Wireless

Part 1.

무선 랜

01 무선 랜

무선랜

유선 LAN과 무선 단말 사이를 무선주파수를 이용하여 전송하는 제반 기술 및 시스템
전파를 이용한 데이터 통신

유썬 LAN이 트위스트 페어 , 동축케이블 , 광(Fiber)등을 전송선로로 이용하는 반면 무선 LAN은 대기를 통하여 전파를 전송한다

무선 LAN은 유선 LAN을 대체하기 보다는 기간망과 이동(Mobile)사용자 간 수십 미터 이내의 종단 연결점을 제공한다는 개념으로 Mobility와 Scalability를 발휘할 수 있는 장점이 있다

Access Point(엑세스 포인트)
- 기존 유선 랜(Hub나 스위치와 연결)과 무선 랜 연결시 사용하는 장비이다
- Data의 전송 및 Buffering 기능을 제공하며, 하나의 Access point는 수십 명 - 수백명의 사용자를 지원하고 수 km까지 지원 가능 하다

01 무선 랜

무선랜

네트워크 타입

Ad-Hoc Network	Infrastructure Network
Access Point 없이 무선 클라이언트 상호 간의 데이터 전송하는 방식 유선 네트워크에 대한 접근을 지원하지 않기 때문에 Access point를 필요로 하지 않음	유선 랜과 무선 랜 간의 통신이 가능한 구조 Access Point를 기반으로 무선 클라이언트 간에 데이터 전송하는 방식

01 무선 랜

무선랜

무선랜을 구성하는 계층

MAC 계층	CSMA/CA 매체 접근 제어 방식 Carrier Sense Multiple Access with Collision Avoidance CSMA/CD와는 달리 네트워크의 케이블에 데이터의 전송이 없는 경우라도 충돌을 대비하여 확인을 위한 신호를 전송 확인 신호가 충돌없이 전송된 것을 확인하면 이어서 데이터 전송
PHY 계층	무선 랜에 대한 물리적 특성을 정의 - 협대역 마이크로웨이브 - 적외선 - 확산대역(DSSS,FHSS)

01 무선 랜

무선랜

CSMA/CA 통신 방식

1 Listen Air Space(radio wave)	전파(radio wave) 를 통한 통신이 일어나고 있는지 확인
2 Set Randomwait timer before sending frame	다시 랜덤한 시간 동안 대기 (충돌 방지목적)
3 After timer has passed,listen again and send	랜덤한 시간이 지난 후 한번더 통신여부 확인 후 프레임 전송
4 Wait for an Ack	데이터 전달후 수신확인신호(ACK)를 받기위한 대기
5 if no Ack, resend the frame(다시 1번으로)	만약 정해진 시간동안 Ack 를 받지 못했다면 전송 실패한 것으로 간주, 1 로 돌아가 전송 시도

01 무선 랜

무선랜

인코딩 방식

FHSS(Frequency Hopping Spread Spectrum)

무선 신호(radio signal)를 많은 주파수 채널로 빠르게 바꿔가면서 호핑(건너뜀) 하며 전송하는 방식
복잡한 알고리즘을 이용
잡음과 간섭 같은 고질적인 통신 문제에 강점이 있는 방식
최초의 IEEE802.11 무선 방식이 이방식을 이용해서 인코딩
IEEE802,11a ,802,11b, 802.11g 는 현재 이방식을 사용하고 있지 않음

DSSS(Direct Sequence Spread Spectrum)

여러 채널중 한 채널을 잡고 그채널로만 전송하는 방식
매우 작은 전력으로 넓은 대역으로 전송하기 때문에 잡음에 영향을 적게 받고, 낮은 전력 사용으로 다른 통신에 영향을 덜 주며, 보안도 우수하다는 장점을 가짐
802.11b 무선 통신에서 사용하는 인코딩 방식(2.4GHz)
최대 11개의 채널(한국은 13개 채널까지 가능)을 지원하며, 이중 비중첩 채널은 3개임
무선랜장치 (예: AP) 를 2개이상 이용하여 ESS 망을 구축하는 경우에는 채널간 충돌을 염려하여 비중첩 채널을 사용

01 무선 랜

무선랜

인코딩 방식

OFDM(Orthogonal Frequency Division Multiplexing)

직교 주파수 분할 다중 방식
하나의 시그널을 여러 개의 주파수로 나누어 보내는 방식
전파의 직교성을 이용, 주파수가 서로 겹쳐도 간섭이 일어나지 않아 좀 더 많은 주파수 분할이 가능
IEEE802.11a , IEEE802.11g 가 사용

01 무선 랜

무선랜

IEEE 802.11
- 미국전기전자학회(IEEE)의 작업 그룹에서 개발한 무선 LAN 규격
- 규격에는 802.11 , 802.11a, 802.11b,802.11g, 802.11n이 있으며, 이들 모두 경로 공유 프로토콜로서 반송파 감지다중접속.충돌 예방(CSMA/CA)을 사용하고 있다

무선랜 표준 규격의 종류별 특징

표준규격	속도	범위	주파수	변조	장점	단점
802.11a	54Mbps	35m	5GHz	OFDM	주파수 대역이 구별되어 전파간섭이 적은편	주파수 대역이 달라 호환성 없음
802.11b	11Mbps	38m	2.4GHz	DSSS	가장 많이 사용되고 있음	전송 속도가 느림
802.11g	54Mbps	38m	2.4GHz	DSSS/ OFDM	802.11b와 호환 가능	2.4GHz 기기들로부터 간섭이 있을수 있음
802.11n	248Mbps	70m	2.4GHz/5GHz	OSFM	다중 안테나 기술과 채널을 통한 성능 증가	2.4GHz 기기들로부터 간섭이 있을 수 있으며, 제대로 활용하기 위해 무선랜카드 선택이 중요

OFDM : 직교 주파수 분할 다중 방식(Orthogonal frequency-division multiplexing)
DSSS : 직접 시퀀스 대역 확산(Direct Sequence Spread Spectrum)

01 무선 랜

무선랜

SSID

Service Set Identifier
무선 네트워크에서 사용하는 이름
32바이트로 구성
같은 무선 네트워크 안에 있는 무선 장비들은 모두 같은 SSID를 가져야 함
디폴트값로 설정되어 있으면 100ms 마다 SSID와 기타 구성 정보를 Broadcast로 네트워크로 Flooding

02 무선 랜 보안

무선랜 보안

무선 LAN 접속 방식

무선단말이 무선 매체 또는 무선 네트워크에 엑세스(접근)하는 방식으로 관점에 따라 여러가지로 구분됨

무선 LAN 접속 : 사용자 접속 보안 관점

구분		인증 방식	암호화 방식	비고
개방 인증	SSID 숨김	-	-	보안은 아니나, 현실적으로 사용
	MAC 인증	-	-	보안은 아니나, 현실적으로 많이 사용
공유키	WEP	-	RCA	보안 취약으로 비추천
인증,암호 모두 사용	WPA	802.1x/다양한 EAP	TKIP	
	802.11i	802.1x/다양한 EAP		
	WPA2	802.1x/다양한 EAP	AES	

02 무선 랜 보안

802.11 인증 방식 종류

Pre RSN (과거,기존 방식)

개방 인증 (Open-system Authentication) / MAC 주소 인증 (사실상 무인증임)
- 인증 수준 : 사실 인증이라고 할 수 없고 단말 확인 정도의 수준임
  . 이동노드 MAC 주소의 확인 정도임
  . 개방 인증 요청시 해당 무선 스테이션의 MAC 주소를 송부하게 되어있어,
  이를통해 단말 확인을 하는 정도임

공유키 인증 (Shared Key Authentication) (선택사항임, 사실상 현재 사용 안함)
- 인증 수준 : 쌍방이 동일한 WEP용 암호키를 갖고있음을 단순히 확인하는 정도
  . 무선단말에 대한 인증 임

- 암호 방식 : WEP (보안 취약점 때문에 비 추천)
  . WEP는 공유키에 의한 스트림 암호화 방식인 RC4에 기반을 둔 암호화 알고리즘

02 무선 랜 보안

802.11 인증 방식 종류

RSN 인증 : (더 안전한 현재의 802.11 인증 방식)

RSN 또는 RSNA (Robust Security Network Association) 이라고 불리움
- 한편, Wi-Fi Alliance의 보안 인증 심사규격 명칭으로는, WPA 또는 WPA2 라고도 함

RSN 특징

- 그 이전과는 다른 새로운 하드웨어,소프트웨어 필요

- 802.1X를 통해 Supplicant,Authenticator,Authentication Server 모두 관여
  . (Supplicant : 무선단말, Authenticator : AP, Authentication Server : 인증 서버)
  . 802.11i-2004에서 최초 정의됨
  . 802.1X를 통해 동적으로 생성 정의되는 PMK로부터 암호화 키(Cipher Suite)가 유도됨
  .. 인증 절차로부터 생성된 PMK를 활용하여, 매 패킷 마다 상이한 암호 키 및 무결성 키에 의해 무선구간이 보호됨
  . 한편, 공유키 인증으로 개별적으로 인증된 이동단말은 RSNA으로의 결합이 허용안됨

-> 다음장에 계속

02 무선 랜 보안

802.11 인증 방식 종류

RSN 특징

- 인증 및 암호화의 완벽한 분리 : 802.11i
  . 802.1X에 기반을 두고 무선 LAN에 이를 적용한 표준
    .. `인증`과 `암호화` 두 기능이 완벽하게 분리됨
    .. 즉, 인증이 성공한 후 비로소, 인증 서버는 세션 암호화키를 생성,배포하게됨
  . 암호 방식 : TKIP(선택), CCMP(필수)
    .. 패킷별로 상이한 키로 암호화가 적용됨
  . 인증 방식
    .. PSK(Pre Shared Key) : 무선단말 및 AP 간에 사전에 특정 키를 공유 (개인,SOHO)
    .. 802.1X/EAP(EAP-TLS,EAP-TTLS,PEAP,EAP-FAST 등) : 인증서버 필요 (대규모 망)

- 무선 LAN의 이동 보안 (802.11 로밍 보안)
  . 무선 단말이 여러 AP를 거치며 핸드오프 시에도 보안 제공
  . 위장 AP 및 위장 단말 차단 등

END

고생하셨습니다