(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0140240
(43) 공개일자 2016년12월07일

(51) 국제특허분류(Int. Cl.)
*H04L 1/18* (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
*H04L 1/1887* (2013.01)
*H04L 1/188* (2013.01)
(21) 출원번호 10-2015-0076626
(22) 출원일자 2015년05월29일
심사청구일자 2015년05월29일

(71) 출원인
**한발대학교 산학협력단**
대전광역시 유성구 동서대로 125 (덕명동)
(72) 발명자
**김은기**
대전광역시 유성구 어은로 57 한빛아파트 117동 502호
**박승범**
대전광역시 서구 문예로 174, 101동 604호 (둔산동, 샘머리아파트1단지)
**안재원**
세종특별자치시 조치원읍 이화로 5 신흥주공아파트 208동 402호
(74) 대리인
**특허법인충정**

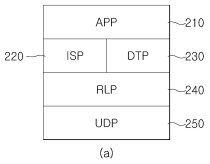
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **WAVE 시스템을 위한 에러제어 기능을 개선한 보안통신 프로토콜을 이용한 데이터통신 방법 및 그 장치**

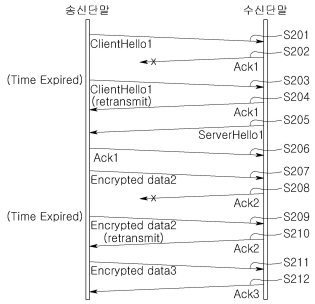
## (57) 요 약

비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서, 송신단말이, 전송하려는 데이터를 비연결지향성 프로토콜의 최대 전송 단위(MTU, Maximum Transmission Unit)에 맞춰 단편화하며, 단편화된 데이터에 대해 순차적으로 일련번호를 부여하는 단계; 및 송신단말이 단편화된 데이터를 일련번호에 따라 순차적으로 수신단말로 전송하되, 수신단말은 자동 반복 요청(ARQ, Automatic Repeat Request) 방식을 통해 상기 데이터 전송을 제어하는 단계를 포함하는, 본 발명의 일 실시예에 따른 데이터통신 방법이 개시된다.

*대 표 도* - 도2



(a)



(b)

(52) CPC특허분류
*H04L 63/0428* (2013.01)
*H04L 63/16* (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1425087633
부처명 중소기업청
연구관리전문기관 한국산학연협회
연구사업명 산학연협력기술개발
연구과제명 하이패스 서비스 기반 eSafety 융복합형 단거리 전용 무선통신 단말 개발
기 여 율 1/1
주관기관 한밭대학교산학협력단
연구기간 2014.06.01 ~ 2015.05.31

# *명 세 서*

## *청구범위*

### 청구항 1

비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서,

송신단말이, 전송하려는 데이터를 상기 비연결지향성 프로토콜의 최대 전송 단위(MTU, Maximum Transmission Unit)에 맞춰 단편화하며, 상기 단편화된 데이터에 대해 순차적으로 일련번호를 부여하는 단계; 및

상기 송신단말이 상기 단편화된 데이터를 일련번호에 따라 순차적으로 수신단말로 전송하되, 상기 수신단말의 자동 반복 요청(ARQ, Automatic Repeat Request) 방식의 제어하에 상기 데이터를 전송하는 단계를 포함하는, 데이터통신 방법.

### 청구항 2

제1항에 있어서,

상기 전송하는 단계는,

상기 송신단말이, 상기 수신단말로부터 상기 일련번호에 바탕한 응답신호(Ack, Acknowledgement)를 전달받는 경우 다음 일련번호의 데이터를 전송하고, 상기 응답신호를 일정시간 내에 전달받지 못하는 경우, 해당 일련번호의 데이터를 재전송하는 단계를 포함하는, 데이터통신 방법.

### 청구항 3

제1항에 있어서,

상기 단편화 이전에,

상기 송신단말이 통신 초기설정을 위한 ClientHello 메시지를 상기 수신단말로 전송하고, 상기 수신단말로부터 상기 Client Hello에 대응하는 ServerHello 메시지를 전송받아 상호간 보안통신의 초기설정을 하는 단계; 및

상기 송신단말이, 상기 초기설정을 바탕으로 전송하려는 데이터를 처리하는 단계를 포함하는, 데이터통신 방법.

### 청구항 4

제3항에 있어서,

상기 초기설정을 하는 단계는,

상기 송신단말이 상기 수신단말로부터 상기 ClientHello 메시지에 대한 응답신호를 일정시간 내에 전달받지 못하는 경우, 상기 ClientHello 메시지를 재전송하는 단계를 포함하는, 데이터통신 방법.

### 청구항 5

제4항에 있어서,

상기 ClientHello 메시지는 전송하려는 데이터에 대한 제1 순서번호, 키 교환 알고리즘, 해시 알고리즘 및 암호화 알고리즘 정보 중 적어도 하나를 포함하고,

상기 제1 순서번호는 상기 송신단말을 특정하는 정보를 포함하는, 데이터통신 방법.

**청구항 6**

제5항에 있어서,

상기 데이터를 처리하는 단계는,

상기 암호화 알고리즘 정보를 바탕으로 상기 데이터를 암호화하는 단계를 포함하는, 데이터통신 방법.

**청구항 7**

제6항에 있어서,

상기 ClientHello 메시지는 상기 키 교환 알고리즘으로 생성된 상기 송신단말의 공개키를 포함하고,

상기 ServerHello 메시지는 상기 키 교환 알고리즘으로 생성된 상기 수신단말의 공개키를 포함하는, 데이터통신 방법.

**청구항 8**

제7항에 있어서,

상기 키 교환 알고리즘은 DH(Diffie-Hellman) 키 교환 알고리즘을 포함하는, 데이터통신 방법.

**청구항 9**

제8항에 있어서,

상기 암호화 알고리즘은

ECDSA(Elliptic Curve Digital Signature Algorithm), ECIES(Elliptic Curve Integrated Encryption Scheme) 및 AES(Advanced Encryption Standard) 중 적어도 하나를 포함하는, 데이터통신 방법.

**청구항 10**

제9항에 있어서,

상기 데이터를 암호화하는 단계는

상기 송신단말 및 수신단말의 공개키를 바탕으로 상기 DH 키 교환 알고리즘에 따라 세션키를 생성하는 단계; 및

상기 ECDSA 및 ECIES 중 적어도 하나를 이용하여 상기 세션키를 암호화하는 단계를 포함하는, 데이터통신 방법.

**청구항 11**

제10항에 있어서,

상기 데이터를 암호화하는 단계는

상기 세션키를 이용하여 상기 데이터를 상기 AES 알고리즘으로 암호화하는 단계를 포함하는, 데이터통신 방법.

**청구항 12**

제11항에 있어서,

상기 데이터를 암호화하는 단계는

상기 제1 순서번호, 상기 암호화된 데이터 및 상기 해시 알고리즘을 이용하여 MAC(Message Authentication Code) 정보를 생성하는 단계; 및

상기 MAC 정보를 상기 암호화된 데이터 뒤에 추가하는 단계를 포함하는, 데이터통신 방법.

**청구항 13**

제12항에 있어서,

상기 해시 알고리즘은 HMAC-SHA(Hash-based Message Authentication Code- Secure Hash Algorithm)을 포함하는, 데이터통신 방법.

**청구항 14**

제1항 또는 제3항에 있어서,

상기 데이터통신은 WAVE(Wireless Access in Vehicular Environments) 환경에서 이루어지는 것을 포함하는, 데이터통신 방법.

**청구항 15**

비연결지향성 프로토콜을 이용한 데이터통신 단말에 있어서,

전송하려는 데이터를 상기 비연결지향성 프로토콜의 최대 전송 단위(MTU, Maximum Transmission Unit)에 맞춰 단편화하며, 상기 단편화된 데이터에 대해 순차적으로 일련번호를 부여하고, 상기 단편화된 데이터를 일련번호에 따라 순차적으로 수신단말로 전송하되, 상기 수신단말의 자동 반복 요청(ARQ, Automatic Repeat Request) 방식의 제어 하에 상기 데이터를 전송하는 RLP부를 포함하는, 데이터통신 단말.

**청구항 16**

제15항에 있어서,

상기 RLP부는

상기 수신단말로부터 상기 일련번호에 바탕한 응답신호(Ack, Acknowledgement)를 전달받는 경우 다음 일련번호의 데이터를 전송하고, 상기 응답신호를 일정시간 내에 전달받지 못하는 경우, 해당 일련번호의 데이터를 재전송하는 것을 포함하는, 데이터통신 단말.

**청구항 17**

제15항에 있어서,

통신 초기설정을 위한 ClientHello 메시지를 상기 수신단말로 전송하고, 상기 수신단말로부터 상기 Client Hello에 대응하는 ServerHello 메시지를 전송받아 상호간 보안통신의 초기설정을 하는 ISP부; 및

상기 초기설정을 바탕으로 전송하려는 데이터를 처리하는 DTP부를 더 포함하는, 데이터통신 단말.

**청구항 18**

제15항에 있어서,

상기 데이터통신은 WAVE(Wireless Access in Vehicular Environments) 환경에서 이루어지는 것을 포함하는, 데이터통신 단말.

## 발명의 설명

### 기 술 분 야

[0001] 본 발명은 에러제어 기능을 개선한 보안통신 프로토콜을 이용한 데이터통신 방법에 관한 것이다. 보다 구체적으로, 본 발명은 비연결지향성 프로토콜을 이용한 데이터 통신에 있어서, 에러제어 기능을 개선한 보안통신 프로토콜을 이용한 데이터통신 방법에 관한 것이다.

### 배 경 기 술

[0002] 데이터 전송 과정에 있어서, 자체적으로 오류를 처리하며 데이터의 순서를 교정하는 연결지향성 프로토콜과 달리, 비연결지향성 프로토콜은 이러한 기능을 제공하지 않음으로써 신뢰성 있는 데이터 전송을 보장하지 못하므로, 네트워크 구성에 있어서, 이러한 점을 고려한 프로토콜 및 데이터통신 방법의 선택이 필요하다.

[0003] 한편, 최근 네트워크에 대한 많은 보안상 이슈의 등장에 따라, 비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서도, 신뢰성을 높일 수 있는 방법이 필요하며, 이는 특히 최근에 부각되는 차량 또는 기반시설 간의 무선 통신(WAVE, Wireless Access in Vehicular Environments)에 있어서 또한 중요한 이슈가 되고 있다.

[0004] WAVE 시스템은 일반적으로, 실시간 전송을 지원하기 위해 UDP(User Datagram Protocol) 상위에서 동작하며, UDP 상위에서 보안기능을 지원하기 위해 범용적으로 DTLS(Datagram Transport layer Security) 프로토콜을 사용하고 있다. 하지만, DTLS 프로토콜은 암호화된 정보의 전송 시 에러제어 기능을 지원하지 않으며, 이러한 방식은 암호화 특성상 일부분의 데이터 손실로 인한 전체 데이터의 손실을 초래할 수 있는 위험성을 가지고 있다.

[0005] 따라서, WAVE 시스템과 같은 비연결지향성 프로토콜을 이용한 실시간 전송을 필요로 하는 분야에 있어서, 암호화된 데이터 전송 시에도 에러제어 기능을 지원하여 데이터 손실을 최소화하고, 데이터의 무결성과 기밀성 및 인증을 보장하는 데이터통신 방법이 필요한 실정이다.

## 발명의 내용

### 해결하려는 과제

[0006] 본 발명의 일 실시예에 따른 데이터통신 방법은, 비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서, 에러제어 기능을 지원함으로써 데이터 손실을 최소화하는 것을 목적으로 한다.

[0007] 또한, 본 발명의 일 실시예에 따른 데이터통신 방법은, 비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서, 암호화 알고리즘을 통한 데이터의 기밀성을 보장하는 것을 목적으로 한다.

[0008] 또한, 본 발명의 일 실시예에 따른 데이터통신 방법은, 비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서, 키 교환 알고리즘을 통한 상호 인증 및 데이터의 기밀성을 보장하는 것을 목적으로 한다.

[0009] 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

### 과제의 해결 수단

[0010] 본 발명의 일 실시예에 따른 데이터통신 방법은,

[0011] 비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서, 송신단말이, 전송하려는 데이터를 상기 비연결지향성 프로토콜의 최대 전송 단위(MTU, Maximum Transmission Unit)에 맞춰 단편화하며, 상기 단편화된 데이터에 대해 순차적으로 일련번호를 부여하는 단계; 및 상기 송신단말이 상기 단편화된 데이터를 일련번호에 따라 순차적으로 수신단말로 전송하되, 상기 수신단말의 자동 반복 요청(ARQ, Automatic Repeat Request) 방식의 제어하에 상기 데이터를 전송하는 단계를 포함할 수 있다.

[0012] 상기 전송하는 단계는, 상기 송신단말이, 상기 수신단말로부터 상기 일련번호에 바탕한 응답신호(Ack, Acknowledgement)를 전달받는 경우 다음 일련번호의 데이터를 전송하고, 상기 응답신호를 일정시간 내에 전달받지 못하는 경우, 해당 일련번호의 데이터를 재전송하는 단계를 포함할 수 있다.

[0013] 상기 단편화 이전에, 상기 송신단말이 통신 초기설정을 위한 ClientHello 메시지를 상기 수신단말로 전송하고, 상기 수신단말로부터 상기 Client Hello에 대응하는 ServerHello 메시지를 전송받아 상호간 보안통신의 초기설정을 하는 단계; 및 상기 송신단말이, 상기 초기설정을 바탕으로 전송하려는 데이터를 처리하는 단계를 포함할 수 있다.

[0014] 상기 초기설정을 하는 단계는, 상기 송신단말이 상기 수신단말로부터 상기 ClientHello 메시지에 대한 응답신호를 일정시간 내에 전달받지 못하는 경우, 상기 ClientHello 메시지를 재전송하는 단계를 포함할 수 있다.

[0015] 상기 ClientHello 메시지는 전송하려는 데이터에 대한 제1 순서번호, 키 교환 알고리즘, 해시 알고리즘 및 암호화 알고리즘 정보 중 적어도 하나를 포함하고, 상기 제1 순서번호는 상기 송신단말을 특정하는 정보를 포함할 수 있다.

[0016] 상기 데이터를 처리하는 단계는, 상기 암호화 알고리즘 정보를 바탕으로 상기 데이터를 암호화하는 단계를 포함할 수 있다.

[0017] 상기 ClientHello 메시지는 상기 키 교환 알고리즘으로 생성된 상기 송신단말의 공개키를 포함하고, 상기 ServerHello 메시지는 상기 키 교환 알고리즘으로 생성된 상기 수신단말의 공개키를 포함할 수 있다.

[0018] 상기 키 교환 알고리즘은 DH(Diffie-Hellman) 키 교환 알고리즘을 포함할 수 있다.

[0019] 상기 암호화 알고리즘은 ECDSA(Elliptic Curve Digital Signature Algorithm), ECIES(Elliptic Curve Integrated Encryption Scheme) 및 AES(Advanced Encryption Standard) 중 적어도 하나를 포함할 수 있다.

[0020] 상기 데이터를 암호화하는 단계는 상기 송신단말 및 수신단말의 공개키를 바탕으로 상기 DH 키 교환 알고리즘에 따라 세션키를 생성하는 단계; 및 상기 ECDSA 및 ECIES 중 적어도 하나를 이용하여 상기 세션키를 암호화하는 단계를 포함할 수 있다.

[0021] 상기 데이터를 암호화하는 단계는 상기 세션키를 이용하여 상기 데이터를 상기 AES 알고리즘으로 암호화하는 단계를 포함할 수 있다.

[0022] 상기 데이터를 암호화하는 단계는 상기 제1 순서번호, 상기 암호화된 데이터 및 상기 해시 알고리즘을 이용하여 MAC(Message Authentication Code) 정보를 생성하는 단계; 및 상기 MAC 정보를 상기 암호화된 데이터 뒤에 추가하는 단계를 포함할 수 있다.

[0023] 상기 해시 알고리즘은 HMAC-SHA(Hash-based Message Authentication Code- Secure Hash Algorithm)을 포함할 수 있다.

[0024] 상기 데이터통신은 WAVE(Wireless Access in Vehicular Environments) 환경에서 이루어지는 것을 포함할 수 있다.

[0025] 본 발명의 다른 실시예에 따른 데이터통신 장치는,

[0026] 비연결지향성 프로토콜을 이용한 데이터통신 단말에 있어서, 전송하려는 데이터를 상기 비연결지향성 프로토콜의 최대 전송 단위(MTU, Maximum Transmission Unit)에 맞춰 단편화하며, 상기 단편화된 데이터에 대해 순차적으로 일련번호를 부여하고, 상기 단편화된 데이터를 일련번호에 따라 순차적으로 수신단말로 전송하되, 상기 수신단말의 자동 반복 요청(ARQ, Automatic Repeat Request) 방식의 제어 하에 상기 데이터를 전송하는 RLP부를 포함할 수 있다.

[0027] 상기 RLP부는 상기 수신단말로부터 상기 일련번호에 바탕한 응답신호(Ack, Acknowledgement)를 전달받는 경우 다음 일련번호의 데이터를 전송하고, 상기 응답신호를 일정시간 내에 전달받지 못하는 경우, 해당 일련번호의 데이터를 재전송하는 것을 포함할 수 있다.

[0028] 통신 초기설정을 위한 ClientHello 메시지를 상기 수신단말로 전송하고, 상기 수신단말로부터 상기 Client Hello에 대응하는 ServerHello 메시지를 전송받아 상호간 보안통신의 초기설정을 하는 ISP부; 및 상기 초기설정을 바탕으로 전송하려는 데이터를 처리하는 DTP부를 더 포함할 수 있다.

[0029] 상기 데이터통신은 WAVE(Wireless Access in Vehicular Environments) 환경에서 이루어지는 것을 포함할 수 있다.

## 발명의 효과

[0030] 본 발명의 일 실시예에 따른 데이터통신 방법은, 비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서 에러제어 기능을 지원함으로써 데이터 손실을 최소화할 수 있다.

[0031] 또한, 본 발명의 일 실시예에 따른 데이터통신 방법은, 비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서, 암호화 알고리즘을 통한 데이터의 기밀성을 보장할 수 있다.

[0032] 또한, 본 발명의 일 실시예에 따른 데이터통신 방법은, 비연결지향성 프로토콜을 이용한 데이터통신 방법에 있어서, 키 교환 알고리즘을 통한 상호 인증 및 데이터의 기밀성을 보장할 수 있다.

## 도면의 간단한 설명

[0033] 도 1(a)는 종래의 DTLS(Datagram Transport Layer Security)를 이용한 비연결지향성 데이터통신의 보안통신 프로토콜 계층구조의 일 예를 도시한 도면이다.

도 1(b)는 종래의 DTLS(Datagram Transport Layer Security)를 이용한 비연결지향성 데이터통신의 보안통신 프로토콜을 이용한 에러 제어를 도시한 도면이다.

도 2(a)는 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 보안통신 프로토콜 계층구조를 도시한 도면이다.

도 2(b)는 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 보안통신 프로토콜을 이용한 에러 제어를 도시한 도면이다.

도 3은 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 보안통신 방법을 도시한 순서도이다.

도 4는 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 ClientHello, ServerHello 메시지의 구조를 도시한 도면이다.

도 5는 본 발명의 일 실시예에 따른 비연결지향성 데이터통신 단말의 구성을 도시한 도면이다.

## 발명을 실시하기 위한 구체적인 내용

[0034] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0035] 본 발명의 일 실시예에 따른 데이터통신 방법은 실시간 전송을 필요로 하는 분야에서 데이터의 무결성, 기밀성 및 인증을 보장하며, 에러제어 기능을 지원할 수 있으며, 특히 최근 부상하는 WAVE(Wireless Access in Vehicular Environments) 시스템하에서의 데이터통신에도 적용될 수 있다. 즉, 본 발명의 일 실시예에 따른 데이터통신 방법은 일반적으로 실시간 데이터 전송 목적으로 사용되는 비연결지향성 프로토콜을 이용한 데이터통신에 모두 적용될 수 있다.

[0036] 이러한 본 발명의 일 실시예에 따른 데이터통신 방법에 대해 도면을 참조하며 설명한다.

[0037] 도 1(a)는 종래의 DTLS(Datagram Transport Layer Security)를 이용한 비연결지향성 데이터통신의 보안통신 프로토콜 계층구조의 일 예를 도시한 도면이다.

[0038] 도시된 바와 같이, 기존의 비연결지향성 데이터통신의 보안통신 프로토콜은 APP(Application Layer)(110), DTLS(Datagram Transport Layer Security)(120) 및 UDP(User Datagram Protocol)(130)을 포함할 수 있다. 그 중 특히 DTLS(120)는 데이터 전송에 있어서 보안기능을 담당한다.

[0039] 비연결지향성 데이터통신은 주로 실시간 데이터 전송에 활용되며, 이러한 비연결지향성 프로토콜의 상위에서 보안기능을 지원하는 DTLS(100)는 오버헤드가 크고, 부분적인 에러제어 기능만을 지원한다는 단점이 있다.

[0040] 상기 비연결지향성 프로토콜은 UDP를 포함한다.

[0041] 도 1(b)는 종래의 DTLS(Datagram Transport Layer Security)를 이용한 비연결지향성 데이터통신의 보안통신 프로토콜을 이용한 에러제어를 도시한 도면이다.

[0042] 도시된 바와 같이, 종래의 DTLS(120)를 이용한 비연결지향성 데이터통신의 보안통신 프로토콜을 이용한 에러제어는, 초기설정 메시지인, ClientHello 및 HelloVerify Request 메시지를 통한 초기 연결설정 과정에서만 에러제어 기능을 수행하며, 이후에는 수신단말의 응답메시지 없이 단방향 전송을 한다. 따라서, 전체 데이터가 없이는 복호화가 이루어지지 않는 암호화 알고리즘에 의해, 데이터 전송 과정에서의 부분적인 손실이 발생하는 경우 남은 데이터의 복호화가 불가능하다는 단점이 있다.

[0043] 도 2(a)는 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 보안통신 프로토콜 계층구조를 도시한 도면이다.

[0044] 도시된 바와 같이, 위와 같은 종래 기술의 단점을 개선하기 위해 제안된 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 보안통신 프로토콜 계층구조는 ISP(Initial Setup Protocol)(210), DTP(Datagram Transport Layer Security)(220) 및 RLP(Record Layer Protocol)(230)를 포함할 수 있다.

[0045] 구체적으로는, 상기 ISP(220)는 송신단말 및 수신단말의 초기설정 메시지인 ClientHello, ServerHello 메시지의 생성 및 전송을 통해 통신 초기설정을 수행할 수 있다.

[0046] 상기 ClientHello 메시지는 제1 순서번호, 키 교환 알고리즘, 해시 알고리즘 및 암호화 알고리즘 중 적어도 하나를 포함할 수 있으며, 상기 제1 순서번호는 송신단말, 수신단말 또는 데이터를 특정하기 위한 번호를 포함할 수 있다.

[0047] 또한, 상기 ClientHello 메시지는 상기 키 교환 알고리즘으로 생성된 상기 송신단말의 공개키를 포함할 수 있으며, 상기 ServerHello 메시지는 상기 키 교환 알고리즘으로 생성된 상기 수신단말의 공개키를 포함할 수 있다. 상기 키 교환 알고리즘은 DH(Diffie-Hellman) 키 교환 알고리즘을 포함할 수 있다.

[0048] 상기 DTP(230)는 상기 ISP(220)를 통해 초기설정된 정보를 이용하여 전송하려는 데이터를 암호화할 수 있다.

[0049] 구체적으로는, 상기 DTP(230)는 상기 공개키를 바탕으로 상기 DH 키 교환 알고리즘에 따라 세션키를 생성할 수 있으며, 상기 암호화 알고리즘을 이용하여 상기 세션키를 암호할 수 있다. 상기 암호화 알고리즘은 ECDSA(Elliptic Curve Digital Signature Algorithm), ECIES(Elliptic Curve Integrated Encryption Scheme) 및 AES(Advanced Encryption Standard) 중 적어도 하나를 포함할 수 있다.

[0050] 또한, 상기 DTP(230)는 생성된 상기 세션키를 이용하여 상기 데이터를 상기 AES 알고리즘으로 암호화할 수 있다.

[0051] 이에 더하여 상기 DTP(230)는 데이터의 무결성을 담보하기 위하여, 상기 제1 순서번호, 상기 암호화된 데이터 및 상기 해시 알고리즘을 이용하여 MAC(Message Authentication Code) 정보를 생성할 수 있으며, 상기 MAC 정보를 상기 암호화된 데이터 뒤에 추가할 수 있다. 상기 해시 알고리즘은 HMAC-SHA(Hash-based Message Authentication Code- Secure Hash Algorithm)을 포함할 수 있다.

[0052] 상기 RLP(240)는 ISP(220)와 DTP(230) 데이터를 실제로 송신 및 수신할 수 있으며, 또한 ISP(220)와 DTP(230) 데이터를 전송계층, 일례로 비연결지향성 프로토콜의 MTU(Maximum Transmission Unit)에 맞게 단편화할 수 있다. 즉, 상기 ISP(220), DTP(230)는 상기 전송계층의 상위에서 동작하기 때문에 에러 제어 기능과 최대 전송단위(MTU, Maximum Transfer Unit)에 맞게 데이터를 나누어 주는 기능이 필요하므로, 상기 RLP(240)는 ISP(220)와 DTP(230)의 하위 계층에 위치하여 이러한 기능을 지원할 수 있다.

[0053] 도 1(a), (b)에서 설명한 바와 같이, 기존의 UDP에서 보안기능을 지원하는 프로토콜인 DTLS는 타이머(Timer)를 이용한 부분적인 에러 제어 기능만을 지원하는 단점이 있으며, RLP(240)는 이를 개선하여, 자동 반복 요청(ARQ, Automatic Repeat Request) 기법을 이용하여 에러를 제어할 수 있다. 상기 자동 반복 요청 기법은 정지대기방식(Stop and Wait, Idle ARQ)을 포함할 수 있다.

[0054] 구체적으로는, 상기 RLP(240)는 상기 데이터를 상기 비연결지향성 프로토콜의 최대 전송 단위(MTU, Maximum Transmission Unit)에 맞춰 단편화할 수 있으며, 상기 단편화된 데이터에 대해 순차적으로 일련번호를 부여할 수 있다. 상기 비연결지향성 프로토콜은 UDP(User Datagram Protocol)를 포함할 수 있으며, 상기 일련번호는 오

프셋(Offset) 정보를 포함할 수 있다.

[0055] 상기 RLP(240)는 이렇게 상기 단편화된 데이터를 상기 일련번호에 따라 순차적으로 수신단말로 전송할 수 있으며, 상기 수신단말 RLP(240)는 자동 반복 요청(ARQ, Automatic Repeat Request) 방식을 통해 상기 전송을 제어함으로써, 에러제어 기능을 수행할 수 있다.

[0056] 일례로, 상기 송신단말에서, 상기 단편화된 데이터를 상기 일련번호에 따라 순차적으로 수신단말로 전송하되, 상기 수신단말로부터 상기 일련번호에 바탕한 응답신호(Ack, Acknowledgement)를 전달받는 경우 다음 일련번호의 데이터를 전송할 수 있으며, 상기 응답신호를 일정시간 내에 전달받지 못하는 경우, 해당 일련번호의 데이터를 재전송할 수 있다.

[0057] 상기 응답신호는 수신된 데이터의 일련번호를 포함할 수 있으며, 상기 응답신호는 RLP(240)에서 송신 및 수신할 수 있다.

[0058] 이러한 재전송 과정은, 상기 ISP(220)를 통한 초기설정 과정에서도 활용될 수 있다. 즉, 상기 송신단말이 상기 수신단말로부터 상기 ClientHello 메시지에 대한 응답신호를 일정시간 내에 전달받지 못하는 경우, 상기 ClientHello 메시지를 재전송할 수 있으며, 상기 수신단말이 상기 송신단말로부터 상기 ServerHello 메시지에 대한 응답신호를 일정시간 내에 전달받지 못하는 경우, 상기 ClientHello 메시지를 재전송할 수 있다.

[0059] 위와 같은 과정을 통해, 초기설정 메시지인 ClientHello와 ServerHello 뿐만 아니라, 암호화된 데이터 등의 전송 시에도 일련번호에 따른 응답 메시지(Ack, Acknowledgement)의 송신 및 수신을 이용한 에러제어 기능을 구현할 수 있다.

[0060] 한편, 이러한 데이터통신은 WAVE(Wireless Access in Vehicular Environments) 환경에서 이루어지는 것을 포함할 수 있으며, 이 경우 송신단말 또는 수신단말은 차량 또는 기반시설을 포함할 수 있다.

[0061] 도 2(b)는 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 보안통신 프로토콜을 이용한 에러제어를 도시한 도면이다.

[0062] 도시된 바와 같이, 본 발명에서 제안된 방식은 비연결지향성 프로토콜을 이용한 암호화 데이터 전송 시에도 응답신호를 이용한 에러제어를 지원함으로써, 통신의 신뢰성을 더욱 높일 수 있다.

[0063] 일례로, 송신단말은 수신단말로 초기설정 메시지인 ClientHello1 메시지를 전송할 수 있다(S201).

[0064] 상기 전송 후 일정시간 내에 상기 수신단말로부터 응답신호(Ack1)을 전달받지 못하는 경우(S202), 상기 ClientHello1 메시지를 재전송할 수 있다(S203).

[0065] 상기 재전송한 ClientHello1 메시지에 대한 응답신호(Ack1)를 일정시간 내에 받은 경우(S204), 상기 SeverHello1 신호가 전송되기를 기다릴 수 있다(S205).

[0066] 상기 SeverHello1 신호를 전송받은 경우(S205), 그에 대한 응답신호(Ack1)을 상기 수신단말로 전송할 수 있다(S206).

[0067] 상기 과정을 통해 상기 송신단말과 상기 수신단말의 보안통신 초기설정 과정이 이루어질 수 있다.

[0068] 한편, 초기설정 과정에서의 상기 응답신호는, ClientHello1 메시지에 대한 ServerHello1 메시지, ServerHello1 메시지에 대한 Encrypted data1으로 대체될 수 있다.

[0069] 그 후, 상기 초기설정에 의해 정해진 바대로, 상기 송신단말은 전송하려는 데이터를 암호화하고, 상기 비연결지향성 프로토콜의 최대 전송 단위에 맞춰 상기 암호화된 데이터를 단편화하며, 상기 단편화된 데이터에 순차적으로 일련번호를 부여하여, 상기 일련번호 대로 상기 수신단말로 데이터를 전송할 수 있다(S207)

[0070] 상기 수신단말로부터 전송한 데이터에 대한 응답신호(Ack2)를 전달받지 못한 경우(S208), 상기 송신단말은 해당 데이터를 재전송하며(S209), 상기 수신단말로부터 응답신호(Ack2)를 전달받는 경우, 다음 일련번호의 데이터를 전송할 수 있다(S211).

[0071] 즉, 위와 같은 상기 일련번호에 따른 응답신호를 바탕으로, 비연결지향성 프로토콜을 이용한 암호화 데이터 전송시에도 에러제어 기능을 구현하여, 통신의 신뢰성을 향상시킬 수 있다.

[0072] 도 3은 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 보안통신 방법을 도시한 순서도이다. 도시된 바와 같이, 상기 순서도는 도2(a)에서의 ISP(220), DTP(230), RLP(240)의 각 기능에 대해 시계열적으로 도시하고

있으며, 각 기능에 관하여는 위에서 자세히 설명하였으므로, 간단히 살펴보기로 한다.

[0073] S310 단계에서, 상호간 보안통신의 초기설정을 할 수 있다.

[0074] 구체적으로는, 송신단말에서 전송하려는 데이터의 제1 순서번호, 키 교환 알고리즘, 해시 알고리즘 및 암호화 알고리즘 정보 중 적어도 하나를 포함한 ClientHello 메시지를 수신단말로 전송할 수 있으며, 상기 수신단말에서는 전송된 상기 ClientHello 메시지를 저장하고, ServerHello 메시지를 송신단말로 전송하여 상호간 보안통신의 초기설정을 할 수 있다. 상기 제1 순서번호는 상기 송신단말을 특정하는 정보를 포함할 수 있으며, 상기 수신단말, 또는 상기 데이터를 특정하는 정보를 포함할 수 있다.

[0075] S320 단계에서, 초기설정을 바탕으로 전송하려는 데이터를 암호화할 수 있다.

[0076] 상기 암호화에 관하여는 도2(a)에 관한 기재를 통해 설명하였으므로 생략하기로 한다.

[0077] S330 단계에서, 암호화된 데이터를 전송계층의 최대 전송 단위에 맞춰 단편화할 수 있으며, 단편화된 데이터에 대해 순차적으로 일련번호를 부여할 수 있다. 상기 전송계층은 비연결지향성 프로토콜, 일예로 UDP를 포함할 수 있다. 상기 일련번호는 오프셋(Offset) 정보를 포함할 수 있다.

[0078] S340 단계에서, 단편화된 데이터를 일련번호에 따라 순차적으로 수신단말로 전송하되, 수신단말이 자동 반복 요청 방식을 통해 데이터 전송을 제어할 수 있다.

[0079] 구체적으로는, 상기 송신단말에서, 상기 단편화된 데이터를 상기 일련번호에 따라 순차적으로 수신단말로 전송하되, 상기 수신단말로부터 상기 일련번호에 바탕한 응답신호(Ack, Acknowledgement)를 전달받는 경우 다음 일련번호의 데이터를 전송하고, 상기 응답신호를 일정시간 내에 전달받지 못하는 경우, 해당 일련번호의 데이터를 재전송할 수 있다.

[0080] 도 4는 본 발명의 일 실시예에 따른 비연결지향성 데이터통신의 ClientHello, ServerHello 메시지의 구조를 도시한 도면이다.

[0081] 도시된 바와 같이, ClientHello, ServerHello 메시지는 Encryption ID, MAC ID, Seq number, Ya 필드를 포함할 수 있다. 상기 Encryption ID 필드는 제1 순서번호를 포함할 수 있으며, 상기 MAC ID 필드는 MAC 정보를 포함할 수 있다. 또한, 상기 Seq number 필드는 일련번호를 포함할 수 있으며, 상기 Ya 필드는 키 교환 알고리즘, 해시 알고리즘, 암호화 알고리즘 및 키 교환 알고리즘을 이용한 공개키, 개인키, 세션키 정보 등을 포함할 수 있다.

[0082] 상술한 ISP(220), DTP(230) 및 RLP(240)에서의 동작을 통한 데이터통신 방법에 대해, WAVE 시스템하에서, 차량이 송신단말, 기반시설이 수신단말인 경우를 예로 들어, 보다 자세히 설명한다.

[0083] 상기 차량은 상기 ISP(Initial Setup Protocol)를 통해 상기 기반시설과 통신 초기설정을 할 수 있다. 일례로, 상기 차량은 제1 순서번호, 키 교환 알고리즘으로 생성된 차량의 공개키와 암호화 알고리즘 및 해시 알고리즘 중 적어도 하나가 포함된 ClientHello 메시지를 생성할 수 있다. 상기 키 교환 알고리즘은 DH(Diffie-Hellman) 키 교환 알고리즘을 포함할 수 있다.

[0084] 한편, 상기 DH 키 교환 알고리즘은 중간자 공격(MITM, Man In The Middle attack) 공격의 위험에 노출될 수 있는 단점이 있으므로, 이를 보완하기 위해 상기 DH 키 교환 알고리즘으로 만들어진 세션 키에 대해 상기 암호화 알고리즘을 이용하여 보호할 수 있다. 상기 암호화 알고리즘은 ECDSA(Elliptic Curve Digital Signature Algorithm), ECIES(Elliptic Curve Integrated Encryption Scheme) 및 AES(Advanced Encryption Standard) 중 적어도 하나를 포함할 수 있다.

[0085] 상기 암호화 알고리즘으로 ECDSA, ECIES 및 AES를 포함하는 경우, 상기 ClientHello 메시지 뒤에 상기 ECDSA로 생성한 전자서명 값 r과 s를 붙일 수 있다. 이 때 상기 차량은 인증서를 발급받기 위해 사용했던 자신의 개인키로 전자 서명을 생성할 수 있다. 그리고 상기 차량의 인증서를 ECIES 암호화 과정에서 생성된 값 R, C, d에 붙일 수 있다.

[0086] 상기 기반시설이 수신단말인 경우, 상기 기반시설의 공개키 정보는 공개되어 있을 수 있으므로, 상기 암호화에 사용되는 키는 상기 기반시설의 공개키를 포함할 수 있다. 상기 차량은 이러한 과정을 통해 ISP 데이터를 생성하여, 상기 기반시설에 전송할 수 있다.

[0087] 수신단말인, 상기 기반시설은 상기 차량으로부터 전송받은 상기 ISP 데이터에서 R, C, d를 ECIES로 복호화할 수 있다. 복호화에 사용된 키는 상기 기반시설의 개인키를 포함할 수 있다.

[0088] 복호화한 결과 상기 기반시설은 상기 차량의 인증서를 얻을 수 있으며, 상기 차량의 인증서에서 공개키를 추출하여 수신한 전자 서명의 r과 s가 유효한지 확인할 수 있다.

[0089] 전자 서명이 유효하다고 확인되면 상기 기반시설은 상기 차량의 ClientHello 메시지를 저장하고 ServerHello 메시지를 생성할 수 있다. 상기 ServerHello 메시지에는 상기 DH 키 교환 알고리즘으로 생성된 상기 기반시설의 공개키와 상기 기반시설의 초기 설정에 관련된 정보가 포함될 수 있다.

[0090] 한편, 상기 기반시설은 상기 ServerHello 메시지 뒤에 ECDSA로 생성한 전자 서명값 r과 s를 붙일 수 있다. 이때 상기 기반시설은 자신의 개인키로 전자 서명을 생성할 수 있다. 상기 차량이 상기 기반시설의 공개키를 알고 있는 경우에는, ServerHello 메시지에 상기 기반시설의 인증서를 붙이지 않는다.

[0091] 상기 기반시설은 이러한 과정을 통해 ISP 데이터를 만들어 차량에게 전송할 수 있으며, 상기 ServerHello 메시지를 수신한 상기 차량은 상기 기반시설의 전자 서명을 확인할 수 있다.

[0092] 이후, DTP는 ISP에서 초기설정된 정보를 이용하여 전송하려는 데이터를 암호화할 수 있다. 또한, 상기 차량과 상기 기반시설은 상기 ISP를 통한 초기설정을 마친 후 DTP를 통해 데이터를 송신 또는 수신할 수 있다.

[0093] 상기 차량은 상기 DH 키 교환 알고리즘으로 생성된 차량의 공개키와 상기 ServerHello 메시지를 통해 얻게 된 상기 기반시설의 공개키를 이용하여 세션 키를 생성할 수 있으며, 생성된 세션 키를 이용하여 전송하려는 데이터를 상기 AES 알고리즘으로 암호화할 수 있다.

[0094] 이러한 암호화만 하여 데이터를 전송할 경우, 재전송 공격과 같은 공격에 취약해 질 수 있으므로, 이를 보완하기 위해 암호화된 데이터와 제1 순서번호를 이용하여 MAC을 생성하고, 상기 MAC을 데이터 뒤에 붙여 전송할 수 있다.

[0095] 상기 MAC 생성은 초기설정시의 상기 해시 알고리즘을 통해 생성될 수 있으며, 상기 해시 알고리즘은 HMAC-SHA(Hash-based Message Authentication Code- Secure Hash Algorithm)을 포함할 수 있다.

[0096] 상기 데이터를 수신한 상기 기반시설은 데이터와 MAC 부분을 분리할 수 있으며, 상기 ClientHello 메시지에 포함된 상기 제1 순서번호와 상기 암호화된 데이터를 이용하여 MAC을 생성할 수 있다. 상기 기반시설은 생성한 MAC과 수신한 MAC과의 비교를 통해 무결성이 보장된 데이터임을 확인할 수 있으며, 이 후 초기설정 과정에서 정해진 암호화 알고리즘을 이용하여 데이터를 복호화하여 상위 계층에 전송할 수 있다.

[0097] 도 5는 본 발명의 일 실시예에 따른 비연결지향성 데이터통신 단말의 구성을 도시한 도면이다. 도시된 바와 같이 상기 데이터통신 단말(500)은 통신부(510), 제어부(520) 및 인터페이스부(530)을 포함할 수 있다.

[0098] 상기 통신부(510) 및 인터페이스부(530)는 외부 단말과의 통신을 수행할 수 있으며, 상기 제어부(520)는 상기 통신으로 송신되거나, 수신되는 데이터의 처리를 수행할 수 있다.

[0099] 구체적으로는 상기 제어부(520)는 ISP부, DTP부, RLP부를 포함할 수 있다.

[0100] 즉, 위에서 설명한 ISP(220), DTP(230), RLP(240) 등은 송신단말, 또는 수신단말에 각각 ISP부(521), DTP부(522), RLP부(523) 등으로 구성되어 해당 기능을 수행할 수 있다.

[0101] 일례로, 상기 ISP부(521)는 통신 초기설정을 위한 ClientHello 메시지를 상기 수신단말로 전송하고, 상기 수신단말로부터 상기 Client Hello에 대응하는 ServerHello 메시지를 전송받아 상호간 보안통신의 초기설정을 할 수 있으며, 상기 DTP부(522)는 상기 초기설정을 바탕으로 전송하려는 데이터를 처리할 수 있다.

[0102] 상기 RLP부(523)는 전송하려는 데이터를 상기 비연결지향성 프로토콜의 최대 전송 단위(MTU, Maximum Transmission Unit)에 맞춰 단편화하며, 상기 단편화된 데이터에 대해 순차적으로 일련번호를 부여하고, 상기 단편화된 데이터를 일련번호에 따라 순차적으로 수신단말로 전송하되, 상기 수신단말의 자동 반복 요청(ARQ, Automatic Repeat Request) 방식의 제어 하에 상기 데이터를 전송할 수 있다.

[0103] 또한, 상기 RLP부(523)는, 상기 수신단말로부터 상기 일련번호에 바탕한 응답신호(Ack, Acknowledgement)를 전달받는 경우 다음 일련번호의 데이터를 전송하고, 상기 응답신호를 일정시간 내에 전달받지 못하는 경우, 해당 일련번호의 데이터를 재전송할 수 있다.

[0104] 여기서, '부'라는 용어는 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미하며, '부'는 어떤 역할들을 수행한다. 그렇지만 '부'는 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. '부'는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.

따라서, 일 예로서 '부'는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 '부'들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 '부'들로 결합되거나 추가적인 구성요소들과 '부'들로 더 분리될 수 있다.

[0105] 또한, 상기 ISP부, DTP부, RLP부 등은 컴퓨터상에서 수행하기 위한 프로그램을 포함하는 컴퓨터 판독가능 저장 매체를 포함할 수 있다. 상기 컴퓨터 판독가능 저장 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들일 수 있다. 컴퓨터 판독가능 저장 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 플롭티컬 디스크와 같은 자기-광 매체 및 롬, 램, 플래시 메모리 등과 같은, 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0106] 이상에서 살펴본 바와 같이, 본 발명의 일 실시예에 따른 비연결지향성 프로토콜을 이용한 데이터통신 방법은 초기설정 과정에서 순서번호를 교환하고, 순서번호와 응답메시지를 이용하여 에러제어 기능을 지원할 수 있다. 이를 통해 데이터의 부분적인 손실을 최소화할 수 있으며, 데이터의 무결성, 기밀성, 인증을 보장할 수 있다. 특히, 본 발명의 일 실시예에 따른 비연결지향성 프로토콜을 이용한 데이터통신 방법은 WAVE(Wireless Access in Vehicular Environments) 통신기술에서 차량 간 통신(vehicle-to-vehicle), 차량과 기반시설(vehicle-to-infrastructure)에 적용 가능하다.

[0107] 이상과 첨부된 도면을 참조하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

## *부호의 설명*

[0108] 110 : APP(Application Layer)

120 : DTLS(Datagram Transport Layer Security)

130 : UDP(User Datagram Protocol)

210 : APP(Application Layer)

220 : ISP(Initial Setup Protocol)

230 : DTP(Data Transfer Protocol)

240 : RLP(Record Layer Protocol)

250 : UDP(User Datagram Protocol)

500 : 송신단말

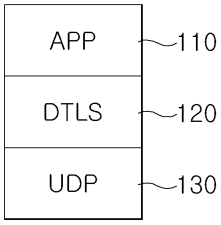
510 : 인터페이스부

520 : 제어부 521 : ISP부

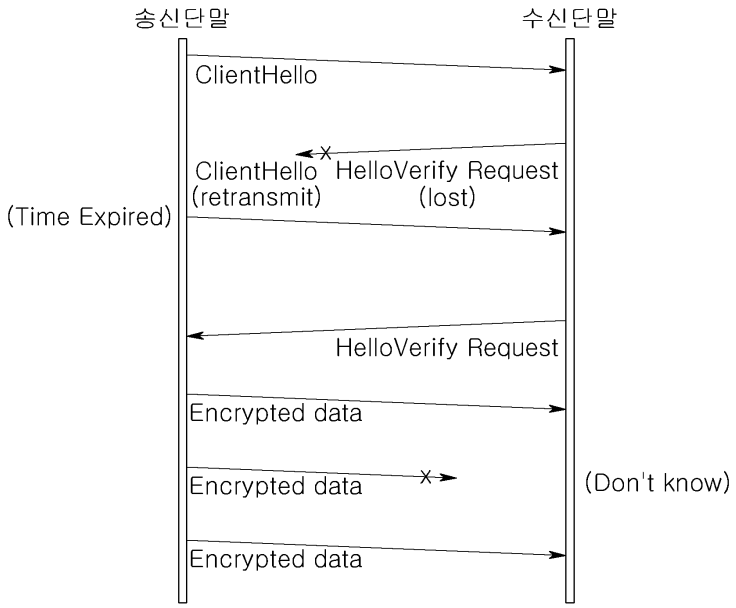
522 : DTP부 523 : RLP부

## 도면

### 도면1

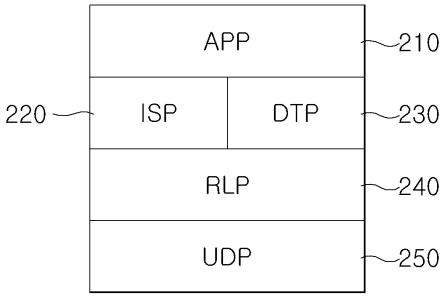

APP
110
DTLS
120
UDP
130

(a)

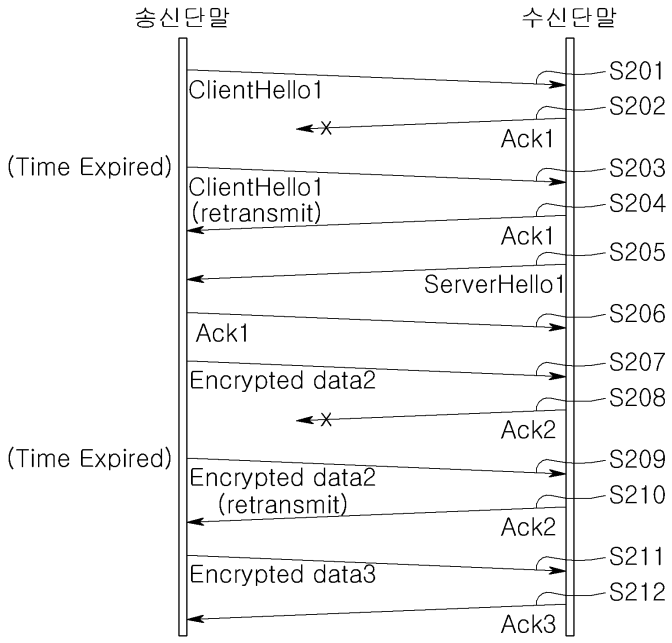

송신단말
수신단말
ClientHello
ClientHello
(retransmit)
HelloVerify Request
(lost)
(Time Expired)
HelloVerify Request
Encrypted data
Encrypted data
(Don't know)
Encrypted data

(b)

도면2

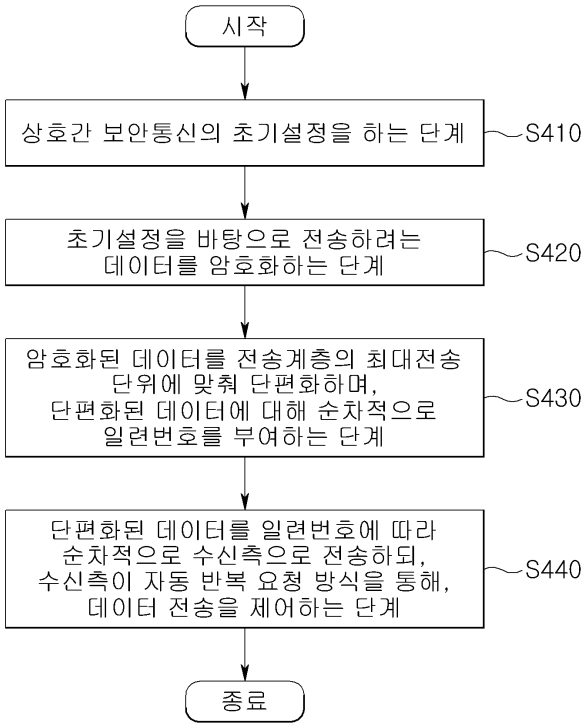

APP
210
220
ISP
DTP
230
RLP
240
UDP
250

(a)

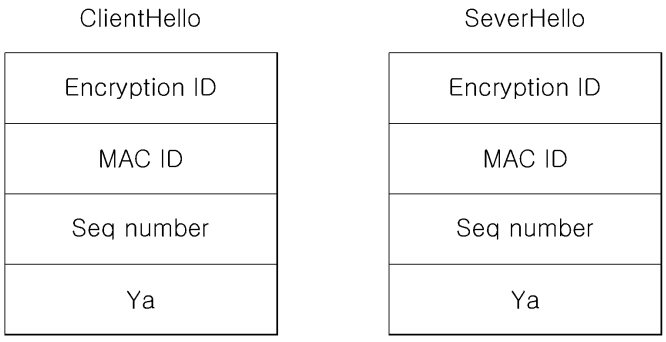

송신단말
수신단말
S201
ClientHello1
S202
Ack1
(Time Expired)
S203
ClientHello1
(retransmit)
S204
Ack1
S205
ServerHello1
S206
Ack1
S207
Encrypted data2
S208
Ack2
(Time Expired)
S209
Encrypted data2
(retransmit)
S210
Ack2
S211
Encrypted data3
S212
Ack3

(b)

도면3


시작
상호간 보안통신의 초기설정을 하는 단계
S410
초기설정을 바탕으로 전송하려는 데이터를 암호화하는 단계
S420
암호화된 데이터를 전송계층의 최대전송 단위에 맞춰 단편화하며, 단편화된 데이터에 대해 순차적으로 일련번호를 부여하는 단계
S430
단편화된 데이터를 일련번호에 따라 순차적으로 수신측으로 전송하되, 수신측이 자동 반복 요청 방식을 통해, 데이터 전송을 제어하는 단계
S440
종료

도면4


ClientHello
Encryption ID
MAC ID
Seq number
Ya
SeverHello
Encryption ID
MAC ID
Seq number
Ya

도면5

