2021/04/02, 2021 보안 기초 세미나

Network Security Essentials

- Chapter 6 무선 네트워크 보안-

박 재 형(jaehyoung@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- IEEE 802.11 무선 LAN
- IEEE 082.11i 무선 LAN 보안
- 무선 응용 프로토콜
- 무선 전송 계층 보안
- 종단-대-종단 보안

목 차

- IEEE 802.11 무선 LAN
- IEEE 082.11i 무선 LAN 보안
- 무선 응용 프로토콜
- 무선 전송 계층 보안
- 종단-대-종단 보안

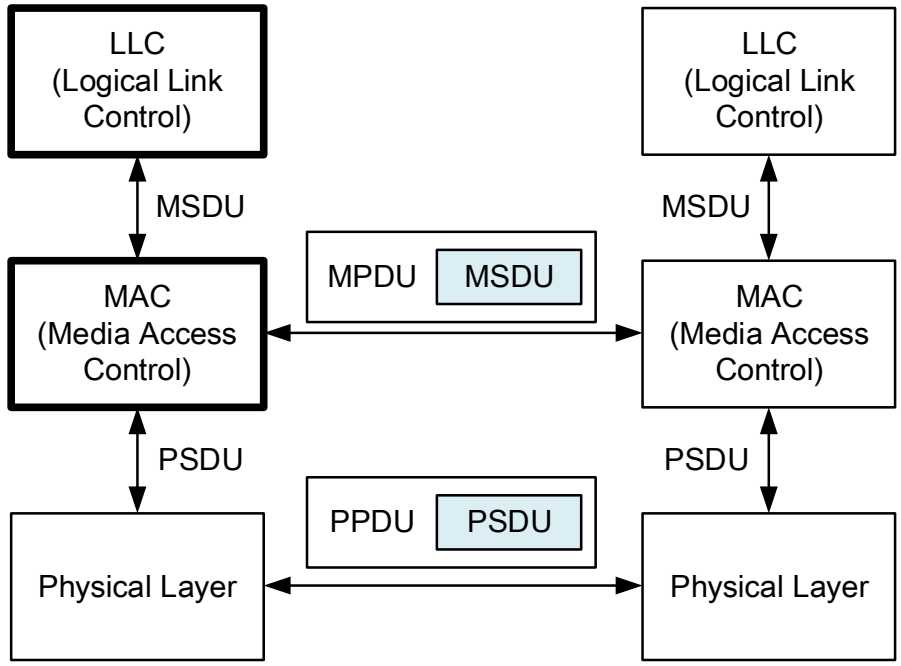
IEEE 802.11 무선 LAN

- 개요
  - IEEE(Institute of Electrical and Electronics Engineers) 802
    - 근거리 통신망과 도시권 통신망을 관할하는 전기 전자 기술자 협회의 표준 규칙들의 계열을 의미
  - IEEE 802.11
    - WLAN(Wireless Local Area Network)에 관한 프로토콜과 전송 규격 개발을 목표로 한 그룹
      - Wi-Fi(Wireless Fidelity Alliance)는 무선 LAN 제품으로 정의됨

종류	속도	거리	주파수 대역
IEEE 802.11a	54 Mbps	300m	5.0 GHz
IEEE 802.11b	11 Mbps	450m	2.4 GHz
IEEE 802.11g	54 Mbps	450m	2.4 GHz
IEEE 802.11n	300 Mbps	450m	2.4/5.0 GHz

IEEE 802.11 무선 LAN

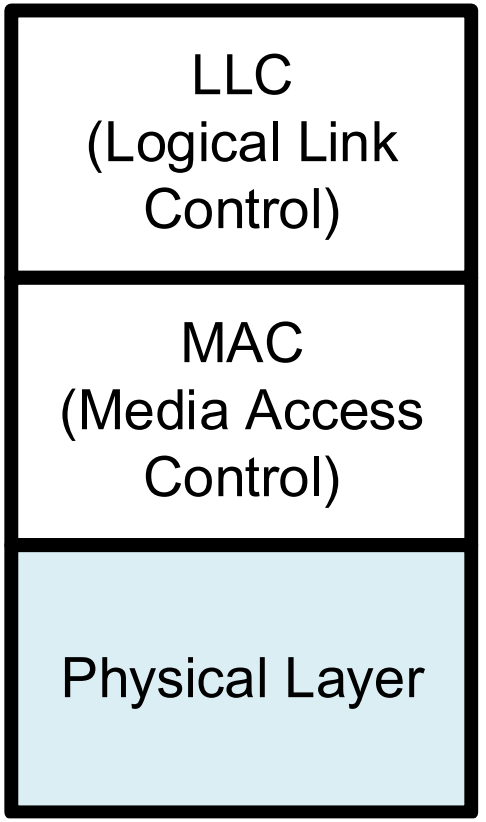
- IEEE 802 프로토콜 구조
  - 논리적 연결 제어(LLC)
  - 매체 접근 제어(MAC)
  - 물리 계층(Physical Layer)



  - 데이터 유닛
    - MAC 서비스 데이터 유닛(MSDU, MAC Service Data Unit)
    - MAC 프로토콜 데이터 유닛(MPDU, MAC Protocol Data Unit)
    - 물리 계층 서비스 데이터 유닛(PSDU, Physical layer Service Data Unit)
    - 물리 계층 프로토콜 데이터 유닛(PPDU Physical layer Protocol Data Unit)

IEEE 802.11 무선 LAN

- IEEE 802 프로토콜 구조
  - 물리 계층(Physical Layer)
    - 신호의 인코딩 및 디코딩과 비트의 송•수신 기능
    - 전송 매체에 대한 규격
      - e.g., 주파수 범위, 안테나 특성 등
    - 네트워크 모델과 같이 캡슐화,디캡슐화 기능
    - 상위 계층에서 받은 데이터는 PSDU
    - 전송되는 데이터는 PPDU

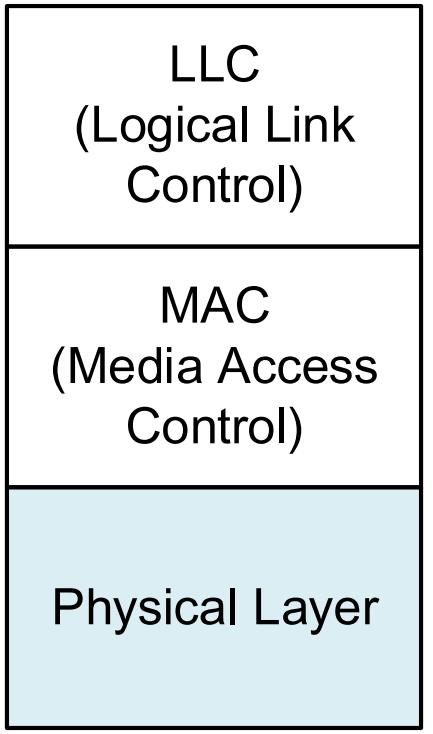


IEEE 802.11 무선 LAN

- IEEE 802 프로토콜 구조
  - PPDU 포맷

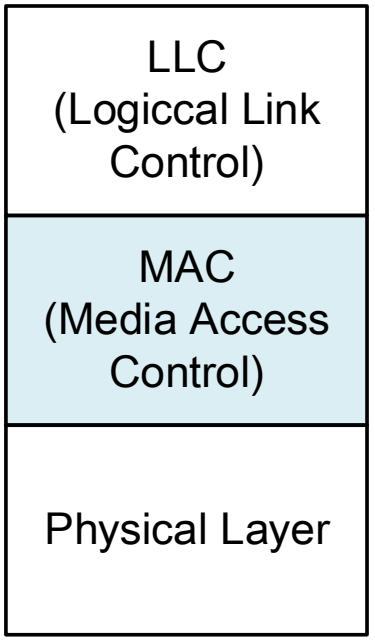
SYNC	SFD	Signal	Service	Length	CRC	PSDU

필드	기능
SYNC	동기화를 위한 비트패턴
SFD	프레임 시작
Signal	PSDU/MPDU에 사용할 신호 변조 방법을 나타냄
Service	신호 변조 방식 및 전송 주파수 등을 나타냄
Length	PSDU를 전송하는데 필요한 시간(ms)을 나타냄
CRC	순환 중복 검사 값을 통한 오류 감지
PSDU	물리 계층 서비스 데이터 유닛(2 진수)



IEEE 802.11 무선 LAN

- IEEE 802 프로토콜 구조
  - 매체 접근 제어(MAC)
    - LAN 상의 네트워크 매체들을 질서 있고 효율적으로 사용할 수 있도록 하기 위한 접근 제어 기능 등을 수행
    - 상위 계층의 MSDU를 받아 MPDU를 생성하여 전송
      - MAC 주소와 오류 감지 필드를 갖는 프레임으로 구성됨



- MPDU 포맷

MAC Control	Destination MAC Address	Source MAC Address	MSDU	CRC

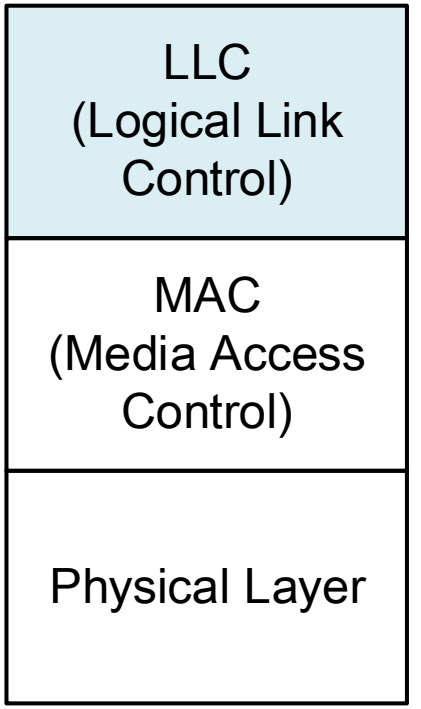
필드	기능
MAC Control	MAC 프로토콜 동작에 필요한 모든 프로토콜 제어정보를 포함
CRC	순환 중복 검사 값을 통한 오류 감지

IEEE 802.11 무선 LAN

- IEEE 802 프로토콜 구조
  - 논리적 연결 제어(LLC)
    - CRC(Cyclic Redundancy Check)를 통해 오류 적발 시, 오류 복구 기능
      - 프레임 추적과 재전송 기능을 가짐
    - MSDU를 생성하여 MAC 계층에 전달
  - MSDU 포맷

DASP	SSAP	Control	Data

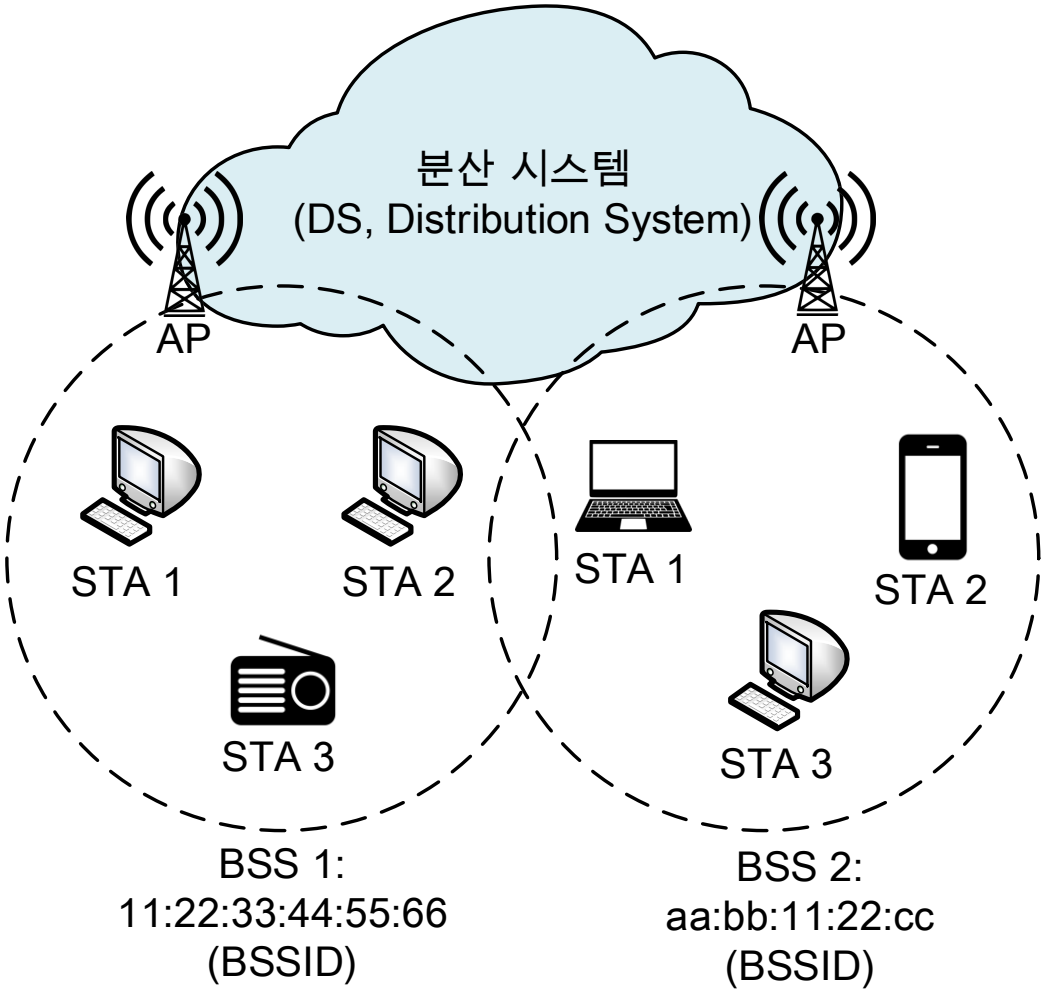
필드	기능
DSAP (Destination Service Access Point)	목적지의 주소
SSAP (Source Service Access Point)	발신지의 주소
Control	프레임 또는 ACK의 번호를 나타냄



IEEE 802.11 무선 LAN

- IEEE 802.11 구성 요소와 모델

용어	설명
DS(Distribution System)	AP가 연결된 유/무선 네트워크
AP(Access Point)	브리지 역할과 중계 지점 역할을 하는 장비
STA(Station)	무선 사용자 단말 (지국)
BSS(Basic Service Set)	AP와 연결된 다수의 STA로 구성된 집합
BSSID	BSS를 구분하기 위한 유일 식별자
IBSS(Independent BSS)	AP가 없는 형태의 무선 LAN 구성
ESS(Extended Service Set)	하나의 DS에 두 개 이상의 BSS가 연결된 집합



IEEE 802.11 무선 LAN

- IEEE 802.11 서비스
  - 유선 LAN과 동일한 수준의 서비스를 무선 LAN에도 제공할 수 있도록 정의된 서비스

서비스	제공자	기반이 되는 기능
인증	STA	LAN 접근과 보안
인증 제거	STA	LAN 접근과 보안
프라이버시	STA	LAN 접근과 보안
MSDU 전달	STA	MSDU 전달
연관	DS	MSDU 전달
연관 제거	DS	MSDU 전달
분배	DS	MSDU 전달
통합	DS	MSDU 전달
재연관	DS	MSDU 전달

IEEE 802.11 무선 LAN

- IEEE 802.11 서비스
  - DS 내부 메시지 분배
    - 분배(Distribution) 서비스
      - MSDU를 반드시 DS를 통해 하나의 BSS에 속한 STA에서 다른 BSS에 속한 STA로 전달할 때 사용하는 서비스
    - 통합(Integration) 서비스
      - IEEE 802.11 LAN에 속한 STA와 통합된 IEEE 802.1x LAN에 속한 장비 간의 통신 서비스
        - IEEE 802.1x LAN: 물리적으로 DS에 연결된 유선 LAN 표준

IEEE 802.11 무선 LAN

- IEEE 802.11 서비스
  - 연관 관련 서비스
    - DS 내부에서 목적지 STA까지 메시지를 전달하기 위해서는 전달해야 할 AP(Access Point)의 ID를 알아야 함
    - 각 연관을 통해 각 STA의 정보(ID, 위치)를 관리
    - 무선 인터넷에서는 이동성 장비에 대해 전이(Transition) 개념 정의

개념	정의
전이 없음	• 해당하는 BSS 외부로의 이동이 없음
BSS 전이	• 동일 ESS 내부에서 서로 다른 BSS간의 STA 이동을 의미 • 이동 후, 데이터 전송을 위해 주소 지정 기능이 이동한 STA의 주소를 알 수 있어야 함
ESS 전이	• ESS에 속한 BSS에서 관련이 없는 ESS로 이동하는 것을 의미 • 이동할 가능성이 있는 경우만 지원함

IEEE 802.11 무선 LAN

- IEEE 802.11 서비스
  - 연관 관련 서비스
    - AP의 ID를 알아내기 위해서 각 STA는 현재 BSS 내의 AP와 연관을 유지해야함

서비스	설명
연관 (Association)	• STA와 AP간의 초기 연관 수립(STA의 ID와 주소) • 연관된 주소를 가진 프레임을 라우팅 가능
재연관 (Reassociation)	• 하나의 AP에서 확립된 연관을 다른 AP로 전달할 수 있는 기능 • 이동 STA에 대한 전이를 처리
연관 제거 (Disassociation)	• 기존에 존재하는 연관이 종료됨을 통지 • ESS 전이 또는 종료되기 전에 통지해야 함(MAC 관리 기능으로 통지 없이 사라지는 STA을 처리 가능)

목 차

- IEEE 802.11 무선 LAN
- IEEE 082.11i 무선 LAN 보안
- 무선 응용 프로토콜
- 무선 전송 계층 보안
- 종단-대-종단 보안

IEEE 802.11i 무선 LAN 보안

- 유선 LAN과 무선 LAN 차이
  - 유선 LAN의 물리적 연결은 일부 인증 포함
    - 무선 LAN은 범위 안의 모든 장비가 인증 시도 가능
  - 유선 LAN은 통신 시, 물리적 연결이 필수적임
    - 무선 LAN은 기본적으로 브로드캐스트 개념

- WPA(Wi-Fi Protected Access)
  - Wi-Fi 연합에서 Wi-Fi 표준의 일부로서 공표
  - IEEE 802.11이 가진 대부분의 보안 문제 해결
    - WPA2는 IEEE 802.11i WLAN 보안 표준의 모든 특성을 가짐
  - 최신 802.11i 표준 버전을 RSN(Robust Security Network) 라고 함

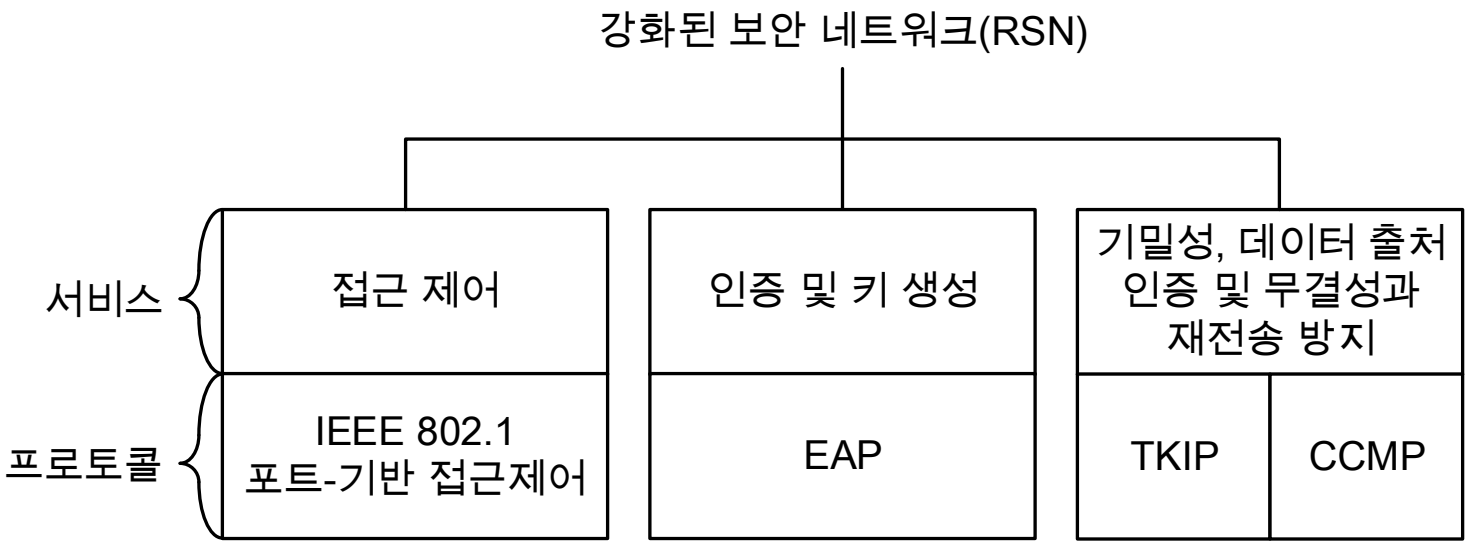
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - 802.11i RSA 보안 규격에 정의됨

서비스	설명
인증	• 프로토콜을 통한 사용자와 AS 간의 상호인증 후, 무선 링크상에서 클라이언트와 AP 간에 사용할 임시 키 생성을 정의
접근 제어	• 인증 기능의 사용, 적절한 메시지 라우팅, 키 교환을 통해 이루어지도록 함 • 인증 프로토콜로 통해 접근 제어 기능 구현
메시지 무결성을 통한 프라이버시	• MAC 계층의 데이터와 데이터 인증을 위한 MIC(Message Integrity Code)를 함께 암호화

IEEE 802.11i 무선 LAN 보안

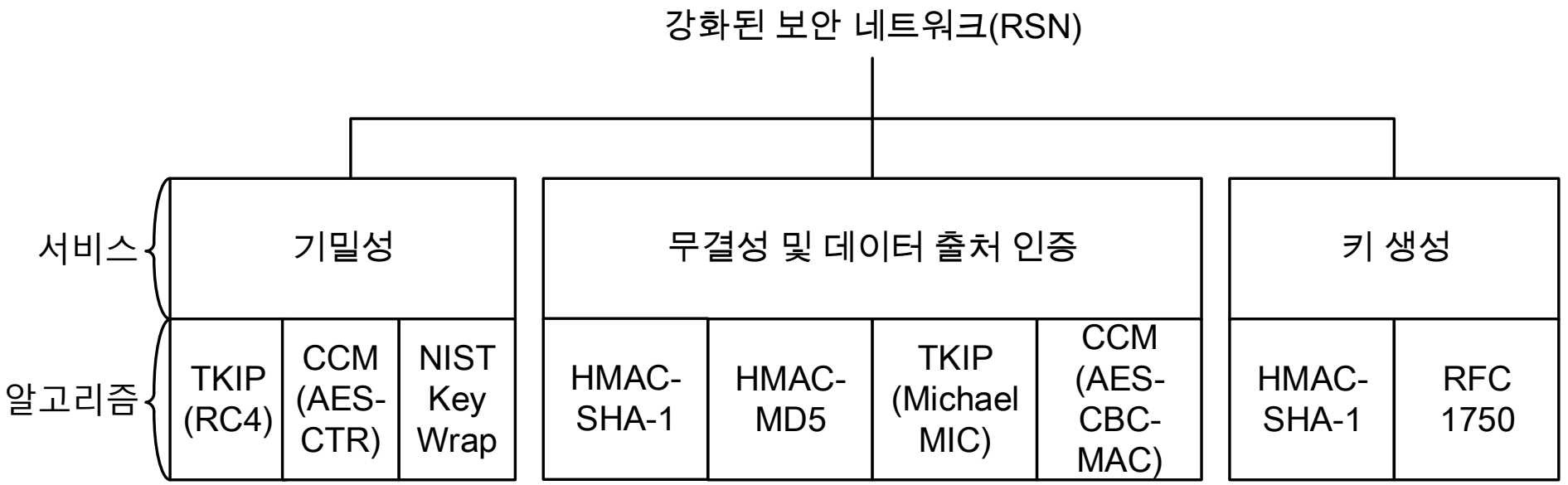
- IEEE 802.11i 서비스
  - RSN의 서비스와 프로토콜



용어	설명
EAP	확장 인증 프로토콜
TKIP	임시 키 무결성 프로토콜
CCMP	암호블록 체인 MAC 프로토콜을 갖는 카운터 모드

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - RSN의 서비스와 알고리즘



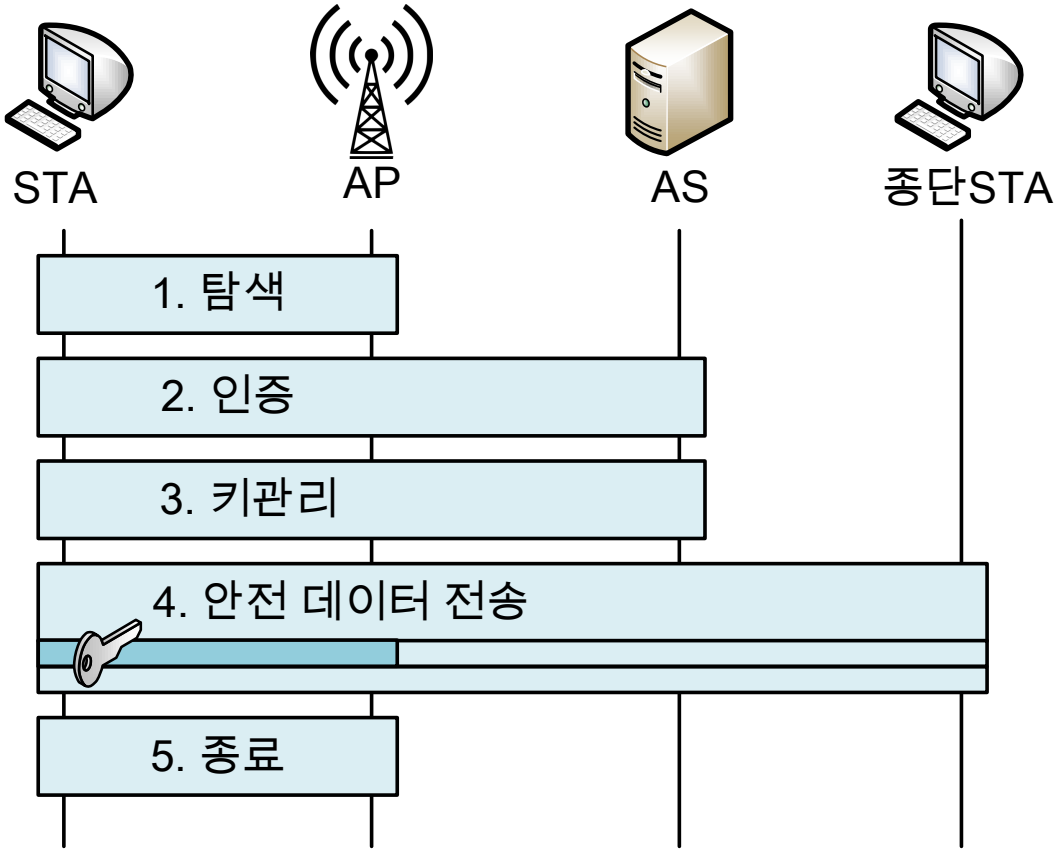
용어	설명
CBC-MAC	암호블록 블록체인 메시지 인증 코드
CCM	암호블록 체인 메시지 인증 코드를 갖는 카운터 모드

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - 동작 과정
    - 5단계로 이루어지며, 각 단계별 구체적인 특성은 구성과 통신 단말에 따라 달라짐

구성과 통신 단말에 따른 분류
동일한 BSS에 있으면서 AP를 통해 통신하는 두 STA
동일한 IBSS에 있으면서 직접 상호 통신하는 두 STA
서로 다른 BSS에 있으며 DS를 통해 각각의 AP를 경유하여 통신하는 두 STA
AP와 DS를 연결된 유선 네트워크 상의 종단 STA과 통신하는 무선 STA

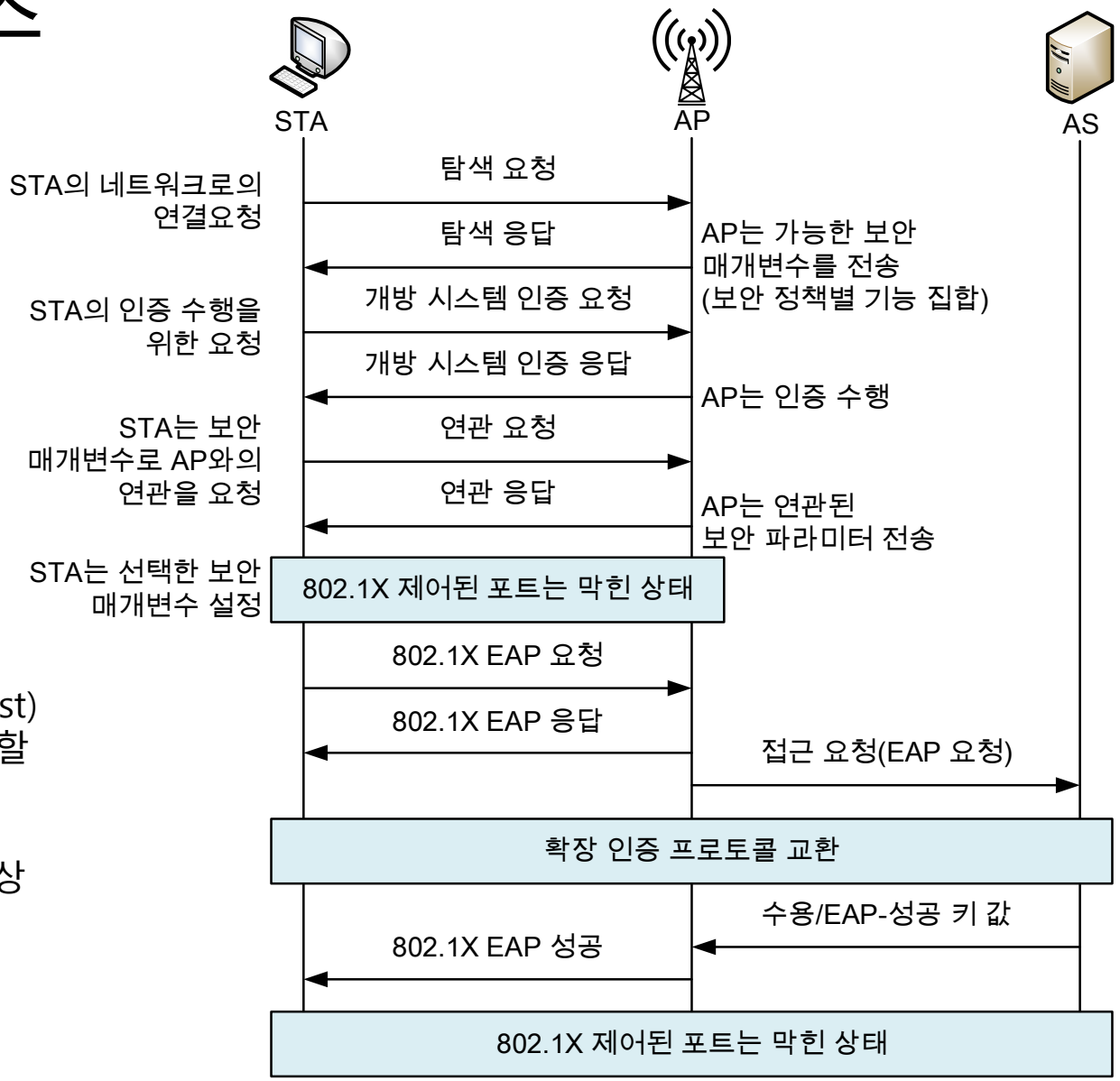
- AS: Authentication Server



IEEE 802.11i 무선 LAN 보안

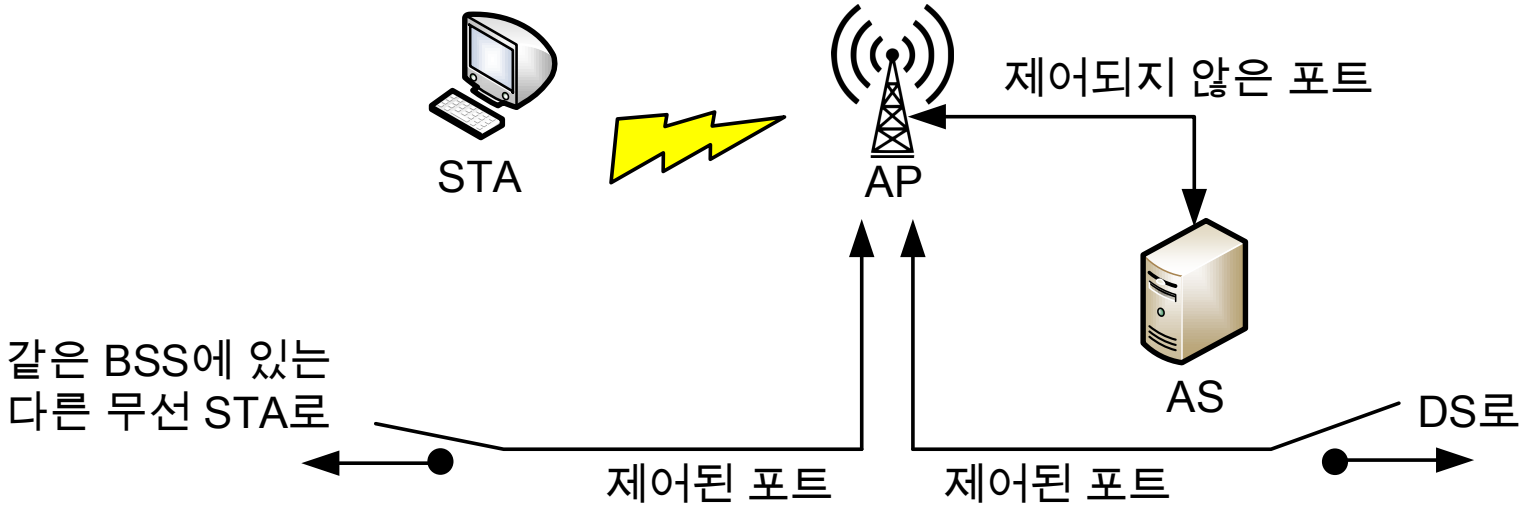
- IEEE 802.11i 서비스
  - 동작 과정
    - 1단계: 탐색

- 네트워크와 보안 기능 탐색
  - Beacon 프레임 공지 또는 Probe Request/Response 프레임을 통해 STA와 AP가 대응되는 보안 기능 탐색
- 개방 시스템 인증
  - 보안 없이 STA와 AP 간의 ID를 교환
- 연관
  - STA는 연관 요청(Association Request) 프레임을 전송하여, 이후 AP와 사용할 보안 기능에 대한 협상
  - 인증 및 키 관리도구, 암호도구 쌍, 그룹 키 암호도구 등을 선택하여 협상
    - 공통 암호도구가 없거나, 보안 공격 의심 시, 연관요청 거부



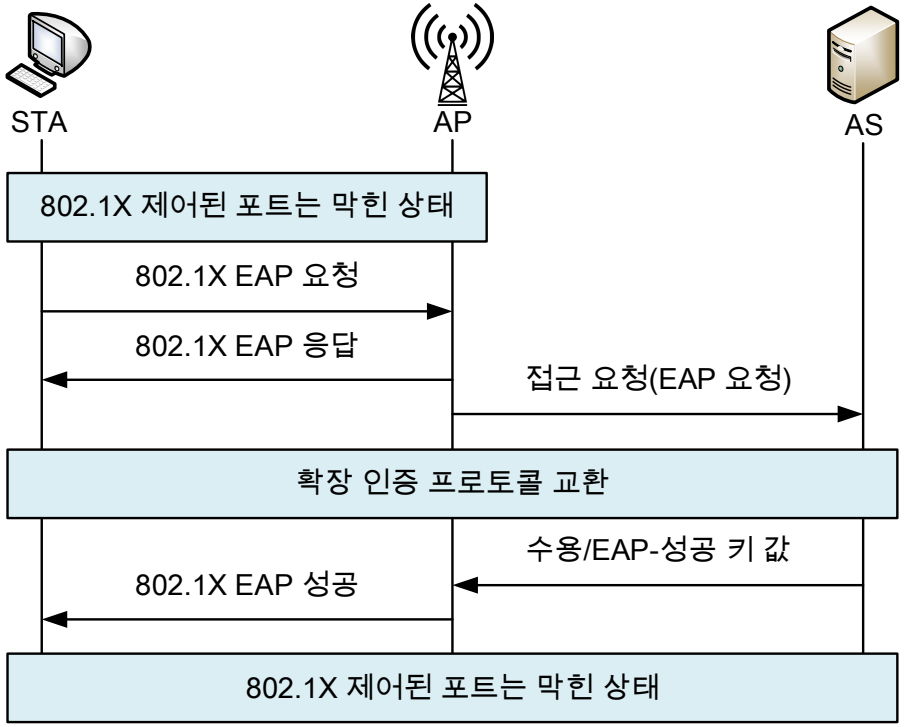
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - 동작 과정
    - 2단계: 인증
      - 접근 제어
        - IEEE 802.1X: 표준으로 정의된 포트 기반 네트워크 접근 제어 방식
          - EAP(Extensible Authentication Protocol) 사용
          - IEEE 802.11i에서는 LAN용 접근 제어 기능을 제공하기 위해 사용
          - 포트 개념 사용



IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - 동작 과정
    - 2단계: 인증
      - MPDU 교환
        - AS 연결
          - STA는 해당하는 BSS의 AP를 통해 AS로 접근을 요청
      - EAP 교환
        - STA와 AS는 상호 인증을 위한 EAP 수행
      - 안전한 키 전달
        - AS는 마스터 세션 키(MSK)를 생성해 AP를 통해 STA로 전달

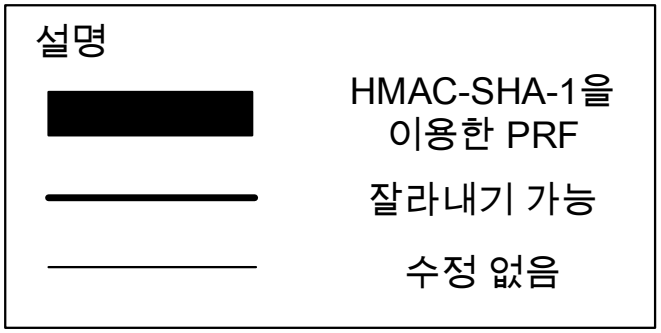


IEEE 802.11i 무선 LAN 보안

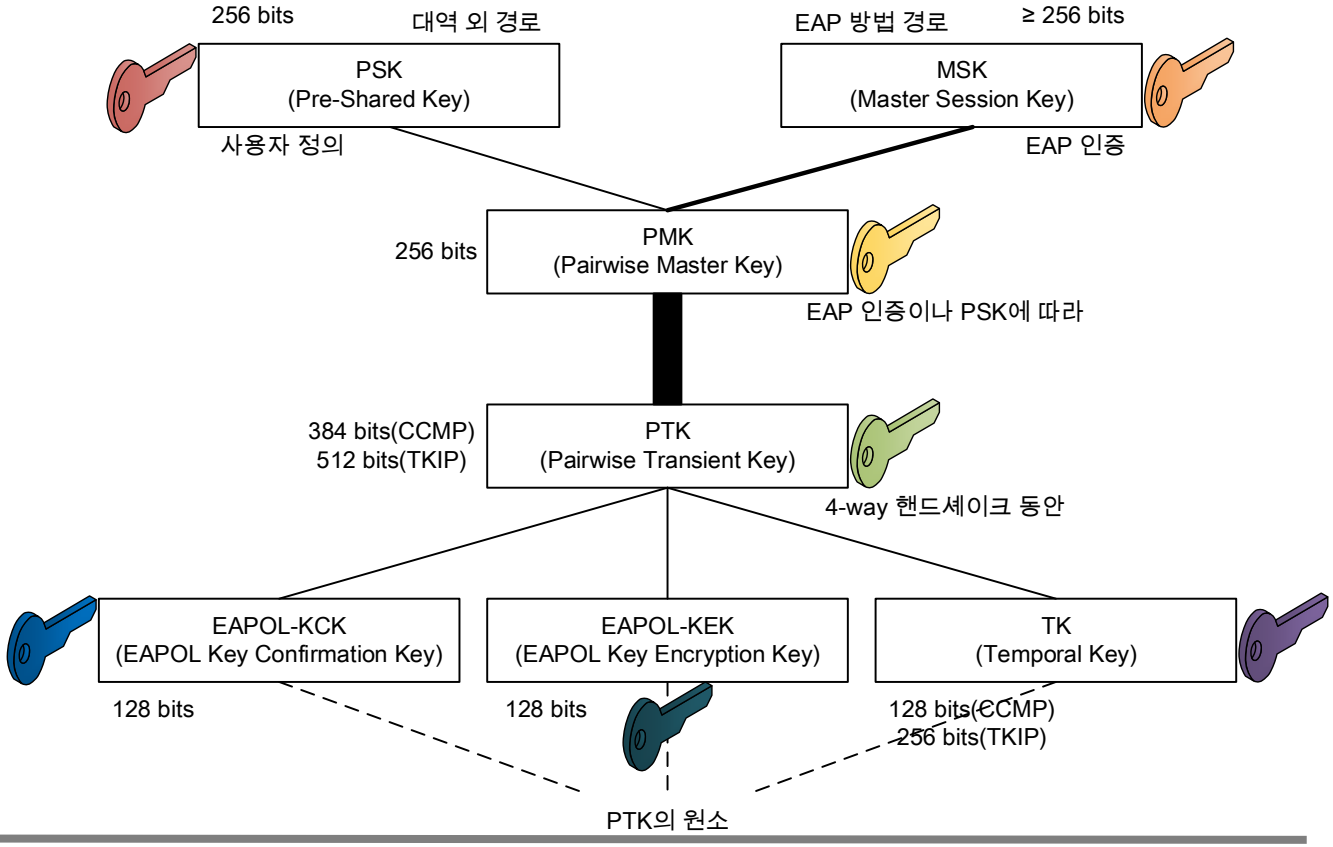
- IEEE 802.11i 서비스
  - 동작 과정
    - 2단계: 인증
      - EAP 교환
        - EAP와 결합되어 사용되는 프로토콜
        - EAPO(EAP over Layer)
          - STA와 AP 간의 메시지 전달
        - RADIUS(Remote Authentication Dial In User Service) 프로토콜 사용
          - 사용으로 AP와 AS 간의 메시지 전달
            - 인증자가 PPP(Point to Point Protocol) 프레임 등으로 STA의 ID와 암호를 받아 암호화하여 인증 서버로 UDP를 통해 전송
            - 인증 서버는 ID와 암호를 확인하고 허가 또는 거절
              - 거절 시, 거절된 이유 전송

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - 동작 과정
    - 3단계: 키 관리
      - 각 연관 쌍 별 키 생성과 관리

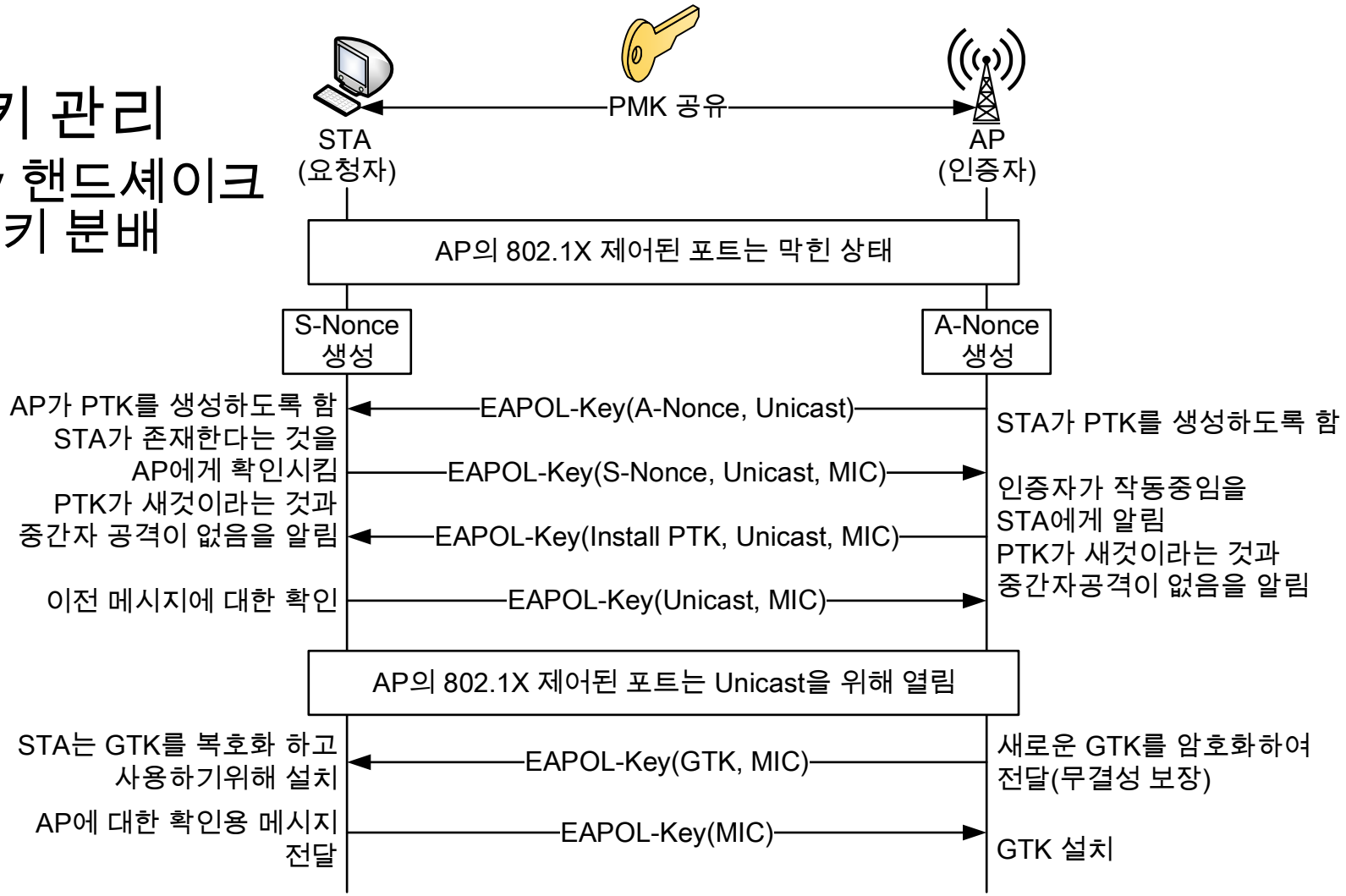


키	생성 및 관리
PSK	AP와 STA가 사전에 공유하는 비밀키
MSK	STA와 AP간의 상호 인증에서 생성된 세션 키, AS가 생성해 상호 공유
PMK	PSK로 PMK를 생성하거나 MSK의 일부를 잘라 PMK 생성
PTK	PMK, STA, AP의 MAC 주소, 비표를 PRF(Pseudo Random Function)의 입력으로 생성한 해시 값
KCK	메시지 인증을 위한 MIC 생성용 키
KEK	GTK(Group Temporal Key) 분배를 위한 키
TK	트래픽 보호용 키



IEEE 802.11i 무선 LAN 보안

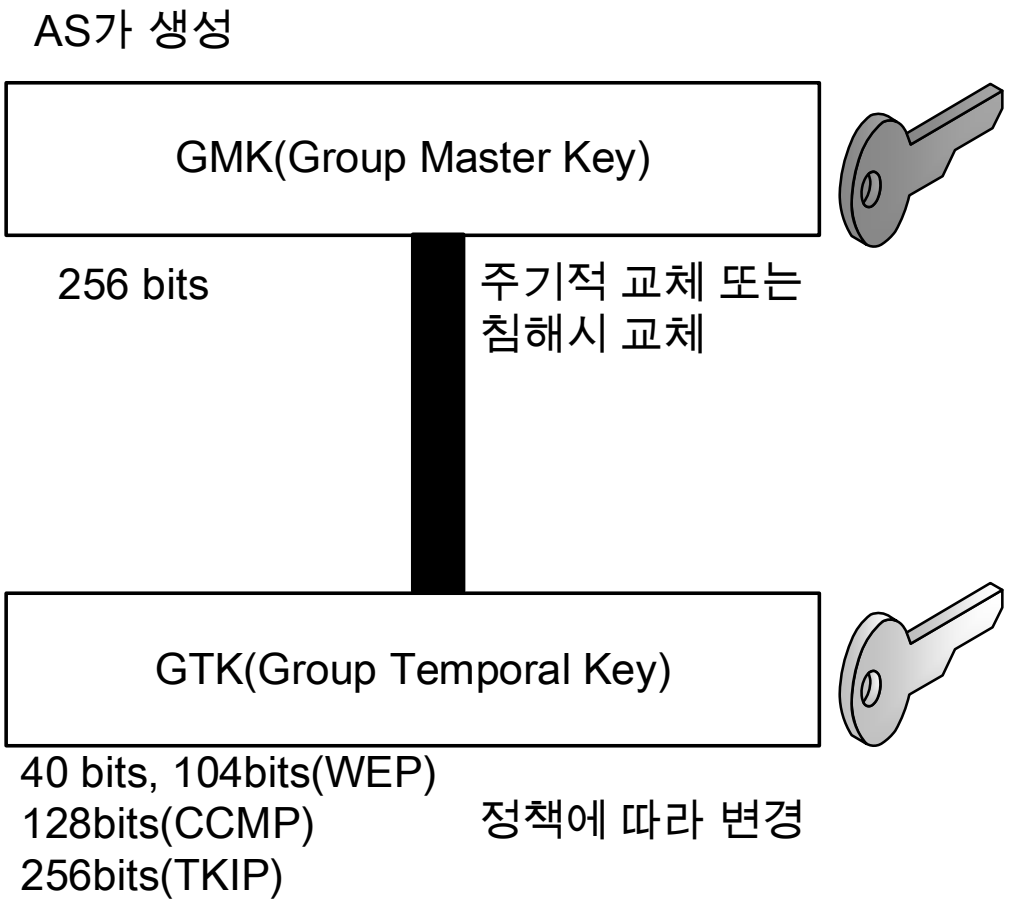
- IEEE 802.11i 서비스
  - 동작 과정
    - 3단계: 키 관리
      - 4-way 핸드셰이크
        쌍 별 키 분배



IEEE 802.11i 무선 LAN 보안

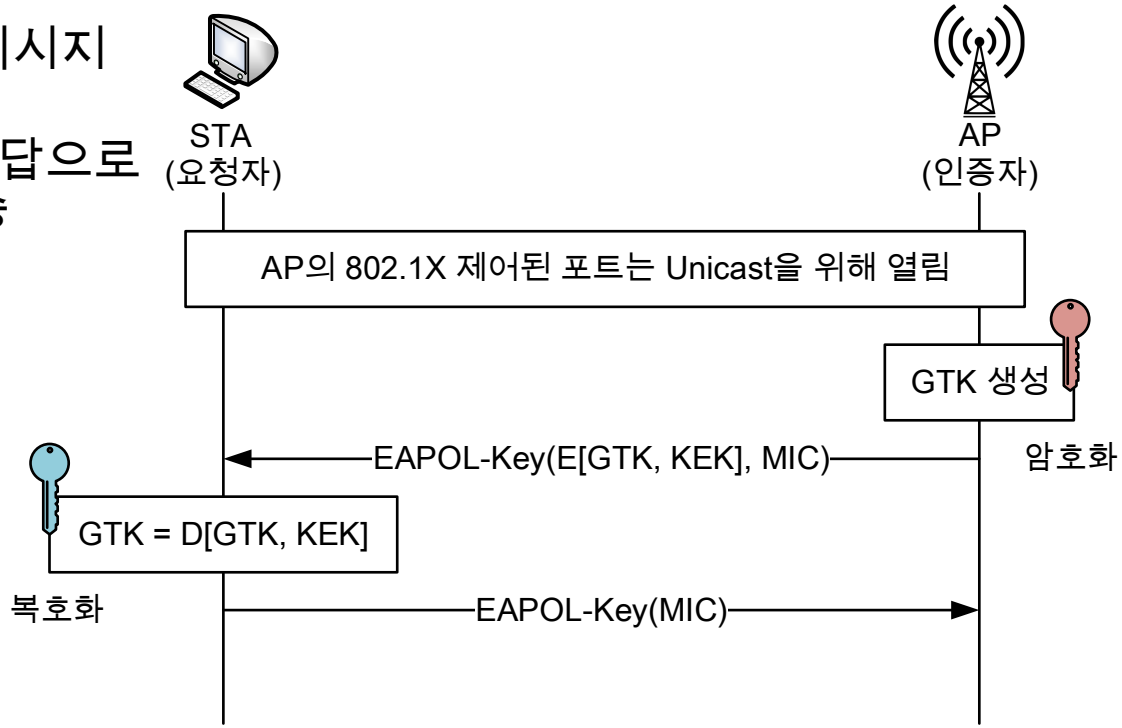
- IEEE 802.11i 서비스
  - 동작 과정
    - 3단계: 키 관리
      - 멀티캐스트용 그룹 키 생성

키	생성 및 관리
GMK	• AS가 생성 • 주기적으로 교체하거나 침해 시, 교체
GTK	• GMK와 정책에 따른 입력을 통해 생성 • AP가 생성해 연관된 지국에게 전달



IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - 동작 과정
    - 3단계: 키 관리
      - 멀티캐스트용 그룹 키 분배
        - AP가 GTK 생성 후, KEK를 통해 암호화(RC4 또는 AES)
        - 암호문과 MIC를 포함한 메시지 전송
        - 수신 메시지 복호화 후, 응답으로 MIC를 포함한 메시지 전송



IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - 동작 과정
    - 4단계: 안전한 통신
      - TKIP(Temporal Key Integrity Protocol) 제공 서비스
        - 메시지 무결성
          - MAC 프레임과 키를 입력으로 64bits MIC를 생성하고 함께 전송
        - 데이터 기밀성
          - 데이터와 MIC를 RC4로 암호화하여 데이터 기밀성 제공
      - CCMP(Counter CBC MAC Protocol) 제공 서비스
        - 메시지 무결성
          - 암호 블록 체인 인증 코드(CBC-MAC)사용
        - 데이터 기밀성
          - AES-CTR을 사용한 암호화

목 차

- IEEE 802.11 무선 LAN
- IEEE 082.11i 무선 LAN 보안
- 무선 응용 프로토콜
- 무선 전송 계층 보안
- 종단-대-종단 보안

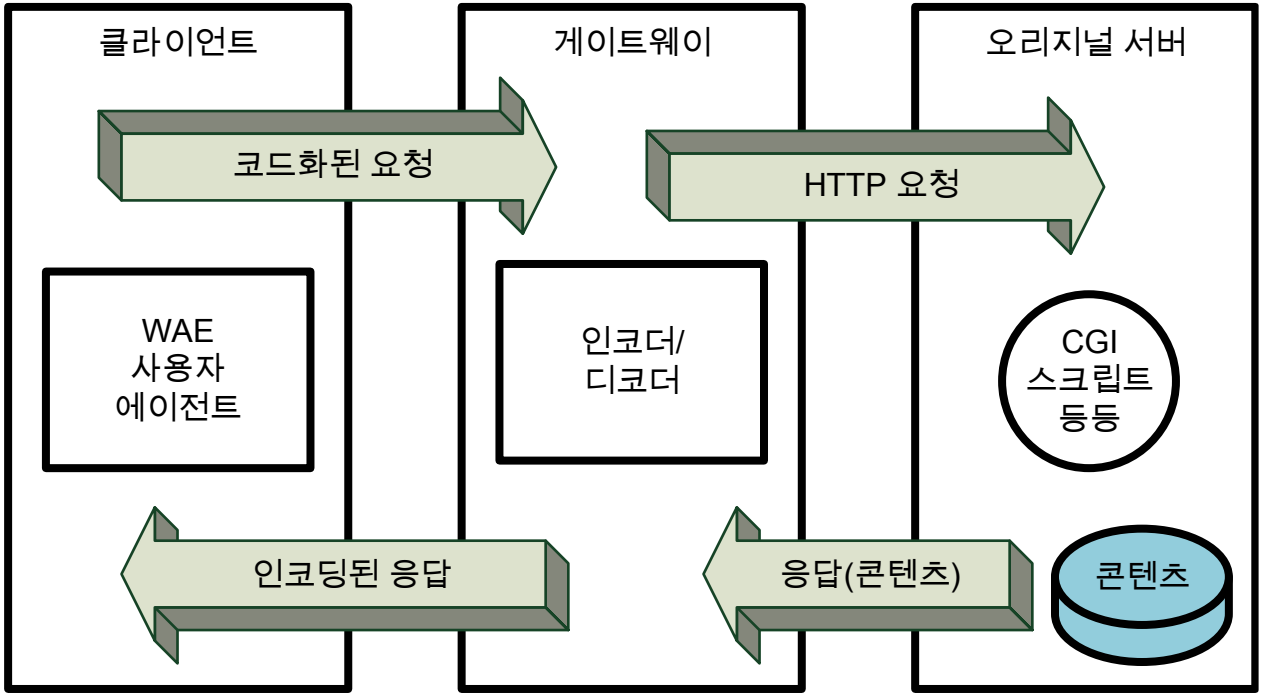
무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 개요
    - 1989년 WAP 포럼에서 개발한 통합 표준화를 위한 프로토콜 규격
      - 무선 터미널에서의 인터넷 서비스이용, 무선 프로토콜 개발, 다양한 콘텐츠와 응용기술 개발을 위함
  - 무선 네트워크의 특성

특성	설명
통신환경	좁은 대역폭, 낮은 전송률
하드웨어	저사양 CPU, 적은 메모리 및 배터리 사양
사용자 인터페이스	입/출력 장치, 응용 프로그램의 제한

무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 정의
    - 무선 장치를 위한 애플리케이션 프레임워크 및 네트워크 프로토콜의 표준
  - WAP 프로그래밍 모델

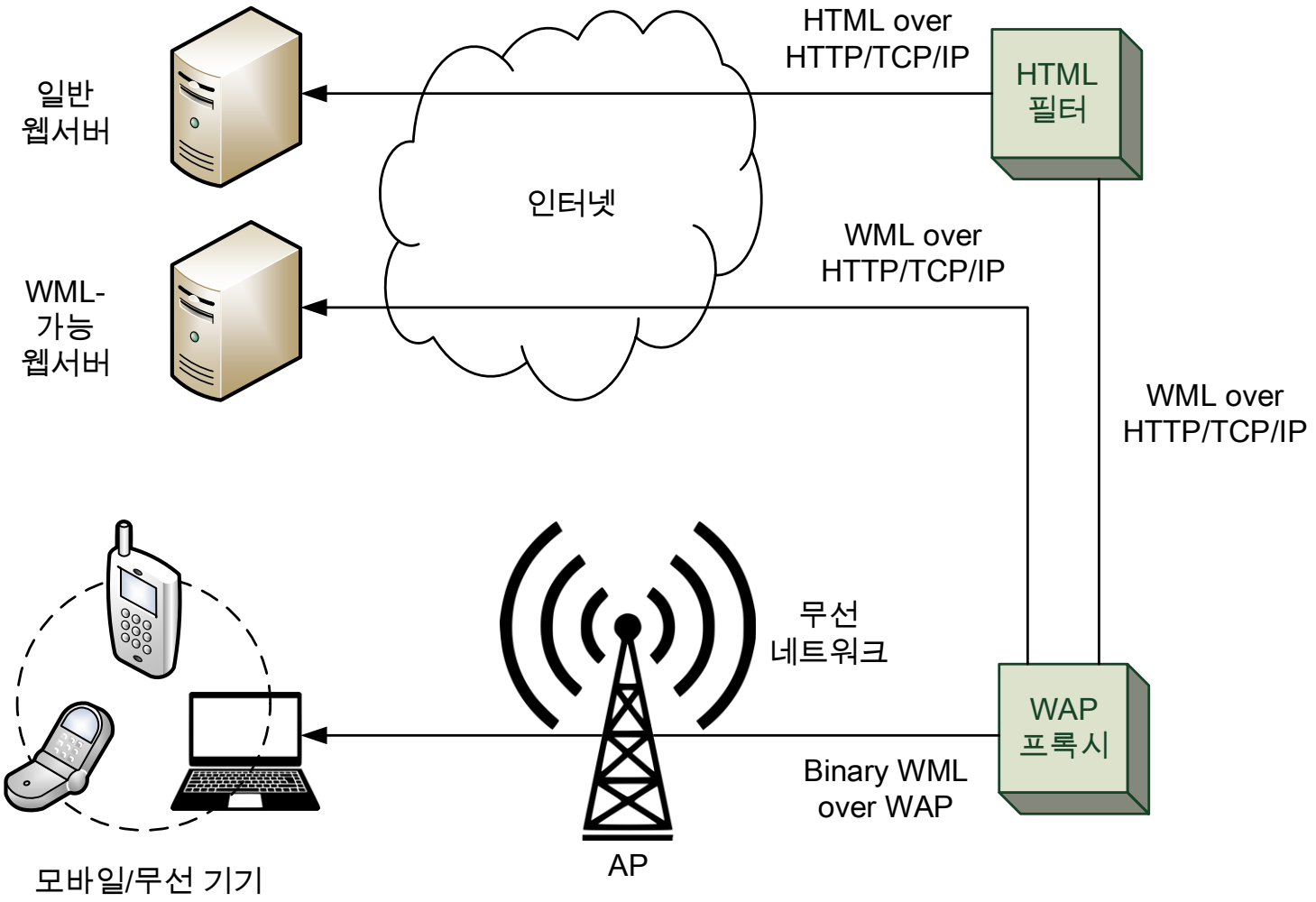


무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - WML(Wireless Markup Language)
    - 정의
      - WAP에 정의된 마크업 언어
        - e.g., HTML, JavaScript 등
    - 특징
      - 제한된 사용자 입력 기능을 가진 모바일 장비에서 콘텐츠와 양식을 표현하기 위해 설계된 언어
      - WML 서비스에서 직접 음성 통화를 가능하도록 하는 응용 인터페이스 무선 전화 응용(WTA, Wireless Telephony Application Interface)을 규정
        - WTA
          - 개발자와 사용자에게 더 나은 모바일 네트워크 서비스가 가능하도록 하는 전화에 특화된 애플리케이션

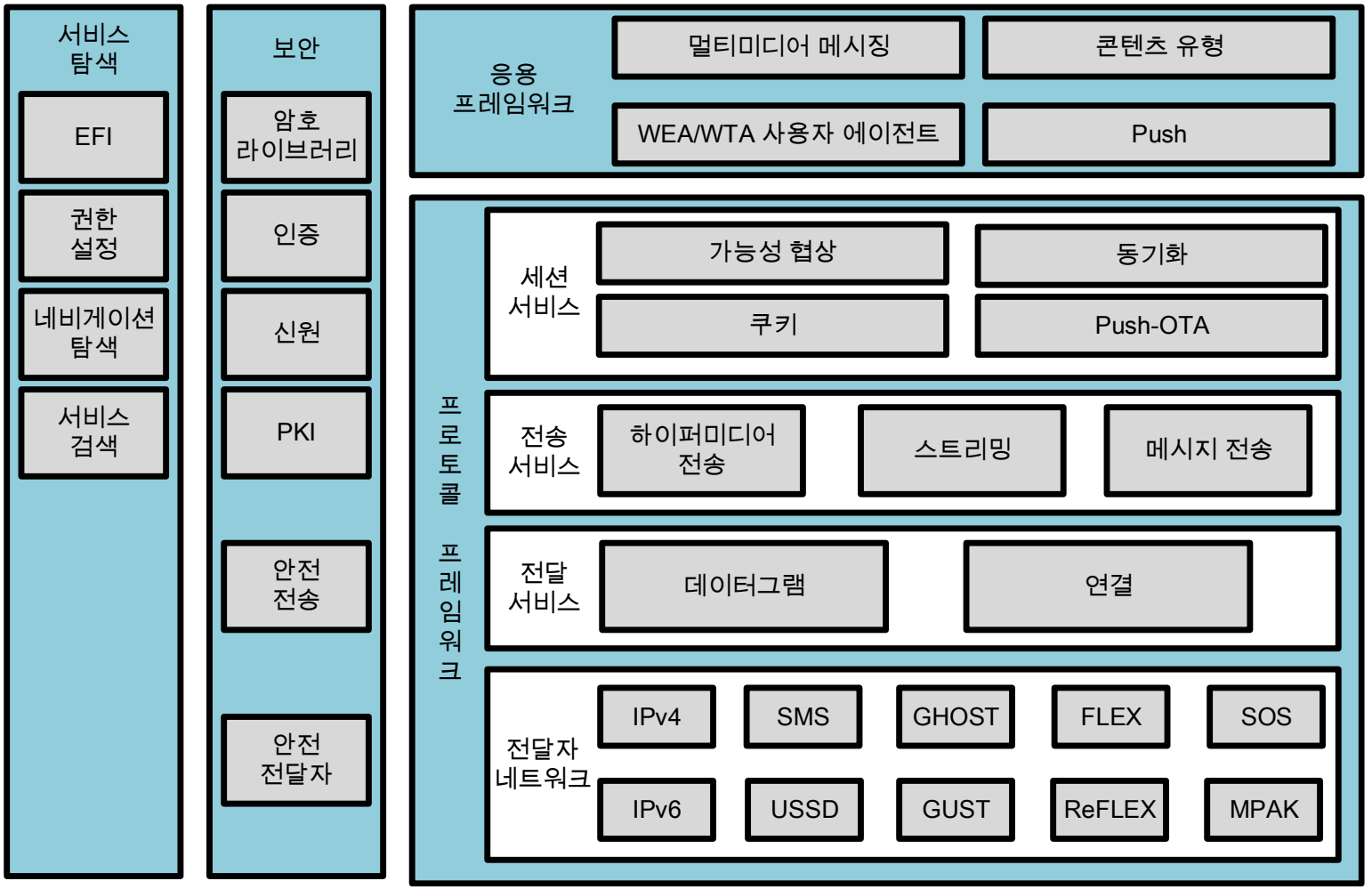
무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 기반 구조



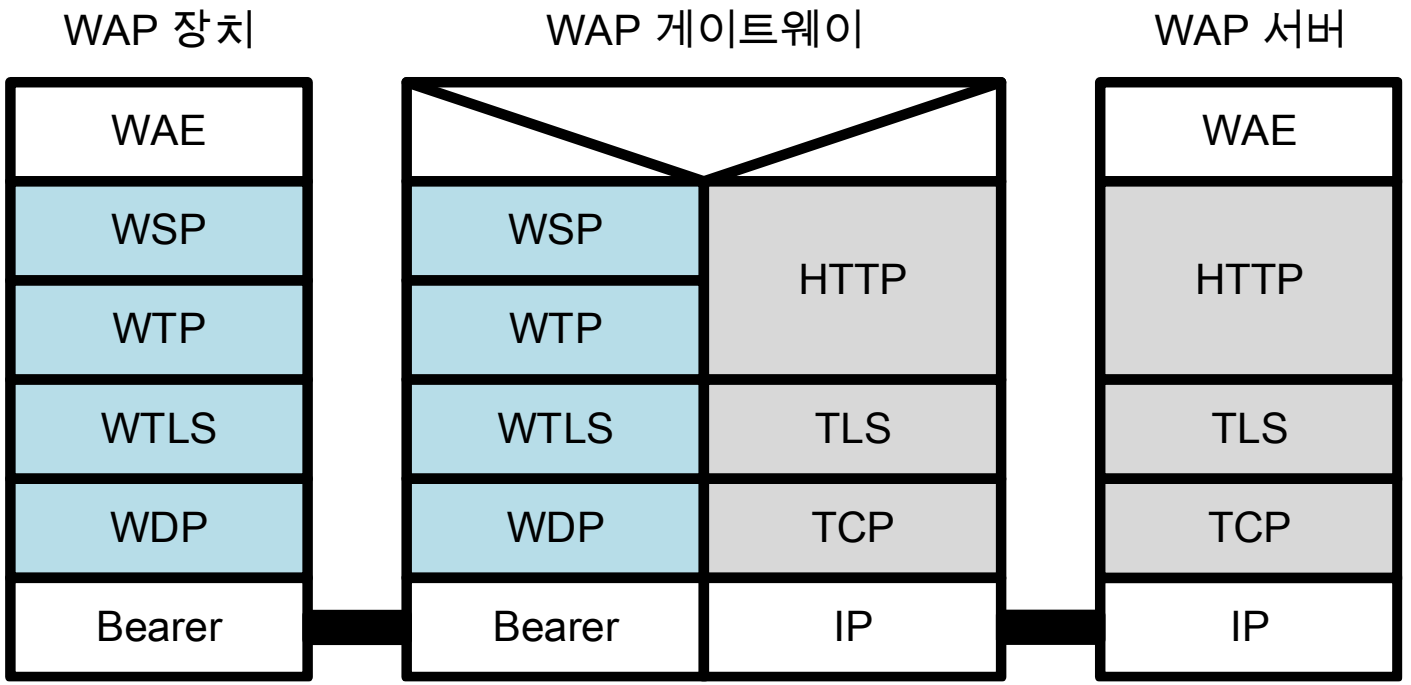
무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - WAP 구조



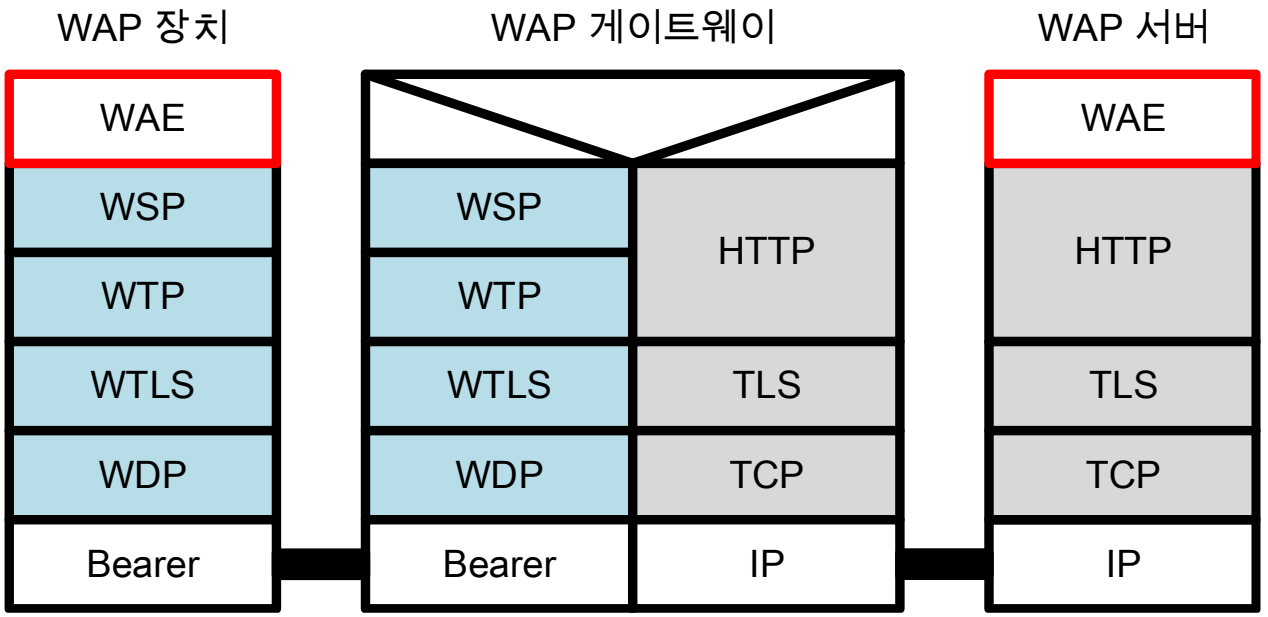
무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 스택 구조



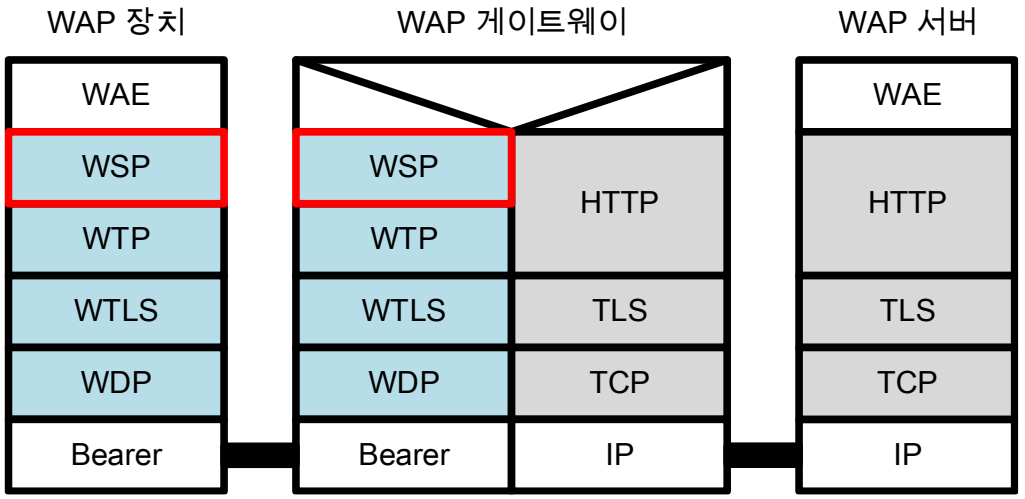
무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 스택 구조
    - WAE(Wireless Application Environment)
      - WAP 스택의 상위계층
      - 지원하는 응용 프로그램과 장비 개발을 위한 도구와 형식의 집합



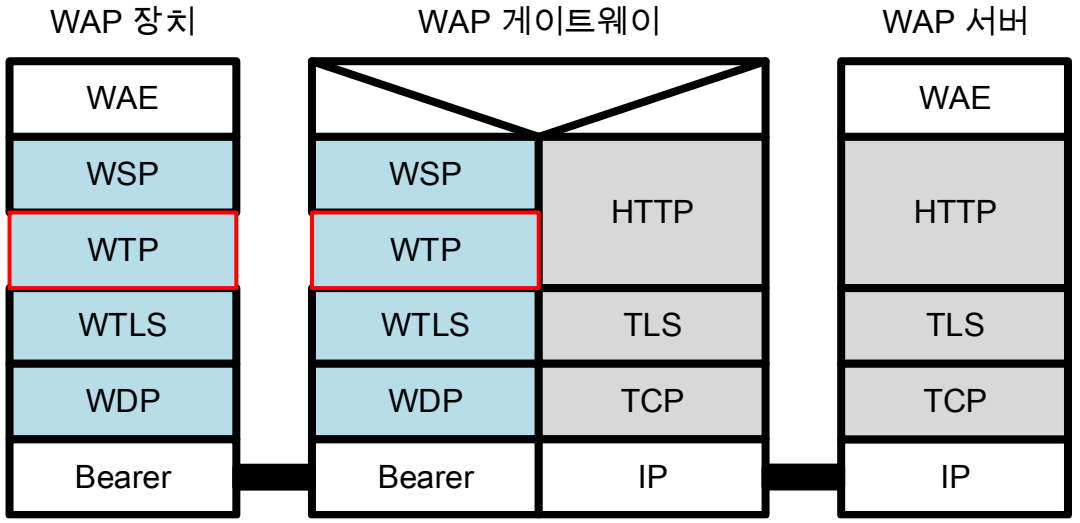
무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 스택 구조
    - WSP(Wireless Session Layer Protocol)
      - 세션을 생성하고 이미 접속 중인 세션을 종료하는 기능 제공
      - WAE를 두개의 세션 서비스로 연결시키는 계층
        - 연결형 서비스(WTP)
          - 클라이언트가 인터넷 서비스를 받는 동안 접속 상태를 유지하며 동작
        - 비연결형 서비스(WDP)
          - 컨텐츠만 전달하고 이후, 바로 접속 종료하는 방식의 동작



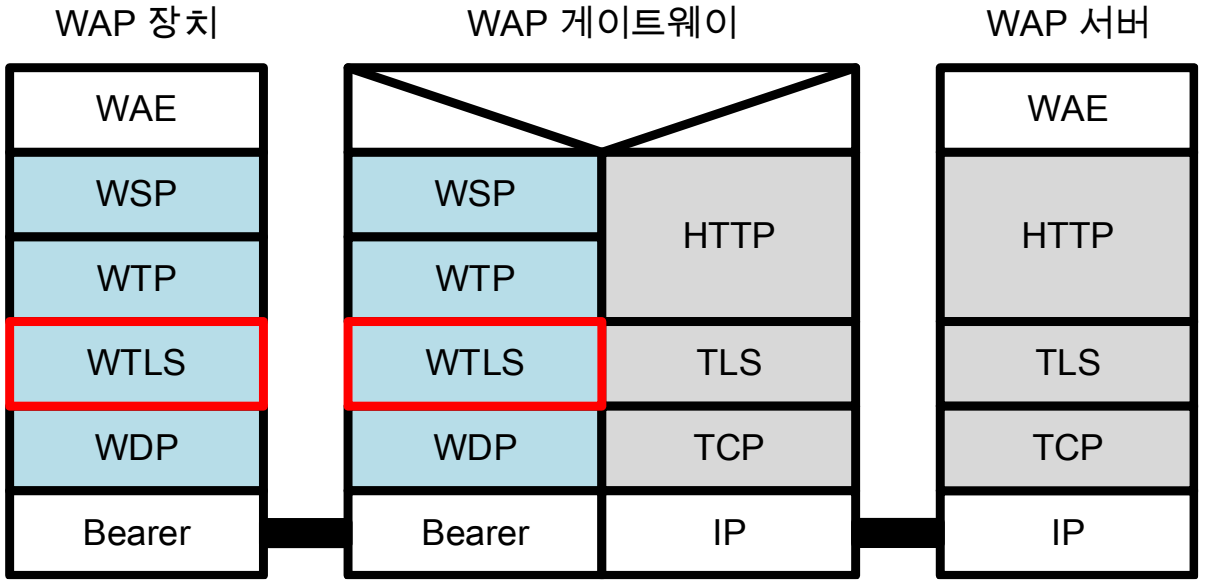
무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 스택 구조
    - WTP(Wireless Transaction Protocol)
      - 트랜잭션 형태의 데이터 전송 기능 제공
        - 유선에 비해 낮은 대역폭을 가지는 무선 통신에 알맞음
      - 데이터의 송수신은 요청/응답 패킷 형태로 이루어지며, 오류가 발생한 패킷만 재전송 요청



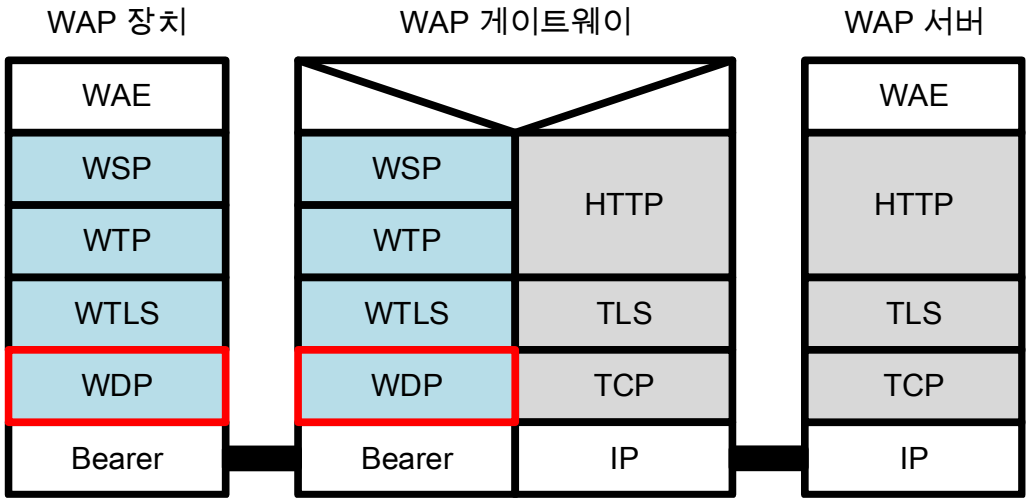
무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 스택 구조
    - WTLS(Wireless Transport Layer Security)
      - TLS를 기반으로 WAP에 적용
      - WAP에서 안전한 통신을 위해 정의한 보안 프로토콜
      - WAP 장치와 WAP G/W 간의 보안 서비스 제공



무선 응용 프로토콜

- 무선 응용 프로토콜(WAP, Wireless Application Protocol)
  - 스택 구조
    - WDP(Wireless Datagram Protocol)
      - 다양한 네트워크에 의해 지원되는 Bearers 서비스를 이용하는 데이터 위에서 동작
        - Bearer
          - WAP G/W와 휴대폰을 연결하는 통신 망 또는 전송 방식
          - 모든 Bearer는 WDP 하위에 위치
      - 포트번호 주소화, 분리 및 재조립, 오류 탐지



목 차

- IEEE 802.11 무선 LAN
- IEEE 082.11i 무선 LAN 보안
- 무선 응용 프로토콜
- 무선 전송 계층 보안
- 종단-대-종단 보안

무선 전송 계층 보안

- 정의
  - WAP에서 안전한 통신을 위해 정의한 보안 프로토콜
- 특징
  - TLS를 바탕으로 무선 환경에 최적화 됨
  - 메시지 인증, 암호화, 인증서를 통한 상호 인증 기능제공
    - 데이터 무결성, 기밀성, 인증 보장
  - WAP 장치와 WAP G/W간의 보안 서비스 제공

무선 전송 계층 보안

- WTLS 연결과 세션 개념
  - 연결(Connection)
    - OSI 계층 모델에 해당하는 서비스를 제공하기 위해 대등 관계에서의 데이터 전송을 의미
    - 모든 연결은 한 개의 세션과 연관됨
  - 세션(Session)
    - 클라이언트와 서버 사이의 핸드셰이크 프로토콜을 사용한 연결을 의미
    - 각 연결마다 해당하는 새로운 보안 매개변수 협상을 방지
      - 연결이 공유하는 하나의 보안 매개변수 집합 정의

무선 전송 계층 보안

- WTLS 매개변수
  - 연결 상태

매개변수	설명
세션 식별자 (Session Identifier)	기존 세션상태나 재시작 가능 세션상태를 구분하기 위한 서버가 부여한 바이트 열
프로토콜 버전 (Protocol Versions)	WTLS 프로토콜 버전
대등 인증서 (Peer Certificate)	대등(Peer)의 인증서
압축 방법 (Compression Method)	암호화하기 전에 행하는 압축 알고리즘
암호명세 (Cipher Spec)	데이터 암호화 알고리즘(RC5, DES 등)과 MAC을 계산하기 위한 해시 알고리즘 (MD5, SHA-1 등)
마스터 비밀 (Master Secret)	클라이언트와 서버가 공유하는 20Byte 비밀 값
순서번호 (Sequence Number)	송•수신 되는 각 메시지에 대한 순서번호 값
키 갱신 (Key Refresh)	어떤 연결 상태변수(암호화 키, MAC 비밀 키, IV 등)가 계산되는 빈도
재개 가능성 (Is Resumable)	새로운 연결을 시작하는데 세션을 이용할 수 있는지에 대한 여부

무선 전송 계층 보안

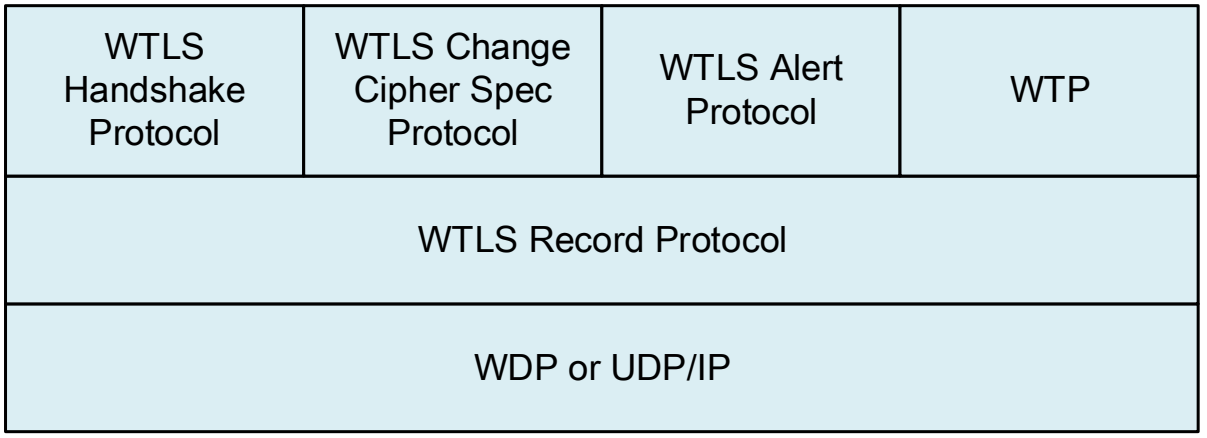
- WTLS 매개변수
  - 세션 상태

매개변수	설명
연결 종료 (Connection End)	해당 개체가 안전 연결에서 서버 역할을 하는지 클라이언트역할을 하는지 여부
대량 암호화 알고리즘 (Bulk Cipher Algorithm)	알고리즘의 키 크기, 키의 비밀 부분, 블록암호/스트림 암호 여부, 암호의 블록 크기
MAC 알고리즘 (MAC Algorithm)	MAC 계산에 사용될 키의 크기, MAC 알고리즘으로 계산된 해시 값 크기
압축 알고리즘 (Compression Algorithm)	압축 알고리즘으로 압축할 경우, 필요한 정보
마스터 비밀 (Master Secret)	클라이언트와 서버가 공유하는 20바이트 비밀 값
클라이언트 랜덤 (Client Random)	클라이언트가 제공하는 16비트 값
서버 랜덤 (Server Random)	서버가 제공하는 16비트 값
순서번호 모드 (Sequence Number Mode)	해당 안전 연결에서 순서번호를 보내는데 사용하는 시스템
키 갱신 (Key Refresh)	연결 상태 변수(암호화 키, MAC 비밀키, IV 등)가 계산되는 빈도

무선 전송 계층 보안

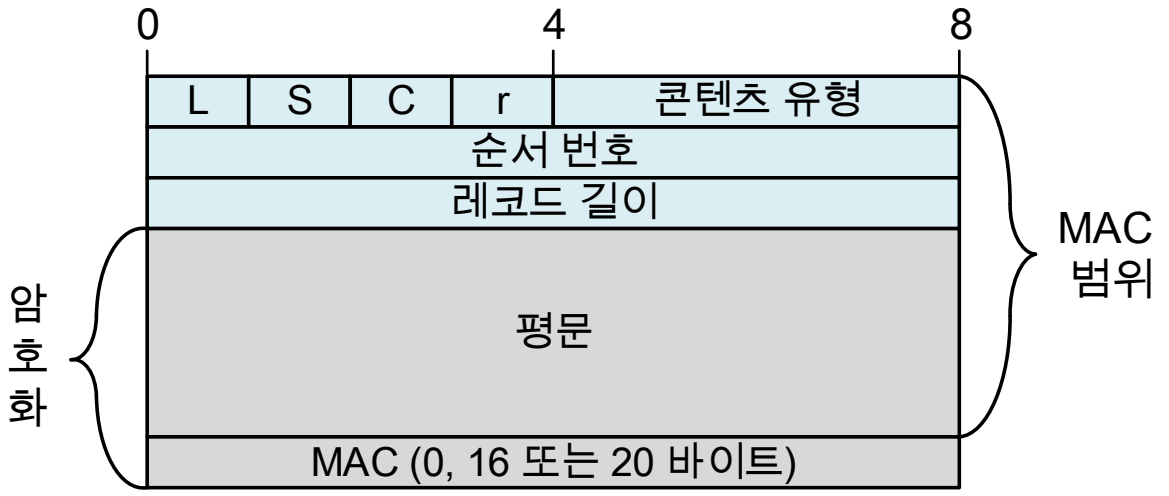
- WTLS 구조
  - WTLS 프로토콜 스택

WTLS 프로토콜 스택	설명
WTLS 핸드셰이크 프로토콜 (Handshake Protocol)	통신하기 전에 필요한 보안 설정들을 매개변수를 통해 협상 (세션 키, 암호화 알고리즘, 인증 방법 등)
WTLS 암호명세 변경 프로토콜 (Change Cipher Spec Protocol)	협상한 보안 설정 들의 적용 상태를 알림
WTLS 경고 프로토콜 (Alert Protocol)	세션의 종료 또는 오류 발생 시, 알림
WTLS 레코드 프로토콜 (Record Protocol)	데이터 암/복호화 및 압축



무선 전송 계층 보안

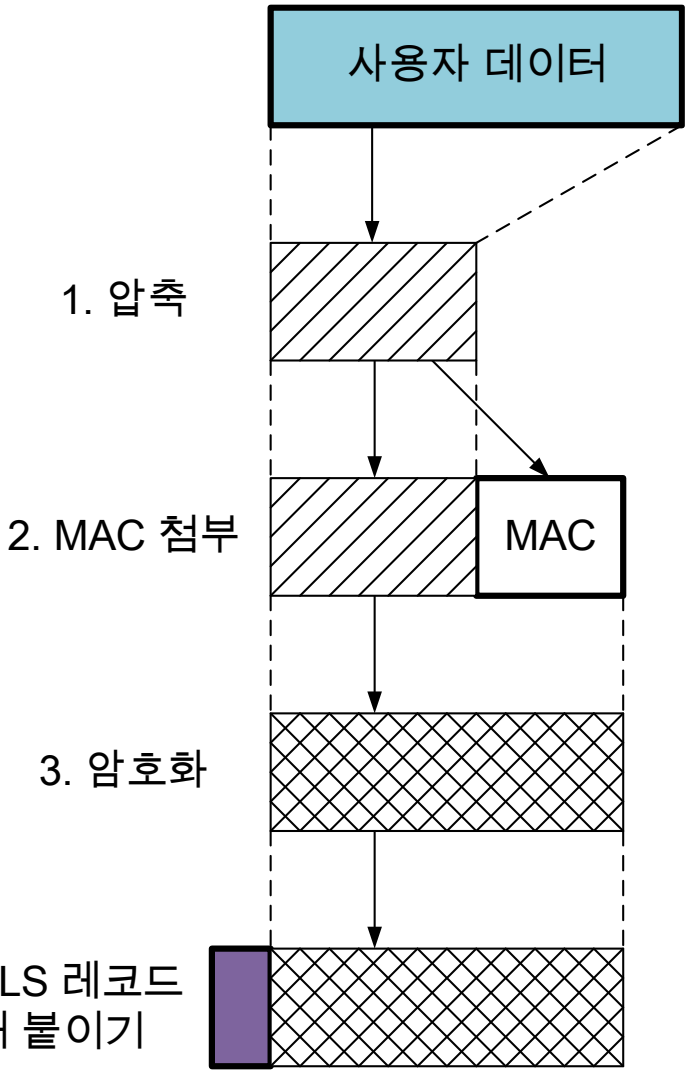
- WTLS 레코드 프로토콜(Record Protocol)
  - 정의
    - 상위 계층으로부터 사용자 데이터를 받아 PDU 안에 캡슐화를 담당하는 프로토콜
  - 포맷



필드	설명
레코드 길이 필드 표식(L)	레코드 길이 필드 존재 여부
순서번호 필드 표식(S)	순서번호 필드 존재 여부
암호명세 표식(C)	암호명세 여부 (0일 경우, 압축, MAC, 암호화 없음)
콘텐츠 유형	WTLS 레코드 프로토콜 상위 프로토콜

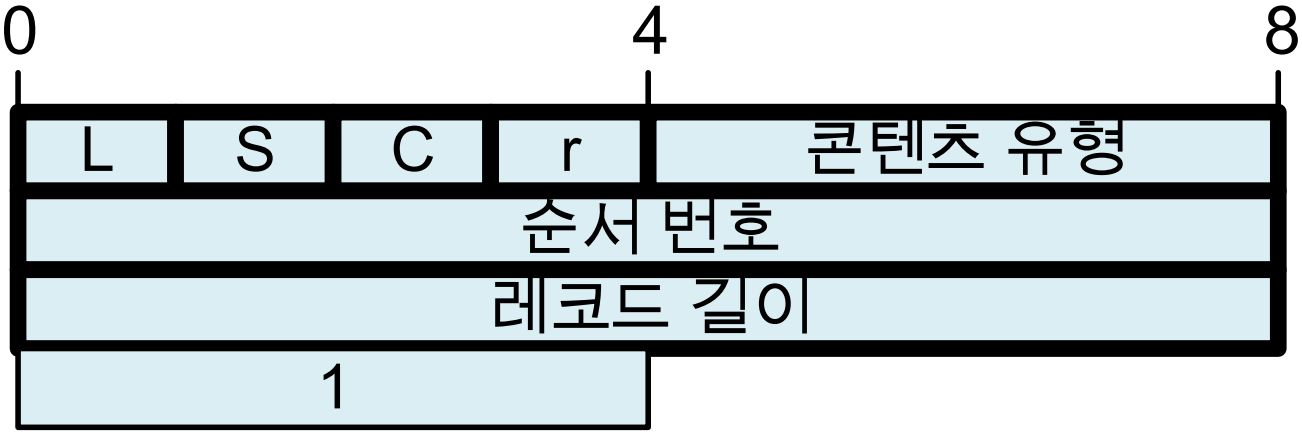
무선 전송 계층 보안

- WTLS 레코드 프로토콜(Record Protocol)
  - 동작과정
    1. 압축
       - 협상한 알고리즘으로 압축
    2. MAC 첨부
       - HMAC 알고리즘을 한 MAC 계산
    3. 암호화
       - 협상한 알고리즘으로 암호화
         - e.g., DES, 3DES, RC5 등
    4. WTLS 헤더 붙이기
  - WTLS에서 단편화는 이루어지지 않음
    - UDP/WDP 계층에서 단편화가 이루어짐



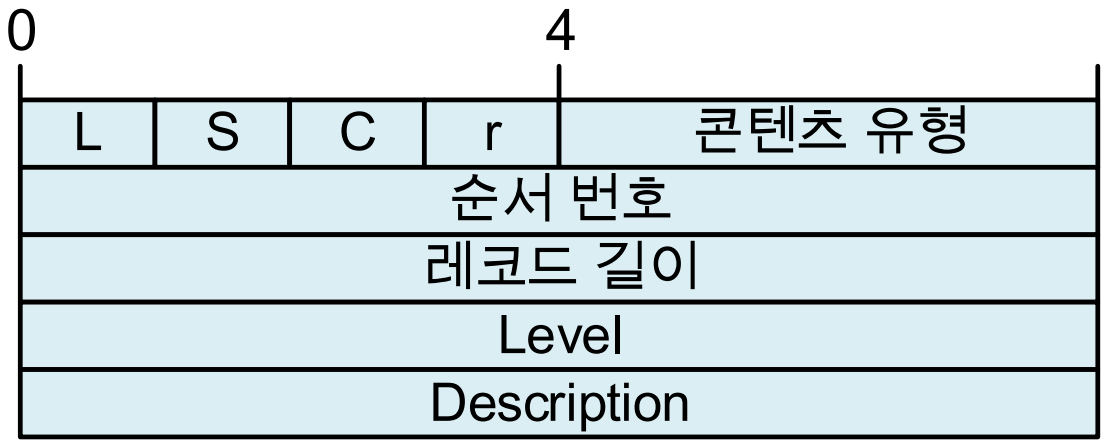
무선 전송 계층 보안

- WTLS 암호명세 변경 프로토콜(Change Cipher Spec Protocol)
  - 정의
    - 핸드셰이크 프로토콜에서 협상된 내용이 적용됨을 알림
  - 포맷



무선 전송 계층 보안

- WTLS 경고 프로토콜(Alert Protocol)
  - 정의
    - 대등 장비에 WTLS와 연관된 경고를 알리기 위한 프로토콜
  - 포맷



필드	설명
레벨 (Level)	위험(Warning), 심각 (Fatal) 2가지 값을 가짐
경고 (Description)	특정 경고를 나타내는 코드 삽입 (일반, 항상 심각 경고)

무선 전송 계층 보안

- WTLS 경고 프로토콜(Alert Protocol)
  - 항상 심각(Always Fatal) 경고

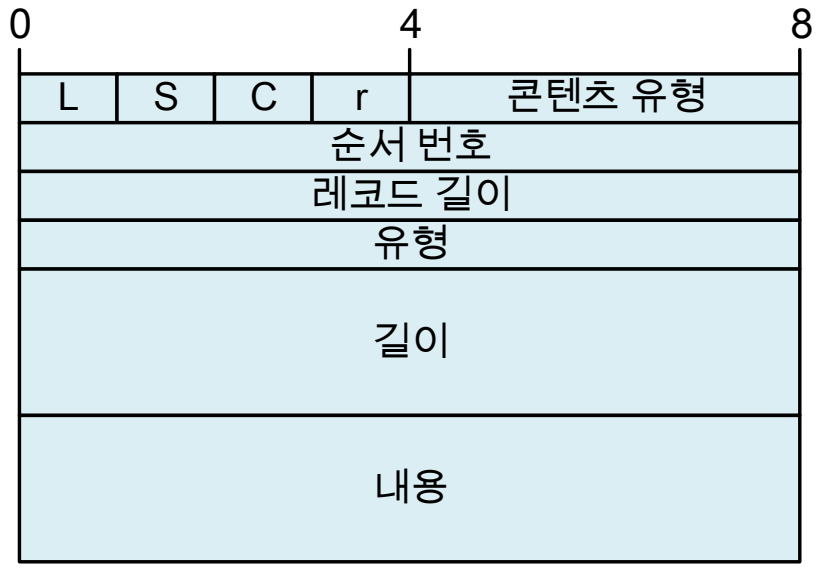
유형	설명
Session_Close_Notify	송신자가 현재 연결 상태나 안전 세션을 통해 메시지를 보내지 않는 것을 알림
Unexpected_Message	예상하지 못한 메시지가 수신됨
Bad_Record_MAC	부정확한 MAC이 수신됨
Decompression_Failure	압축해제 함수가 부정확한 입력을 받음
Handshake_Failure	핸드셰이크 메시지의 필드가 허용된 값의 범위를 초과함

  - 일반적인 경고

유형	설명
Connection_Close_Notify	송신자가현재 상태로는 더 이상 메시지를 보내지 않을 것이라고 알림
Bad_Certificate	수신한 인증서에 대한 문제가 있음을 알림(확인할 수 없는 서명 등)
Unsupported_Certificate	지원되지 않은 형식의 인증서 수신
Certificate_Revoked	수신된 인증서가 취소됨
Certificate_Expired	수신된 인증서의 유효기간이 경과함
Certificate_Unknown	수신된 인증서에 대해 알 수 없는 문제가 발생

무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 정의
    - 통신하기 전에 필요한 보안 설정들의 협상을 수행하는 프로토콜
  - 포맷



필드	설명
유형	핸드셰이크 프로토콜 메시지 식별
길이	메시지 길이
내용	유형에 해당하는 내용

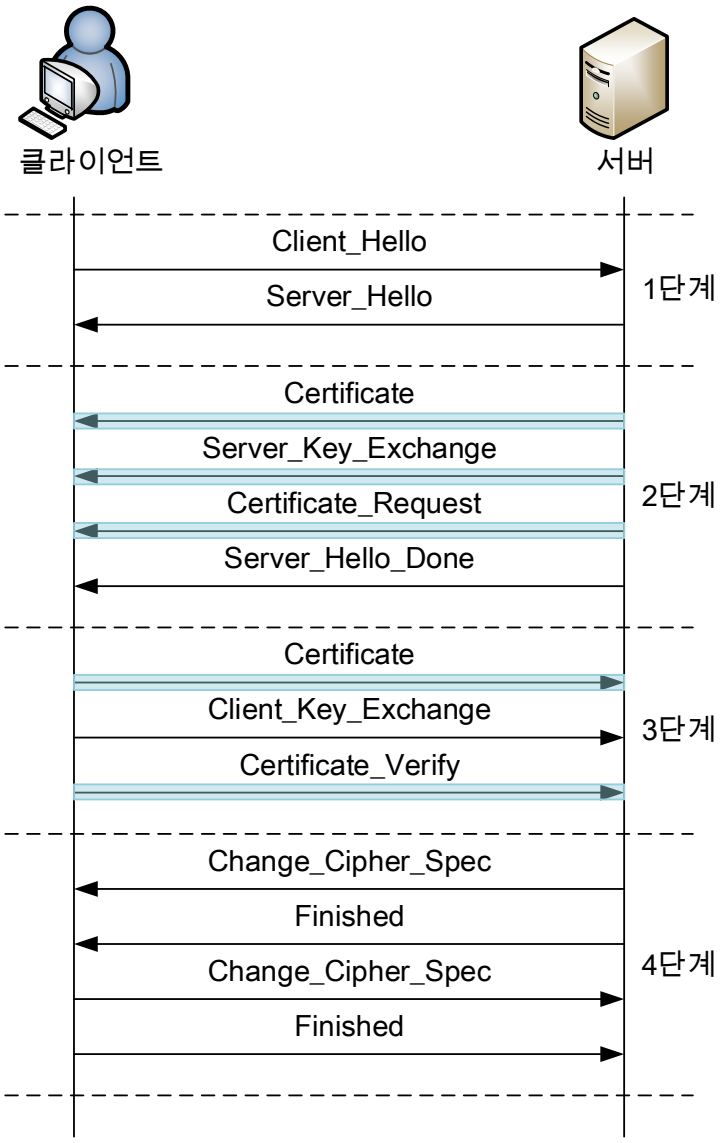
무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 종류
    - 완전-핸드셰이크(Full-Handshake)
      - 새로운 세션을 시작할 때 사용되는 프로토콜
    - 최적화된 완전-핸드셰이크(Optimized Full-Handshake)
      - 서버는 클라이언트 인증을 위해 인증서를 요청하지 않고 서버 내 보관된 인증서를 기반으로 인증 수행
    - 단축-핸드셰이크(Abbreviated-Handshake)
      - 기존 세션을 재개해서 다시 이용할 경우 사용되는 프로토콜

무선 전송 계층 보안

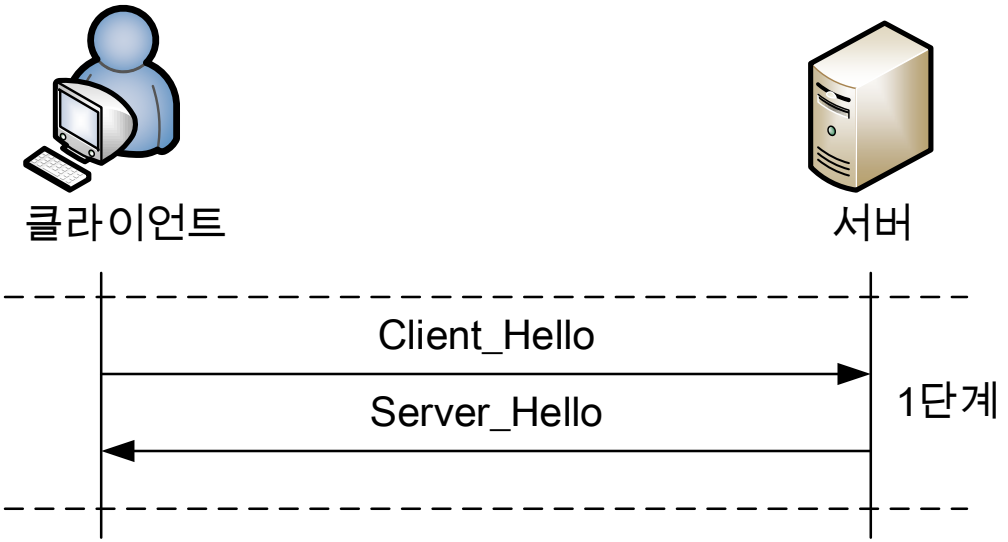
- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정

메시지 유형	매개변수
Client_Hello	버전(Version), 랜덤(Random), 세션 ID(Session ID), 암호도구 (Cipher Suite), 압축 방법 (Compression Method)
Server_Hello	
Certificate	연속된 X.509v3 인증서 (Chain of X.509v3 Certificate)
Server_Key_Exchange	매개변수(Parameters), 서명(Signature)
Certificate_Request	유형(Type), 기관(Authorities)
Server_Hello_Done	없음(Null)
Certificate_Verify	서명(Signature)
Client_Key_Exchange	매개변수(Parameters), 서명(Signature)
Finished	해시 값(Hash Value)



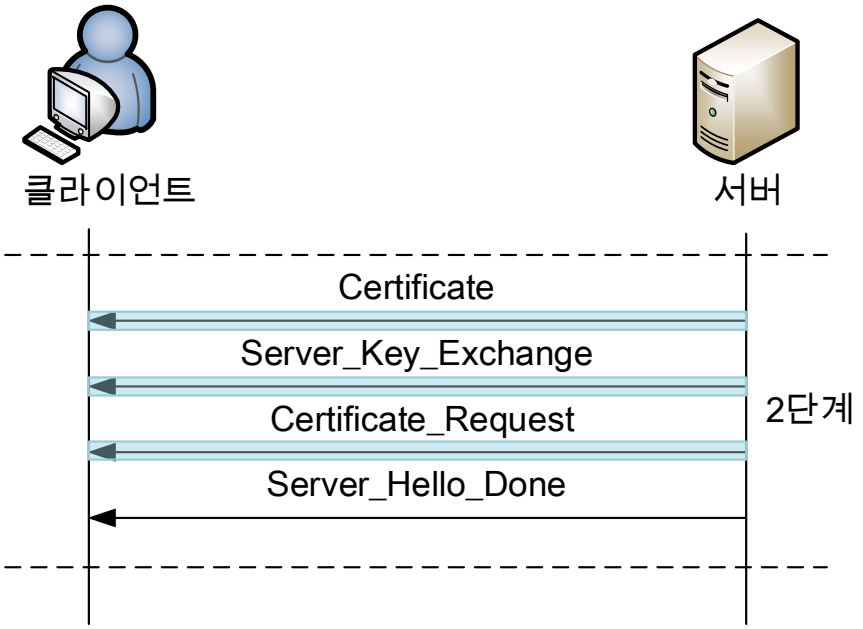
무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 1단계: 보안 기능 설정
      1. 지원 가능한 암호 방식, 키 교환 방식,서명 방식, 압축 방식을 서버에게 알림
      2. 수용 가능한 암호 방식, 키 교환 방식,서명 방식, 압축 방식을 응답. 또한, 새로운 세션 ID 할당



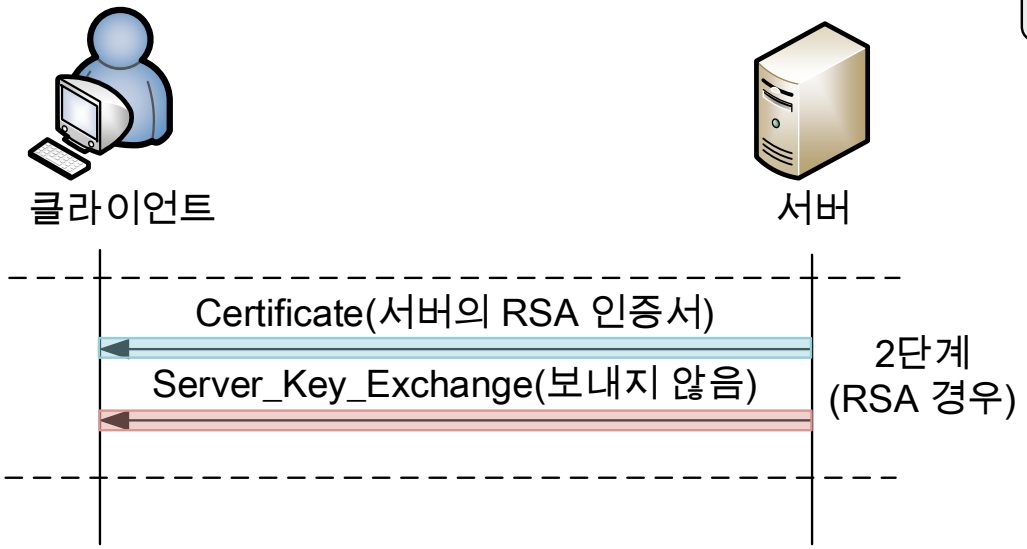
무선 전송 계층 보안

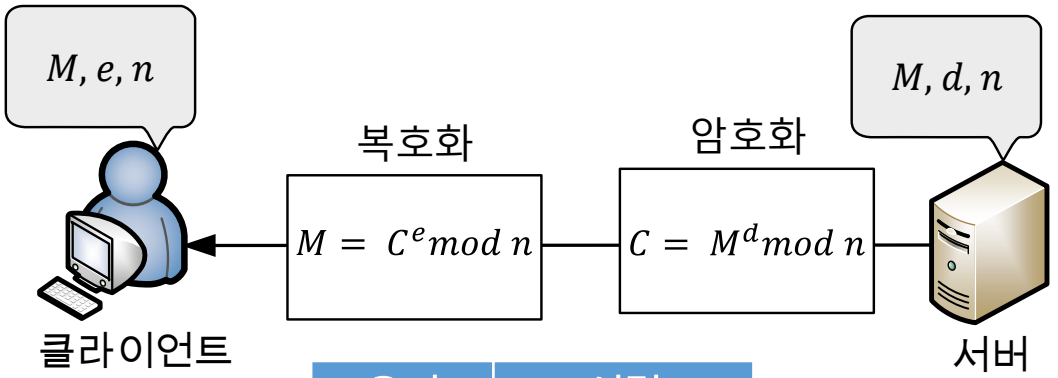
- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 2단계: 서버 인증과 키 교환
      1. 서버의 인증서 전달
      2. 키 교환 알고리즘에 따라, Server_Key_Exchange 전달
         - RSA, 익명 Diffie-Hellman, 타원곡선 Diffie-Hellman 등
      3. 클라이언트의 인증서 요청
      4. Server_Hello_Done 메시지 전송



무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 2단계: 서버 인증과 키 교환(RSA)
      1. 서버의 인증서 전송
      2. Server_Key_Exchange는 전송하지 않음

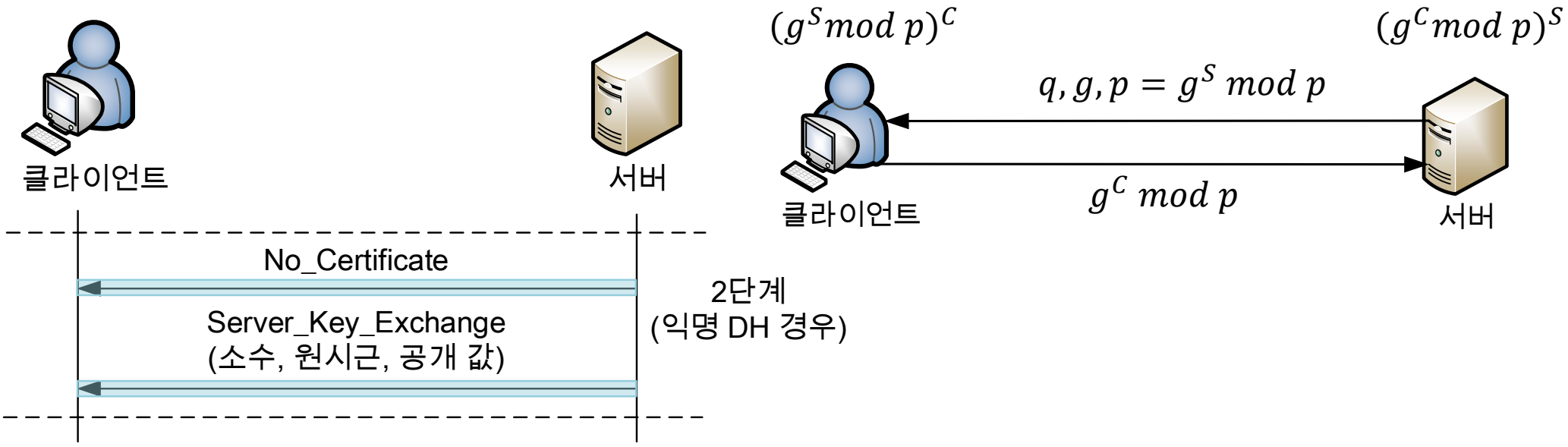




용어	설명
C	암호문
M	평문
d	개인키
e	공개키
n	소수의 곱

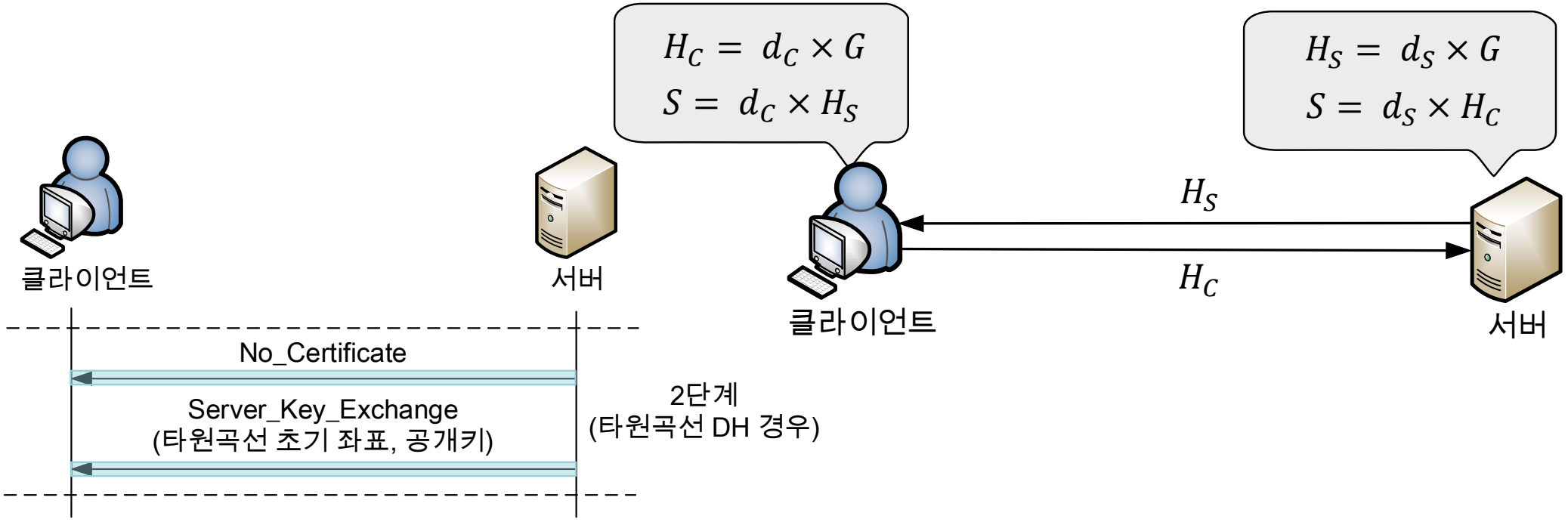
무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 2단계: 서버 인증과 키 교환(익명 Diffie-Hellman)
      1. No_Certificate 메시지 전송
      2. Server_Key_Exchange 메시지로 Diffie_Hellman에 사용되는 소수(q), 원시근(g), 공개 값(p)를 전송
    - Pre_Master_Secret 계산: $g^{CS} \ mod \ p$



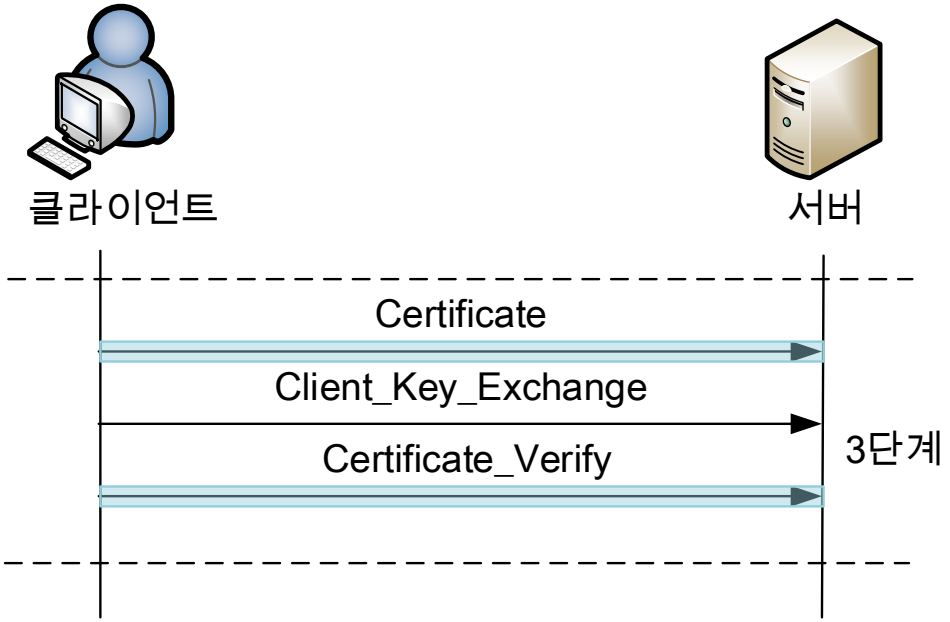
무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 2단계: 서버 인증과 키 교환(타원곡선 Diffie-Hellman)
      1. No_Certifiacet 메시지 전송
      2. Server_Key_Exchange 메시지로 Diffie_Hellman에 사용되는 타원곡선 초기 좌표(G), 공개키(H_S)를 전송



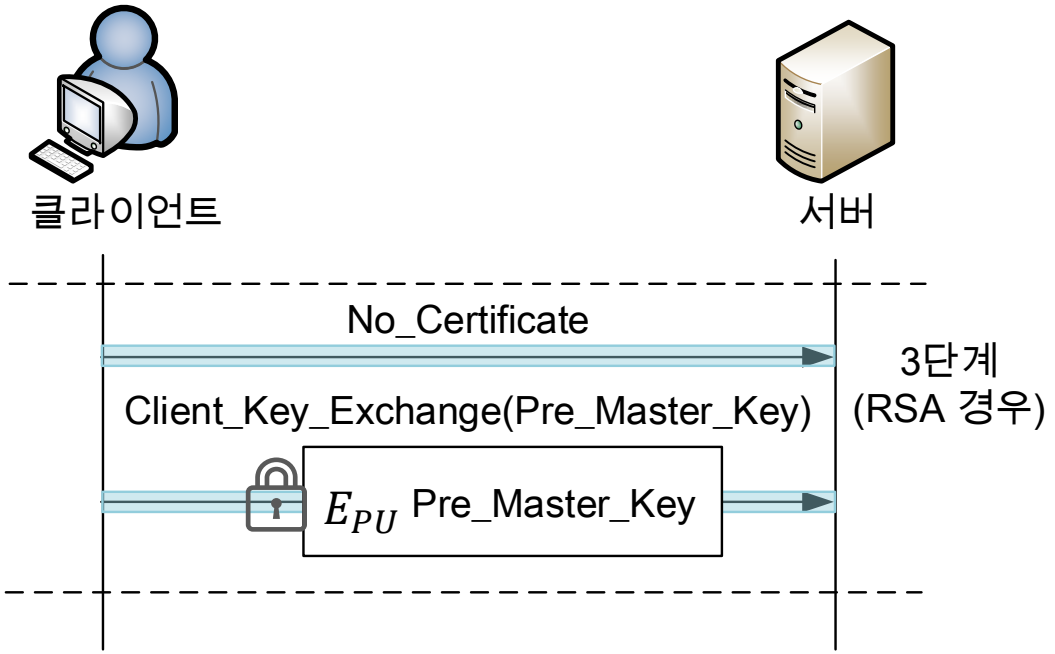
무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 3단계: 클라이언트 인증과 키 교환
      1. 클라이언트의 인증서 전달
      2. 키 교환 알고리즘에 따른 응답 값과 Pre_Master_Key 전송
         - RSA, 익명 Diffie-Hellman, 타원곡선 Diffie-Hellman 등
      3. 클라이언트인증서의 확인을 위한 Certificate_Verify 메시지를 보냄



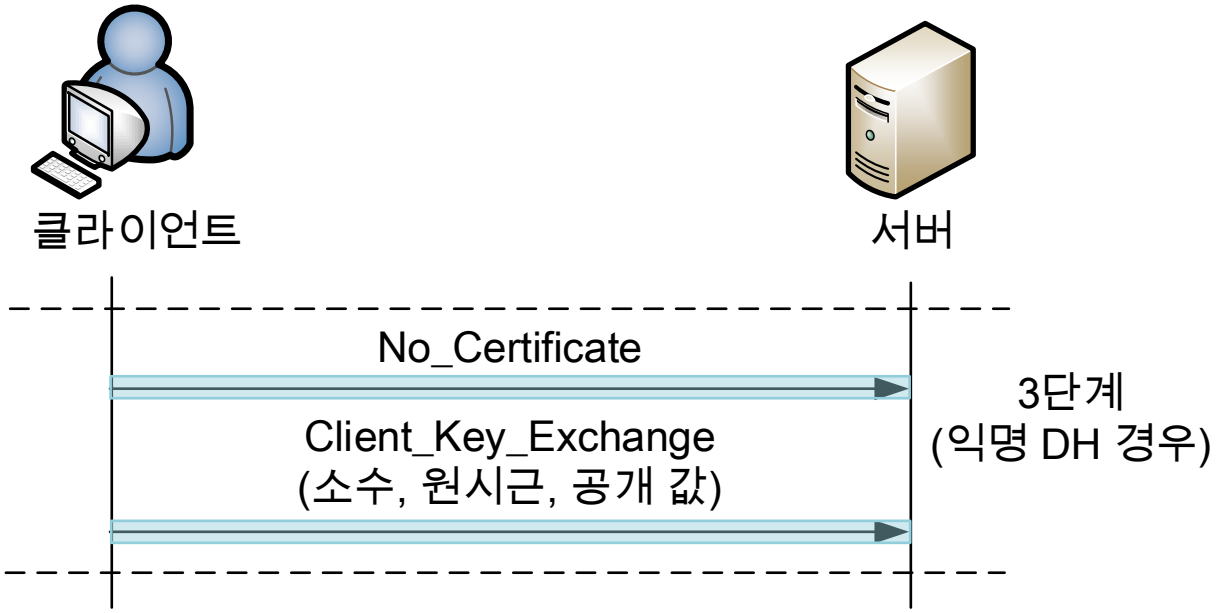
무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 3단계: 클라이언트 인증과 키 교환(RSA)
      1. No_Certificate 전송
      2. Pre_Master_Secret 계산: Client_Version + Nonce
      3. 서버의 공개키(PU)로 Pre_Master_Secret를 암호화(E)하여 전송



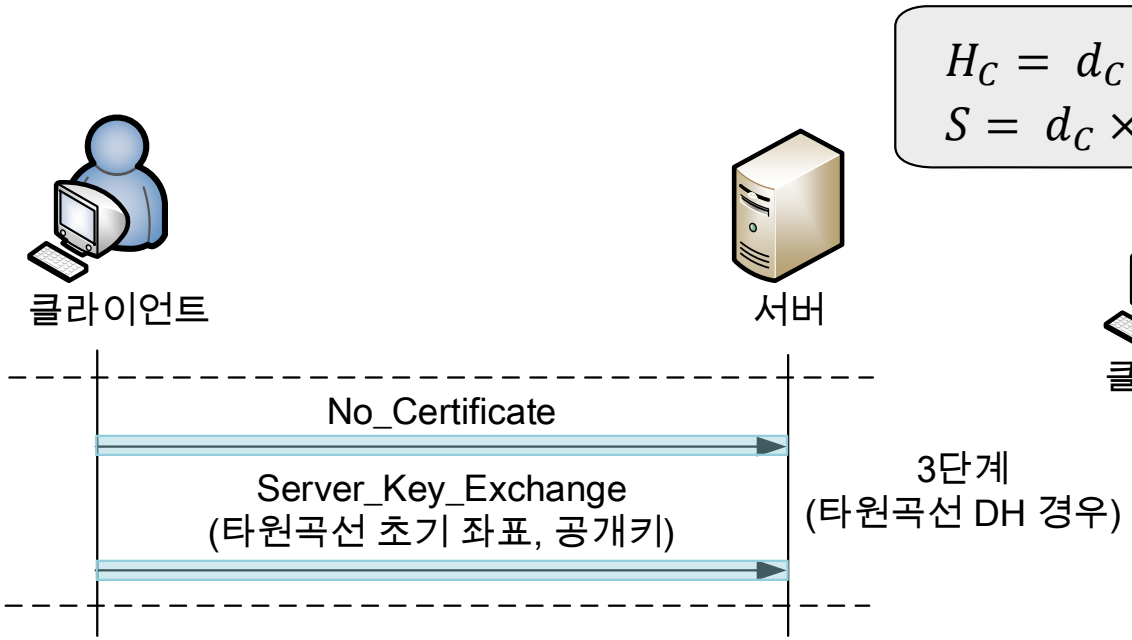
무선 전송 계층 보안

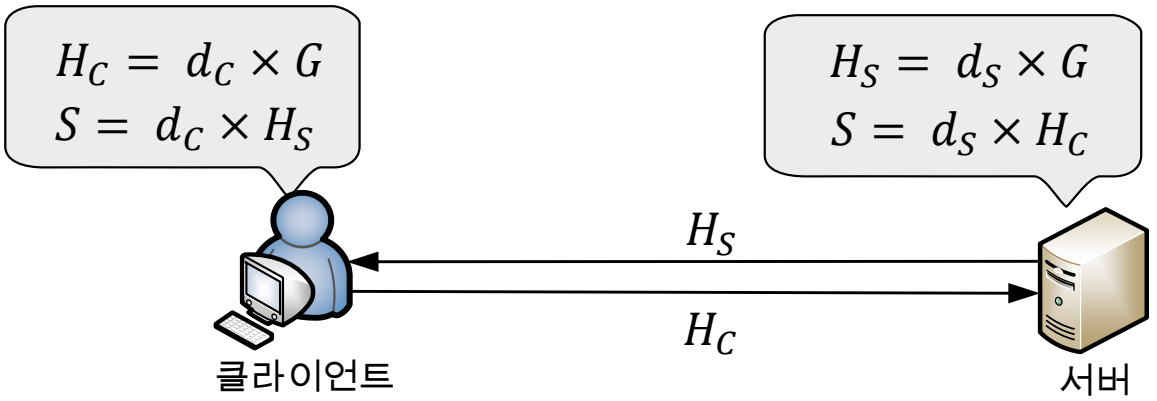
- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 3단계: 클라이언트 인증과 키 교환(익명 Diffie-Hallman)
      1. No_Certificate 전송
      2. Client_Key_Exchange 메시지로 Diffie_Hellman에 사용되는 소수(q), 원시근(g), 공개 값(p)를 전송



무선 전송 계층 보안

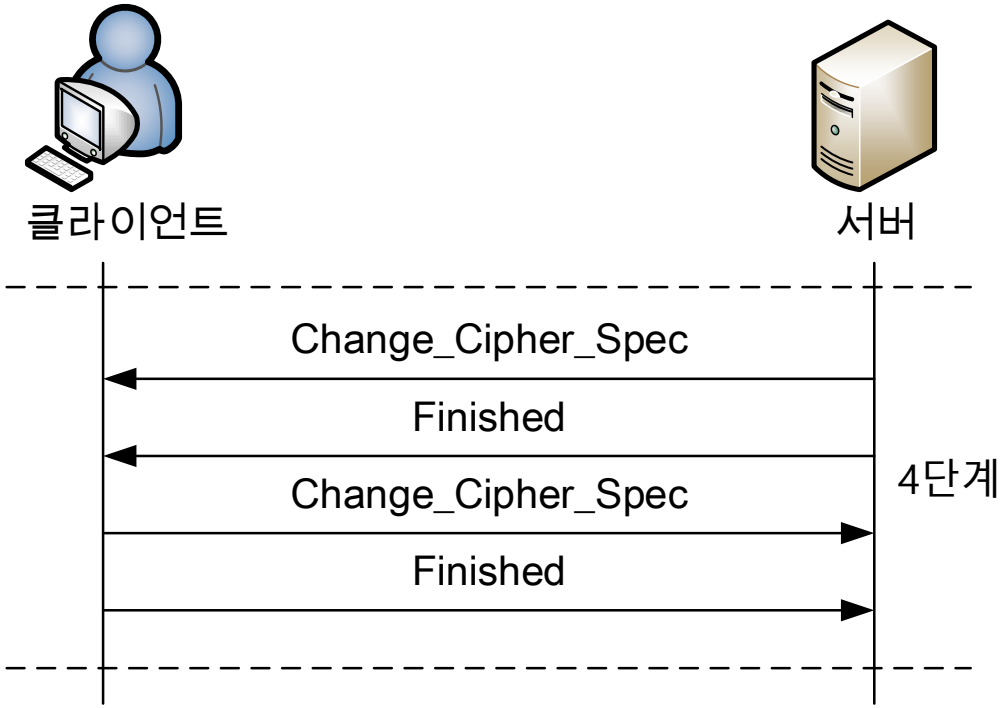
- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 3단계: 클라이언트 인증과 키 교환(타원곡선 Diffie-Hallman)
      1. No_Certifiacet 메시지 전송
      2. Server_Key_Exchange 메시지로 Diffie_Hellman에 사용되는 타원곡선 초기 좌표(G), 공개키(H_C)를 전송





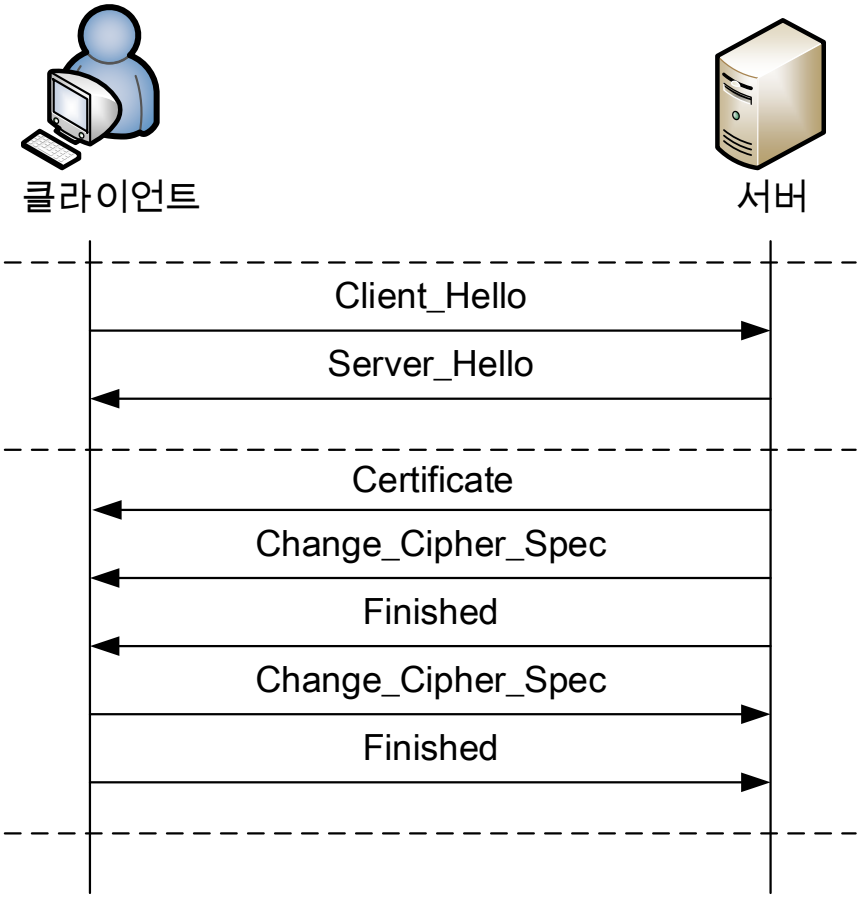
무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 동작과정
    - 4단계: 종료
      - 안전한 연결종료
        - Finished 메시지는 키 교환과 인증 과정이 성공적임을 나타냄



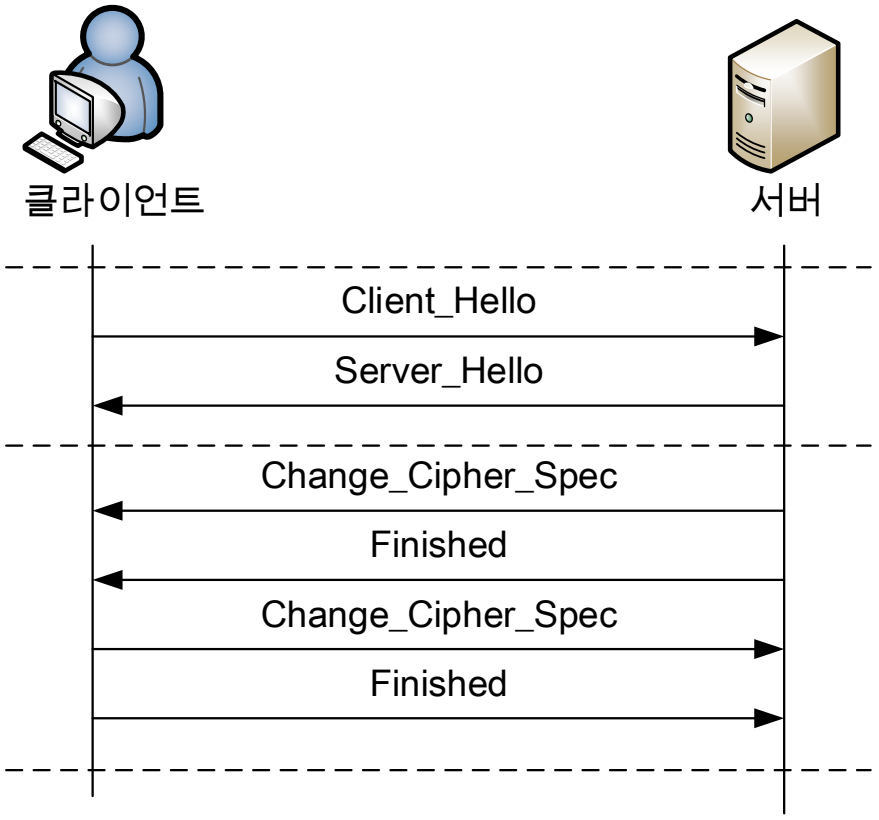
무선 전송 계층 보안

- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 최적화된 완전-핸드셰이크(Optimized Full-Handshake)
    - 서버가 클라이언트의 인증서를 다른 경로를 통해 가지고 있는 경우
    - 동작과정



무선 전송 계층 보안

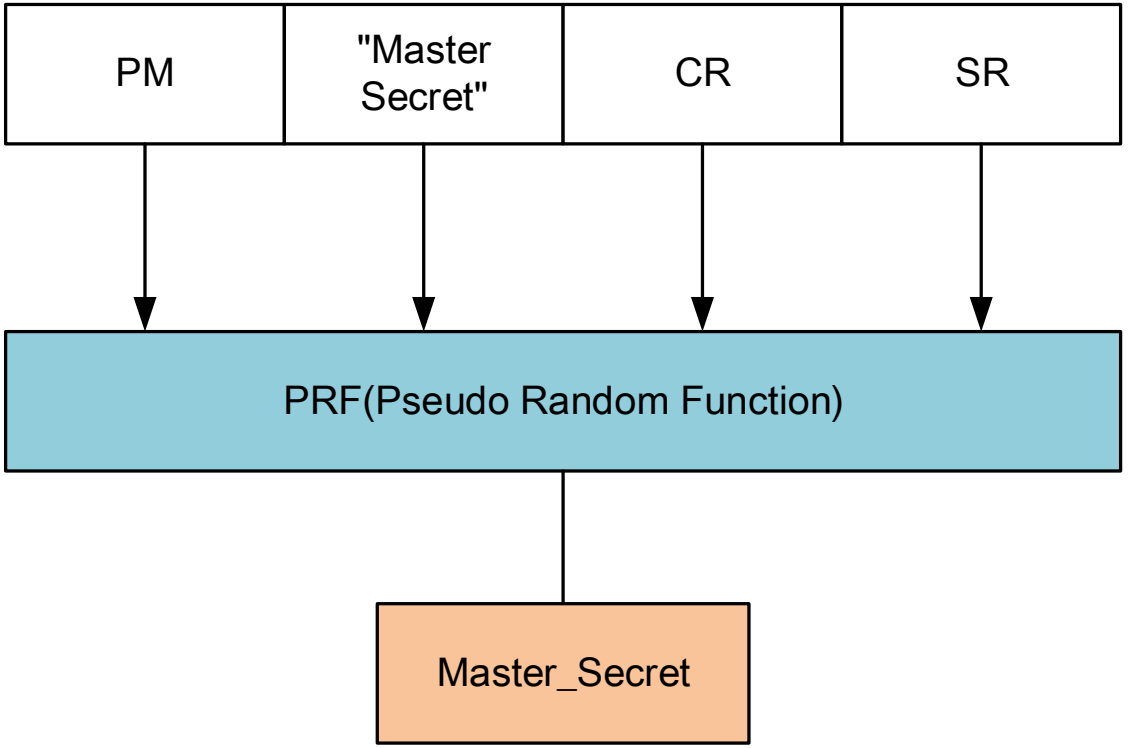
- WTLS 핸드셰이크 프로토콜(Handshake Protocol)
  - 단축-핸드셰이크(Abbreviated-Handshake)
    - 이전 보안 세션을 재개하는 경우
      - 서버와 클라이언트 인증을 위한 정보는 교환하지 않음
  - 동작 과정



무선 전송 계층 보안

- 암호 계산
  - Master Secret 암호계산과정

매개 변수	설명
PM	Pre_Master_Key
“Master Secret”	문자열 입력 값
CR	클라이언트의 랜덤 값
SR	서버의 랜덤 값



목 차

- IEEE 802.11 무선 LAN
- IEEE 082.11i 무선 LAN 보안
- 무선 응용 프로토콜
- 무선 전송 계층 보안
- 종단-대-종단 보안

WAP 종단-대-종단 보안

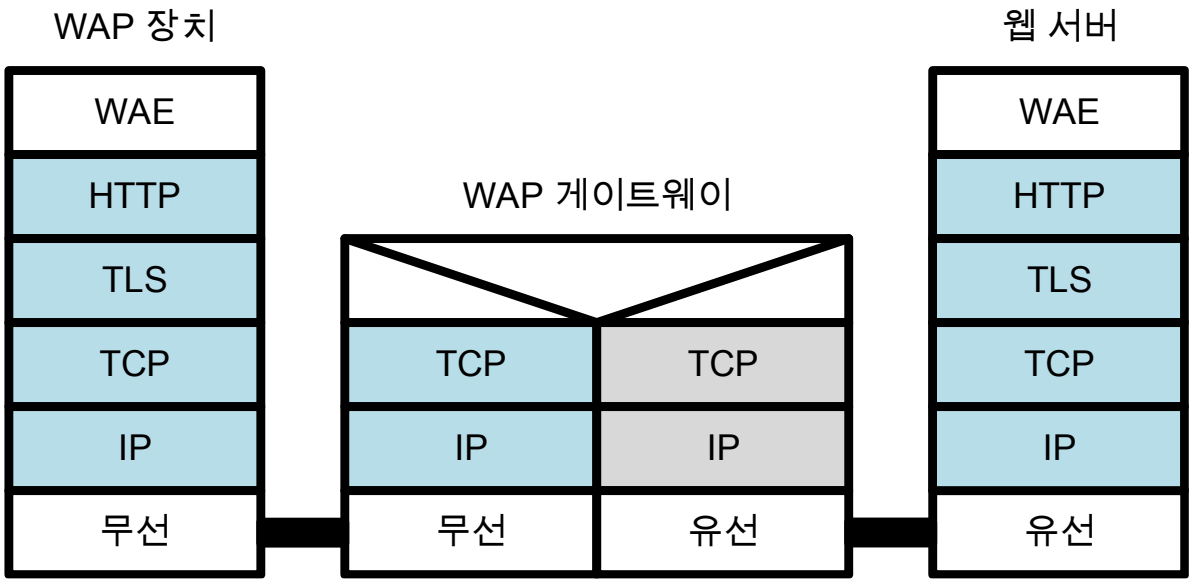
- 한계점
  - WTLS의 사용
    - TLS를 무선 환경에 적용하기 위해 수정한 프로토콜
      - 제한된 환경으로 인해 일부 알고리즘 사용 제한
  - WAP 종단간 불안정성
    - WAP가 사용하는 프로토콜과 인터넷 프로토콜이 서로 다름
      - 두 프로토콜의 연결을 위한 WAP G/W의 사용으로 인해 발생하는 한계점 존재

WAP 종단-대-종단 보안

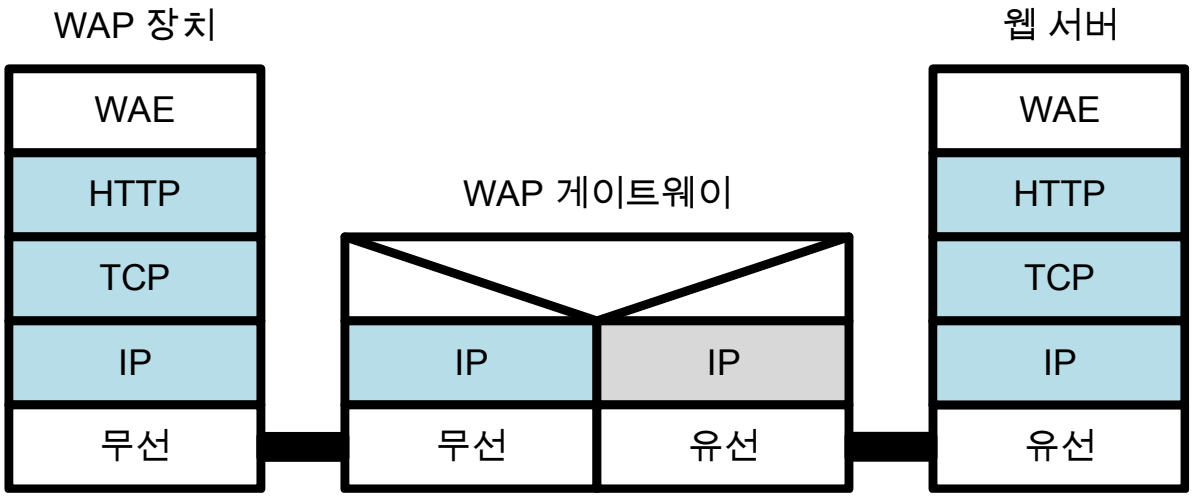
- 대응 방안
  - TLS 사용
    - 두 종단 사이에 안전한 TLS 세션 설치
    - WAP G/W는 TCP 계층의 G/W로 동작
      - G/W를 통과하는 동안 TCP 데이터는 암호화 되어있기 때문에 종단-대-종단 보안유지가능
  - IPsec 사용
    - 클라이언트나 G/W에서 IPsec을 사용함으로써, 모든 과정에서 데이터가 암호화됨
      - 종단-대-종단 보안 유지 가능

WAP 종단-대-종단 보안

- 보안 구조
  - TLS 기반



  - IPsec 기반



Thanks!

박 재 형 (jaehyoung@pel.sejong.ac.kr)