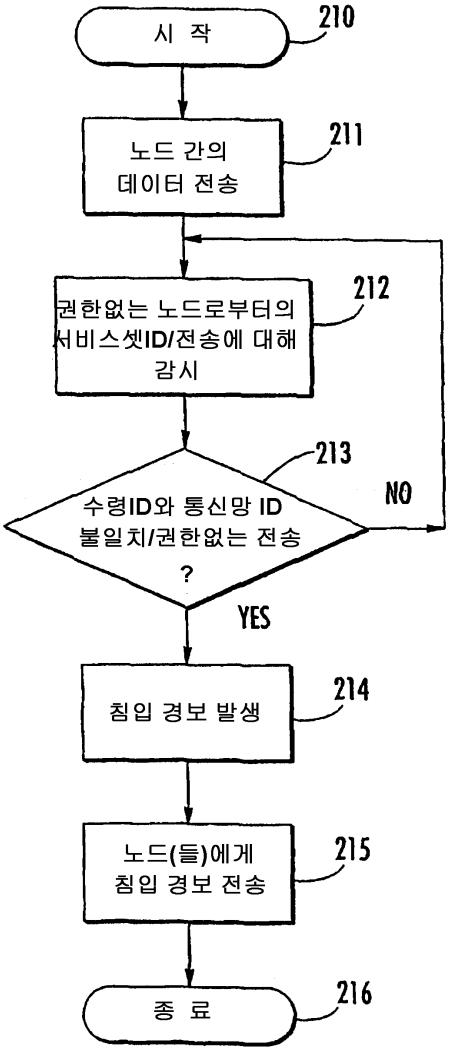
도면19


시 작
190
지국 간의
데이터 전송
191
미리 결정된
패킷 형태의 충돌에 대해
전송 감시
192
미리 결정된
패킷형태의
충돌감지
?
193
NO
YES
침입 경보 발생
194
종 료
195

도면20


시 작
200
지국 간의
데이터 전송
201
동일한 MAC 주소의
충돌에 대해
전송 감시
202
미리결정된
횟수의 충돌
감지
?
203
NO
YES
침입 경보 발생
204
종 료
205

도면21


시 작
210
노드 간의
데이터 전송
211
권한없는 노드로부터의
서비스셋ID/전송에 대해
감시
212
수령ID와 통신망 ID
불일치/권한없는 전송
?
213
NO
YES
침입 경보 발생
214
노드(들)에게
침입 경보 전송
215
종 료
216