(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년05월11일
(11) 등록번호 10-1519151
(24) 등록일자 2015년05월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) *H04L 9/30* (2006.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2008-7027745
(22) 출원일자(국제) 2007년04월13일
심사청구일자 2012년04월12일
(85) 번역문제출일자 2008년11월13일
(65) 공개번호 10-2008-0110672
(43) 공개일자 2008년12월18일
(86) 국제출원번호 PCT/CA2007/000608
(87) 국제공개번호 WO 2007/118307
국제공개일자 2007년10월25일
(30) 우선권주장
60/791,434 2006년04월13일 미국(US)
(56) 선행기술조사문헌
US20040136527 A1
US20050076197 A1
US20060112431 A1
US8069483 B1

(73) 특허권자
써티콤 코포레이션
캐나다 온타리오주 엘4더블유 0비5 미시사우가 타호 에이 타호 블러바드 4701 6층
(72) 발명자
스트루익, 마리너스
캐나다 온타리오주 엠4케이 3케이8 토론토, 칼로우 애비뉴 723
(74) 대리인
김태홍

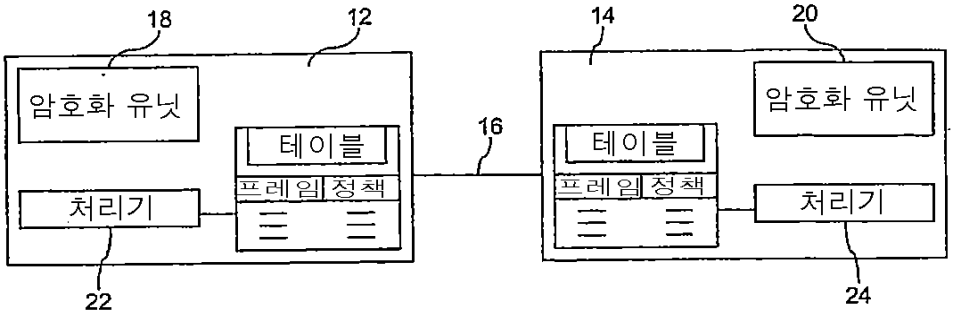
전체 청구항 수 : 총 46 항 심사관 : 이병수

(54) 발명의 명칭 **전자 통신에서 적응적 보안 레벨을 제공하는 방법 및 장치**

(57) 요 약

데이터 통신 시스템에서 제 1 통신자와 제 2 통신자간의 통신 방법은 송신자에 의해 메시지를 구성하는 단계, 프레임 타입을 결정하는 단계, 및 상기 프레임 타입의 표현을 상기 메시지의 헤더에 포함시키는 단계를 포함한다. 상기 메시지는 수신자에게 전달되고 상기 프레임 타입이 사용되어 정책 점검을 수행한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

복수의 프레임들을 전송하기 위한 방법에 있어서,

통신 디바이스가 복수의 프레임들을 준비하는 단계로서, 각각의 프레임은 헤더, 데이터, 및 복수의 보안 특성들을 갖는 것인, 상기 복수의 프레임들을 준비하는 단계;

프레임-바이-프레임(frame-by-frame) 기반으로, 상기 통신 디바이스가,

상기 프레임에서 전송된 전송의 타입에 기초하여 상기 프레임의 프레임 타입 - 상기 프레임 타입을 위해 요구되는 보안 특성들은 정책에 의해 표시됨 - 을 결정하고,

상기 프레임 타입에 기초하여 상기 전송의 타입을 표시하는 프레임 타입 데이터를 상기 프레임의 헤더에 포함시킴으로써,

각각의 프레임을 처리하는 단계; 및

상기 통신 디바이스가 전송을 위해 상기 복수의 프레임들을 제공하는 단계를 포함하고,

상기 프레임 타입은 복수의 미리 결정된 프레임 타입들 중 하나의 프레임 타입이고, 상기 복수의 미리 결정된 프레임 타입들은 데이터 타입, 명령 타입, 수령 통지(acknowledgement) 타입, 및 비컨 타입 중 두 개 이상의 타입들을 포함하고, 상기 헤더는 키의 표시(representation)와 보안 레벨의 표시를 포함하고, 상기 정책은 상기 키에 대해 수용 가능(acceptable)한 프레임 타입을 표시하며, 상기 정책은 상기 보안 레벨에 대해 수용 가능한 프레임 타입을 표시하는, 복수의 프레임들을 전송하기 위한 방법.

청구항 2

제1항에 있어서, 상기 통신 디바이스는 전송을 위해 상기 복수의 프레임들을 적어도 하나의 수신 디바이스에 제공하고, 상기 정책은 상기 적어도 하나의 수신 디바이스의 정책을 포함하고,

상기 복수의 프레임들을 전송하기 위한 방법은, 상기 적어도 하나의 수신 디바이스가,

상기 복수의 프레임들을 수신하는 단계;

각각의 프레임에 대해, 상기 프레임 타입을 상기 프레임의 상기 헤더로부터 결정하는 단계; 및

각각의 프레임에 대해, 상기 프레임 타입이 상기 복수의 보안 특성들에 대해 수용 가능한지 여부를 결정하기 위해 상기 프레임 타입을 상기 정책과 비교하는 단계를 더 포함하는 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 3

제2항에 있어서, 상기 정책이 부합되면 상기 프레임을 수용하고, 그렇지 않으면 상기 프레임을 거절하는 단계를 더 포함하는, 복수의 프레임들을 전송하기 위한 방법.

청구항 4

제2항에 있어서, 상기 정책은 상기 프레임의 보안 특성들의 하나 이상의 조합들이 존재하는 어택(attack)에 손상되기 쉬운(vulnerable) 프레임 타입들을 표시하고,

상기 복수의 프레임들을 전송하기 위한 방법은, 상기 조합들 중 하나가 발견되면 상기 프레임을 거절하는 단계를 더 포함하는 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 5

제2항에 있어서, 각각의 프레임은 상기 보안 레벨을 표시하는 하나 이상의 보안 비트들을 포함하고,

상기 복수의 프레임들을 전송하기 위한 방법은, 상기 적어도 하나의 수신 디바이스가 각각의 프레임에 대한 보

안 레벨을 결정하기 위해 상기 보안 비트들을 이용하는 단계를 더 포함하는 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 6

제5항에 있어서, 상기 프레임에 대한 상기 데이터는 암호화(encrypt)되는 것과 서명(sign)되는 것 중 어느 하나 이상이 이루어지고,

상기 복수의 프레임들을 전송하기 위한 방법은, 상기 적어도 하나의 수신 디바이스가 상기 프레임에 대한 상기 데이터를 해독(decrypting)하는 것, 인증하는 것, 또는 둘 다를 더 포함하는 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 7

제2항에 있어서, 상기 정책은 프레임 타입들을 상기 복수의 프레임들의 속성(attribute)들과 상관시키는 룩 업 테이블(look up table)을 포함하는 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 8

제1항에 있어서, 상기 복수의 프레임들을 준비하는 단계는, 각각의 프레임에 대해, 상기 프레임에 대한 보안 레벨을 선택하는 단계를 포함하는 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 9

제8항에 있어서, 상기 보안 레벨에 따라, 상기 프레임의 상기 데이터를 암호화하는 단계와 상기 프레임의 상기 데이터를 서명하는 단계 중 어느 하나 이상의 단계를 더 포함하는, 복수의 프레임들을 전송하기 위한 방법.

청구항 10

제8항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고, 상기 최소 수용 가능한 보안 레벨은 상기 프레임의 상기 데이터에 독립적인 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 11

제8항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고, 상기 최소 수용 가능한 보안 레벨은 상기 프레임의 상기 데이터에 종속적인 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 12

제8항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고,

상기 최소 수용 가능한 보안 레벨이 상기 프레임에 대한 프레임 타입에 따라 상이할 수 있도록, 상기 최소 수용 가능한 보안 레벨은 부분적으로 데이터 종속적인 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 13

제1항에 있어서, 각각의 프레임은 에러 코드를 나타내는 하나 이상의 비트들을 갖는 푸터(footer)를 포함하는 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 14

제1항에 있어서, 상기 프레임에 대한 상기 헤더는, 상기 프레임에 대한 상기 프레임 타입의 수용 가능성을 결정하기 위해, 발송자(originator), 상기 보안 레벨, 키 식별자 및 상기 키 식별자에 대응하는 키의 표시를 포함하는 것인, 복수의 프레임들을 전송하기 위한 방법.

청구항 15

복수의 프레임들을 수신하기 위한 방법에 있어서,

통신 디바이스가 복수의 프레임들을 수신하는 단계로서, 각각의 프레임은 헤더, 데이터, 및 복수의 보안 특성들을 갖고, 각각의 프레임의 헤더는 상기 프레임에 의해 전송된 전송의 타입을 표시하는 프레임 타입 데이터, 키

의 표시(representation), 및 보안 레벨의 표시를 포함하는, 상기 복수의 프레임들을 수신하는 단계; 및

각각의 프레임에 대해, 상기 통신 디바이스가,

상기 프레임의 헤더 내의 프레임 타입 데이터에 의해 표시되는 전송의 타입에 기초하여 상기 프레임의 프레임 타입을 식별하는 단계로서, 상기 프레임 타입은 복수의 미리 결정된 프레임 타입들 중 하나의 프레임 타입이고, 상기 복수의 미리 결정된 프레임 타입들은 데이터 타입, 명령 타입, 수령 통지(acknowledgement) 타입, 및 비컨 타입 중 두 개 이상의 타입들을 포함하는 것인, 상기 프레임 타입을 식별하는 단계; 및

상기 프레임의 보안 특성들에 기초하여 상기 프레임을 수용할지 여부를 결정하기 위해 상기 프레임에 대한 프레임 타입을 정책과 비교하는 단계로서, 상기 정책은 상기 키와 상기 보안 레벨에 대해 수용 가능(acceptable)한 프레임 타입을 표시하는 것인, 상기 프레임 타입을 비교하는 단계

를 포함하는, 복수의 프레임들을 수신하기 위한 방법.

청구항 16

제15항에 있어서, 각각의 프레임에 대해, 상기 정책이 부합되면 상기 프레임을 수용하고, 그렇지 않으면 상기 프레임을 거절하는 단계를 더 포함하는, 복수의 프레임들을 수신하기 위한 방법.

청구항 17

제15항에 있어서, 상기 정책은 상기 프레임의 보안 특성들의 하나 이상의 조합들이 존재하는 어택(attack)에 손상되기 쉬운(vulnerable) 프레임 타입들을 표시하고,

상기 복수의 프레임들을 수신하기 위한 방법은, 상기 조합들 중 하나가 발견되면 상기 프레임을 거절하는 단계를 더 포함하는 것인, 복수의 프레임들을 수신하기 위한 방법.

청구항 18

제15항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고, 상기 최소 수용 가능한 보안 레벨은 상기 프레임의 상기 데이터에 독립적인 것인, 복수의 프레임들을 수신하기 위한 방법.

청구항 19

제15항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고, 상기 최소 수용 가능한 보안 레벨은 상기 프레임의 상기 데이터에 종속적인 것인, 복수의 프레임들을 수신하기 위한 방법.

청구항 20

제15항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고,

상기 최소 수용 가능한 보안 레벨이 상기 프레임에 대한 프레임 타입에 따라 상이할 수 있도록, 상기 최소 수용 가능한 보안 레벨은 부분적으로 데이터 종속적인 것인, 복수의 프레임들을 수신하기 위한 방법.

청구항 21

제15항에 있어서, 각각의 프레임은 보안 레벨을 표시하는 하나 이상의 보안 비트들을 포함하고,

상기 복수의 프레임들을 수신하기 위한 방법은, 상기 통신 디바이스가 상기 보안 레벨을 결정하기 위해 상기 보안 비트들을 이용하는 단계를 더 포함하는 것인, 복수의 프레임들을 수신하기 위한 방법.

청구항 22

제21항에 있어서, 각각의 프레임에 대한 상기 데이터는 암호화(encrypt)되는 것과 서명(sign)되는 것 중 어느 하나 이상이 이루어지고,

상기 복수의 프레임들을 수신하기 위한 방법은 상기 통신 디바이스가 상기 프레임에 대한 상기 데이터를 해독(decrypting)하는 것, 인증하는 것, 또는 둘 다를 더 포함하는, 복수의 프레임들을 수신하기 위한 방법.

청구항 23

제15항에 있어서, 상기 정책은 프레임 타입들을 수용 가능한 보안 특성들과 상관시키는 룩 업 테이블(look up table)을 포함하는 것인, 복수의 프레임들을 수신하기 위한 방법.

청구항 24

통신 디바이스를 포함하는 통신 시스템에 있어서,

상기 통신 디바이스는,

복수의 프레임들을 준비하는 것 - 각각의 프레임은 헤더, 데이터, 및 복수의 보안 특성들을 가짐 -;

프레임-바이-프레임(frame-by-frame) 기반으로,

상기 프레임에서 전송된 전송의 타입에 기초하여 상기 프레임의 프레임 타입 - 상기 프레임 타입을 위해 요구되는 보안 특성들은 정책에 의해 표시됨 - 을 결정하고,

상기 프레임 타입에 기초하여 상기 전송의 타입을 표시하는 프레임 타입 데이터를 상기 프레임의 헤더에 포함시키고,

키의 표시(representation)를 상기 프레임의 상기 헤더에 포함시키고,

보안 레벨의 표시를 상기 프레임의 상기 헤더에 포함시킴으로써,

각각의 프레임을 처리하는 것; 및

전송을 위해 상기 복수의 프레임들을 제공하는 것을 포함하는 동작들을 수행하도록 작동되고,

상기 프레임 타입은 복수의 미리 결정된 프레임 타입들 중 하나의 프레임 타입이고, 상기 복수의 미리 결정된 프레임 타입들은 데이터 타입, 명령 타입, 수령 통지(acknowledgement) 타입, 및 비컨 타입 중 두 개 이상의 타입들을 포함하고, 상기 정책은 상기 키에 대해 수용 가능(acceptable)한 프레임 타입을 표시하며, 상기 정책은 상기 보안 레벨에 대해 수용 가능한 프레임 타입을 표시하는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 25

제24항에 있어서, 적어도 하나의 수신 디바이스를 더 포함하고,

상기 통신 디바이스는 전송을 위해 상기 복수의 프레임들을 상기 적어도 하나의 수신 디바이스에 제공하고, 상기 정책은 상기 적어도 하나의 수신 디바이스의 정책을 포함하며, 상기 적어도 하나의 수신 디바이스는,

상기 복수의 프레임들을 수신하는 것;

각각의 프레임에 대해, 상기 프레임 타입을 상기 프레임의 상기 헤더로부터 결정하는 것; 및

각각의 프레임에 대해, 상기 프레임 타입이 상기 복수의 보안 특성들에 대해 수용 가능한지 여부를 결정하기 위해 상기 프레임 타입을 상기 정책과 비교하는 것을 포함하는 동작들을 수행하도록 작동되는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 26

제25항에 있어서, 상기 적어도 하나의 수신 디바이스는, 상기 정책이 부합되면 상기 프레임을 수용하고, 그렇지 않으면 상기 프레임을 거절하는 것을 더 포함하는 동작들을 수행하도록 작동되는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 27

제25항에 있어서, 상기 정책은 상기 프레임의 보안 특성들의 하나 이상의 조합들이 존재하는 어택(attack)에 손상되기 쉬운(vulnerable) 프레임 타입들을 표시하고, 상기 적어도 하나의 수신 디바이스는 상기 조합들 중 하나가 발견되면 상기 프레임을 거절하는 것을 더 포함하는 동작들을 수행하도록 작동되는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 28

제25항에 있어서, 각각의 프레임은 상기 보안 레벨을 표시하는 하나 이상의 보안 비트들을 포함하고, 상기 적어

도 하나의 수신 디바이스는 상기 보안 레벨을 결정하기 위해 상기 보안 비트들을 이용하는 것을 더 포함하는 동작들을 수행하도록 작동되는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 29

제25항에 있어서, 각각의 프레임에 대한 상기 데이터는 암호화(encrypt)되는 것과 서명(sign)되는 것 중 어느 하나 이상이 이루어지고, 상기 적어도 하나의 수신 디바이스는 상기 프레임에 대한 상기 데이터를 해독(decrypting)하는 것, 인증하는 것, 또는 둘 다를 더 포함하는 동작들을 수행하도록 작동되는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 30

제25항에 있어서, 상기 정책은 프레임 타입들을 상기 복수의 프레임들의 속성(attribute)들과 상관시키는 룩 업 테이블(look up table)을 포함하는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 31

제24항에 있어서, 상기 복수의 프레임들을 준비하는 것은, 각각의 프레임에 대해, 상기 프레임에 대한 보안 레벨을 선택하는 것을 포함하는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 32

제31항에 있어서, 상기 보안 레벨에 따라, 상기 프레임의 상기 데이터를 암호화하는 것과 상기 프레임의 상기 데이터를 서명하는 것 중 어느 하나 이상을 더 포함하는 동작들을 수행하도록 작동되는 적어도 하나의 수신 디바이스를 더 포함하는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 33

제31항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고, 상기 최소 수용 가능한 보안 레벨은 상기 프레임의 상기 데이터에 독립적인 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 34

제31항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고, 상기 최소 수용 가능한 보안 레벨은 상기 프레임의 상기 데이터에 종속적인 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 35

제31항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고,

상기 최소 수용 가능한 보안 레벨이 상기 프레임에 대한 프레임 타입에 따라 상이할 수 있도록, 상기 최소 수용 가능한 보안 레벨은 부분적으로 데이터 종속적인 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 36

제24항에 있어서, 각각의 프레임은 에러 코드를 나타내는 하나 이상의 비트들을 갖는 푸터(footer)를 포함하는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 37

제24항에 있어서, 상기 프레임에 대한 상기 헤더는, 상기 프레임에 대한 상기 프레임 타입의 수용 가능성을 결정하기 위해, 발송자(originator), 상기 보안 레벨, 키 식별자 및 상기 키 식별자에 대응하는 키의 표시를 포함하는 것인, 통신 디바이스를 포함하는 통신 시스템.

청구항 38

컴퓨터 실행 가능한 명령어를 포함하는 비일시적 컴퓨터 판독가능 매체에 있어서,

상기 컴퓨터 실행 가능한 명령어는 통신 디바이스가,

복수의 프레임들을 수신하는 것 - 각각의 프레임은 헤더, 데이터, 및 복수의 보안 특성들을 갖고, 각각의 프레

임의 헤더는 상기 프레임에 의해 전송된 전송의 타입을 표시하는 프레임 타입 데이터, 키의 표시(representation), 및 보안 레벨의 표시를 포함함 -;

각각의 프레임에 대해,

상기 프레임의 헤더 내의 프레임 타입 데이터에 의해 표시되는 전송의 타입에 기초하여 상기 프레임의 프레임 타입 - 상기 프레임 타입은 복수의 미리 결정된 프레임 타입들 중 하나의 프레임 타입이고, 상기 복수의 미리 결정된 프레임 타입들은 데이터 타입, 명령 타입, 수령 통지(acknowledgement) 타입, 및 비컨 타입 중 두 개 이상의 타입들을 포함함 - 을 결정하는 것 -; 및

상기 프레임의 보안 특성들에 기초하여 상기 프레임을 수용할지 여부를 결정하기 위해 상기 프레임에 대한 프레임 타입을 정책 - 상기 정책은 상기 키에 대해 수용 가능(acceptable)한 프레임 타입과 상기 보안 레벨에 대해 수용 가능한 프레임 타입을 표시함 - 과 비교하는 것

을 포함하는 동작들을 수행하도록 하는 것인, 비일시적 컴퓨터 판독가능 매체.

청구항 39

제38항에 있어서, 상기 동작들은, 상기 정책이 부합되면 상기 프레임을 수용하고, 그렇지 않으면 상기 프레임을 거절하는 것을 더 포함하는 것인, 비일시적 컴퓨터 판독가능 매체.

청구항 40

제38항에 있어서, 상기 정책은 상기 프레임의 보안 특성들의 하나 이상의 조합들이 존재하는 어택(attack)에 손상되기 쉬운(vulnerable) 프레임 타입들을 표시하고, 상기 동작들은 상기 조합들 중 하나가 발견되면 상기 프레임을 거절하는 것을 더 포함하는 것인, 비일시적 컴퓨터 판독가능 매체.

청구항 41

제38항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고, 상기 최소 수용 가능한 보안 레벨은 상기 프레임의 상기 데이터에 독립적인 것인, 비일시적 컴퓨터 판독가능 매체.

청구항 42

제38항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고, 상기 최소 수용 가능한 보안 레벨은 상기 프레임의 상기 데이터에 종속적인 것인, 비일시적 컴퓨터 판독가능 매체.

청구항 43

제38항에 있어서, 상기 보안 레벨은 최소 수용 가능한 보안 레벨의 표시를 제공하고,

상기 최소 수용 가능한 보안 레벨이 상기 프레임에 대한 프레임 타입에 따라 상이할 수 있도록, 상기 최소 수용 가능한 보안 레벨은 부분적으로 데이터 종속적인 것인, 비일시적 컴퓨터 판독가능 매체.

청구항 44

제38항에 있어서, 상기 프레임은 상기 보안 레벨을 표시하는 하나 이상의 보안 비트들을 포함하고, 상기 동작들은 상기 보안 레벨을 결정하기 위해 상기 보안 비트들을 이용하는 것을 더 포함하는 것인, 비일시적 컴퓨터 판독가능 매체.

청구항 45

제44항에 있어서, 상기 프레임에 대한 상기 데이터는 암호화(encrypt)되는 것과 서명(sign)되는 것 중 어느 하나 이상이 이루어지고, 상기 동작들은 상기 프레임에 대한 상기 데이터를 해독(decrypting)하는 것, 인증하는 것, 또는 둘 다를 더 포함하는 것인, 비일시적 컴퓨터 판독가능 매체.

청구항 46

제38항에 있어서, 상기 정책은 프레임 타입들을 상기 복수의 프레임들의 속성(attribute)들과 상관시키는 룩 업 테이블(look up table)을 포함하는 것인, 비일시적 컴퓨터 판독가능 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 전자 통신에서 적응적 보안 레벨을 제공하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 전자 통신에서, 엿듣는 사람이 메시지를 차단하는 것을 방지할 필요가 종종 있다. 또한, 송신자의 검증 가능 식별자인 메시지의 인증을 표시하는 것이 바람직하다. 이것들의 목적은 보통 암호화의 사용을 통해 달성된다. 개인 키 암호화는 통신을 시작하기 전에 비밀 키를 공유할 것을 요구한다. 공개 키 암호화는 일반적으로 이러한 공유된 비밀 키를 요구하지 않는 것이 바람직하다. 대신, 각 통신자는 개인 키 및 공개 키로 이루어진 키 쌍을 갖는다. 상기 공개 키는 어느 편리한 수단에 의해 제공될 수 있고, 비밀을 유지할 필요는 없다.

[0003] 정밀한 구현을 결정하는 암호화 알고리즘에서의 많은 변화 및 다양한 파라미터가 존재한다. 무선 통신용 표준에 있어서, 일반적으로 사전에 각 프레임 타입에 대한 파라미터들을 설정한다. 하지만, 이 접근은 상기 파라미터들의 유연성을 제한한다. 하나의 디바이스가 다수의 다른 디바이스와 통신하는 경우, 각 통신을 위한 개별 파라미터들을 정의할 필요가 있을 것이다.

발명의 상세한 설명

[0004] 따라서, 본 발명은 상기한 바와 같은 종래의 문제점을 해결하기 위한 전자 통신에서 적응적 보안 레벨을 제공하는 방법 및 장치를 제공함에 그 목적이 있다.

[0005] 일 양상에 의하면, 본 발명에 따른 데이터 통신 시스템에서 제 1 통신자와 제 2 통신자간의 통신 방법은 제 1 통신자에 의해 헤더 및 데이터를 갖는 적어도 하나의 프레임을 포함하는 데이터 스트림을 구성하고, 프레임 타입의 표현을 상기 헤더에 포함시키고, 상기 프레임은 제 2 통신자에게 전달하여 상기 제 2 통신자가 상기 프레임 타입에 따라 상기 프레임의 수용 여부를 결정하도록 하는 것을 포함하는 것을 특징으로 한다.

[0006] 다른 양상에 의하면, 본 발명에 따른 데이터 통신 시스템에서 제 1 통신자와 제 2 통신자 간의 통신을 인증하는 방법은, 상기 제 2 통신자가 상기 제 1 통신자로부터 프레임 타입의 표시를 갖는 헤더 및 데이터를 구비하는 프레임을 수신하고; 상기 헤더를 기초로 하여 상기 프레임 타입을 결정하고; 상기 프레임 타입을 정책에 상관시켜, 상기 프레임 타입이 상기 프레임의 적어도 하나의 특성용으로 수용 가능한 지의 여부를 결정하는 것을 포함하는 것을 특징으로 한다.

[0007] 또 다른 양상에 의하면, 본 발명에 따른 데이터 통신 시스템에서 한 쌍의 통신자 간 통신 방법은 상기 한 쌍의 통신자 중의 하나가 상기 통신 시스템에 관련된 보완 규칙의 적용으로부터 면제받도록 하여, 상기 하나의 통신자가 상기 한 쌍의 통신자의 다른 하나와의 통신을 초기화하도록 하는 것을 포함하는 것을 특징으로 한다.

실 시 예

[0022] 도 1을 참조하면, 통신 시스템(10)은 통신 링크(16)에 연결된 한 쌍의 통신자(12 및 14)를 포함한다. 통신자(12 및 14)는 각각 암호화 유닛(18 및 20)을 포함한다.

[0023] 통신자(12 및 14)는 각각 처리기(22 및 24)를 포함할 수 있다. 각 처리기는 디스플레이 및 키보드, 마우스, 또는 다른 적당한 디바이스와 같은 사용자 입력 디바이스에 결합될 수 있다. 상기 디스플레이가 터치에 반응하면, 상기 디스플레이 자체가 상기 사용자 입력 디바이스로서 이용될 수 있다. 이하에 더욱 자세히 설명되는 바와 같이, 컴퓨터로 독출 가능한 저장 매체(도시안됨)가 각 통신자(12 및 14)의 동작에 관련된 단계들 또는 알고리즘들을 수행하기 위하여, 상기 처리기(22 및 24)에게 지시하고/하거나 상기 처리기(22 및 24)를 구성하도록 상기 처리기(22 및 24)에게 명령을 제공하기 위한 각 처리기(22 및 24)에 결합된다. 상기 컴퓨터로 독출 가능한 저장 매체는 예로서 자기 디스크, 자기 테이프, CD ROM과 같은 광학적으로 독출 가능한 매체, 및 PCMCIA 카드와 같은

반도체 메모리와 같은 하드웨어 및/또는 소프웨어를 포함할 수 있다. 각 경우에, 상기 매체는 소형 디스크, 플로피 디스켓, 카세트와 같은 휴대 제품의 형태이거나, 하드 디스크 드라이브, 반도체 메모리 카드, 또는 지지 시스템에 제공된 RAM과 같은 대형의 비 휴대형 제품의 형태일 수 있다. 상기에서 열거된 예의 매체들은 단독으로 또한 결합하여 이용될 수 있다는 것에 주목해야 한다.

[0024] 상기 통신자들(12 및 14) 간에 데이터를 전달하기 위하여, 패킷 스트림(30)이 정의된 프로토콜에 따라 상기 통신자들 중의 하나에서 조립된다. 상기 패킷 스트림(30)은 도 2에 개략적으로 도시되어 있고, 각각 헤더(32) 및 데이터(34)를 갖는 적어도 하나의 프레임(31)으로 이루어진다. 일부의 프로토콜에서, 상기 패킷 자체는 개별 프레임의 집합으로 이루어진 헤더(32a) 및 데이터(34a)를 갖는 프레임으로 구성될 수 있다. 상기 헤더(32)는 비트들의 스트링으로 구성되고 비트 스트림 내의 특정 위치에 제어 정보를 포함한다.

[0025] 헤더들(34) 각각에는 보안 제어 비트들(33)이 포함된다. 상기 보안 제어 비트들(33)은 보안 모드 비트(35) 및 보존 레벨 비트들(36 및 37)을 포함한다.

[0026] 이 실시 예에서, 보안 모드 비트(35)는 암호화가 온 또는 오프인 지를 나타내기 위해 사용된다. 보존 레벨 비트들(36 및 37)은 0, 32, 64, 또는 128 비트 키 크기와 같은 4개의 보존 레벨 중 어느 것이 사용되는 지를 나타내는데 사용된다. 보안 모드 비트(35)는 인증과 같은 대체 동작 모드를 나타내는데 사용될 수 있고, 비트 수는 다른 결합을 조정하기 위해 증가되거나 감소될 수 있다. 보안 비트들을 스트림(30)의 각 프레임(31)에 제공하는 것은 상기 보안 레벨이 한 쌍의 통신자를 기초로 하는 것보다 차라리 프레임-바이-프레임에 기초할 수 있도록 하여, 통신을 구성하는데 큰 유연성을 제공하는 것으로 인식된다.

[0027] 보안을 제공하기 위하여, 어떤 최소 보안 레벨이 이용될 수 있다. 이 레벨은 합의된 규칙을 통하여 모든 통신자들 중에서 결정되어야 한다. 이 규칙은 정적 또는 동적일 수 있다.

[0028] 동작에 있어서, 통신자(12)는 도 4에 참조 부호 110으로 표시된 단계들을 수행하여 정보를 통신자(14)에게 보낸다. 먼저, 통신자(12)는 단계 102에서 데이터 및 헤더를 준비한다. 그 후, 이것은 단계 104에서 보안 레벨을 선택한다. 상기 보안 레벨은 상기 수신자가 요구한 최소 보안 레벨, 수신자의 특징, 및 전송할 데이터의 종류를 고려함으로써 결정된다. 만일 상기 보안 레벨이 암호화를 포함하면, 단계 106에서 상기 통신자(12)는 상기 데이터를 암호화한다. 만일 상기 보안 레벨이 인증을 포함하면, 단계 108에서 상기 통신자(12)는 상기 데이터를 서명한다. 그 후, 단계 110에서 상기 통신자(12)는 상기 보안 모드 및 보안 레벨을 표시하는 비트들을 상기 프레임 제어에 포함시킨다. 그 후, 단계 112에서 상기 통신자(12)는 상기 프레임을 상기 통신자(14)로 보낸다.

[0029] 상기 프레임을 수신하는 경우, 상기 통신자(14)는 도 5에 참조 부호 120으로 표시된 단계들을 수행한다. 먼저, 단계 122에서 상기 통신자(14)는 상기 프레임을 수신한다. 그 후, 상기 통신자(14)는 단계 124에서 상기 보안 비트들을 추출한다. 만일 상기 모드 보안 비트들(34)이 암호화를 나타내면, 단계 126에서 상기 통신자(14)는 상기 데이터의 암호를 해독한다. 만일 상기 보안 비트들이 인증을 나타내면, 단계 126에서 상기 통신자(14)는 상기 서명을 인증한다. 마지막으로, 상기 통신자(14)는 단계 128에서 상기 보안 레벨이 소정의 최소 요구를 맞도록 보장하기 위해 상기 보안 레벨을 점검한다. 만일 암호화 또는 인증이 실패하거나, 상기 보안 레벨이 상기 최소 요구에 맞지 않으면, 상기 통신자(14)는 상기 메시지를 거절한다. 그리고 만일 암호화 또는 인증이 성공하고 상기 보안 레벨이 상기 최소 요구에 맞다면, 단계 130에 상기 메시지는 승인된다.

[0030] 보안 비트들 및 조정 가능한 보안 레벨을 제공하는 것은 상기 통신의 각 프레임을 보호하는 경우에 유연성을 제공하는 것으로 인식된다. 따라서, 상기 송신자는 어느 프레임들이 암호화되지만 인증되지 않아야 하는 지를 결정할 수 있다. 일반적으로 인증은 상기 메시지의 길이를 증가시키므로, 이것은 대역폭이 액면 이상인 경우 한정된 환경에서의 절약을 제공한다.

[0031] 다른 실시 예에서, 상기 통신자(12)는 최소 보안 요구에 따라 동일한 메시지를 다중 수신자들(14)에게 보내는 것을 바란다. 이 경우, 상기 통신자(12)는 상기 모든 요구 사항에 부합하기에 충분히 높은 보안 레벨을 선택한다. 그 후, 상기 통신자(12)는 도 4에 도시된 바와 같이 처리하여 상기 보안 레벨을 갖는 메시지를 구성하여 보낸다. 상기 메시지는 수신자들의 최소 요구 사항에 부합하므로, 각 수신자에 의해 수신될 것이다. 이 실시 예는 각 수신자의 요구 사항을 개별적으로 처리하는 것보다 더 큰 효율을 제공하는 것으로 인식된다.

[0032] 다른 실시 예에서, 다른 수의 보안 비트가 사용된다. 실제 수의 비트는 어느 하나의 값에 한정되지 않고, 어느 주어진 응용용으로 미리 결정될 수 있다. 상기 보안 비트들은 알고리즘 파라미터들을 나타내어야 한다. 상기 보안 비트들은 40개의 비트 또는 128개의 비트 만큼의 키의 길이, 사용될 키의 버전, 또는 암호화 시스템의 어느 다른 파라미터들을 결정하는데 사용될 수 있다.

[0033] 상기 실시 예에서, 네트워크 스택이 통신자들 간의 통신을 구현하는데 이용될 수 있다는 것으로 인식된다. 따라서, 도 6을 참조하면, 통신자 A의 네트워크 스택이 참조 부호 130로 도시되어 있다. 통신자 B의 네트워크 스택이 참조 부호 140로 도시되어 있다. 네트워크 스택들은 계층들로 구성되고 동일한 구성을 갖는다. 네트워크 스택(130)은 애플리케이션 계층(APL)(132), 네트워크 계층(NWK)(134), 메시지 인증 계층(MAC)(136), 및 물리 계층(PHY)(138)을 포함한다. 네크워크 스택(140)은 동일 넘버링을 갖는 유사한 성분들을 포함한다.

[0034] 송신자는 그가 어떻게 레이로드를 보호하기를 원하는 지(그리고 페이로드를 보호할 장소, 즉 어느 계층)를 결정한다. 상기 APL 계층에 있어서, 보안이 투명해야 하고, 그 역할은 이것이 데이터(즉, 보안 서비스: 없음, 비밀성, 데이터 인증 또는 둘 다)를 보호하기를 원하는 계층이 어느 것인 지를 나타내는 것에 한정되지 않는다. 실제 암호화 처리가 저 계층에 위임된다.

[0035] 상기 수신자는 상기 수신된 프레임 및 국부적으로 유지된 상태 정보를 기초로 하여 보호된 페이로드를 수신할 지의 여부를 결정된다. 명확히 제공된 보호 레벨의 정보를 포함하는, (상기 송신자의 계층과 동일한 계층에서 행해진) 암호화 처리의 결과는 제공된 보호 레벨이 적당한 지의 여부를 결정하는 애플리케이션 계층으로 넘겨진다. 상기 수신자는 타당 검사에 기초하여 상기 프레임의 적당한 수령을 원래 송신자에게 통지할 수 있다.

[0036] 만일 존재하면, 상기 수령 통지(ACK)는 다시 송신자에게 보내지고, 상기 적당한 레벨로 변한다(만일 보호된 메시지가 APL 계층에 보내지면, ACK가 또한 당연한 저 계층과 유사한 레벨에 도착하여야 한다).

[0037] 상기 송신자 A는 자신의 보안 요구, 및 아마도 의도된 수신자(들)의 보안 요구를 고려하여 SEC에 의해 나타낸 보호 레벨을 이용하여 페이로드 m를 보호하기를 원하는 지를 결정한다. 상기 페이로드 m 및 원하는 보호 레벨 SEC은 실제 암호화 처리를 고려한 저 계층(예를 들면, 도면에서 MAC 계층)으로 넘겨준다. (넘겨진 이 메시지는 의도된 수신자(들), 세분화 정보와 같은 프레임의 처리에서 제공되는 추가 상태 정보를 포함할 수 있다. 만일 암호화 처리가 페이로드 m가 시작하는 동일한 계층에서 발생하면, 저 계층으로의 상기 암호화 처리의 위임은 단지 개념 상의 단계인 것을 주목하라.

[0038] 암호화 처리는 원하는 보호 레벨 SEC에 의해 나타낸 암호화 처리를 이용하여 페이로드 m 및 아마도 프레임 헤드들과 같은 관련 정보를 보호하는 것을 포함한다. 이 정보를 보호하는데 사용되는 키는 상기 송신자와 상기 의도된 수신자(들) 사이에 유지된 공유 키잉 재료로부터 유도된다. 암호화 처리 후, 도 6에 [m]K, SEC로 표시된 상기 보호 프레임이 상기 의도된 수신자(들) B에 전달된다.

[0039] 상기 의도된 수신자(들)는 당해의 상기 송신자와 상기 의도된 수신자(들) 사이에 유지된 공유 키잉 재료로부터 유도된 키를 사용하여, 관측된 보호 레벨 SEC''로 나타낸 암호화 처리를 이용하여, 상기 수신된 보호 프레임으로부터 상기 페이로드 m'을 검색한다. 상기 페이로드 m' 및 상기 관측된 보호 레벨 SEC'는, 상기 페이로드가 상기 송신자로부터 시작된 동일한 레벨로 넘겨진다. 이 경우, 상기 관측된 보호 레벨의 타당성이 결정된다. 만일 상기 관측된 보호 레벨 SEC'가 예측된 보호 레벨 SEC_0에 부합하거나 초과하면, 충분한 것으로 생각된다. 이 경우, 파라미터 SEC_0는 당해의 상기 검색된 페이로드 m'에 의존하거나 의존하지 않는 고정된 예비-협상된 보호 레벨일 수 있다. (SEC_0를 메시지 의존 방식으로 정의하는 것은 미세한 접근 제어 수단을 허용하지만, 일반적으로 증가된 저장 수단 및 처리 요구 사항을 포함한다.

[0040] 예측되고 관측된 보호 레벨들이 비교될 수 있는 경우, 예들 들면, 상기 한 세트의 보호 레벨이 부분 배열이거나 회원 자격 검사가 (한 세트의 보호 레벨의 하나로) 수행되는 경우, 상기 접근은, 전후 관계로 작용한다. 일 예는, 보호가 암호화용 자연 배열과 (데이터 인증 필드의 증가하는 길이에 따라 배열된) 인증의 자연 배열의 데카르트 곱(암호화 오프<암호화 온)을 배열하는 것과 함께 암호화 및/또는 인증의 조합을 포함한다. 또한, 만일 상기 한 세트의 보호 레벨이 최대 요소를 가지면, 상기 송신자는 (변하지 않은) 메시지들이 항상 상기 타당성 검사를 통과하는 것을 보장하기 위한 최대 보호 레벨을 사용할 수 있다. 다른 예에서, 상기 관측된 보호 레벨은 SEC_0와 비교된다. 상기 SEC_0는 단지 최소 보안 레벨이기 보다 차라리 한 세트의 보호 레벨이다. 이 방식으로, 만일 SEC_0 = {None, Auth-32, Auth-64, Auth-128}이고 SEC = Auth-32이면, 상기 타당성 검사는 통과된다. 반면에, SEC_0 = {None, Auth-32, Auth-64, Auth-128}이고 SEC = Auth-32+비밀도(암호화)이면, 상기 타당성 검사는 실패한다.

[0041] 상기 실시 예에서, 각 송신자는 각 의도된 수신자와 상기 예측된 최대 보호 레벨 SEC_0을 예비 협상한다. 그래서, 상기 접근은 일부 애플리케이션에 바람직하게 적응하지 못할 수 있고, SEC_0 파라미터의 변화마다 추가

프로토콜 오버헤드를 포함할 수 있다. 이 단점은 SEC_0 정보를 넘기기 위한 피드백 채널로서, 수신자(들)로부터 송신자로의 상기 수령 통지(ACK) 메카니즘을 이용함으로써 극복된다. 이것은 상기 예측된 보호 레벨에 관한 표시를 각 수령 통지 메시지에 포함시킴으로써 행해진다. 이 정보는 원래 송신자에 의해 대조되어 이것이 메시지-의존적인 지의 여부를 상기 수신자(들)에 의해 예측된 최소 보호 레벨을 업데이트하도록 한다.

[0042] 추가 실시 예에서, 보안 레벨들을 동기화하는 방법이 설명되어 있다. 도 7을 참조하면, 상기 통신 시스템의 다른 실시 예는 참조 부호 160으로 표시되어 있다. 상기 통신 시스템은 라벨 그룹 G에서 송신자 A(162) 및 수신자들(168)을 포함한다. 상기 송신자 A는 파라미터들 SEC_A(164) 및 SEC_G(166)를 포함한다.

[0043] 송신자 A는 메시지 m를 디바이스들의 그룹 G에 안전하게 전달하는 것을 바란다. 상기 송신자 A는 2개의 파라미터, 즉 (1) 상기 최소 레벨 SEC_A 및 (2) 상기 최소 보호 레벨 SEC_G에 접근한다. 상기 최소 레벨 SEC_A 는 상기 송신자 A가 이 메시지를 보호하기를 원하는 레벨이다(일반적으로, SEC_A 는 송신자 A가 정보를 보내는 그룹 및 상기 메시지 자체에 의존하여, 적당한 표기법은 $SEC_A(m, G)$이다. SEC_G는 수신자 그룹 G가 예측하는 레벨이다(적당한 표기법은 이 레벨이 상기 송신자 및 메시지 자체에 의존하면 $SEC_G(m, A)$이다). 여기서, 그룹의 최소 예상 레벨은 각 그룹 회원에 대하여 최소 예상 레벨의 모든 그룹 회원에 대하여 최대이다.

[0044] 초기화:

[0045] 송신자 A는 각 파라미터 SEC_G가 (상기 송신자 A가 안전하게 통신하는 각 그룹 G에 대하여) 최대 보호 레벨로 설정되는 것으로 가정한다.

[0046] 동작 이용:

[0047] 송신자 A는 상기 송신자가 상기 메시지 m를 보호하기를 원하는 최소 보호 레벨 SEC_A를 결정한다. 상기 메시지 m에 적용된 실제 보호 레벨 SEC가 자신의 타당 검사(즉, $SEC \geq SEC_A$) 및 그룹 G(즉, $SEC \geq SEC_G$)에 의한 최대 예측 레벨 둘 다에 에 부합된다.

[0048] 수신자들 그룹 G(즉, $B \in G$)에 속하는 각 수신자 B는 특별한 순간에 (송신자 A 및 메시지 m)에 대한 최대 예측 보호 레벨을 안정한 수령 통지 메시지에 나타낸다.

[0049] 송신자 A는 파라미터 SEC_G를 업데이트하여, 상기 파라미터가 수신한 (즉, 모든 대응 디바이스 B에 대하여 $SEC_G \geq SEC_B$) 각 수령 통지 메시지에 표시된 모든 최대 보호 레벨들과 일치하도록 한다.

[0050] 상기한 과정은 상기 송신자의 요구 및 수신자(들)의 예측을 만족시키는 보호 레벨을 갖는 메시지들을 보내고, 초과 시간에 여기에서의 변화에 적용될 수 있다. 대안으로, 상기 송신자는 예측값 보다 작으므로 불충분한 보호 레벨로 인한 적어도 하나의 수신자에 의해 거절되는 메시지들을 잠재적으로 보내는데 드는 비용으로 자신의 보호 요구만을 고려할 수 있다.

[0051] 상기한 과정은 어느 네트워크 토폴로지로 디바이스들 사이의 상태 정보에 대한 일반적인 자체 동기화 과정 쪽으로 일반화될 수 있다. 이 경우, 상태 정보 상 피드백 정보는 상기 송신자 자신(상기 예에서, 이 그래프는 루트 A를 갖는 트리이고 수신자(들)을 남기고, 상기 동기화는 특정 보안 파라미터를 포함한다) 보다는 차라리 수신자(들)로부터 송신자 쪽으로의 피드백 경로를 따라 부분적으로 처리될 수 있다.

[0052] 도 8에 도시된 바와 같이, 송신자 A는 레벨 SEC로 안전하게 된 페이로드를 B1-B4로 이루어진 디바이스 그룹에 보낸다. 수신자들 B1-B4는 상기 송신자 A에게 (정수들 1, 3, 2, 5가 보호 레벨을 증가하기 위하여 번호가 부여되는 경우 상기 정수로서 도면에 표시된) 상기 예측된 보호 레벨로 피드백을 제공한다. 상기 피드백은 중간 노드들(C1 및 C2)을 통하여 송신자 A에 전달되고, 그룹 G1 및 G2을 나타내는 요약된 수령 통지 메시지를 송신자 A에게 되돌려 보내기 전에, 각 그룹 G1 및 G2에 각 디바이스들의 피드백을 수집하여 처리한다. 상기 중간 디바이스들에 의해 제공된 상기 요약된 피드백들은, 만일 이 정보가 중간 처리 없이 송신자 A로 전달되는 경우에서처럼, 모든 수신자들의 예측을 만족시키는 최소 보호 레벨을 갖는 동일한 정보를 송신자 A에게 제공한다. (여기서, 상기 중간 디바이스들은 연산에서 부정 행위를 하지 않는 것으로 가정한다).

[0053] 다른 실시 예에서, 통신에서의 각 프레임은 도 9에 도시된 바와 같이 구성되고, 참조 부호 190로 표시된다. 상기 프레임(170)은 일반적으로 헤더(172), 페이로드(174), 및 꼬리 말(176)을 포함한다. 상기 꼬리 말(176)은 통상적으로 에러 코드를 나타내는 적어도 하나의 비트를 포함한다. 상기 페이로드(174)는 특정 프레임(170), 예를

들면 메시지에 보내질 데이터를 포함한다.

[0054] 바람직한 헤더(172a)는 또한 도 9에 더욱 상세하게 도시되어 있다. 상기 헤더(172a)는 키 식별자(178), 키(180)의 표시, 프레임 타입(182), 보안 레벨(184), 및 상기 메시지의 송신자(186), 즉 송신자(12)의 표시를 포함한다.

[0055] 헤더(172a)의 각 부분은 전송의 어떤 특성을 나타내는 적어도 하나의 비트 또는 하나의 정보를 포함한다. 상기 키 식별자(178) 및 상기 키(180)의 표시는 통상적으로 예를 들면 방송 및 유니캐스트 통신에서, 무슨 키가 사용되는 지 그리고 상기 키가 어떻게 사용되는 지를 결정하는데 사용된다.

[0056] 상기 프레임 타입(182)은 어떤 방식의 전송이 특별한 프레임(172a)에 이루어지는 지에 대한 표현을 제공한다. 통상적인 프레임 타입(172)은 데이터, 명령, 수령 통지 및 비컨 프레임들을 포함한다. 데이터 타입 프레임들은 데이터를 전송하고, 명령 타입 프레임들은 명령들을 전송하고, 수령 통지 타입 프레임은 송신자에게 정보, 예를 들면 프레임이 적당히 수신된 상기 수신자로부터의 수령 통지를 다시 보내고, 비컨 프레임들은 전송을 시간 간격으로 분리하는데 통상적으로 사용된다.

[0057] 보안을 제공하기 위하여, 최소 보안 레벨을 상기 수신자(14)에게 제공하는 것 외에, 상기 송신자(12)는 상기 프레임 타입(182)을 상기 헤더(172a)에 포함시킨다. 상기 프레임 타입(182)은 상기 수신자(14)에 의해 사용되어, 만일 보안 레벨, 키, 키 사용 등이 전송될 프레임의 타입에 적당한 지를 결정하기 위한 정책 점검을 수행하도록 한다. 예를 들면, 정상적으로는 고 보안성을 가져야 하는 프레임 타입에 대한 적합하지 않은 보안이 거절된다.

[0058] 동작에서, 상기 송신자(12)는 도 10에서 참조 부호 200으로 표시된 단계를 수행하여 정보를 수신자(14)에게 보낸다. 먼저, 송신자(120)는 상기한 단계 102-110에 따라 단계 202에서 상기 프레임을 준비한다. 상기 단계들은 또한 도 9에 도시된 비트들의 표현을 포함하도록 헤더(172a)의 준비를 포함하는 것으로 판단된다. 단계 204에서, 송신자(12)는 프레임 타입(182)을 결정하고, 적어도 하나의 비트를 상기 헤더(172a)에 포함시켜 상기 프레임 타입(182)을 나타낸다. 그 후, 단계 206에서, 송신자(12)는 상기 프레임(170)을 상기 수신자(14)에게 보낸다.

[0059] 상기 수신자(14)가 상기 프레임(170)을 수신하면, 도 11에 참조 부호 208로 표시된 단계들을 수행한다. 먼저, 단계 210에서, 상기 수신자(14)는 상기 프레임을 수신하고, 단계 212에서 상기한 단계 124-126을 수행한다. 단계 214에서, 상기 수신자(14)는 상기 헤더(172a)로부터 상기 프레임 타입(182)을 추출한다. 그 후, 상기 프레임 타입(182)은 단계 126에서 정책 점검을 수행하기 위하여 정책에 상관된다. 특히, 상기 수신자가 룩업 테이블에 접근하여 각 프레임 타입마다 적어도 하나의 정책을 나타낸다. 그 후, 상기 수신자(14)는 상기 정책이 단계 218에서 부합되는 지를 결정하고, 단계 220에서 상기 정책이 부합되는 지의 여부에 따라 상기 프레임(170)을 거절하거나 수용한다.

[0060] 상기 정책 점검은 어느 다른 데이터, 바람직하게는 상기 프레임에 포함된 것에 대한 상기 프레임 타입(182)의 상관을 포함한다. 예를 들면, 상기 정책은 키 타입들과 프레임 타입들 사이의 어느 상관을 포함하여, 상기 키(160)의 표시에 기초하여, 상기 프레임이, 상기 키가 특별한 프레임 타입(182)의 사용에 수용될 수 있는 지에 따라 수용되거나 거절되도록 할 수 있다. 결과로서, 어떤 타입의 키(또는 키 사용)가 부합될 방식을 위하여 요구된다. 만일 상기 키가 정확한 타입이 아니면, 상기 수신자(14)는 상기 프레임(170)을 수용할 수 없다. 만일 단일 헤더(32a)가 도 2에 도시된 바와 같이 다중 프레임(34a)용으로 사용되면, 상기 정책은 또한 상기 메시지에 남은 프레임들을 적용한다.

[0061] 다른 예에서, 상기 방식은 프레임(170)에 포함된 보안 레벨(148), 예를 들면 상기한 최소 보안 레벨 SEC_0에 기초하여 설정된다. 상기 프레임(170)은, 상기 헤더(172)가 상기 송신자(120)에 의해 준비될 때 포함되는 어느 최소 보안 레벨을 포함하고, 이 최소 보안 레벨은 상기 특별한 프레임 타입(162)에 상관된다. 만일 상기 보안 레벨(184)이 상기 프레임 타입(162)에 적당하면, 상기 프레임(170)은 단계 220에서 상기 수신자에 의해 통과되고, 그렇지 않으면 거절된다. 상기 정책은 상기 프레임 타입(182)을 갖는 상기 프레임에 포함된 어느 적당한 정보를 상관하도록 적용될 수 있다.

[0062] 상기한 원리는 보안 점검이 다양한 메시지, 프레임 타입 등에 적용되도록 하여, 어택에 더욱 손상되기 쉬운 보안 특성의 조합에 대하여 보호받을 수 있도록 할 수 있다. 예를 들면, 상기 프레임 타입은 암호화가 사용되지 않는 경우의 어택에 특히 손상되기 쉬운 경우에, 방식은 수신자가 암호화를 이용하지 않기 위해 프레임을 거절하고 단지 인증을 이용할 수 있도록 한다.

[0063] 일반적으로, 다른 입도 레벨을 갖는 3개의 보안 레벨 점검이 존재한다. 제 1 점검은 SEC_0가 메시지에 독립적인 경우이다. 이 경우, 상기 보안의 최소 레벨은 1번 설정되고, 단지 하나의 값이 방식 점검을 수행하기 위하여 국부적으로 저장될 필요가 있다. 하지만, SEC_0가 메시지에 독립적 경우, 모든 메시지들 및 메시지 타입들에 대하여 단지 하나의 최소 보안 레벨이 존재하므로, 최소 입도가 제공된다.

[0064] 제 2 점검은 SEC_0가 메시지에 완전히 의존하는 경우이다. 이 경우, 각 메시지가 자신의 최소 보안 레벨을 가지므로, 고 입도 레벨이 제공된다. 하지만, 이것은 테이블에 국부적으로 저장될 모든 메시지의 열거 및 대응 최소 보안 레벨들을 요구한다.

[0065] 제 3 점검은 SEC_0가 메시지에 부분적으로 의존하는 경우, 즉 도 9 내지 도 11을 참조하면, 메시지들이 다른 타입들(예를 들면, 프레임 타입)으로 분리되고, 최소 보안 레벨은 각 메시지 타입에 할당된다. 이 경우는 상기 최소 보안 레벨에 기초하여 필적하는 공간 요구 사항들 및 정책 점검을 수행하기 위한 입도의 균형을 잡는다. 통상적으로, 메시지들/프레임 타입들의 수는 메시지들/타입들의 수보다 상당히 작고, 그래서 테이블에서 더욱 잘 실현할 수 있다.

[0066] 도 12에 도시된 다른 실시 예에서, 네트워크 N은 중앙 통신자 C를 통하여 통신하는 적어도 하나의 통신자(예를 들면 A, B)를 포함한다. 통신자 A는 예를 들면 상기한 원리의 일부를 이용하여 프레임들(150)을 상기 중앙 통신자 C로 전송함으로써 네트워크 N를 통하여 통신한다. 통신자 A가 먼저 네트워크 N과 결합하기를 원하는 경우, 이들은 키를 가지지 않고 네트워크 N에서 통신하기 위해 인증될 수 없다. 초기화 과정용 일반적인 단계들은 도 13에 도시되어 있다. 단계 224에서, 상기 통신자 C는 먼저 통신자 A가 네트워크 N에 연결하기를 원하는 표현을 얻는다. 그 후, 단계 226에서, 통신자 C는 상태를 나타내는 A를 테이블에 포함시키고, 통신자 C를 위한 상태를 "면제(Exempt)"로 설정한다. 면제 상태는, 통신자 A가 네트워크 N에서 초기화될 때까지 불안전하게 통신할 수 있도록 초기화 과정이 요구된다.

[0067] 단계 228에서, 통신자 A는 프레임을 중앙 통신자 C로 보낸다. 단계 230에서, 통신자 C는 상기 테이블을 확인한다. 제 1 통신에서, 통신자 A의 상태는 면제되고, 키 교환 또는 다른 초기화 과정이 수행되고(단계 232), 통신자 A의 상태는 "비면제(not exempt)"로 변한다(또는 면제 표시자 제거, 0으로 설정 등). 그 후, 통신자 A는 프레임들을 정상 보안 규칙에 따라 통신자 C로 보낸다. 단계 230에서, 통신자 A의 상태는 비면제로서 결정되고, 규칙적인 보안 규칙이 단계 236에서 예를 들어 상기 보안 레벨, 프레임 타입 등을 확인함으로써 적용된다. 통신자 A는 또한 C를 면제하여, 그 역할이 상호 바뀌고, A는 C가 통신하도록 하는 것(예를 들면, A가 다른 네트워크의 일부인 경우)으로 판단될 수 있다.

[0068] 도 12에 설명된 네트워크 N의 구현 예에서, 상기한 최소 보안 레벨 검사는 상기 프레임(150) 및 송신자(186)를 고려한다. 이 경우, 상기 송신자는 통신자 A이고 상기 수신자는 통신자 B이다. 그래서, 상기 최소 보안 레벨에 대한 확인은 $SEC \geq SEC_B(m, A)$이다. 만일 상기 최소 보안 레벨이 송신자 A에 의존하면, 상기한 바와 같이, 이것은 $SEC \geq SEC_B(m)$를 확인하도록 한다. 그 후, 초기 보안 레벨 검사에 의한 것과 같은 저장 고려가 이루어진다(경우 1).

[0069] 만일 상기 최소 보안 레벨이 상기 송신자 A에 완전히 의존하면, 최소 보안 레벨 테이블은 (프레임 m, m의 프레임 타입, 또는 메시지에 의존하여) 열거되지만, 지금은 각 송신자를 위하여 열거된다(경우 2). 만일 상기 최소 보안 레벨이, 송신자가 예를 들면, 상기 테이블에 ExemptSet로 표시된 면제 디바이스들의 명백히 열거된 세트에 있는 경우를 제외하고 송신자 A에 의존하면, 단일 최소 보안 레벨 테이블이 (프레임 타입 등에 잠재적으로 의존하는) 상기 ExemptSet 밖의 디바이스들을 위하여 구현되고, 또한 ExemptSet의 각 개별 회원의 최소 보안 레벨 테이블이 구현된다(경우 3). 그래서, 만일 통신자(및 통신자와 관련된 디바이스)는 ExemptSet 테이블의 일부이고, 경우 2가 이용된다. 만일 디바이스가 ExemptSet 테이블에 존재하지 않는 경우, 경우 1이 이용된다.

[0070] 경우 3은, 만일 통신자들이 상기 ExemptSet 테이블에 있는 통신자들에 대하여 더욱더 친화적으로 구현될 수 있으면, 상기 ExemptSet에 있는 특별한 디바이스에 의존하는 최소 보안 레벨 테이블이 이용된다. 이것은 하나의 보안 레벨 테이블이 상기 ExemptSet에 없는 디바이스에 의존하고, 하나의 테이블이 상기 ExemptSet에 있는 디바이스들을 위하여 구현될 것을 요구한다(경우 4).

[0071] 경우 4의 추가 최적화는, 상기 ExemptSet 테이블에 있는 모든 디바이스들에 대하여, (상기한 바와 같이) 메시지 또는 메시지 타입에 잠재적으로 의존하는 상기 최소 보안 레벨이 ExemptSet 밖에 있는 모드 디바이스들을 위하여 유지하는 상기 최소 보안 레벨로 설정되거나 ExemptSet 내의 모든 디바이스들을 위하여 유지하는 소정 값으

로 설정되는 경우이다. 이것은 단지 2개의 선택(예를 들면, 프레임 당, 프레임 타입, 전체)에 이르게 되므로, 이것은 부울 파라미터를 이용하여 표시될 수 있다.

[0072] 요약하면:

[0073] $SEC \geq SEC_B(m, A)$이고, 여기서,

[0074] 만일 A가 ExemptSet의 회원이 아닌 경우, $SEC_B(m, A) = SEC_B(m)$.

[0075] 만일 A가 ExemptSet의 회원이고 메시지 m에 대한 오버라이드 파라미터 OverrideSEC(m)이 FALSE에 설정되면, $SEC_B(m, A) = SEC_B(m)$. 만일 A가 ExemptSet의 회원이고 메시지 m에 대한 오버라이드 파라미터 OverrideSEC(m)이 TRUE에 설정되면, $SEC_B(m, A) = ExemptSEC_B(m)$.

[0076] 일반적으로, 가장 실제적인 시나리오는 $ExemptSEC_B(m)$이 '비 보안(no security)'으로 설정된 경우이다.

[0077] 만일 수신자 B에 의해 디바이스들이 ExemptSet(및 $ExemptSEC_B(m)$이 '비 보안'으로 설정됨)에 속하는 것으로서 라벨이 부여되는 경우, 하나의 시나리오는 아직 키를 갖지 않는 디바이스가(예를 들면, 네트워크에 막 연결한 참이고, 예를 들면 키 동의 또는 키 전송 프로토콜 또는 PIN 또는 어느 다른 메카니즘을 통하여 키를 설정하여야 하기 때문에) 상기 최소 보안 레벨 점검을 "바이패스"할 수 있게 해주는 것임을 주목한다(즉, 상기 보안 점검이 언제나 성공함).

[0078] 최소 보안 레벨 점검의 바이패스는 수신된 메시지 m, (만일 m의 프레임 타입이 전송된 프레임에 포함되지 않는 경우 상기 수신자에게 보이는-정상적으로는 프레임 타입들 및 다른 프레임 제어 정보가 부호화되지않는) 메시지 m의 프레임 타입, 또는 오버라이드 파라미터 OverrideSEC(m)을 통하여 설정될 수 있는 파라미터에 의존할 수 있다.

[0079] 또한, 상기 수신자에 의한 상기 설정된 ExemptSet에서의 동작이 상기 최소 보안 레벨 점검(상기 세트의 디바이스의 포함은 바이-패싱 또는 낮아진 보안 요구 사항을 허용하고, 반면에 상기 세트로부터의 디바이스의 배제는 보통의 최소 보안 레벨 점검을 복귀하고 당해의 시작 장치에 (가능한 다시) 적용하도록 함)의 동작을 효과적으로 제어하는 것으로 주목된다.

[0080] 그래서, 상기는 탄력적 메카니즘이 상기 시스템의 수명 중에 통신자(및 그 장치)의 과도적인 행위를 고려할 수 있도록 하고, 상기 탄력적 메카니즘이 키를 가지지 않는 경우 디바이스의 어느 초기 상태로부터의 이탈을 키를 구성하는 경우의 스테이지로 촉진하고, 정상적인 엄격한 최소 보안 레벨 방식에 강제로 결합하도록 할 수 있다.

[0081] 상기 오버라이드 파라미터 OverrideSEC(m)는 상기 최소 보안 레벨 점검의 "바이-패싱"의 미세한-튜닝을 가능하게 하고, 이것이 수신된 상기 메시지 m(또는 (명확하게는 테이블 구현 비용으로 가능한 미세 입자의 입도를 만들 수 있는) 메시지 타입)에 의존하도록 한다. 일 예로서, 디바이스가 네크워크에 접속하여 키를 설정해야 하는 시나리오에서, 수신자 디바이스 B(또는 키가 구성된 것을 한번 B에게 통지할 수 있는 네크워크에서의 다른 디바이스 T)에 의해 상기 키를 설정하기 위하여, 사용자는 상기 오버라이드 파라미터를 시작 디바이스에게 최소한으로 요구된 메시지들 또는 메시지 타입들용으로 만 TRUE에 설정할 수 있어서, 디바이스 A의 허용가능한 동작을 제한하지만 모든 동작을 제한하지는 않는다. 이것은 또한 다른 초기화 과정 또는 설정 과정용으로 이용되고, 키 설정에 한정되는 것은 아니다.

[0082] 상기 수신자 B에 의한 상기 오버라이드 파라미터 OverrideSEC(m)에 관한 동작은 매우 유연적이고 저가의 보안 제어 정책의 미세한 튜닝을 허용한다. 일 예로서, 모든 오버라이드 파라미터를 FALSE로 설정함으로써, (수신자 B에 대하여 모든 암호적으로 불안전한 메시지들이 결국 거절되므로), 사용자는 키를 갖지 않는 디바이스들에 대한 모든 네트워크 동작을 효과적으로 정지시킨다. 이것은 스텔스(stealth) 모드라 불린다. 한편, 모든 오버라이드 파라미터들은 TRUE로 설정하는 것은 상기 최소 보안 레벨 점검이 효과적으로 바이-패스되도록 할 수 있으므로, 불안전한 정보의 비제한 흐름을 디바이스 B에 허용한다.

[0083] 상기 보안 규칙들은 프레임-바이-프레임 기반 및 상기 프레임 타입에 기초하여 유연성을 제공하기 위해 제공되어, 정책 점검이 어떤 보안 규칙들 또는 키 타입들이 특별한 프레임 타입을 가지도록 사용될 수 있는 지를 결정할 수 있도록 한다.

산업상 이용 가능성

[0084] 본 발명을 바람직한 실시 예와 연계하여 설명하였지만, 당업자가 기꺼이 이해할 수 있는 바와 같이, 본 발명의 원리 및 범위로부터 벗어남이 없이, 변형 및 변경할 수 있음을 이해할 수 있을 것이다. 따라서, 그러한 변형들은 다음의 청구항들의 범위 내에서 실시될 수 있다.

도면의 간단한 설명

[0008] 본 발명의 실시 예는 예로서, 첨부된 도면들을 참조하여, 다음과 같이 설명한다:

[0009] 도 1은 통신 시스템을 개략적으로 나타낸 블록도이고;

[0010] 도 2는 도 1의 통신 시스템에서 교환하는 정보 프레임을 설명하는 개략도이고;

[0011] 도 3은 도 2의 프레임의 프레임 제어 부분을 나타낸 개략도이고;

[0012] 도 4는 도 1에서 송신자에 의해 수행된 방법을 설명하는 개략도이고;

[0013] 도 5는 도 1에서 수신자에 의해 수행된 방법을 설명하는 개략도이고;

[0014] 도 6은 상기 통신 시스템의 일 실시 예에 이용된 네트워크 프로토콜을 나타낸 개략도이고;

[0015] 도 7은 상기 통신 시스템을 일 실시 예를 나타낸 개략도이고;

[0016] 도 8은 상기 통신 시스템을 다른 실시 예를 나타낸 개략도이고;

[0017] 도 9는 다른 프레임을 나타낸 개략도이고;

[0018] 도 10은 도 9의 프레임을 사용하여 송신자가 수행한 방법을 설명하는 개략도이고;

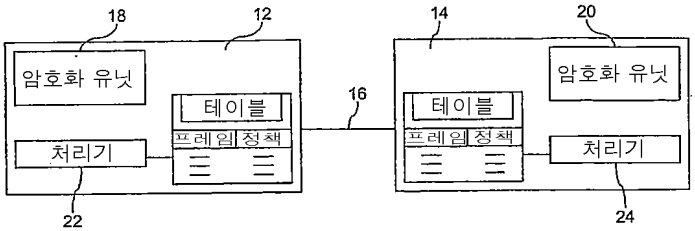
[0019] 도 11은 도 9의 프레임을 사용하여 수신자가 수행한 방법을 설명하는 개략도도이고;

[0020] 도 12는 다른 통신 시스템을 나타낸 개략도이고;

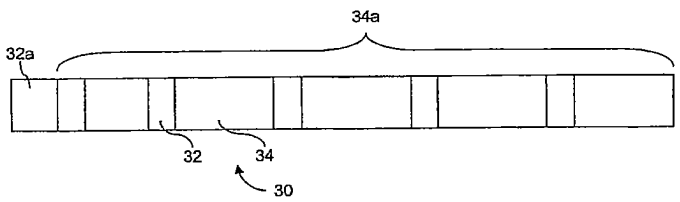
[0021] 도 13은 도 12에서 통신자에 의해 수행한 방법을 설명하는 개략도이다.

도면

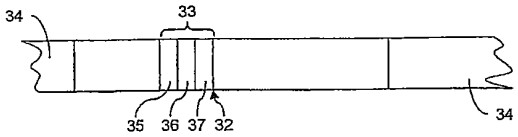
도면1



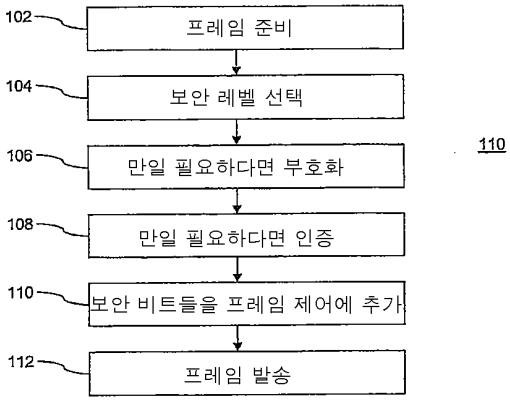
도면2



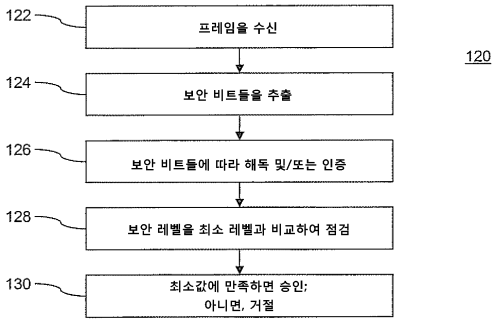
도면3



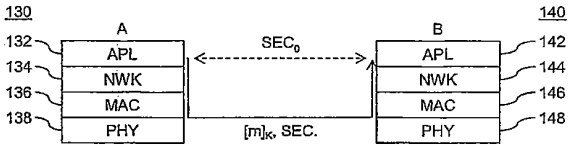
도면4



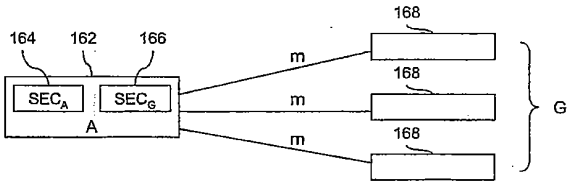
도면5



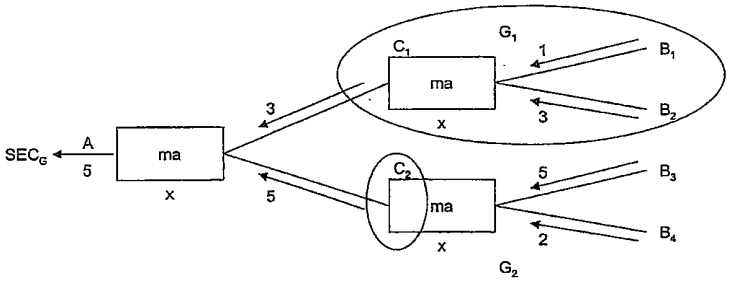
도면6



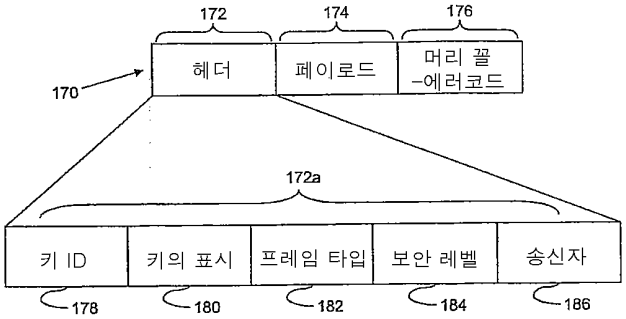
도면7



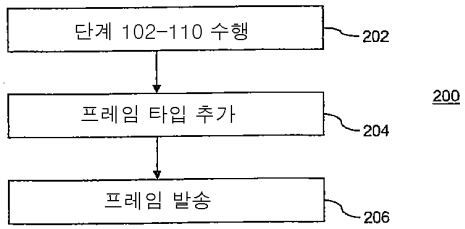
도면8



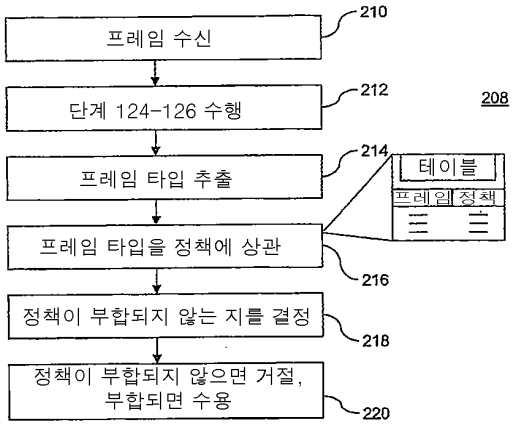
도면9



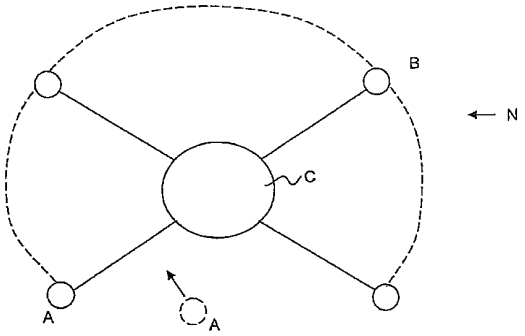
도면10



도면11



도면12



도면13