(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0129478
(43) 공개일자 2019년11월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
H04L 9/06 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/0877 (2013.01)
H04L 63/166 (2013.01)
(21) 출원번호 10-2018-0054201
(22) 출원일자 2018년05월11일
심사청구일자 2018년05월11일

(71) 출원인
국민대학교산학협력단
서울특별시 성북구 정릉로 77 (정릉동, 국민대학교)
(72) 발명자
이옥연
경기도 고양시 일산서구 킨텍스로 284, 1905동 101호 (주엽동, 문촌마을19단지아파트)
이재훈
서울특별시 성북구 정릉로10가길 25, 312호(정릉동)
(뒷면에 계속)
(74) 대리인
정부연

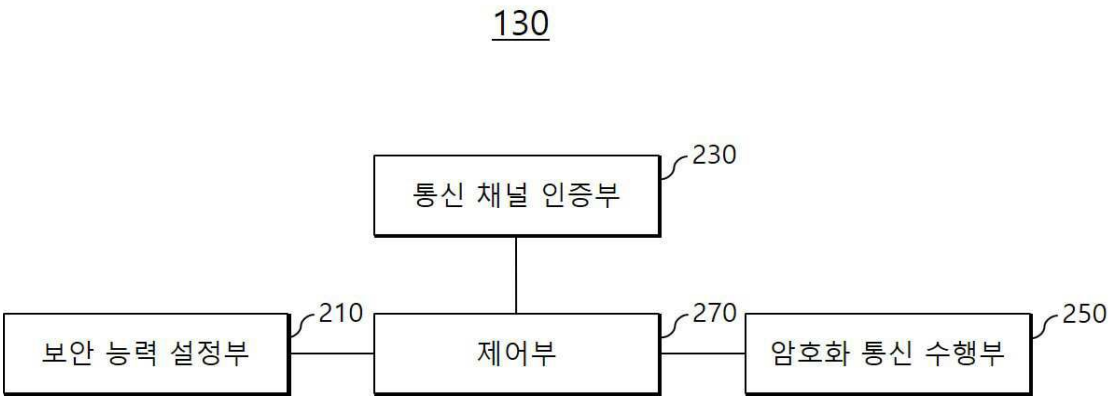
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **SSL/TLS 기반의 네트워크 보안 장치 및 방법**

(57) 요 약

본 발명은 SSL/TLS 기반의 네트워크 보안 장치 및 방법에 관한 것으로, 제1 통신 환경에 따라 채널 암호 수트(Cipher Suite) 집합에 있는 채널 암호 수트를 결정하여 클라이언트의 보안 능력을 설정하는 보안 능력 설정부, 상기 클라이언트에 서버 공개키를 제공하여 상기 클라이언트가 서버 인증을 수행하도록 하고 상기 서버 인증이 성공적으로 수행되면 상기 클라이언트로부터 클라이언트 공개키를 수신하여 상기 클라이언트에 대한 클라이언트 인증을 수행하여, 상호 인증 채널을 생성하는 통신 채널 인증부 및 상기 상호 인증 채널이 생성되면 제2 통신 환경에 따라 데이터 암호 수트 집합에 있는 데이터 암호 수트를 결정하여 상기 상호 인증 채널 상에 통신되는 데이터의 기밀성을 제공하는 암호화 통신 수행부를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/0618 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/3242 (2013.01)
H04L 9/3273 (2013.01)
(72) 발명자
장찬국
서울특별시 성북구 성북로4길 52, 11동 1401호(돈암동, 한신한진아파트)

위한샘
인천광역시 남동구 구월로 192, 1503동 2802호(구월동, 힐스테이트롯데캐슬골드1단지아파트)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711055100
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발
연구과제명 (R&D 바우처) 무선 LTE(4G) 기반 공공 무선망 라우터 운영을 위한 SSL VPN 기술 개발
기 여 율 1/1
주관기관 ㈜ 유비테크
연구기간 2017.04.01 ~ 2018.03.31

명 세 서

청구범위

청구항 1

제1 통신 환경에 따라 채널 암호 수트(Cipher Suite) 집합에 있는 채널 암호 수트를 결정하여 클라이언트의 보안 능력을 설정하는 보안 능력 설정부;

상기 클라이언트에 서버 공개키를 제공하여 상기 클라이언트가 서버 인증을 수행하도록 하고 상기 서버 인증이 성공적으로 수행되면 상기 클라이언트로부터 클라이언트 공개키를 수신하여 상기 클라이언트에 대한 클라이언트 인증을 수행하여, 상호 인증 채널을 생성하는 통신 채널 인증부; 및

상기 상호 인증 채널이 생성되면 제2 통신 환경에 따라 데이터 암호 수트 집합에 있는 데이터 암호 수트를 결정하여 상기 상호 인증 채널 상에 통신되는 데이터의 기밀성을 제공하는 암호화 통신 수행부를 포함하는 SSL/TLS (Secure Socket Layer/Transport Layer Security) 기반의 네트워크 보안 장치.

청구항 2

제1항에 있어서, 상기 보안 능력 설정부는

상기 채널 암호 수트의 보안 강도를 상기 데이터 암호 수트의 보안 강도보다 더 강하게 설정하는 것을 특징으로 하는 SSL/TLS 기반의 네트워크 보안 장치.

청구항 3

제1항에 있어서, 상기 보안 능력 설정부는

상기 제1 통신 환경에 따라 키교환 알고리즘 및 MAC(Message Authentication Code) 알고리즘에 대해 KCMVP(Korea Cryptographic Module Validation Program) 검증필 암호모듈이 적용된 상기 채널 암호 수트를 결정하는 것을 특징으로 하는 SSL/TLS 기반의 네트워크 보안 장치.

청구항 4

제1항에 있어서, 상기 통신 채널 인증부는

상기 서버 인증이 성공적으로 수행된 경우 상기 클라이언트로부터 상기 서버 공개키를 이용하여 암호화된 사전 마스터 비밀(Pre-Master Secret)을 추가로 수신하는 것을 특징으로 하는 SSL/TLS 기반의 네트워크 보안 장치.

청구항 5

제1항에 있어서, 상기 암호화 통신 수행부는

상기 제2 통신 환경에 따라 암호 알고리즘에 대해 KCMVP 검증필 암호모듈이 적용된 상기 데이터 암호 수트를 결정하는 것을 특징으로 하는 SSL/TLS 기반의 네트워크 보안 장치.

청구항 6

제1항에 있어서, 상기 암호화 통신 수행부는

상기 제1 통신 환경 및 상기 제2 통신 환경을 모두 고려하여 상기 데이터 암호 수트를 결정하는 것을 특징으로

하는 SSL/TLS 기반의 네트워크 보안 장치.

청구항 7

제1항에 있어서, 상기 암호화 통신 수행부는

상기 제2 통신 환경에 상관없이 ARIA-128-CBC 및 SHA256으로 구성된 상기 데이터 암호 수트를 결정하여 상기 상호 인증 채널 상에 통신되는 데이터의 기밀성 및 무결성을 제공하는 것을 특징으로 하는 SSL/TLS 기반의 네트워크 보안 장치.

청구항 8

SSL/TLS(Secure Socket Layer/Transport Layer Security) 기반의 네트워크 보안 장치에서 수행되는 네트워크 보안 방법에 있어서,

제1 통신 환경에 따라 채널 암호 수트(Cipher Suite) 집합에 있는 채널 암호 수트를 결정하여 클라이언트의 보안 능력을 설정하는 단계;

상기 클라이언트에 서버 공개키를 제공하여 상기 클라이언트가 서버 인증을 수행하도록 하고 상기 서버 인증이 성공적으로 수행되면 상기 클라이언트로부터 클라이언트 공개키를 수신하여 상기 클라이언트에 대한 클라이언트 인증을 수행하여, 상호 인증 채널을 생성하는 단계; 및

상기 상호 인증 채널이 생성되면 제2 통신 환경에 따라 데이터 암호 수트 집합에 있는 데이터 암호 수트를 결정하여 상기 상호 인증 채널 상에 통신되는 데이터의 기밀성을 제공하는 단계를 포함하는 SSL/TLS 기반의 네트워크 보안 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 SSL/TLS 기반의 네트워크 보안 기술에 관한 것으로, 보다 상세하게는 국내 암호 알고리즘을 IoT 환경을 위한 SSL/TLS에 적용함으로써 보안성을 강화할 수 있는 SSL/TLS 기반의 네트워크 보안 장치 및 방법에 관한 것이다.

배 경 기 술

[0003] 최근 IoT 시장과 산업제어 시스템, 국가기반 시설 등 다양한 분야에서 유/무선 통신을 활용한 통신 환경이 증가함에 따라 공중망에서의 데이터 노출에 대한 위협이 증가하고 있고, 이에 대응하여 안전한 통신환경 구축에 대한 필요성도 함께 증가하고 있다. 이에 대한 보안 대책으로 구간 암호화, SSL VPN 등의 암호 알고리즘을 이용한 통신보안 방법이 있지만, 국가기반시설 등 보안이 매우 중요한 곳에서는 쓰이기 어렵다는 문제점이 존재한다.

[0004] SSL(Secure Socket Layer)은 '보안 소켓 계층'이라는 뜻으로 인터넷을 통해 전달되는 정보 보안의 안전한 거래를 허용하기 위해 Netscape사에서 개발한 인터넷 통신 규약 프로토콜이며, TLS(Transport Layer Security)는 SSL 3.0을 기초로 해서 국제 인터넷 표준화 기구(Internet Engineering Task Force, IETF)가 만든 프로토콜이다. TLS는 SSL 3.0을 보다 안전하게 하고 프로토콜의 스펙을 더 정확하고 안정성 있게 하기 위한 목적으로 고안되었다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국등록특허 제10-0846868(2008.07.10)호

발명의 내용

해결하려는 과제

[0007] 본 발명의 일 실시예는 IoT용 유무선 암호장치에 KCMVP 검증기준을 만족하는 국내 암호 알고리즘을 SSL/TLS에 적용함으로써 보안성을 강화할 수 있는 SSL/TLS 기반의 네트워크 보안 장치 및 방법을 제공하고자 한다.

[0008] 본 발명의 일 실시예는 클라이언트와의 통신 환경에 맞춰 보안 강도를 자동으로 조절함으로써 데이터 기밀성 및 무결성, 난수발생, 메시지 인증, 키 설정, 전자서명을 제공할 수 있는 SSL/TLS 기반의 네트워크 보안 장치 및 방법을 제공하고자 한다.

[0009] 본 발명의 일 실시예는 국내 암호 알고리즘을 적용함으로써 KCMVP 암호모듈을 활용하여 정보보호 제품 개발이 가능한 SSL/TLS 기반의 네트워크 보안 장치 및 방법을 제공하고자 한다.

과제의 해결 수단

[0011] 실시예들 중에서, SSL/TLS (Secure Socket Layer/Transport Layer Security) 기반의 네트워크 보안 장치는 제1 통신 환경에 따라 채널 암호 수트(Cipher Suite) 집합에 있는 채널 암호 수트를 결정하여 클라이언트의 보안 능력을 설정하는 보안 능력 설정부, 상기 클라이언트에 서버 공개키를 제공하여 상기 클라이언트가 서버 인증을 수행하도록 하고 상기 서버 인증이 성공적으로 수행되면 상기 클라이언트로부터 클라이언트 공개키를 수신하여 상기 클라이언트에 대한 클라이언트 인증을 수행하여, 상호 인증 채널을 생성하는 통신 채널 인증부 및 상기 상호 인증 채널이 생성되면 제2 통신 환경에 따라 데이터 암호 수트 집합에 있는 데이터 암호 수트를 결정하여 상기 상호 인증 채널 상에 통신되는 데이터의 기밀성을 제공하는 암호화 통신 수행부를 포함한다.

[0012] 상기 보안 능력 설정부는 상기 채널 암호 수트의 보안 강도를 상기 데이터 암호 수트의 보안 강도보다 더 강하게 설정할 수 있다.

[0013] 상기 보안 능력 설정부는 상기 제1 통신 환경에 따라 키교환 알고리즘 및 MAC 알고리즘에 대해 KCMVP(Korea Cryptographic Module Validation Program) 검증필 암호모듈이 적용된 상기 채널 암호 수트를 결정할 수 있다.

[0014] 상기 통신 채널 인증부는 상기 서버 인증이 성공적으로 수행된 경우 상기 클라이언트로부터 상기 서버 공개키를 이용하여 암호화된 사전 마스터 비밀(Pre-Master Secret)을 추가로 수신할 수 있다.

[0015] 상기 암호화 통신 수행부는 상기 제2 통신 환경에 따라 암호 알고리즘에 대해 KCMVP 검증필 암호모듈이 적용된 상기 데이터 암호 수트를 결정할 수 있다.

[0016] 상기 암호화 통신 수행부는 상기 제1 통신 환경 및 상기 제2 통신 환경을 모두 고려하여 상기 데이터 암호 수트를 결정할 수 있다.

[0017] 상기 암호화 통신 수행부는 상기 제2 통신 환경에 상관없이 ARIA-128-CBC 및 SHA256으로 구성된 상기 데이터 암호 수트를 결정하여 상기 상호 인증 채널 상에 통신되는 데이터의 기밀성 및 무결성을 제공할 수 있다.

[0018] 실시예들 중에서, SSL/TLS 기반의 네트워크 보안 방법은 제1 통신 환경에 따라 채널 암호 수트(Cipher Suite) 집합에 있는 채널 암호 수트를 결정하여 클라이언트의 보안 능력을 설정하는 단계, 상기 클라이언트에 서버 공개키를 제공하여 상기 클라이언트가 서버 인증을 수행하도록 하고 상기 서버 인증이 성공적으로 수행되면 상기 클라이언트로부터 클라이언트 공개키를 수신하여 상기 클라이언트에 대한 클라이언트 인증을 수행하여, 상호 인증 채널을 생성하는 단계 및 상기 상호 인증 채널이 생성되면 제2 통신 환경에 따라 데이터 암호 수트 집합에 있는 데이터 암호 수트를 결정하여 상기 상호 인증 채널 상에 통신되는 데이터의 기밀성을 제공하는 단계를 포함한다.

발명의 효과

[0020] 개시된 기술은 다음의 효과를 가질 수 있다. 다만, 특정 실시예가 다음의 효과를 전부 포함하여야 한다거나 다음의 효과만을 포함하여야 한다는 의미는 아니므로, 개시된 기술의 권리범위는 이에 의하여 제한되는 것으로 이해되어서는 아니 될 것이다.

[0021] 본 발명의 일 실시예에 따른 IoT용 유무선 암호장치에 KCMVP 검증기준을 만족하는 SSL/TLS 기반의 네트워크 보안 장치 및 방법은 클라이언트와의 통신 환경에 맞춰 보안 강도를 자동으로 조절함으로써 데이터 기밀성 및 무결성, 난수발생, 메시지 인증, 키 설정, 전자서명을 제공할 수 있다.

[0022] 본 발명의 일 실시예에 따른 SSL/TLS 기반의 네트워크 보안 장치 및 방법은 국내 암호 알고리즘을 적용함으로써 KCMVP 암호모듈을 활용하여 정보보호 제품 개발이 가능할 수 있다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 일 실시예에 따른 SSL/TLS 기반의 네트워크 보안 시스템을 설명하는 도면이다.

도 2는 도 1에 있는 네트워크 보안 장치를 설명하는 블록도이다.

도 3은 도 1에 있는 네트워크 보안 장치에서 수행되는 네트워크 보안 과정을 설명하는 순서도이다.

도 4는 SSL/TLS의 핸드쉐이크 세부 4단계를 설명하는 도면이다.

도 5 내지 8은 핸드쉐이크 단계를 구성하는 각 단계를 설명하는 도면이다.

도 9는 도 1에 있는 네트워크 보안 장치에서 사용하는 암호 수트를 설명하는 예시도이다.

도 10은 도 1에 있는 네트워크 보안 장치에서 사용하는 데이터 암호 수트를 설명하는 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 발명에 관한 설명은 구조적 내지 기능적 설명을 위한 실시예에 불과하므로, 본 발명의 권리범위는 본문에 설명된 실시예에 의하여 제한되는 것으로 해석되어서는 아니 된다. 즉, 실시예는 다양한 변경이 가능하고 여러 가지 형태를 가질 수 있으므로 본 발명의 권리범위는 기술적 사상을 실현할 수 있는 균등물들을 포함하는 것으로 이해되어야 한다. 또한, 본 발명에서 제시된 목적 또는 효과는 특정 실시예가 이를 전부 포함하여야 한다거나 그러한 효과만을 포함하여야 한다는 의미는 아니므로, 본 발명의 권리범위는 이에 의하여 제한되는 것으로 이해되어서는 아니 될 것이다.

[0026] 한편, 본 출원에서 서술되는 용어의 의미는 다음과 같이 이해되어야 할 것이다.

[0027] "제1", "제2" 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하기 위한 것으로, 이들 용어들에 의해 권리범위가 한정되어서는 아니 된다. 예를 들어, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

[0028] 어떤 구성요소가 다른 구성요소에 "연결되어"있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결될 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어"있다고 언급된 때에는 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 한편, 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0029] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함하다" 또는 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이며, 하나 또는 그 이상의 다른 특징이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0030] 각 단계들에 있어 식별부호(예를 들어, a, b, c 등)는 설명의 편의를 위하여 사용되는 것으로 식별부호는 각 단계들의 순서를 설명하는 것이 아니며, 각 단계들은 문맥상 명백하게 특정 순서를 기재하지 않는 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 단계들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0031] 본 발명은 컴퓨터가 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현될 수 있고, 컴퓨터가 읽을

수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 데이터 저장 장치, 플래시 메모리 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0032] 여기서 사용되는 모든 용어들은 다르게 정의되지 않는 한, 본 발명이 속하는 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한 이상적이거나 과도하게 형식적인 의미를 지니는 것으로 해석될 수 없다.

[0034] SSL VPN은 SSL/TLS 표준보안 프로토콜을 활용한 가상사설망 제품으로써 안전한 통신환경을 제공해 주며, 네트워크 환경에서 식별가능한 개체에 대해 인증 및 식별을 수행함으로써 접근제어통제 기능도 함께 제공할 수 있다. SSL/TLS 표준보안 프로토콜은 네트워크 연결시 상대에 대한 신원을 확인하고 올바른 사용자 또는 개체임을 확인함으로써 통신 연결에 대한 신뢰성을 확보할 수 있다. SSL/TLS 표준보안 프로토콜은 정당하게 공유하고 있는 보안매체를 활용하여 키교환 및 키 일치과정을 거쳐 보안통신에 사용되는 키를 발급할 수 있다. SSL VPN은 이렇게 발급된 키를 사용하여 데이터의 기밀성 및 무결성, 난수발생, 메시지 인증, 키 설정, 전자서명을 제공할 수 있다.

[0035] SSL/TLS 표준보안 프로토콜에서 보안통신에 사용되는 키를 발급하는 과정은 SSL/TLS의 핸드쉐이크(Handshake) 단계로서 내부적으로 4개의 세부단계로 구성될 수 있다. 핸드쉐이크 단계는 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유 키를 결정하고 인증서를 상호 교환하기 위한 과정에 해당할 수 있다. 여기에서, 공유 키를 결정하는 것은 암호 통신을 수행하기 위한 것이고, 인증서를 교환하는 것은 서로 상대를 인증하기 위한 것일 수 있다. 핸드쉐이크 단계는 다음의 도 4 내지 도 8과 함께 보다 자세히 설명한다.

[0037] 도 4는 SSL/TLS의 핸드쉐이크 세부 4단계를 설명하는 도면이다.

[0038] 도 4를 참조하면, SSL/TLS의 핸드쉐이크(Handshake) 단계는 내부적으로 4개의 세부단계로 구성될 수 있다. 핸드쉐이크 단계는 제1 단계(Phase I)에서 보안 능력을 설정하고, 제2 단계(Phase II)에서 서버 인증 및 키교환을 수행할 수 있다. 또한, 핸드쉐이크 단계는 제3 단계(Phase III)에서 클라이언트 인증 및 키교환을 수행하고, 제4 단계(Phase IV)에서 핸드쉐이크 프로토콜을 종료할 수 있다.

[0040] 도 5 내지 8은 핸드쉐이크 단계를 구성하는 각 단계를 설명하는 도면이다.

[0041] 도 5를 참조하면, 핸드쉐이크 제1 단계에서 클라이언트는 서버에게 ClientHello 메시지를 전송할 수 있고, 서버는 ClientHello 메시지에 대응하여 클라이언트에게 ServerHello 메시지를 전송할 수 있다. ClientHello 및 ServerHello 메시지는 세션 ID, 키교환 알고리즘, MAC 알고리즘, 암호 알고리즘 및 초기 random number 등을 포함할 수 있다.

[0042] 보다 구체적으로, 클라이언트는 서버에게 사용가능한 버전 정보, 클라이언트 난수, 세션 ID, 사용가능한 암호 수트 목록, 사용가능한 압축 방법 목록 등을 포함하는 ClientHello 메시지를 전송할 수 있다. 서버는 클라이언트에게 사용하는 버전 정보, 서버 난수, 세션 ID, 사용하는 암호 수트, 사용하는 압축 방법 등을 포함하는 ServerHello 메시지를 전송할 수 있다.

[0044] 도 6을 참조하면, 핸드쉐이크 제2 단계에서 서버는 클라이언트에게 Certificate, ServerKeyExchange, CertificateRequest 및 ServerHelloDone 메시지를 차례대로 전송할 수 있다. Certificate 메시지는 서버의 인증서를 포함할 수 있고, ServerKeyExchange 메시지는 서버의 공개키를 포함할 수 있다. CertificateRequest 메시지는 서버가 이해할 수 있는 인증서 타입 목록이나 인증기관 이름 목록을 포함할 수 있다. 서버의 인증서는 인증 기관에서 발급받은 것이며, 서버가 신뢰할 수 있음을 인증하기 위한 용도로 사용될 수 있다.

[0046] 도 7을 참조하면, 핸드쉐이크 제3 단계에서 클라이언트는 서버에게 Certificate, ClientKeyExchange 및 CertificateVerify 메시지를 차례대로 전송할 수 있다. Certificate 메시지는 클라이언트의 인증서를 포함할 수 있고, ClientKeyExchange 메시지는 클라이언트의 공개키를 포함할 수 있다. CertificateVerify 메시지는 서버의 인증서를 검증한 결과를 포함할 수 있다.

[0047] 보다 구체적으로, 클라이언트는 서버로부터 수신한 Certificate 메시지에서 서버의 인증서를 획득할 수 있고, 해당 인증서가 유효 기간이 만료된 것인지, 신뢰할 수 있는 인증 기관에서 발급된 것인지, 해당 서버에서 정식으로 발급된 인증서에 해당하는지 등을 확인함으로써 서버의 인증서를 검증할 수 있다. 예를 들어, 클라이언트는 자체적으로 보관하고 있는 신뢰할 수 있는 인증 기관의 공개키를 이용하여 서버의 인증서에 부가되어 있는 전자서명을 검증함으로써 인증서 검증을 수행할 수 있다. 클라이언트는 서버의 인증서가 신뢰할 수 있는 것으로 판단한 경우 서버에 CertificateVerify 메시지를 전송하여 알릴 수 있다.

[0049] 도 8을 참조하면, 핸드쉐이크 제4 단계에서 클라이언트는 서버에게 ChangeCipherSpec 및 Finished 메시지를 차례로 전송할 수 있고, 서버는 이에 대한 응답으로 ChangeCipherSpec 및 Finished 메시지를 전송할 수 있다. ChangeCipherSpec 메시지는 암호화 방식이 변경되었으며 이후 전송되는 것들은 협상한 CipherSpec와 키값에 의해 암호/해시되어 전송됨을 알리는 메시지이고, Finished 메시지는 핸드쉐이크 과정이 끝났음을 알리는 메시지이다.

[0050] 보다 구체적으로, 클라이언트는 서버에게 ChangeCipherSpec 메시지를 전송하여 클라이언트에서 허용될 수 있는 Cipherspec을 알릴 수 있고, 서버는 클라이언트가 전송한 Cipherspec에서 서버가 허용하는 Cipherspec을 ChangeCipherSpec 메시지에 포함시켜 클라이언트에 전송할 수 있다. 클라이언트 및 서버는 마지막으로 Finished 메시지를 전송하여 핸드쉐이크 과정이 끝났음을 알릴 수 있다.

[0052] 도 1은 본 발명의 일 실시예에 따른 SSL/TLS 기반의 네트워크 보안 시스템을 설명하는 도면이다.

[0053] 도 1을 참조하면, SSL/TLS 기반의 네트워크 보안 시스템(100)은 클라이언트(110), 네트워크 보안 장치(130) 및 데이터베이스(150)를 포함할 수 있다.

[0054] 클라이언트(110)는 통신 채널을 통해 네트워크 보안 장치(130)와 통신을 수행하는 컴퓨팅 장치에 해당하고, 스마트폰, 노트북 또는 컴퓨터로 구현될 수 있으며, 반드시 이에 한정되지 않고, 태블릿 PC 등 다양한 디바이스로도 구현될 수 있다. 클라이언트(110)는 네트워크 보안 장치(130)와 네트워크를 통해 연결될 수 있고, 적어도 하나의 클라이언트(110)는 네트워크 보안 장치(130)와 동시에 연결될 수 있다.

[0055] 네트워크 보안 장치(130)는 클라이언트(110)와의 통신을 위하여 데이터의 기밀성 및 무결성을 제공하는 통신 채널을 생성할 수 있는 컴퓨터 또는 프로그램에 해당하는 서버로 구현될 수 있다. 네트워크 보안 장치(130)는 클라이언트(110)와 블루투스, WiFi, LTE, Ethernet 등을 통해 무선으로 연결될 수 있고, 네트워크를 통해 클라이언트(110)와 데이터를 주고 받을 수 있다.

[0056] 네트워크 보안 장치(130)는 데이터베이스(150)를 포함하여 구현될 수 있고, 데이터베이스(150)와 별도로 구현될 수 있다. 데이터베이스(150)와 별도로 구현된 경우 네트워크 보안 장치(130)는 데이터베이스(150)와 연결되어 데이터를 송수신할 수 있다.

[0057] 데이터베이스(150)는 네트워크 보안 장치(130)가 클라이언트(110)와의 통신 채널을 생성하기 위해서 사용하는 다양한 정보들을 저장할 수 있다. 예를 들어, 데이터베이스(150)는 클라이언트(110) 및 네트워크 보안 장치(130) 간의 상호 인증을 위하여 서로 주고 받는 인증 데이터를 저장할 수 있고, 통신 보안을 위하여 사용하는 암호 알고리즘 및 설정 정보를 저장할 수 있으며, 반드시 이에 한정되지 않고, 클라이언트(110) 및 네트워크 보안 장치(130) 간의 통신 채널을 생성하는 과정에서 다양한 형태로 수집 또는 가공된 정보들을 저장할 수 있다.

[0058] 데이터베이스(150)는 특정 범위에 속하는 정보들을 저장하는 적어도 하나의 독립된 서브-데이터베이스들로 구성될 수 있고, 적어도 하나의 독립된 서브-데이터베이스들이 하나로 통합된 통합 데이터베이스로 구성될 수 있다. 적어도 하나의 독립된 서브-데이터베이스들로 구성되는 경우에는 각각의 서브-데이터베이스들은 블루투스, WiFi, LTE 등을 통해 무선으로 연결될 수 있고, Ethernet 등의 유선 네트워크를 통해 상호 간의 데이터를 주고 받을 수 있다. 통합 데이터베이스로 구성되는 경우에는 각각의 서브-데이터베이스들을 하나로 통합하고 상호 간

의 데이터 교환 및 제어 흐름을 관리하는 제어부를 포함할 수 있다.

[0060] 도 2는 도 1에 있는 네트워크 보안 장치를 설명하는 블록도이다.

[0061] 도 2를 참조하면, 네트워크 보안 장치(130)는 보안 능력 설정부(210), 통신 채널 인증부(230), 암호화 통신 수행부(250) 및 제어부(270)를 포함할 수 있다.

[0062] 보안 능력 설정부(210)는 제1 통신 환경에 따라 채널 암호 수트(Cipher Suite) 집합에 있는 채널 암호 수트를 결정하여 클라이언트(110)의 보안 능력을 설정할 수 있다. 여기에서, 채널 암호 수트는 클라이언트(110)와 네트워크 보안 장치(130) 간의 상호 인증을 수행하는 과정에서 사용되는 키교환 알고리즘 및 MAC 알고리즘의 추천 세트에 해당할 수 있고, 채널 암호 수트 집합은 보안 능력 설정부(210)에서 선택 가능한 다양한 채널 암호 수트들을 모아 놓은 것에 해당할 수 있다.

[0063] 제1 통신 환경은 클라이언트(110) 및 네트워크 보안 장치(130) 간의 무선 통신 품질에 영향을 줄 수 있는 외부 요소로서 무선 통신 채널과 직접 관련 있는 요소에 해당할 수 있고, 예를 들어, 클라이언트(110) 및 네트워크 보안 장치(130) 간의 거리, 무선 통신의 종류 및 통신 신호의 세기 등을 포함할 수 있다. 보안 능력 설정부(210)는 제1 통신 환경에 가장 적합한 채널 암호 수트를 결정하여 클라이언트(110)의 보안 능력을 설정할 수 있다. 다른 실시예에서, 보안 능력 설정부(210)는 제1 통신 환경에 상관없이 클라이언트(110)에서 요청하는 채널 암호 수트로 해당 클라이언트(110)의 보안 능력을 설정할 수 있다.

[0064] 일 실시예에서, 보안 능력 설정부(210)는 채널 암호 수트의 보안 강도를 데이터 암호 수트의 보안 강도보다 더 강하게 설정할 수 있다. 보안 능력 설정부(210)는 클라이언트(110) 및 네트워크 보안 장치(130) 간의 통신 채널 생성 과정이 데이터 전송 과정보다 상대적으로 보안에 더 취약한 점을 고려하여 통신 채널 생성 과정에서 사용되는 채널 암호 수트의 보안 강도를 데이터 암호 수트의 보안 강도보다 더 강하게 설정할 수 있다. 보안 능력 설정부(210)는 보안 강도가 일정 수준 이상인 알고리즘으로만 구성된 채널 암호 수트들 중에서 어느 하나를 선택함으로써 암호 수트의 보안 강도를 설정할 수 있다.

[0065] 일 실시예에서, 보안 능력 설정부(210)는 제1 통신 환경에 따라 키교환 알고리즘 및 MAC(Message Authentication Code) 알고리즘에 대해 KCMVP(Korea Cryptographic Module Validation Program) 검증필 암호모듈이 적용된 채널 암호 수트를 결정할 수 있다. 여기에서, KCMVP는 한국 암호모듈 검증제도에 해당하고 국가 및 공공기관에 도입되는 상용 보안제품에 대한 안전성을 확보하기 위해 국가정보원에 의해 시행되고 있다.

[0066] 보안 능력 설정부(210)는 채널 암호 수트 집합에서 KCMVP 검증을 통과한 키교환 알고리즘 및 MAC 알고리즘을 포함하여 구성된 채널 암호 수트를 결정함으로써 클라이언트(110) 및 네트워크 보안 장치(130) 간의 통신 채널 생성에 있어서 보안 강도를 강화할 수 있다. 예를 들어, 보안 능력 설정부(210)는 KCMVP 검증필 암호모듈에서 제공하는 공개키 기반의 암호 알고리즘인 RSA 및 ECDSA 중 적어도 하나를 포함하여 구성된 암호 수트를 채널 암호 수트로서 결정할 수 있다.

[0067] 통신 채널 인증부(230)는 클라이언트(110)에 서버 공개키를 제공하여 클라이언트(110)가 서버 인증을 수행하도록 하고 서버 인증이 성공적으로 수행되면 클라이언트(110)로부터 클라이언트 공개키를 수신하여 클라이언트(110)에 대한 클라이언트 인증을 수행하여, 상호 인증 채널을 생성할 수 있다. 여기에서, 서버는 네트워크 보안 장치(130)에 해당할 수 있다.

[0068] 클라이언트(110)는 통신 채널 인증부(230)로부터 제공받은 서버 공개키와 서버 인증서를 이용하여 서버 인증을 수행할 수 있다. 보다 구체적으로, 클라이언트(110)는 서버 공개키와 서버 인증서가 신뢰할 수 있는 것인지 확인함으로써 서버 인증을 수행할 수 있다. 예를 들어, 클라이언트(110)는 신뢰할 수 있는 인증기관 목록을 자체적으로 보관할 수 있고, 통신 채널 인증부(230)로부터 제공받은 서버 공개키와 서버 인증서가 신뢰할 수 있는 인증기관에서 발행된 것인지, 유효 기간이 만료되지 않았는지 등을 확인하여 서버 인증을 수행할 수 있다.

[0069] 클라이언트(110)에서의 서버 인증이 성공적으로 수행된 경우 통신 채널 인증부(230)는 클라이언트(110)로부터 클라이언트 공개키를 수신하여 클라이언트 인증을 수행할 수 있다. 보다 구체적으로, 통신 채널 인증부(230)는 클라이언트 공개키와 클라이언트 인증서가 신뢰할 수 있는 것인지 확인함으로써 클라이언트 인증을 수행할 수 있다.

[0070] 일 실시예에서, 통신 채널 인증부(230)는 서버 인증이 성공적으로 수행된 경우 클라이언트(110)로부터 서버 공개키를 이용하여 암호화된 사전 마스터 비밀(Pre-Master Secret)을 추가로 수신할 수 있다. 여기에서, 사전 마

스터 비밀(Pre-Master Secret)은 클라이언트(110)가 만든 난수에 해당할 수 있고, 마스터 비밀(Master Secret)을 생성하는데 사용될 수 있다. 예를 들어, 서버 및 클라이언트(110)는 사전 마스터 비밀, 클라이언트 난수 및 서버 난수를 이용하여 마스터 비밀을 각각 생성할 수 있다.

[0071] 마스터 비밀(Master Secret)은 클라이언트(110)와 서버가 합의한 비밀값에 해당할 수 있고, 통신의 기밀성을 보장하는데 사용될 수 있다. 마스터 비밀은 클라이언트(110)와 서버 간의 통신 암호화에 사용되는 세션키를 생성하는데 사용될 수 있다. 예를 들어, 마스터 비밀은 대칭 암호키, 메시지 인증 코드키 및 대칭 암호 CBC 모드에서 이용하는 초기화 벡터를 생성하는데 사용될 수 있다.

[0072] 클라이언트(110)는 임의의 사전 마스터 비밀을 생성할 수 있고 서버 공개키를 이용하여 사전 마스터 비밀을 암호화할 수 있다. 또한, 클라이언트(110)는 사전 마스터 비밀을 ClientKeyExchange 메시지에 포함시켜 네트워크 보안 장치(130)로 전송할 수 있다. 통신 채널 인증부(230)는 전송받은 정보를 복호화하여 사전 마스터 비밀을 획득할 수 있고, 사전 마스터 비밀을 이용하여 마스터 비밀을 생성할 수 있다.

[0073] 암호화 통신 수행부(250)는 상호 인증 채널이 생성되면 제2 통신 환경에 따라 데이터 암호 수트 집합에 있는 데이터 암호 수트를 결정하여 상호 인증 채널 상에 통신되는 데이터의 기밀성을 제공할 수 있다. 클라이언트(110) 및 네트워크 보안 장치(130) 간의 상호 인증이 완료된 경우, 클라이언트(110)와 네트워크 보안 장치(130)는 동일한 세션키를 공유할 수 있고, 암호화 통신 수행부(250)는 세션키를 이용하여 데이터를 암호화하거나 또는 복호화할 수 있다.

[0074] 여기에서, 데이터 암호 수트는 클라이언트(110)와 네트워크 보안 장치(130) 간의 데이터 전송 과정에서 사용되는 암호 알고리즘의 추천 세트에 해당할 수 있고, 데이터 암호 수트 집합은 암호화 통신 수행부(250)에서 선택 가능한 다양한 데이터 암호 수트들을 모아 놓은 것에 해당할 수 있다. 제2 통신 환경은 무선 통신 품질에 영향을 줄 수 있는 외부 요소로서 클라이언트(110)와 직접 관련 있는 요소에 해당할 수 있고, 예를 들어, 클라이언트(110)의 성능, 호환성 및 중요성 등을 포함할 수 있다.

[0075] 암호화 통신 수행부(250)는 제2 통신 환경에 가장 적합한 데이터 암호 수트를 결정할 수 있고 데이터 암호 수트에 포함된 암호 알고리즘 및 세션키를 이용하여 데이터를 암호화하거나 또는 복호화함으로써 데이터의 기밀성을 제공할 수 있다. 다른 실시예에서, 암호화 통신 수행부(250)는 제2 통신 환경에 상관없이 클라이언트(110)에서 요청하는 데이터 암호 수트를 결정하여 상호 인증 채널 상에 통신되는 데이터의 기밀성을 제공할 수 있다.

[0076] 일 실시예에서, 암호화 통신 수행부(250)는 제2 통신 환경에 따라 암호 알고리즘에 대해 KCMVP 검증필 암호모듈이 적용된 데이터 암호 수트를 결정할 수 있다. 암호화 통신 수행부(250)는 데이터 암호 수트 집합에서 KCMVP 검증을 통과한 암호 알고리즘을 포함하여 구성된 데이터 암호 수트를 결정함으로써 클라이언트(110) 및 네트워크 보안 장치(130) 간의 데이터 교환에 있어서 보안 강도를 강화할 수 있다. 예를 들어, 암호화 통신 수행부(250)는 KCMVP 검증필 암호모듈에서 제공하는 국내 암호 알고리즘인 ARIA, SEED, HiGHT 및 LEA 중 적어도 하나를 포함하여 구성된 암호 수트를 데이터 암호 수트로서 결정할 수 있다.

[0077] 일 실시예에서, 암호화 통신 수행부(250)는 제1 통신 환경 및 제2 통신 환경을 모두 고려하여 데이터 암호 수트를 결정할 수 있다. 보다 구체적으로, 암호화 통신 수행부(250)는 클라이언트(110) 및 네트워크 보안 장치(130) 간의 거리, 무선 통신의 종류, 통신 신호의 세기, 클라이언트(110)의 성능, 호환성 및 중요성 중 적어도 하나를 고려하여 데이터 암호 수트를 결정함으로써 무선 통신의 보안 강도를 조절할 수 있다.

[0078] 일 실시예에서, 암호화 통신 수행부(250)는 제1 통신 환경 및 제2 통신 환경 각각에 가중치를 부여하고 가중화된 제1 통신 환경 및 제2 통신 환경에 따라 데이터 암호 수트를 결정할 수 있다. 예를 들어, 암호화 통신 수행부(250)는 제1 통신 환경에 포함된 요소들에 2의 가중치를 부여하고, 제2 통신 환경에 포함된 요소들에 0.5의 가중치를 부여한 후, 각각의 요소들에 의해 결정되는 전체 통신 환경을 고려하여 데이터 통신에 요구되는 보안 강도를 결정할 수 있고, 해당 보안 강도를 충족하는 데이터 암호 수트를 결정할 수 있다.

[0079] 일 실시예에서, 암호화 통신 수행부(250)는 제2 통신 환경에 상관없이 ARIA-128-CBC 및 SHA256으로 구성된 데이터 암호 수트를 결정하여 상호 인증 채널 상에 통신되는 데이터의 기밀성 및 무결성을 제공할 수 있다. 암호화 통신 수행부(250)는 클라이언트(110) 및 네트워크 보안 장치(130) 간의 상호 인증 채널이 생성된 후 제2 통신 환경을 고려하여 적절한 데이터 암호 수트를 결정할 수도 있지만, 제2 통신 환경을 고려하기 힘들거나 또는 불가능한 경우에 있어서 미리 결정된 데이터 암호 수트를 사용할 수 있다. 암호화 통신 수행부(250)는 128비트 키 길이와 CBC 운영모드로 설정된 ARIA 및 해시함수인 SHA256으로 구성된 데이터 암호 수트를 기본 설정으로 제공하여 별도의 설정이 없더라도 보안 강도가 낮은 암호 알고리즘이 사용되지 않도록 할 수 있다.

[0080] 제어부(270)는 네트워크 보안 장치(130)의 전체적인 동작을 제어하고, 보안 능력 설정부(210), 통신 채널 인증부(230) 및 암호화 통신 수행부(250) 간의 제어 흐름 또는 데이터 흐름을 관리할 수 있다.

[0082] 도 3은 도 1에 있는 네트워크 보안 장치에서 수행되는 네트워크 보안 과정을 설명하는 순서도이다.

[0083] 도 3을 참조하면, 네트워크 보안 장치(130)는 보안 능력 설정부(210)를 통해 제1 통신 환경에 따라 채널 암호 수트 집합에 있는 채널 암호 수트를 결정하여 클라이언트(110)의 보안 능력을 설정할 수 있다(단계 S310).

[0084] 네트워크 보안 장치(130)는 통신 채널 인증부(230)를 통해 클라이언트(110)에 서버 공개키를 제공하여 클라이언트(110)가 서버 인증을 수행하도록 하고 서버 인증이 성공적으로 수행되면 클라이언트(110)로부터 클라이언트 공개키를 수신하여 클라이언트(110)에 대한 클라이언트 인증을 수행하여, 상호 인증 채널을 생성할 수 있다(단계 S330).

[0085] 네트워크 보안 장치(130)는 암호화 통신 수행부(250)를 통해 상호 인증 채널이 생성되면 제2 통신 환경에 따라 데이터 암호 수트 집합에 있는 데이터 암호 수트를 결정하여 상호 인증 채널 상에 통신되는 데이터의 기밀성을 제공할 수 있다(단계 S350).

[0087] 도 9는 도 1에 있는 네트워크 보안 장치에서 사용하는 암호 수트를 설명하는 예시도이다.

[0088] 도 9를 참조하면, 네트워크 보안 장치(130)는 핸드쉐이크 과정에서 사용하는 키교환 알고리즘, MAC 알고리즘 및 암호 알고리즘, 전자서명 알고리즘 등을 부품과 같이 교환할 수 있다. 보다 구체적으로, 네트워크 보안 장치(130)는 사용하고 있던 암호 알고리즘에 결함이 발견된 경우 해당 암호 알고리즘을 다른 암호 알고리즘으로 교체하여 사용할 수 있다. 네트워크 보안 장치(130)는 핸드쉐이크 과정에서 사용하는 암호 기술들의 추천 세트를 암호 수트로 정의하여 사용할 수 있고, 도 9에서는 KCMVP 검증필 암호들로 구성된 암호 수트의 일 실시예가 표시되어 있다.

[0090] 도 10은 도 1에 있는 네트워크 보안 장치에서 사용하는 데이터 암호 수트를 설명하는 예시도이다.

[0091] 도 10을 참조하면, 네트워크 보안 장치(130)는 클라이언트(110)와의 상호 인증 채널이 생성된 후 데이터의 기밀성 및 무결성을 제공하기 위하여 블록 암호 알고리즘을 사용할 수 있다. 네트워크 보안 장치(130)는 블록 암호 알고리즘으로서 KCMVP 검증필 암호모듈에서 제공하는 국내 암호 알고리즘 ARIA, SEED, HiGHT, LEA를 사용할 수 있다. 특히, 네트워크 보안 장치(130)는 블록 암호 알고리즘 중 하나인 SEED에 대하여 SSL에서 제공하는 암호 알고리즘이 아닌, KCMVP 검증필 암호 모듈에서 제공하는 암호 알고리즘을 사용할 수 있다.

[0092] 또한, 네트워크 보안 장치(130)는 핸드쉐이크의 모든 단계에서 사용되는 해시함수로서 KCMVP 검증필 암호모듈에서 제공하는 해시함수를 사용할 수 있다. 도 10에서, 네트워크 보안 장치(130)는 데이터 기밀성을 위해 블록암호 알고리즘으로서 ARIA, SEED, HiGHT 및 LEA 중 어느 하나를 사용할 수 있고, 운영모드로서 ECB, CBC 및 GCM 중 어느 하나를 사용할 수 있다. 네트워크 보안 장치(130)는 해시함수로서 SHA256를 사용할 수 있다.

[0094] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0096] 100: SSL/TLS 기반의 네트워크 보안 시스템

110: 클라이언트 130: 네트워크 보안 장치

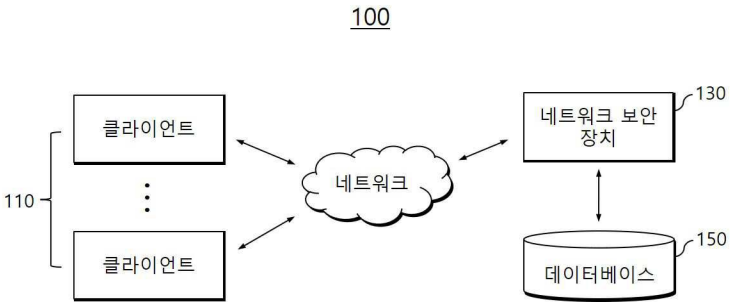
150: 데이터베이스

210: 보안 능력 설정부 230: 통신 채널 인증부

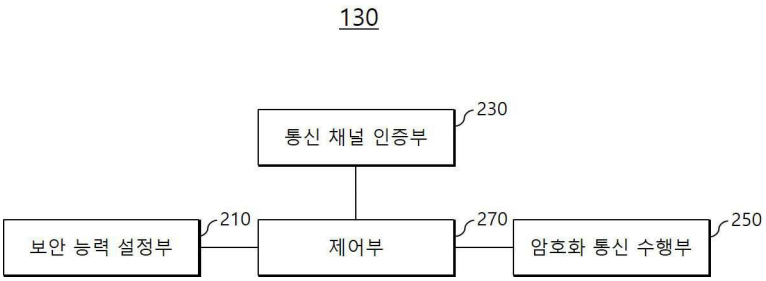
250: 암호화 통신 수행부 270: 제어부

도면

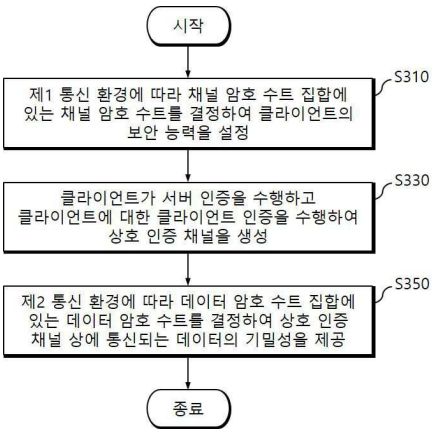
도면1



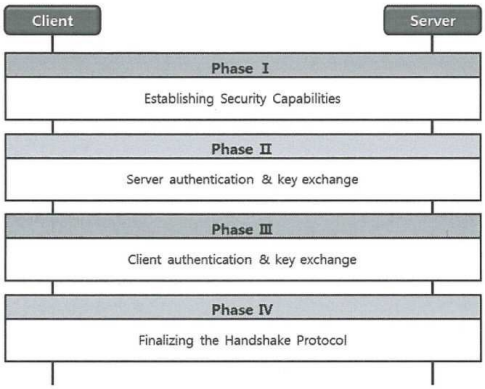
도면2



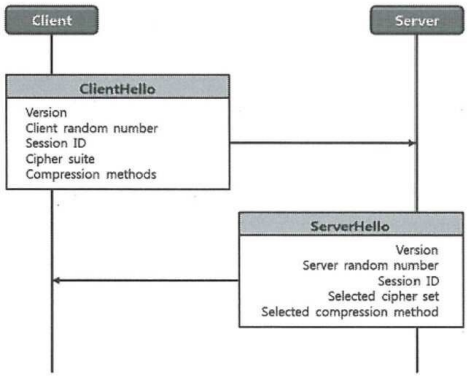
도면3



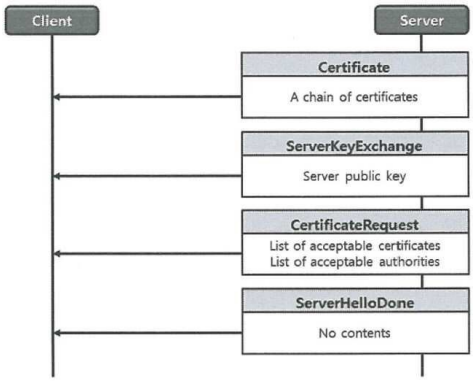
도면4


Client
Server
Phase I
Establishing Security Capabilities
Phase II
Server authentication & key exchange
Phase III
Client authentication & key exchange
Phase IV
Finalizing the Handshake Protocol

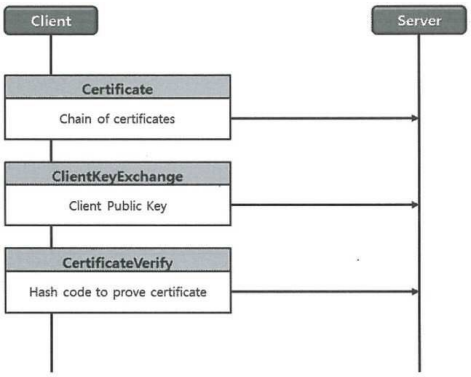
도면5


Client
Server
ClientHello
Version
Client random number
Session ID
Cipher suite
Compression methods
ServerHello
Version
Server random number
Session ID
Selected cipher set
Selected compression method

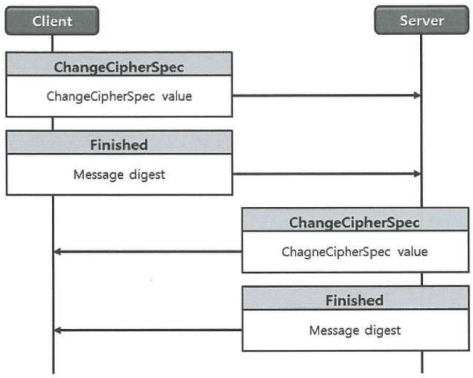
도면6


Client
Server
Certificate
A chain of certificates
ServerKeyExchange
Server public key
CertificateRequest
List of acceptable certificates
List of acceptable authorities
ServerHelloDone
No contents

도면7



도면8



도면9

Cipher ID	Cipher Name	Key Exchange	Encryption	Function for HMAC	Hash Function for PRF
0xFF00	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256	ECDH	ARIA-128-GCM	SHA-256	SHA-256
0xFF01	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_192_GCM_SHA256	ECDH	ARIA-192-GCM	SHA-256	SHA-256
0xFF02	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA256	ECDH	ARIA-256-GCM	SHA-256	SHA-256
0xFF03	TLS_KCMVP_ECDH_ECDSA_WITH_SEED_GCM_SHA256	ECDH	SEED-GCM	SHA-256	SHA-256
0xFF04	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_128_GCM_SHA256	ECDH	LEA-128-GCM	SHA-256	SHA-256
0xFF05	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_192_GCM_SHA256	ECDH	LEA-192-GCM	SHA-256	SHA-256
0xFF06	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_256_GCM_SHA256	ECDH	LEA-256-GCM	SHA-256	SHA-256
0xFF20	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256	ECDH	ARIA-128-CBC	SHA-256	SHA-256
0xFF21	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_192_CBC_SHA256	ECDH	ARIA-192-CBC	SHA-256	SHA-256
0xFF22	TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA256	ECDH	ARIA-256-CBC	SHA-256	SHA-256
0xFF23	TLS_KCMVP_ECDH_ECDSA_WITH_SEED_CBC_SHA256	ECDH	SEED-CBC	SHA-256	SHA-256
0xFF24	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_128_CBC_SHA256	ECDH	LEA-128-CBC	SHA-256	SHA-256
0xFF25	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_192_CBC_SHA256	ECDH	LEA-192-CBC	SHA-256	SHA-256
0xFF26	TLS_KCMVP_ECDH_ECDSA_WITH_LEA_256_CBC_SHA256	ECDH	LEA-256-CBC	SHA-256	SHA-256
0xFF40	TLS_KCMVP_RSA_WITH_ARIA_128_GCM_SHA256	DH	ARIA-128-GCM	SHA-256	SHA-256
0xFF41	TLS_KCMVP_RSA_WITH_ARIA_192_GCM_SHA256	DH	ARIA-192-GCM	SHA-256	SHA-256
0xFF42	TLS_KCMVP_RSA_WITH_ARIA_256_GCM_SHA256	DH	ARIA-256-GCM	SHA-256	SHA-256
0xFF43	TLS_KCMVP_RSA_WITH_SEED_GCM_SHA256	DH	SEED-GCM	SHA-256	SHA-256
0xFF44	TLS_KCMVP_RSA_WITH_LEA_128_GCM_SHA256	DH	LEA-128-GCM	SHA-256	SHA-256
0xFF45	TLS_KCMVP_RSA_WITH_LEA_192_GCM_SHA256	DH	LEA-192-GCM	SHA-256	SHA-256
0xFF46	TLS_KCMVP_RSA_WITH_LEA_256_GCM_SHA256	DH	LEA-256-GCM	SHA-256	SHA-256
0xFF60	TLS_KCMVP_RSA_WITH_ARIA_128_CBC_SHA256	DH	ARIA-128-CBC	SHA-256	SHA-256
0xFF61	TLS_KCMVP_RSA_WITH_ARIA_192_CBC_SHA256	DH	ARIA-192-CBC	SHA-256	SHA-256
0xFF62	TLS_KCMVP_RSA_WITH_ARIA_256_CBC_SHA256	DH	ARIA-256-CBC	SHA-256	SHA-256
0xFF63	TLS_KCMVP_RSA_WITH_SEED_CBC_SHA256	DH	SEED-CBC	SHA-256	SHA-256
0xFF64	TLS_KCMVP_RSA_WITH_LEA_128_CBC_SHA256	DH	LEA-128-CBC	SHA-256	SHA-256
0xFF65	TLS_KCMVP_RSA_WITH_LEA_192_CBC_SHA256	DH	LEA-192-CBC	SHA-256	SHA-256
0xFF66	TLS_KCMVP_RSA_WITH_LEA_256_CBC_SHA256	DH	LEA-256-CBC	SHA-256	SHA-256

도면10

	입력 스트링	블록암호알고리즘	키길이	운영모드
데이터 기밀성	"ARIA-128-CBC"	ARIA	128	CBC
	"SEED-CBC"	SEED	128	CBC
	"LEA-128-CBC"	LEA	128	CBC
	"ARIA-128-GCM"	ARIA	128	GCM
	"SEED-GCM"	SEED	128	GCM
	"LEA-128-GCM"	LEA	128	GCM
	입력 스트링	해시 함수		
데이터 무결성	"SHA256"	SHA256		