# WLAN에서 WPA-PSK 를 이용한 WDS 구간의 암호화

## An Encryption Scheme on the WDS Link using WPA-PSK in Wireless LANs


**최 정 희** (광운대학교 전자통신학과, 석사과정)
**민 상 원** (광운대학교 전자통신학과, 교수)
**조 용 천** (광운대학교 전자통신학과, 박사과정)
**정 광 모** (전자부품연구원, 책임연구원)
**박 영 충** (전자부품연구원, 선임연구원)



Key Words : WLAN, SECURITY, WDS


목 차



## Ⅰ. 서론

최근 해킹, 도청, 바이러스 등의 관심이 증폭되어 있어서 보안에 대한 관심이 높아져 있다. 하지만 유선 네트워크에 비하여 무선 네트워크의 보안성이 취약한 점은 사실이다. 이에 대한 무선 네트워크의 보안의 취약점을 극복하기 위해서 많은 연구가 이루어졌고 많은 성과를 거두어서 상용 제품으로까지 나와 있다.

현재 상용 제품으로 나와 있는 AP들은 기존에 사업자 시장에서 802.1x를 통해 사용자 인증과 암호화를 위해 사용하던 EAP-MD5, Dynamic WEP Key를 사용하는 TLS, TTLS, PEAP등의 인증 방식을 수용할 뿐만 아니라 802.11i 규격에서 무선 LAN 데이터 보호를 위한 암호화 알고리즘인 TKIP과 AES-CCMP 등의 여러 알고리즘을 다 제공하여 많은 부분에서 보안에 대한 취약점을 해결하였다. 또한 여러 기능을 통해 초기에 나온 제품들과의 호환성을 유지할 수 있도록 되어 있다. 이런 기술들의 발전으로 인해서 무선 네트워크에서 보안에 대한 많은 문제점이 해결되었다.

보안 문제가 많은 부분에서 보완이 되면서 보안과 더불어 관심사가 된 것은 무선 LAN에서 범위에 대한 확장이다. 이에 대해 WDS (Wireless Distribution System) 기능이 발전되었다.

WDS 기능은 AP들 간에 무선 네트워크를 구성할 수 있게 해 주는 기능으로서 인터넷에 연결되어 있지 않은 AP가 인터넷이 연결되어 있는 AP에 WDS로 연결하면, 인터넷에 연결되어 있지 않은 AP에 접속되어 있는 무선 클라이언트들이 인터넷을 사용할 수 있게 된다. 다시 말해서 이 기능은 AP가 무선 Bridge 혹은 Repeater의 역할을 해 줌으로써 한 AP가 제공하던 무선 통신 범위를 확장할 수 있도록 해 주는 기능이다. 이 기능은 유선으로 복잡하게 연결되어야 하거나 약간의 이동 거리를 위해서 새로 망을 설치해야 하는 번거로움을 대체할 수 있는 방법으로 사용되어 지고 있으며 좀 더 확장된 개념으로 mesh network로까지 확장될 수 있다.

그러나 WDS기능을 통해서 무선 LAN 을 이용할 수 있는 범위는 확장이 되었지만 여전히 보안에 대한 이슈는 남게 되었다. 즉 WDS기능은 AP간의 통신을 위해서 만들어진 기능이고, 이 WDS구간을 사용하고 있는 AP들은 서로의 통신을 위해서 이 구간을 OPEN 모드나 Static WEP를 사용하여 통신을 하고 있다. 이 두 모드에서는 기존에 무선 LAN이 갖고 있던 보안의 취약점을 그대로 갖고 있다. AP의 무선 보안 기능이 강화되면서 새롭게 개발된 기능을 WDS 을 이용하게 되면 강화된 기능을 사용하지 못하게 되며 일반 보안 기능이 없는 무선 LAN 초기 제품의 문제점을 그대로 안고 사용하게 되는 것이다.

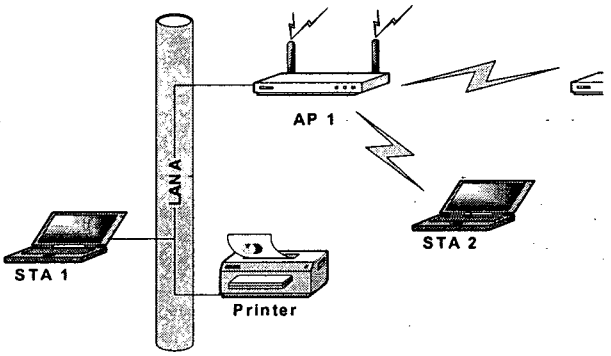
본 논문에서는 WDS 구간에서 현재까지 나와 있는 보안 방법 중 WPA-PSK 방식을 사용하여 이 구간의 데이터를 암호화 함 으로써 WDS 기능을 통해 무선 LAN의 무선 연결 범위를 확장시킬 뿐 만 아니라 보안의 대한 취약점을 어느 정도 간단한 방법을 통해 해결함으로써 보다 안전하게 무선 LAN을 사용할 수 있도록 할 수 있는 방안을 제안한다.

## Ⅱ. WDS 링크의 WPA-PSK 암호화

### 1. WDS 를 이용한 REPEATER MODE

그림 1과 같이 AP1은 망과 연결되어 있어서 STA2는 직접 망과 연결된 STA1 과 Printer를 AP1 을 통해서 직접 통신을 할 수 가 있다. 이 때 AP2는 WDS를 이용하여 AP1과 WDS 연결을 하게 되면 AP2에 붙어 있는 STA3 는 STA1, STA2, 그리고 Printer와 연결하여 사용할 수 있게 된다. 여기

서 주의해야 할 점은 AP1 과 AP2를 WDS로 연결할 때에는 AP1과 AP2는 같은 채널을 사용해야만 한다. 또한 본 논고에서는 WPA-PSK 의 암호화를 위해서 AP1과 AP2는 서로 같은 SSID를 사용하도록 한다. 이처럼 WDS를 사용하게 되면 보다 넓은 무선 영역을 확보하게 되며 간단한 방법으로 설치가 끝나게 된다. WDS기능은 이미 많은 AP에서 지원하고 있고 많은 문서에 나와 있기 때문에 본 논문에서는 WDS에 대한 기술적인 설명은 생략하도록 한다.




<그림 1> Wireless Repeater Mode

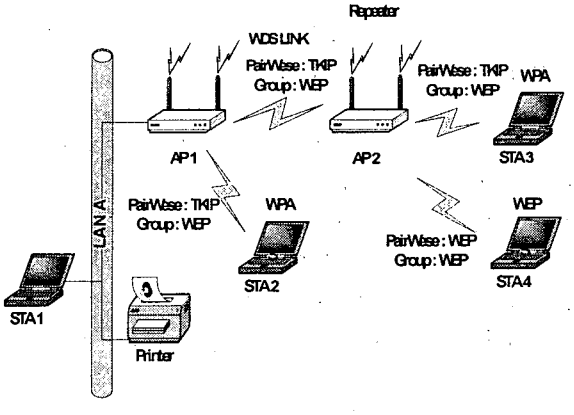
서두에서 말한 바와 같이 지금 현재 시중에 나와 있는 AP들은 많은 암호화 방법을 통해서 데이터를 암호화 할 수 있으며, 그림1>에서도 AP2와 STA3에서도 다양한 방법의 암호화를 통해서 데이터를 암호화 할 수 있다. 다양한 암호화 방법 중에는 본 논문에서는 각 가정이나 SOHO 에서 인증 서버를 갖고 사용할 수 가 없기 때문에 WPA-PSK 의 방법을 사용하는 방법에 대하여 논하겠다. WPA-PSK 방법은 무선 단말과 AP에서 사용자가 직접 입력하는 패스워드를 사용하여 인증과 마스터 세션 키 생성을 생성하는 방식이다. 이를 이용하여 간단한 방법으로 최소한의 WDS구간에서 WPA-PSK 를 이용하여 데이터 보안을 할 수 있다. 미리 정해진 PSK (Pre-Shared-Key) 값을 갖고 802.11i에서 정한 4단계 핸드쉐이크 키 교환이 완료된 후에 동적으로 결정된 키를 TKIP 알고리즘에 적용함으로써 무선 데이터를 보호하며, 또한 TKIP 알고리즘에는 메시지 무결성 확인 기능이 추가되어 있어서 데이터 무결성이 지원된다. 이 방법을 사용하여 AP 간 이루어진 WDS구간에서 WPA-PSK 를 사용하기 위해서는 AP2가 무선 단말의 역할을 해 주어야 한다. 그러기 위해서는 좀 더 복잡한 기능이 AP에 추가 되어야 하기 때문에 본 논문에서는 보다 간단한 방법을 제안함으로써 WDS구간에서 WPA-PSK 암호화를 사용하여 데이터를 암호화할 수 있도록 한다.

## 2. WPA-PSK 를 이용한 WDS구간 암호화

현재 일반 제품으로 나와 있는 AP에서는 많은 방법을 통해서 데이터 암호화를 제공한다. 처음 AP가 출시 되었을 당시에는 우선 연결이 주목적이었기 때문에 데이터의 보안이 없는 일반 OPEN 모드로만 동작을 하게 되었다. 그 다음 데이터 보안에 대한 개념이 처음으로 시작된 것은 WEP 보안부터이다. 그러나 이 WEP 보안은 IV(Initialization Vector)의 평문 전송, 키 스트림의 단순성으로 인하여 악의적인 공격자에 의해 WEP키 값이 노출될 수 있는 취약한 알고리즘이다. 그 다음 동적 WEP키를 사용하는 보안이 나왔으며, 지금 현재는 WPA보안이 주를 이루고 있으며 이는 TKIP과 CCMP 알고리즘을 이용한 보안 방법이다. 그러나 이런 알고리즘을 제공하기 위해서는 모든 장비가 한꺼번에 업그레이드 되거나 새로 구입을 해야만 한다. 그래서 AP가 보다 완벽한 보안 방법을 제시하고는 있지만 기존의 보안 방법도 또한 동시에 지원할 수 있는 형태로 개발이 되어야지만 기존에 사용하고 있던 제품을 같이 사용할 수가 있는 것이다.

특히 Wi-Fi 폰 같은 제품군은 먼저 통화 품질에 많은 신경을 쓰면서 개발이 되었기 때문에 보안 같은 개념은 초기 무선 LAN 제품이 그러하듯이 OPEN과 WEP만을 제공하는 군이 대부분이다. 이렇든 여러 제품군에서 AP에서 제공하는 모든 기능을 아직까지 제공하지 않기 때문에 AP에서는 여러 보안 모드가 혼재한 모드를 제공해야만 한다. 그 중에서 본 논문는 AP가 WPA모드를 제공하고 이에 그룹키를 WEP으로 사용하고 있으면서 WDS 연결을 지원하고 있을 때와, 단순히 AP는 WPA모드를 선택하고 WDS 연결을 지원할 때에 대해서 논하겠다.

그림 2에서 보는 바와 같이 WPA을 지원하는 단말과 WPA를 지원하지 않는 단말이 서로 공존하는 모드가 있을 수 있다. 이 때 WPA를 지원하는 단말에는 4-Handshaking을 통해서 Pairwise key와 Group key 키가 전달이 된다. Group key는 multicast/broadcast data를 암호화하기 위해서 사용하는 암호화키이고, Pairwise Key는 Unicast data를 암호화하기 위한 KEY이다. 이 때 Pairwise Key는 TKIP을 사용하고 Group key는 미리 정해 놓은 WEP 키를 사용하여 통신을 한다. 반면 WPA를 지원하지 않는 단말에서는 Pairwise key와 Group key를 고정WEP 키를 사용하여 데이터를 암호화한다. 이때는 WPA를 지원하지 않는 단말이기 때문에 4-Handshaking을 하는 것이 아니라 고정 WEP 키에서 적용되는 방식을 사용한다. 또한 WDS 링크상에 있는 다른 AP하고의 통신은 WPA를 지원하지 않는 단말과 같이 고정 WEP 키를 사용하는 방식을 사용하여 통신을 하게 된다. 즉 WDS 링크상에도 고정 WEP키를 사용하여 통신을 하게 된다.

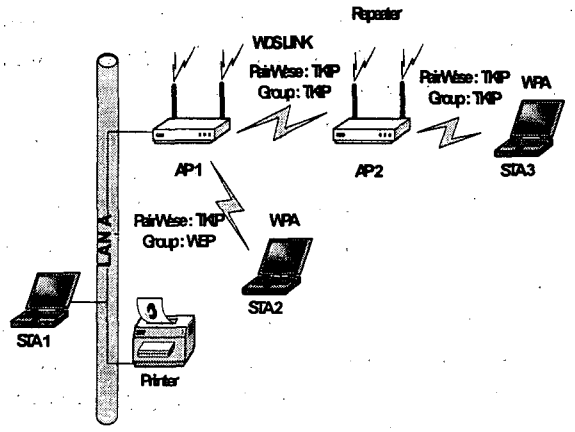



<그림 2> WEP, WPA, WDS 가 공존하는 모드

그림 3에서는 무선 링크상에는 WPA을 지원하는 단말과 WDS 링크만이 연결되어 있다. 이 때에는 WPA 를 지원하는 단말은 Pairwise Key와 Group Key모두를 TKIP으로 사용하게 되고 WDS링크로 연결되어 있는 구간에서도 key를 TKIP으로 사용하게 된다. WDS로 연결될 때 무선단말과 같이 AP에서 WPA Supplicant 기능이 들어가 있다면 4-handshake 를 통해서 키를 주고 받을 수 있지만 현재에서 이 논문에서 제안하고자 하는 알고리즘은 간단한 방법으로서 고정 WEP키가 아닌 TKIP 알고리즘을 사용함으로써 WDS링크상에서 WPA-PSK 로 암호화하는데 있다. 다음에서 WDS 링크상에서 키를 만드는 방법에 대해서 고찰하기로 한다.

### 3. WDS 링크를 위한 KEY 생성 방식

KEY를 생성하기 위해서 AP에서는 사용자의 입력에 의해서 Passphrase로부터 key를 추출한다. 이 때 passphrase는 WDS 링크를 위해서 따로 입력 받을 수도 있고, 혹은 현재 AP에서 사용하고 있는 Passphrase를 그대로 입력받아서 사용할 수 도 있다.

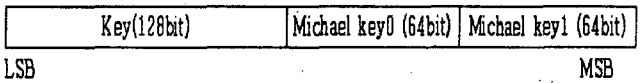



<그림 3> WPA, WDS만 있는 모드

키 입력의 길이는 8~63으로 받을 수 있고, 여기에 SSID값을 더하여 이것으로부터 hash function을 통해 256bit의 KEY를 생성시킨다. 원래 PSK에서 이 KEY에 여러 가지 입력 파라미터를 이용하여 PTK를 생성하여 암호화하기 위한 KEY를 생성하지만 본 논문에서는 지금 입력 passphrase로부터 hash function을 통해 구한 256bit의 key를 사용한다.

그림 4에서와 같이 hash function으로 부터 나온 256bit의 key를 하위 128bit는 TKIP용 KEY 값으로 사용하고 상위 128bit 중에서 하위 64bit를 Michael Key로 사용한다. WDS 링크로 연결되는 두 AP는 이 64bit 키만을 사용하게 된다.

여기에서 좀 더 확장을 해서 만약 WDS링크로 연결이 되는 AP들의 하드웨어가 CCMP를 지원한다면 하위 128bit를 사용하여 암호화 할 수도 있다.




<그림 4> Hash function으로 부터 나온 256 bit key

## IV. 결론 및 향후 과제

무선 LAN 의 사용 범위가 작은 공간에서 좀 더 넓은 공간으로의 이동이 되어 감으로써. 보다 넓은 지역에서도 무선 서비스가 가능한 방법을 찾고 있다. 그 방법으로서 AP와 무선단말의 송수신 파워를 크게 함으로써 좀 더 넓은 범위를 제공할 수 있겠지만 물리적인 한계와 법 규정에 따라서 일정 파워 이상의 출력을 낼 수는 없는 실정이다. 하지만 WDS 기능을 통해 간단하게 무선 영역을 넓힐 수 있다. 앞으로 WDS 기능은 기술적으로 좀 더 강화 되어 갈 것이며 이에 이용폭은 점점 더 늘어나갈 것으로 예상이 된다. 하지만 AP 가 갖고 있는 무선 보안의 방법을 모두 다 이용하기 위해서는 AP에서 보다 많은 수정을 요하게 되고 이 수정은 곧바로 비용을 증가시키게 된다.

본 논문에서 제안한 간단한 방법으로 무선 데이터의 보안을 좀 더 강화 시키고 그럼으로써 수정에 따른 기간과 비용을 줄일 수 있는데 본 논문은 중점을 두고 있다. 하지만 기능을 제공하는데 있어서 어느 정도의 제약 사항이 있기 때문에 향후에는 보다 향상된 방법을 통해서 무선 영역을 넓히고 보안에 좀 더 강한 방법을 찾기 위한 지속적인 연구가 필요한 것이다. 하지만 무엇보다 더 중요한 것은 이를 사용하는 사람들이 보다 보안에 대한 인식이 중요하다. 최소한의 보안 기능을 사용한다면 보다 안전하게 무선을 통해서 데이터 통신을 사용할 수 있을 것이다.

## 참고문헌


1. Merritt Maxim and David Pollino, "Wireless Security". McGraw-Hill, 2002.
2. ISO/IEC, "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications", ISO/IEC 8802-11, ANSI/IEEE Std 802.11, 1999.
3. IEEE, "Standard for Local and metropolitan area networks - Port-Based Network Access Control - Amendment 1: Technical and Editorial Corrections". IEEE P802.1aa/D6.1. Jun.2003
4. IEEE, "LAN/MAN Specific Requirements-Part 11 : Wireless Medium Access Control ( MAC ) and physical layer( PHY ) specification : Medium Access Control (MAC) Security Enhancements", IEEE Std 802.11i/D4.0.May, 2003.
5. Wi-Fi Alliance "Wi-Fi Protected Access." WPA Version 1.2, Dec 2002.