(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
H04L 12/22

(45) 공고일자 2005년03월31일
(11) 등록번호 10-0479260
(24) 등록일자 2005년03월18일

(21) 출원번호 10-2002-0062077
(22) 출원일자 2002년10월11일

(65) 공개번호 10-2004-0033159
(43) 공개일자 2004년04월21일

(73) 특허권자 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 강유성
대전광역시서구내동서우아파트103동403호

정병호
대전광역시서구월평동진달래아파트110동105호

(74) 대리인 이영필
이해영

심사관 : 신성길

(54) 무선 데이터의 암호 및 복호 방법과 그 장치

요약

본 발명은 무선 랜 단말기와 액세스포인트간 키서술자의 구조, 그리고 데이터의 암호 및 복호방법과 그 장치에 관한 것으로서, 상기 액세스포인트에서 생성하는 난수인 키 초기벡터; 암호알고리즘을 지시하는 키 서술자 타입; 상기 키 초기벡터와 상기 무선 랜 단말기와 액세스포인트간에 공유하는 마스터 세션 키를 암호키로 하여 상기 암호알고리즘에 의하여 암호화되는 적어도 둘 이상의 키 재료;를 포함하는 것을 특징으로 하며, 하나의 무선구간 암호 키만을 교환하는 종래의 키 교환 방식과는 달리 본 발명에 따른 키 교환 방식에서는 키 서술자 교환 동작의 결과로써 무선 랜 단말기와 액세스포인트 사이에서 n개의 무선구간 암호 키가 교환되기 때문에 무선구간 암호 키 갱신을 위해서 별도의 키 서술자 교환 절차를 부가적으로 수행하지 않고 이미 교환되어 있는 무선구간 암호 키들 중에 하나를 사용하여 무선구간 암호 키를 갱신할 수 있기 때문에 신속한 키 갱신의 효과가 있다. 그리고, 본 발명에 따른 다수의 무선구간 암호 키 교환 방식의 장점 중의 또 다른 하나는 전송 프레임마다 서로 다른 무선구간 암호 키를 적용한 암호화 연산을 수행할 수 있기 때문에 무선구간 데이터 보안성을 향상시키는 효과가 있다

대표도

도 3

색인어

무선랜 보안, 액세스포인트, 키 교환, 무선 랜 단말기

명세서

도면의 간단한 설명

도 1은 종래의 무선랜 사용자 인증 네트워크의 구성도이다.

도 2는 무선 랜 단말기와 액세스포인트 사이에서 종래의 키 서술자를 보여주는 도면이다.

도 3은 본 발명에 따른 키 서술자와 상기 키 서술자를 주고 받는 무선 랜 단말기와 액세스포인트를 보여주는 도면이다.

도 4는 본 발명에 따른 키 서술자의 일부로써 n개의 무선구간 암호 키 재료를 전송하는 데이터 프레임의 구조를 보여주는 도면이다.

도 5는 태그필드가 지시하는 무선구간 암호 알고리즘과 해당 무선구간 암호 키에 따라 암호화된 데이터 프레임의 구조를 보여주는 도면이다.

도 6은 본 발명에 의한 키 서술자를 이용하여 무선구간 암호 키를 교환하는 흐름을 보여주는 도면이다.

도 7은 본 발명에 의한 키 서술자를 이용하여 무선구간 암호 키를 기초로 데이터를 암호화하고 복호화하는 흐름을 보여주는 도면이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 무선랜 시스템을 구성하는 액세스포인트와 무선 랜 단말기간에 데이터를 교환함에 있어, 보안기능의 처리를 전담하는 하드웨어 기능블럭을 별도로 내장하여 다수의 무선구간 암호 키를 생성, 저장하고 상기 무선구간 암호 키들을 무선 랜 단말기와 교환하는 액세스포인트 및 상기의 액세스포인트를 이용한 키 교환 과 데이터의 암호화 및 복호화방법, 그리고 상기 무선 랜 단말기와 액세스포인트간에 교환하는 새로운 키 서술자 구조에 관한 것이다.

일반적으로, 무선랜 시스템은 무선랜 사용자가 노트북 컴퓨터 또는 기타 통신장치에 무선랜 카드를 장착하여 액세스포인트와 무선구간 통신을 수행하고, 해당 액세스포인트의 브릿징 기능을 이용하여 웹 서버에 접속하는 네트워크 구성을 의미하는 공지의 기술이다.

무선랜 시스템에 사용되는 액세스포인트는 무선 랜 단말기와 통신하는 무선구간 통신 담당과 기존의 인터넷 환경과 통신하는 유선구간 통신 담당을 동시에 수행하며, 무선구간 데이터를 유선구간으로 전달하는 브릿징 기능을 수행한다. 종래의 액세스포인트는 브릿징 기능을 통한 데이터 통신에는 문제가 없지만, 무선구간에서의 데이터 보안과 무선 랜 단말기 인증을 지원하지 못하는 단점이 있다. 무선랜 시스템을 사용하고자 하는 무선 랜 단말기에 대한 인증과 무선 랜 단말기가 액세스포인트와 통신하는 무선구간 데이터의 보안은 무선랜 보안 시스템을 구성하는 핵심요소이다.

무선랜 보안 시스템을 구축하기 위한 노력의 일환으로 미국의 IEEE 802 위원회는 IEEE 802.1X 규격을 발표하였으며, IEEE 802.11i 태스크 그룹은 무선구간 암호 기술에 대한 규격 제정을 위한 논의를 진행하고 있다. IEEE 802.1X 규격에서는 무선랜 사용자의 인증과 무선구간에서 사용할 암호 키(이하, 무선구간 암호 키) 교환에 대한 상태 머신을 정의하고 있으며, IEEE 802.11i 규격에서는 교환된 무선구간 암호 키를 사용하는 암호 알고리즘에 대한 표준화를 진행하고 있다.

이하, 종래의 무선랜 보안 시스템 구축을 위한 무선랜 사용자 인증 및 무선구간 암호 키 교환과 교환된 무선구간 암호 키 사용 방식을 첨부한 도면을 참조하여 설명한다.

도 1은 무선 랜 단말기, 액세스포인트 및 인증서버로 구성된 종래의 무선랜 사용자 인증 시스템 구성도이다. 먼저 무선 랜 단말기(101)가 어느 특정업체의 액세스포인트(103)를 통해서 기존의 인터넷 서비스를 이용하기 위해서는 해당업체의 인증서버(105)로부터 정당한 사용자임을 인증 받아야 한다. 인증 메시지가 전송될 때, 무선 랜 단말기(101)와 액세스포인트(103) 사이에서는 무선구간(S1) 데이터가 전송되고, 액세스포인트(103)는 인증서버(105)가 인식할 수 있는 인증 메시지 프레임을 재구성하여 유선구간(S2) 데이터를 인증서버(105)에게 전송한다.

일반적으로 인증 프로토콜은 사용자에 대한 인증과 키 교환을 동시에 수행하게 된다. 대표적인 인증 프로토콜로는 티엘에스(TLS: Transport Layer Security) 프로토콜이 있는데, 무선랜 시스템에서는 다양한 인증 프로토콜로 확장 운용될 수 있는 이에이피(EAP: Extensible Authentication Protocol) 프로토콜이 사용되며, 그 확장 형태 중 하나로써 이에이피-티엘에스를 사용할 수 있다. 만약 이에이피-티엘에스 프로토콜을 사용하여 인증을 성공한다면, 결과적으로 인증서버(105)가 무선 랜 단말기(101)를 인증함과 동시에 인증서버(105)와 무선 랜 단말기(101) 각각은 키(이하, "마스터 세션 키"라고 한다)를 공유하게 된다. 인증서버(105)는 상기의 마스터 세션 키를 액세스포인트(103)에게 전달하고, 이를 전달받은 액세스포인트(103)는 이 마스트 세션 키를 이용하여 실제 무선구간에서 사용될 무선구간 암호 키를 무선 랜 단말기(101)와 교환한다.

도 2는 무선 랜 단말기(101)와 종래의 액세스포인트(103) 사이에서 종래의 키 서술자(210)를 교환하는 키 교환 시스템 구성도이다. 종래의 액세스포인트(103)는 종래의 구성요소로서 연산처리부(220)인 프로세서, 메모리, 통신 모뎀 등으로 구성되어 있다. 종래의 키 서술자(210)는 공지의 구성으로써 키 재료(217)를 암호화하는 암호 알고리즘을 알려주는 키 서술자 타입(211), 키 길이(212), 재전송 공격을 막기 위한 일련번호이며 일반적으로 NTP(Network Time Protocol)시간을 전송하는 재전송 카운터(213), 키 재료를 암호화하기 위해 마스터 세션 키와

결합하여 사용되는 난수인 키 초기벡터(214), 키 서술자에 대한 일련번호인 키 인덱스(215), 그리고 키 서술자의 무결성을 보장하기 위한 키 서명(216), 그리고 끝으로 무선 랜 단말기(101)와 교환할 키 재료(217)로 구성되며, 여기서의 키 재료(217)가 바로 무선구간 암호 키로써 한 개가 사용되는 것으로 정의되어 있다.

종래의 키 서술자(210)의 필드 중 키 초기벡터(214), 키 서명(216), 그리고 키 재료(217)는 그 생성 및 처리를 위해서 난수 발생 또는 암호 알고리즘 처리 과정을 거쳐야 한다. 종래의 액세스포인트(103)는 이러한 보안기능 처리를 종래의 연산처리부(220)에서 처리하고 있어서 다수의 무선 랜 단말기가 종래의 액세스포인트에 접속하여 인증 및 암호 알고리즘 처리를 요청할 경우 심각한 병목현상을 초래한다.

상기의 설명은 무선랜 보안 시스템에서의 무선랜 사용자 인증에 대한 설명과 이와 더불어 수행되는 무선 랜 단말기(101)와 인증서버(105) 사이의 마스터 세션 키 교환, 그리고 무선 랜 단말기(101)와 액세스포인트(103) 사이의 무선구간 암호 키 교환을 위한 종래의 키 서술자(210) 형태와 이를 처리하는 종래의 액세스포인트(103)에 대한 일반적인 동작을 기술하고 있다.

그러나, 종래의 키 서술자(210)는 무선구간 암호 키로 사용될 키 재료를 하나만 정의하고 있기 때문에 무선구간 암호 키 갱신 또는 메시지별로 상이한 무선구간 암호 키를 사용하기 위해서는 별도의 키 서술자 전송을 위한 절차를 부가적으로 필요로 하게 되며, 이러한 부가적인 절차로 인하여 트래픽 증가와 처리시간 증가의 단점이 발생하게 된다. 또한 상기의 설명에서 언급했듯이 종래의 액세스포인트(103)는 키 서술자 생성 및 전송을 위한 보안기능 처리의 병목현상이 발생하게 되어 무선구간에서의 트래픽과 처리시간이 증가하는 문제점이 발생하게 된다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 무선 랜 단말기와 액세스포인트간에 키 서술자 생성 및 전송을 위한 보안기능처리의 병목현상을 극복하기 위한 키 서술자 데이터구조를 제공하는데 있다.

본 발명이 이루고자 하는 다른 기술적 과제는 상기 키 서술자 데이터 구조를 이용하여 무선 랜 단말기와 액세스포인트간의 안정적인 무선구간 통신과 안전한 암호화 데이터 전송을 보장하기위한 액세스포인트, 그리고 상기 액세스포인트와 무선 랜 단말기간의 암호 및 복호방법 및 그 장치를 제공하는데 있다.

발명의 구성 및 작용

상기의 기술적 과제를 해결하기 위하여 본 발명에 의한 키 서술자 데이터 구조는 상기 액세스포인트에서 생성하는 난수인 키 초기벡터; 암호알고리즘을 지시하는 키 서술자 타입; 상기 키 초기벡터와 상기 상기 무선 랜 단말기와 액세스포인트간에 공유하는 마스터 세션 키를 암호키로 하여 상기 암호알고리즘에 의하여 암호화되는 적어도 둘 이상의 키 재료;를 포함하는 것을 특징으로 한다.

상기의 다른 기술적 과제를 해결하기 위하여 본 발명에 의한 액세스포인트는 상기 네트워크간에 통신되는 데이터를 처리하고 상기 액세스포인트의 제어를 수행하는 연산처리부; 상기 인증서버로부터 마스터 세션 키를 수신한 후 저장하는 마스터세션키수신부; 상기 마스터세션키와 키 초기벡터를 암호키로 하여 키 서술자 타입이 지시하는 암호알고리즘에 따라 키 재료를 암호화하는 보안기능처리부; 상기 암호화된 키 재료를 포함하는 키 서술자를 출력하는 송신부; 및 상기 송신부가 출력하는 키 서술자와 데이터를 상기 무선 랜 단말기로 송수신하는 인터페이스부;를 포함하는 것을 특징으로 한다.

상기의 다른 기술적 과제를 이루기 위하여 본 발명에 의한 암호키 교환 방법은 상기 액세스포인트가 인증서버로부터 마스터 세션 키를 수신함으로써 상기 무선 랜 단말기와 상기 마스터 세션 키를 공유하는 단계; 상기 액세스포인트에서 적어도 둘 이상의 키 재료를 생성하는 단계; 상기 마스터 세션 키와 키 초기벡터에 기초하여 암호화된 키 재료를 포함하는 키서술자를 상기 무선 랜 단말기로 송신하는 단계; 및 상기 무선 랜 단말기가 수신한 상기 키 서술자로부터 무선구간 암호 키를 검출하는 단계;를 포함하는 것을 특징으로 한다.

상기의 다른 기술적 과제를 이루기 위하여 본 발명에 의한 암호 및 복호 방법은 상기 액세스포인트에서 적어도 둘 이상의 키 재료를 생성하는 단계; 상기 키 재료를 포함하는 키 서술자를 상기 무선 랜 단말기로 송신한 후 상기 무선 랜 단말기가 수신한 상기 키 서술자로부터 무선구간 암호 키를 검출하는 단계; 상기 액세스포인트가 태그필드에 규정된 알고리즘에 따라 데이터를 암호화하여 상기 태그와 함께 암호화된 데이터를 송신하는 단계; 및 상기 무선 랜 단말기가 암호화된 데이터를 수신한 후 상기 알고리즘과 상기 무선구간 암호 키에 기초하여 복호화하는 단계;를 포함하는 것을 특징으로 한다.

이하 첨부된 도면을 참조하면서 본 발명의 바람직한 일 실시예를 설명한다.

본 발명의 의한 데이터 암호 및 복호방법은 본 발명에 의한 키 서술자의 구조 및 키 서술자 교환방법이 선행되므로, 키 서술자 와 키서술자 교환방법은 데이터의 암호 및 복호방법의 한 단계로 취급하면서 전체적으로 설명하도록 한다. 도 3은 본 발명에 따른 키 서술자와 상기 키 서술자를 주고 받는 무선 랜 단말기와 액세스포인트를 보여주는 도면이고, 도 4는 본 발명에 따른 키 서술자의 일부로써 n개의 무선구간 암호 키 재료를 전송하는 데이터 프레임의 구조를 보여주는 도면이다. 한편 도 6은 본 발명에 의한 키 서술자를 이용하여 무선구간 암호 키를 교환하는 흐름을 보여주는 도면이고, 도 7은 본 발명에 의한 키 서술자를 이용하여 무선구간 암호 키를 기초로 데이터를 암호화하고 복호화하는 흐름을 보여주는 도면이다.

도 3의 연산처리부(303)는 종래의 연산처리부의 구성, 즉 CPU, 롬,램, 모뎀등의 구성을 가진다. 따라서 도 2에서 설명한 바 있으므로 그 설명은 생략하도록 한다. 우선 본 발명에 의한 액세스포인트는 인증서버로부터 마스터 세션 키를 수신한 후 저장하여 아래에서 설명할 키 재료를 형성할 때 출력하는 마스터세션키수신부(307), 상기 마스터세션

키와 키 초기벡터를 암호키로 하여 키 서술자 타입이 지시하는 암호 알고리즘에 따라 키 재료를 암호화하는 보안기능처리부(305), 상기 암호화된 키 재료를 포함하는 키 서술자를 출력하는 송신부(309), 및 상기 송신부(309)가 출력하는 키 서술자와 데이터를 상기 무선 랜 단말기로 송수신하는 인터페이스부(311)로 구성된다. 여기서 보안기능처리부(305)는 무선구간에 적용되는 암호알고리즘을 지정하는 태그를 생성하는 태그생성부, 무선구간 암호 키의 길이를 지정하는 암호키길이생성부 그리고 무선구간 암호 키값을 생성하는 키값생성부의 세부 기능블럭으로 구성할 수 있다. 전체적으로 살펴보면, 액세스포인트(301)가 인증서버(105)로부터 마스터 세션 키를 안전하게 수신하게 되면, 보안기능처리부 (305)는 키 서술자(310)의 필드 중 키 초기벡터(214)용 난수를 생성하고, 키 서명(216)을 위한 해쉬 함수 수행 및 서명 알고리즘 동작, 그리고 무선구간 암호 키 재료들(311, 312, ..., 31n)을 생성하기 위한 난수 발생 또는 키값 생성 알고리즘 동작으로써 키 서술자(310)를 구성한다(601,701단계). 여기서 무선구간 암호 키 재료들(311, 312, ..., 31n)은 마스터 세션 키와 키 초기벡터(214)를 암호 키로 사용하여 키 서술자 타입(211)이 지시한 암호 알고리즘에 따라 암호화된다. 액세스포인트(301)의 송신부(309)는 상기 키 서술자(310)를 인터페이스부(311)를 통하여 무선 랜 단말기(101)로 송신한다(603,703단계).

액세스포인트(301)로부터 키 서술자(310)를 수신한 무선 랜 단말기(101)는 상기 키 서술자(310)를 분석하고, 자신이 보유한 마스터 세션 키와 수신된 키 초기벡터(214)를 암호 키로 사용하여 무선구간 암호 키 재료들(311, 312, ..., 31n)을 복원해 낸다(605,705단계). 키 서명(216)은 무선 랜 단말기(101)가 수신한 키 서술자(310)의 무결성을 보장하는데 사용된다. 무선 랜 단말기(101)는 무선구간 암호 키 재료들(311, 312, ..., 31n)을 성공적으로 복원한 경우, 정상적인 성공임을 알리는 응답을 액세스포인트(301)로 전송하며, 무선구간 암호 키 재료들(311, 312, ..., 31n)의 복원이 실패한 경우에 무선 랜 단말기(101)는 키 서술자(310)가 다시 전송되기를 기다린다(607,707단계). 상기의 구성에서 무선 랜 단말기(101)는 키 서술자(310)를 생성하여 전송하는 동작을 수행하지 않는데, 이에 따라 액세스포인트(301)가 키 서술자(310)를 수신하여 분석하는 절차 구현의 부담이 없어지기 때문에 본 발명에 의한 액세스포인트(301)는 키 서술자 생성과 전송만을 구현하고 있으면 된다.

그리고, 하나의 무선구간 암호 키만을 교환하는 종래의 키 교환 방식과는 달리 본 발명에 따른 상기의 키 서술자(310) 교환 동작의 결과로써 무선 랜 단말기(101)와 액세스포인트(301) 사이에서 다수의 무선구간 암호 키가 교환되기 때문에 무선구간 암호 키 갱신을 위해서 별도의 키 서술자 교환 절차를 부가적으로 수행하지 않고 이미 교환되어 있는 무선구간 암호 키들 중에 다른 하나를 사용하여 무선구간 암호 키를 갱신할 수 있다. 또한 본 발명에 의한 키 서술자(310)교환 방식의 결과 전송 프레임마다 다른 암호 알고리즘 또는 다른 무선구간 암호 키를 적용하여 데이터 보안성을 향상시킬 수 있다.

다음으로 도 4와 도 5를 참조하면서 실제 데이터가 교환되는 절차를 설명한다. 도 4는 본 발명에 따른 키 서술자(310)의 일부로써 n개의 무선구간 암호 키 재료를 전송하는 데이터 프레임 구조도이고, 도 5는 태그(Tag) 필드가 지시하는 무선구간 암호 알고리즘과 해당 무선구간 암호 키에 따라 암호화된 데이터 프레임을 보여주는 도면이다.

본 발명에 따른 키 서술자(310)의 일부로써 전송되는 n개의 무선구간 암호 키 재료(311, 312, ..., 31n)들은 각각 태그(Tag), 길이(Length), 값(Value) 구조로 이루어져 있으며, 상기의 태그(401, 411, ..., 4n1)는 무선구간 암호 알고리즘을 지시하고, 상기의 길이(402, 412, ..., 4n2)는 무선구간 암호 키의 길이를 나타내고, 상기의 값(403, 413, ..., 4n3)은 무선구간 암호 키를 의미한다.

예를 들어, 태그 1은 무선랜 암호 알고리즘 중의 하나인 더블유이피(WEP) 알고리즘, 태그 2는 무선랜 암호 알고리즘 중의 하나인 티킵(TKIP) 알고리즘, 태그 3은 무선랜 보안 시스템에서 사용될 수 있는 대칭키 알고리즘 중의 하나인 에이이에스-씨씨엠(AES-CCM) 모드, 태그 4는 무선랜 보안 시스템에서 사용될 수 있는 대칭키 알고리즘 중의 하나인 에이이에스-오씨비(AES-OCB) 모드, 태그 5는 일반적인 대칭키 알고리즘 중의 하나인 시드(SEED), 그리고, 태그 6은 일반적인 공개키 알고리즘 중의 하나인 알에스에이(RSA) 알고리즘을 정의하고 있다고 가정해보자.

무선구간(S1)에서 암호화가 필요한 데이터들은 항상 태그(401) 필드를 선행하고, 상기 태그(401) 필드 뒤에 해당 무선구간 암호 키(403)로 암호화한 데이터(501)를 전송하게 되는데, 상기의 예를 적용해 보면, 태그 1을 선행하고 태그 필드 뒤로 더블유이피(WEP) 알고리즘으로 암호화한 데이터를 전송한다. 만약 액세스포인트(301)와 무선 랜 단말기(101) 사이의 무선구간 암호 키 갱신이 요구된다 하더라도 이미 교환해 놓은 다수의 무선구간 암호 키 재료들 중에서 하나를 선택하여 태그 필드의 값에 설정하고 설정된 태그에 해당하는 암호 알고리즘과 무선구간 암호 키를 이용하면 되기 때문에 별도의 키 서술자(310) 교환 없이 무선구간 암호 키 갱신이 이루어질 수 있다. 또한 태그 필드를 선행시키는 구조에서는 암호화된 데이터의 무선구간 암호 알고리즘을 태그 필드를 통해 파악할 수 있기 때문에 액세스포인트(301)와 무선 랜 단말기(101)가 미리 무선구간 암호 알고리즘을 협상해야 하는 사전 절차를 생략할 수도 있게 된다(609단계).

만일 무선구간 데이터 보안성을 향상시키기 위하여 전송 프레임마다 암호 알고리즘을 다르게 적용하고자 하는 경우에, 도 5에서 보이는 것처럼 태그 필드를 선행시키고, 해당 암호 알고리즘과 해당 무선구간 암호 키를 이용하여 전송 프레임마다 다르게 암호화 데이터를 생성할 수 있다. 그리고, 태그 필드의 값을 연속적인 값으로 설정하는 것이 아니라 태그 필드의 순서가 랜덤(random)하게 선택되도록 하여 암호 알고리즘도 드러나지 않도록 할 수 있다.

상기와 같은 태그 필드 선행 구조에서는 태그 필드에 대한 보호 대책이 필요하게 된다. 따라서 본 발명에서는 마스터 세션 키를 이용하여 태그 필드를 보호하는 방법을 적용한다. 상기의 태그 필드 보호방법은 마스터 세션 키를 암호 키로 하고, 액세스포인트(301)와 무선 랜 단말기(101) 사이에서 대칭키 암호 알고리즘을 사용하여 태그 필드를 보호한다. 상기의 태그 필드 보호방법에서 사용되는 대칭키 암호 알고리즘은 액세스포인트(301)와 무선 랜 단말기(101)가 암호 알고리즘을 미리 정해놓고 해당 암호 알고리즘을 사용할 수 있으며, 임의의 태그 값을 약속해 놓고 키 서술자를 통해 교환된 무선구간 암호 알고리즘 중에서 미리 약속한 태그 값에 해당하는 암호 알고리즘을 사용할 수 있다(709단계).

상기 방식으로 암호화된 데이터는 상기 암호 알고리즘과 무선구간 암호 키를 기초로 하여 원래의 데이터로 복원된다(711단계).

결과적으로 본 발명에 따른 액세스포인트(301)는 키 서술자(310) 생성 및 전송을 위한 난수 생성, 해쉬 함수 처리와 암호 알고리즘 연산을 보안기능처리부(305)가 전담할 뿐 아니라 도 5에서 보이는 데이터 전송 구조에서의 암호화된 태그 필드와 암호화된 데이터 필드를 복호화하는 암호 알고리즘 연산도 담당함으로써 종래의 액세스포인트(103)에서 발생하는 보안기능 처리 시간의 지연으로 인한 병목현상을 극복할 수 있다.

본 발명에 의한 무선 랜 단말기와 액세스포인트간의 데이터 암 호 및 복호방법은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 하드 디스크, 플로피 디스크, 플래쉬 메모리, 광 데이타 저장장치등이 있으며, 또한 캐리어 웨이브(예를들면 인터넷을 통한 전송)의 형태로 구현되는 것도 포함된다. 또한 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 통신망으로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 읽을 수 있는 코드로서 저장되고 실행될 수 있다. 또한 본 발명에 의한 폰트 롬 데이터구조도 컴퓨터로 읽을 수 있는 ROM, RAM, CD-ROM, 자기 테이프, 하드 디스크, 플로피 디스크, 플래쉬 메모리, 광 데이타 저장장치등과 같은 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다.

발명의 효과

이상에서 설명한 바와 같이 본 발명에 따른 액세스포인트에서는 상기의 보안기능처리부가 키 서술자 생성 및 전송을 위한 난수 발생, 해쉬 함수 처리와 암호 알고리즘 연산을 전담하며, 상기의 키 서술자를 통해 무선 랜 단말기와 교환한 무선구간 암호 키를 사용하는 암호화 연산도 전담하기 때문에 다수의 무선 랜 단말기들이 암호화 연산을 요구하는 데이터를 전송하더라도 종래의 액세스포인트에서 발생하는 데이터 전송속도의 현저한 저하를 충분히 극복할 수 있는 효과가 있다.

또한, 하나의 무선구간 암호 키만을 교환하는 종래의 키 교환 방식과는 달리 본 발명에 따른 키 교환 방식에서는 키 서술자 교환 동작의 결과로써 무선 랜 단말기와 액세스포인트 사이에서 n개의 무선구간 암호 키가 교환되기 때문에 무선구간 암호 키 갱신을 위해서 별도의 키 서술자 교환 절차를 부가적으로 수행하지 않고 이미 교환되어 있는 무선구간 암호 키들 중에 하나를 사용하여 무선구간 암호 키를 갱신할 수 있기 때문에 신속한 키 갱신의 효과가 있다. 그리고, 본 발명에 따른 다수의 무선구간 암호 키 교환 방식의 장점 중의 또 다른 하나는 전송 프레임마다 서로 다른 무선구간 암호 키를 적용한 암호화 연산을 수행할 수 있기 때문에 무선구간 데이터 보안성을 향상시키는 효과가 있다.

특히, 본 발명에 따른 액세스포인트와 상기의 액세스포인트를 이용한 다수의 무선구간 암호 키 교환 방식은 무선랜 시스템의 보안성 강화와 신속한 암호화 연산을 제공하기 때문에, 무선랜 시스템의 물리계층 전송속도 증가를 위한 기술개발과 더불어 무선랜 시스템을 이용한 초고속 무선인터넷 활성화에 크게 기여할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

무선 랜 단말기와 액세스 포인트간에 교환되는 키 서술자에 있어서,

상기 액세스포인트에서 생성하는 난수인 키 초기벡터;

제1암호 알고리즘을 지시하는 키 서술자 타입; 및

상기 무선 랜 단말기와 상기 액세스 포인트가 공유하는 마스터 세션 키 및 상기 키 초기벡터를 암호키로 하여 상기 제1암호 암고리즘에 의해 암호화되는 적어도 둘 이상의 키 재료; 및

상기 키 재료는 상기 무선 랜 단말기와 상기 액세스 포인트 사이의 무선 구간에서 사용되는 제2암호 알고리즘을 지정하는 태그 필드, 상기 무선구간에 사용되는 암호 키의 길이를 지정하는 길이 필드 및 상기 무선 구간에 사용되는 암호 키를 나타내는 키 값을 포함하는 것을 특징으로 하는 키 서술자 구조.

청구항 2.

삭제

청구항 3.

키 서술자를 이용하여 무선 랜 단말기와 액세스포인트사이에서 무선구간 암호 키를 교환하는 방법에 있어서,

(a) 상기 액세스포인트가 인증서버로부터 마스터 세션 키를 수신함으로써 상기 무선 랜 단말기와 상기 마스터 세션 키를 공유하는 단계;

(b) 상기 액세스포인트가 무선구간 암호 알고리즘을 지정하는 태그, 상기 무선구간 암호 알고리즘에 해당하는 무선구간 암호 키의 길이 및 상기 암호 키의 실제 값을 포함하는 키 재료를 적어도 둘 이상 생성하는 단계;

(c) 상기 액세스포인트가 난수인 키 초기벡터를 생성하고, 상기 생성한 키 초기벡터 및 상기 마스터 세션 키를 이용하여 상기 키 재료들을 포함하는 키 서술자를 암호화하여 상기 무선 랜 단말기로 전송하는 단계;

(d) 상기 무선 랜 단말기가 상기 수신한 키 서술자를 복호화하여 상기 키 재료들을 복원하는 단계;

(e) 상기 복원된 키 재료들 중 소정의 키 재료에 포함된 암호 알고리즘 및 암호 키 값으로 이전의 무선구간 암호 알고리즘 및 암호 키를 갱신하고, 상기 갱신되는 암호 알고리즘을 나타내는 태그를 상기 암호 키로 암호화된 데이터에 첨부하는 단계;를 포함하는 것을 특징으로 하는 무선구간 암호 키 교환 방법.

청구항 4.

제3항에 있어서, 상기 (b) 단계는

(b1) 무선구간 암호 알고리즘을 지정하는 태그를 생성하는 단계;

(b2) 상기 태그가 지시하는 암호 알고리즘의 무선구간 암호 키의 길이를 생성하는 단계;

(b3) 상기 암호키의 실제 값을 생성하는 단계;를 포함하는 것을 특징으로 하는 무선구간 암호 키 교환 방법.

청구항 5.

제4항에 있어서, 상기 (b1)단계는

상기 태그를 무작위로 배열하는 단계를 더 포함하는 것을 특징으로 하는 무선구간 암호 키 교환 방법.

청구항 6.

제3항에 있어서, 상기 (d)단계는

무선 랜 단말기가 수신한 상기 키 서술자로부터 무선구간 암호 키를 검출한 후 상기 태그를 기초로 상기 무선구간 암호 키를 갱신하는 단계;를 더 포함하는 것을 특징으로 하는 무선구간 암호 키 교환 방법.

청구항 7.

무선 랜 단말기와 액세스포인트간에 데이터의 암호 및 복호 방법에 있어서,

(a) 상기 액세스포인트에서 무선구간 암호 알고리즘을 지정하는 태그, 상기 암호 알고리즘에 대한 무선구간 암호 키의 길이 및 상기 암호 키의 실제 값을 포함하는 키 재료를 적어도 둘 이상 생성하는 단계;

(b) 상기 액세스포인트는 상기 키 재료들을 포함하는 키 서술자를 암호화하여 상기 무선 랜 단말기로 전송하고, 상기 무선 랜 단말기는 상기 키 서술자를 복호화하여 상기 키 재료들을 복원하는 단계;

(c) 상기 키 재료들 중 소정의 키 재료에서 정의된 암호 알고리즘 및 암호 키로 소정의 데이터를 암호화한 후 상기 암호화된 데이터에 상기 암호 알고리즘을 나타내는 태그를 첨부하여 상기 무선구간에서 송수신하는 단계; 및

(d) 상기 암호화된 데이터를 수신하면, 상기 암호화된 데이터에 첨부된 태그에서 지정된 암호 알고리즘을 이용하여 상기 암호화된 데이터를 복호화하는 단계;를 포함하는 것을 특징으로 하는 무선 랜 단말기와 액세스포인트간 데이터의 암호 및 복호방법.

청구항 8.

제7항에 있어서, 상기 (a)단계는

(a1) 무선구간 암호 알고리즘을 지정하는 태그를 생성하는 단계;

(a2) 상기 태그가 지시하는 암호 알고리즘의 무선구간 암호 키의 길이를 생성하는 단계;

(a3) 상기 암호키의 실제 값을 생성하는 단계;를 포함하는 것을 특징으로 하는 무선 랜 단말기와 액세스포인트간 데이터의 암호 및 복호방법.

청구항 9.

제7항에 있어서, 상기 (c)단계는

(c1) 상기 태그필드마다 상이한 알고리즘을 규정하여 프레임마다 상이한 알고리즘에 의하여 암호화하는 단계;를 더 포함하는 것을 특징으로 하는 무선 랜 단말기와 액세스포인트간 데이터의 암호 및 복호방법.

청구항 10.

제9항에 있어서, 상기 (c1)단계는

상기 태그순서를 무작위로 배열하는 단계를 더 포함하는 것을 특징으로 하는 무선 랜 단말기와 액세스포인트간 데이터의 암호 및 복호방법.

청구항 11.

제7항에 있어서, 상기 (c)단계는

마스터세션키를 암호키로 하고, 상기 무선 랜 단말기와 액세스포인트간에 대칭키 알고리즘을 사용하여 상기 태그필드를 암호화하는 것을 특징으로 하는 무선 랜 단말기와 액세스포인트가 데이터의 암호 및 복호방법.

청구항 12.

적어도 하나 이상의 무선 랜 단말기 및 인증서버와 네트워크를 구성하는 액세스포인트에 있어서,

상기 네트워크간에 통신되는 데이터를 처리하고 상기 액세스포인트의 제어를 수행하는 연산처리부;

상기 인증서버로부터 마스터 세션 키를 수신하고, 키 초기벡터를 생성하는 마스터세션키 수신부;

상기 무선 랜 단말기와의 무선구간에 적용될 암호알고리즘을 지정하는 태그, 상기 무선구간의 암호 키의 길이 및 상기 무선구간의 암호 키 값을 포함하는 키 재료를 적어도 둘 이상 생성하고, 상기 키 재료들을 상기 마스터세션키 및 상기 키 초기벡터를 암호 키로 하여 상기 키 재료들을 암호화하는 보안기능처리부;

상기 암호화된 키 재료들을 포함하는 키 서술자를 출력하는 송신부; 및

상기 송신부가 출력하는 키 서술자 및 상기 키 재료의 암호 키로 암호화된 데이터를 송수신하는 인터페이스부;를 포함하는 것을 특징으로 하는 액세스포인트.

청구항 13.

제12항에 있어서, 상기 보안기능처리부는

무선구간에 적용될 암호알고리즘을 지정하는 태그를 생성하는 태그생성부;

무선구간 암호 키의 길이를 지정하는 암호키길이생성부;

무선구간 암호 키값을 생성하는 키값생성부;를 포함하는 것을 특징으로 하는 액세스포인트.

청구항 14.

제 12항에 있어서, 상기 보안기능처리부는,

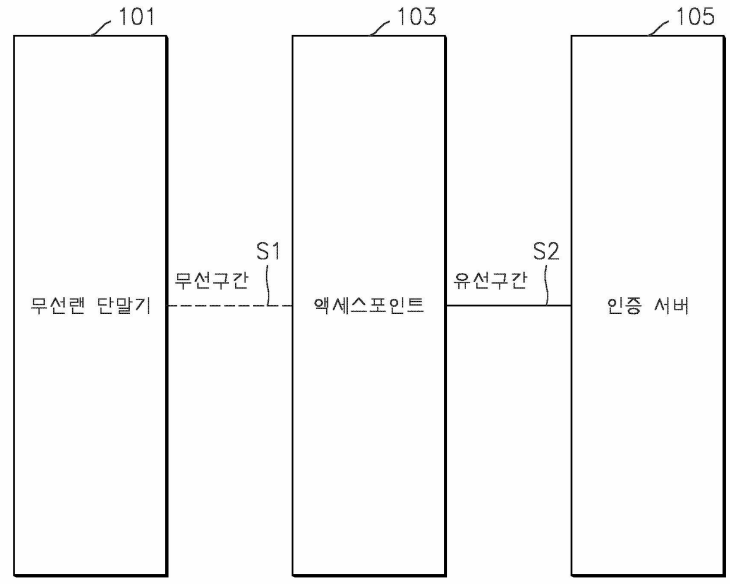
상기 연산처리부의 제어에 의해 상기 무선 랜 단말기와 상기 액세스포인트간에 송수신되는 데이터를 프레임별로 상이한 암호알고리즘으로 암호화하고, 상기 암호화된 데이터의 프레임에 상기 암호 알고리즘을 나타내는 태그를 첨부하여 출력하는 것을 특징으로 하는 액세스포인트.

청구항 15.

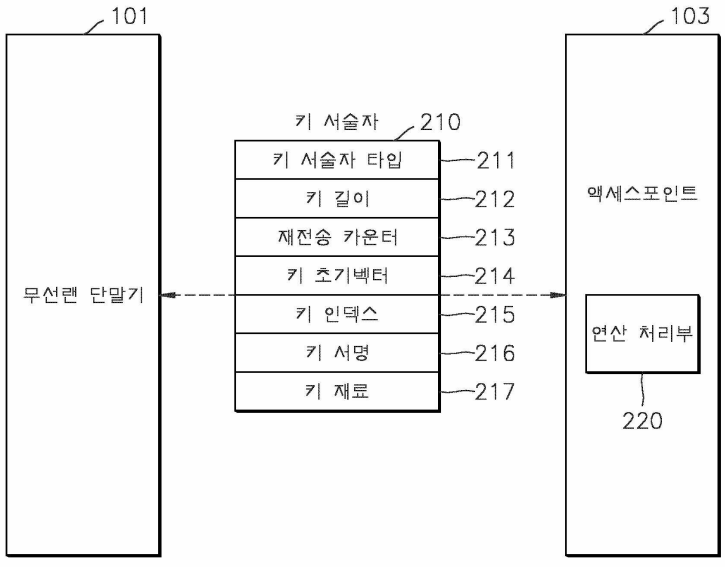
삭제

도면

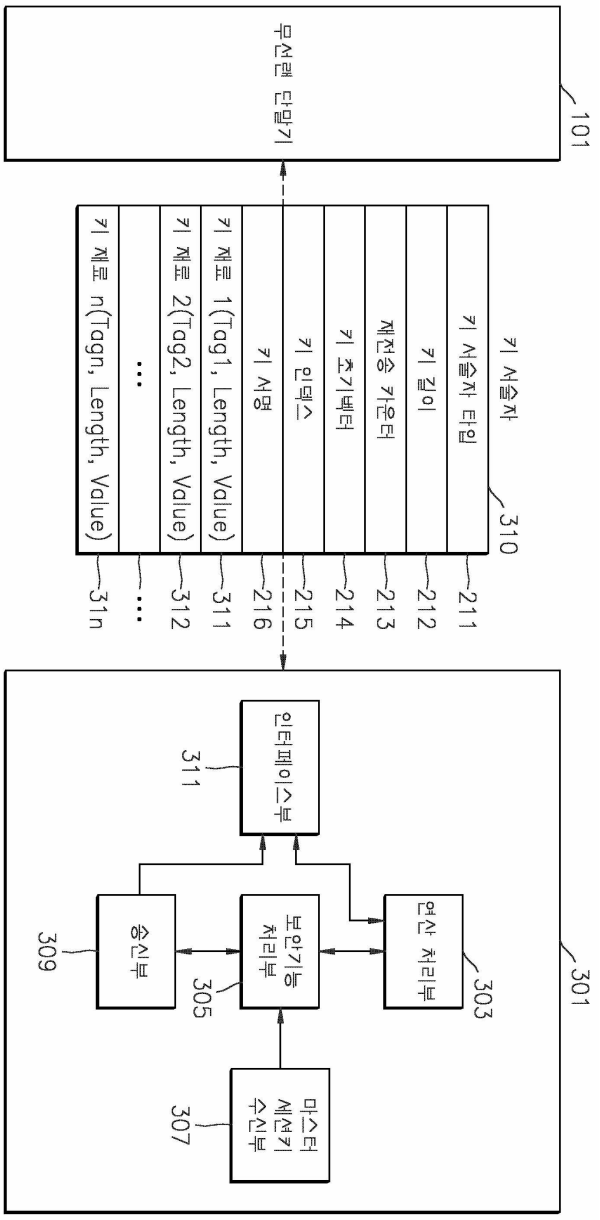
도면1



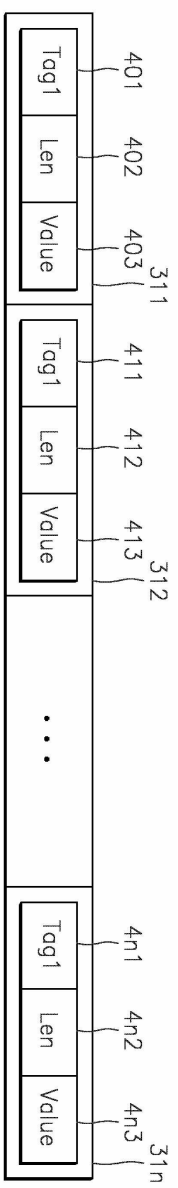
도면2



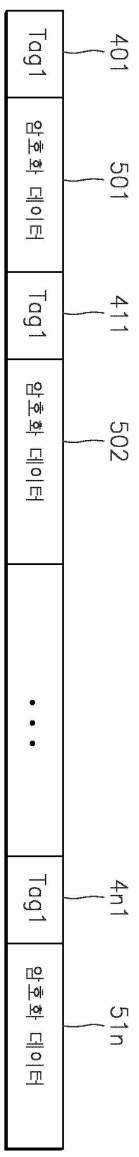
도면3


무선랜 단말기
101
키 서술자
310
키 서술자 타입
211
키 길이
212
제전송 카운터
213
키 초기벡터
214
키 인덱스
215
키 서명
216
키 재료 1(Tag1, Length, Value)
311
키 재료 2(Tag2, Length, Value)
312
...
...
키 재료 n(Tagn, Length, Value)
31n
301
인터페이스부
311
송신부
309
보안기능 처리부
305
연산 처리부
303
마스터 세션키 수신부
307

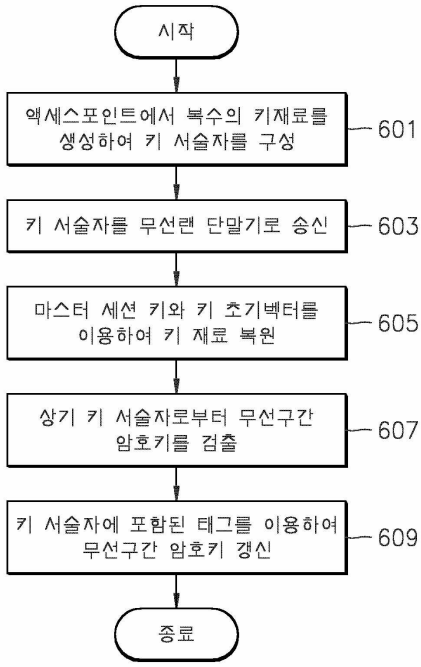
도면4


Tag1
Len
Value
401
402
403
311
Tag1
Len
Value
411
412
413
312
• • •
Tag1
Len
Value
4n1
4n2
4n3
31n

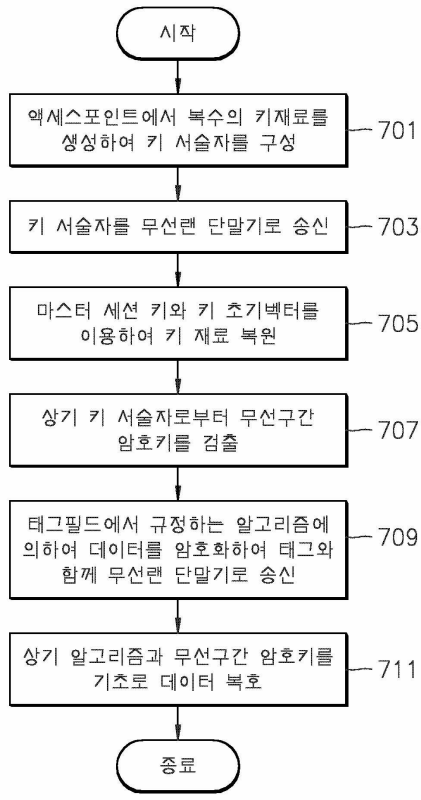
도면5



도면6


시작
액세스포인트에서 복수의 키재료를 생성하여 키 서술자를 구성
601
키 서술자를 무선랜 단말기로 송신
603
마스터 세션 키와 키 초기벡터를 이용하여 키 재료 복원
605
상기 키 서술자로부터 무선구간 암호키를 검출
607
키 서술자에 포함된 태그를 이용하여 무선구간 암호키 갱신
609
종료

도면7


시작
액세스포인트에서 복수의 키재료를 생성하여 키 서술자를 구성
701
키 서술자를 무선랜 단말기로 송신
703
마스터 세션 키와 키 초기벡터를 이용하여 키 재료 복원
705
상기 키 서술자로부터 무선구간 암호키를 검출
707
태그필드에서 규정하는 알고리즘에 의하여 데이터를 암호화하여 태그와 함께 무선랜 단말기로 송신
709
상기 알고리즘과 무선구간 암호키를 기초로 데이터 복호
711
종료