802.11 무선랜에서 1 비트를 이용한 패킷 인증 방안

이 성 렬[†] · 강 지 명[††] · 문 호 건[†††] · 이 명 수[†††] · 김 종 권[††††]

요 약

IEEE 802.11 Wireless LAN은 무선 인터넷, 차세대 유무선 통합망, 홈네트워크망을 위한 필수적인 무선 액세스 기술이다. 그러나, IEEE 802.11 무선랜을 더 넓은 영역으로 확장하기 위해서는 사용자의 프라이버시를 제공하여야 한다. 현재 WEP이나 802.11i등의 보안 메커니즘이 MAC 계층에서 제안되어 있지만 이러한 보안 메커니즘이 VPN과 같이 사용될 경우, 보안 메커니즘의 중복적용이라는 결과가 나오게 되어 이를 해결하기 위해 1 비트를 인증비트로 사용하는 방식이 제안되었다. 본 논문에서는 기존의 1 비트를 인증 비트로 사용하는 방안에서 생길 수 있는 비트 동기화 실패와 그에 따른 패킷 낭비 문제를 제시하고, 동일 패킷의 수신 개수에 대한 카운터를 이용해 동기화를 한번에 맞춤으로써 이런 문제점들을 해결한 알고리즘을 제안한다. 또한, 성능 평가를 통해 제안하는 알고리즘이 패킷인증 성공률을 98%까지 증가시킬 수 있으며 패킷 인증 비트 스트림의 효율성에서도 97%까지의 개선된 성능을 나타냄을 검증하였다.

키워드 : IEEE 802.11 Wireless LAN, 보안 매커니즘, 인증 비트, 프라이버시

Per Packet Authentication Scheme Using One-bit in 802.11 Wireless LAN

Lee Sungryoul[†] · Kang Jimyung[††] · Moon hogun[†††] · Lee myungsoo[†††] · Chong-Kwon Kim[††††]

ABSTRACT

IEEE 802.11 wireless LAN technology is essential for wireless internet, next generation converged network and home network. But, it is certain that user's privacy must be provided to expand the applicable area in IEEE 802.11 WLAN. Recently, WEP and 802.11i security scheme can be used in MAC Layer. But with VPN technology which is applied to WLAN user, it means that security mechanism is used redundantly. One bit authentication mechanism was already proposed to solve this redundancy. In this paper, we analyze problems of 1-bit Authentication mechanism which are failure of synchronization and waste of packet. And we propose new algorithm which synchronizes sender with receiver, at once, using duplicated-packet-count information. We show that our algorithm improves success probability of packet authentication up to 98% and efficiency of authentication bit stream up to 97%.

Key Words : 802.11 Wireless LAN, Security, Authentication Bit, Privacy

1. 서 론

무선랜(Wireless Local Area Network) 기술은 초고속 무선 인터넷, 차세대 유무선 통합망 등의 서비스 제공을 위해서는 필수적으로 제공되어야 하는 무선 액세스 기술이다. 그 중에서도 최근 제정된IEEE 802.11무선랜 기술은 이동성(Mobility)과 빠른 전송 속도를 제공하면서 사용자들의 관심을 끌고 있으며 기존 통신망의 한계를 보완할 무선 통신 수단으로 최근 크게 각광을 받고 있다. 그러나, 유무선 통합망에 의해 제공되는 확장성 및 관리의 효율성을 제공받기 위해서는 반드시 무선 구간에서 취약한 보안기술을 해결해야 한다.

이에 따라 무선랜이 더 영역을 넓혀 대규모의 망으로 사용되기 위해서는 데이터 암호화(Data Encapsulation), 데이터의 무결성(Data Integrity) 등을 제공하는 보안 메커니즘(Security Mechanism)이 제공되어야 한다. IEEE 802.11 표준에서는 접근 제어와 암호화를 위해 WEP(Wired Equivalent Privacy)을 규정하였다[1]. 그러나, WEP은 기본적으로 암호화 알고리즘과 무결성 알고리즘 등이 취약하기 때문에, 보안 수준(Security Level)이 그리 높지 못하다. 이에 IEEE 802.11i TG(Task Group)에서 더욱 견고한 보안 서비스를 제공할 수 있도록 표준 규격을 개발하였고 802.11에서의 보안 기능을 향상 시킨 802.11i 표준이2004년에 완성 되었다[2]. 802.11i에서는 802.1x를 통한 인증을 사용하며, 계층성을 이용하여 보다 효율적인 비밀키(Secret Key)를 생성할 수 있다. 그리고, 기존WEP에서 사용하고 있는 암호화 알고리즘에 비해 향상된 암호화 알고리즘을 사용하여 802.11의 보안 수준을 한 단계 올려놓았다.

※ 본 연구는 KT정보보호단의 지원을 받아 수행되었음.
† 준 회 원 : 서울대학교 컴퓨터공학부 박사과정
†† 준 회 원 : 서울대학교 컴퓨터공학부 석사과정
††† 정 회 원 : KT정보보호단 정보보호기술팀
†††† 정 회 원 : 서울대학교 컴퓨터공학부 교수
논문접수 : 2004년 12월 22일, 심사완료 : 2005년 5월 6일

그러나 개별 사용자들은 자신들의 개별적인VPN(Virtual Private Network)을 이용해 보안을 제공하고자 하는 경향이 있다[6]. 사내망에 무선랜을 통해 접근하는 경우 외부 접근은 모두 VPN을 통해서 이루어지도록 요구하는 것이다. VPN이 사용되는 환경의 경우, VPN기술에서 제공하는 IPSec을 이용한 보안메커니즘과 802.11에서 제공하는 보안 메커니즘을 동시에 적용하는 것은 효율적이지 못하다. 즉 IPSec/VPN과 WEP 프로토콜이 함께 사용되는 환경에서는 보안 메커니즘을 중복하여(Redundancy) 적용한 효과가 나타나게 되고, 단말(Station, STA) 에서는 사용자 인증을 위해 한 패킷에 대해 MAC계층과 IP계층에서 한번씩 총 두 번의 암호화를 수행하게 되어 심각한 컴퓨팅 자원(Computing Resource)의 낭비가 초래된다[7]. 따라서 이러한 VPN등을 사용한 보안 메커니즘을 지원하는 경우는 802.11 MAC 계층에서 복잡한 보안 메커니즘을 지원하지 않고 단지 사용자 인증만을 하는 경량화된 인증방식(Lightweight Authentication Scheme)을 사용하는 것이 더 효율적이다.

경량화된 인증방식에는 대표적으로 인증 비트 스트림(Authenticatin Bit Stream)의 공유를 이용한 접속제어(Access control)방식이 제안되어 있다. 이 방법에서 단말은 패킷 헤더에 접속제어를 위한 1비트를 할당해 두고, 이 비트를 AP와 단말이 공유하고 있는 인증 비트 스트림으로부터 차례로 한 비트씩 대입해서 넣게 된다. 이렇게 해서AP에서는 전송 받은 프레임의 접속제어 비트가 기대되는 비트 값과 일치하면 인증된 사용자로 간주하게 되는 것이다. 이 과정을 거쳐 일정한 비율 이상으로 인증실패를 하게 되면 이 사용자의 접속을 불허하게 되는 방식으로 MAC 계층에서의 접속제어를 할 수 있다. 이러한 과정 중에 데이터나 ACK(Acknowledge) 메세지의 손실에 의해 단말과 AP가 인증 비트 스트림에서 각각 다른 위치를 기대하고 있을 수 있게 된다. 즉 단말과 AP사이의 인증 비트 스트림의 동기화가 필수적으로 제공되어야 하는데 기존 방식에서는 동기화를 제공해 주는 부분이 미흡해 동기화를 보장해 주지 못하고 동기화가 되더라도 시간이 오래 걸리게 되어, 실제 유효한 사용자라고 하더라도 접속에 실패 할 수 있게 되는 등 효율적인 접속제어를 제공할 수가 없고 불필요하게 패킷을 재 전송하는 문제점이 발생한다. 본 논문에서는 이와 같은 인증 비트 스트림 동기화 과정에서 발생할 수 있는 상황과 문제점들에 대해서 분석하고 이런 점을 보완한 새로운 동기화 알고리즘을 사용하는 방식을 제시하고자 한다.

논문의 2장에서는 데이터 암호화 및 접속제어 방안에 대한 살펴보고, 3장에서는 새로운 동기화 알고리즘을 제시한다. 4장에서는 제안된 알고리즘의 성능을 평가하고 5장에서 논문의 결론을 맺는다.

2. 배경 지식 및 기존 연구

본 장에서는 현재 IEEE 802.11 Wireless LAN에서 사용가능한 접근 제어(Access Control)방법과 데이터 프라이버시(Data Privacy)를 제공하기 위해 규정된 WEP에 대해서 살펴보고 이를 바탕으로 기존 WEP 문제점을 해결하기 위해 제안된 방안을 살펴본다. 또한, AP에서 STA가 전송한 패킷의 서비스 제어를 위해 1-bit를 인증 비트로 이용하는 기존 제안에서 동기화 알고리즘(Synchronization Algorithm)의 문제점을 지적하고 그 예를 살펴보도록 하겠다.

2.1 Media Access Control Address Filtering

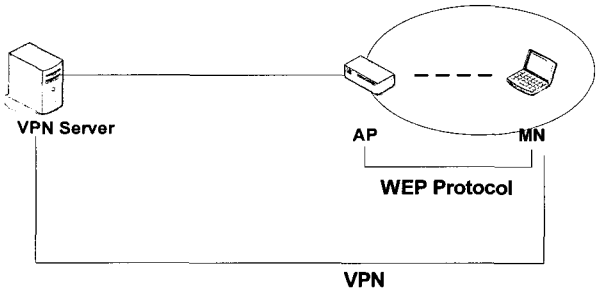
AP에서는 STA의 접근제어를 위해 인증된 STA에 대한 MAC(Media Access Control) address의 list를 관리하게 된다. 만약, STA의 MAC address가 AP가 인증한 MAC address list에 있지 않으면, AP는 STA이 전송한 패킷을 서비스하지 않고 드롭(drop)시킨다. 따라서, MAC address filtering은 인증받지 못한 STA이 전송한 패킷을 MAC address를 기준으로 걸러 낼 수 있도록 해 준다[3]. 그러나, MAC address는 attacker가 AP로 전송되는 패킷을 엿들음(Eavesdropping)으로써 쉽게 노출되는 문제점을 가지고 있다. 이외에 SSID (Service Set Identifier)를 이용하는 접근 제어 방안이 있으나, 이러한 방안 역시 SSID가 암호화 되지 않으므로 쉽게 attacker에게 노출되는 문제점을 가지고 있다.

2.2 Wired Equivalent Privacy (WEP)

WEP은 STA와 AP간 40 bits의 비밀키(Secret Key)를 기반으로 하여 기본 서비스 영역내의 모든 STA의 접근 제어과 데이터 프라이버시를 지원한다. WEP은 RC4를 기반으로 하는 대칭 암호화 알고리즘을 사용하기 때문에 데이터의 암호화와 복호화에 동일한 비밀키와 알고리즘을 사용하여 데이터 프라이버시를 제공하며, 올바른 비밀키를 보유하지 않은 STA이 AP에 접근하는 것을 제어할 수 있다. 그러나, 단지 WEP을 사용하여 데이터를 암호화할 경우 패킷별 인증(Au- thentication)을 제공하지 못하며[3], RC4는 근본적으로 취약한 암호화 알고리즘을 사용하고 있기 때문에 비밀키가 노출될 위험이 높다. WEP에 대한 이론적(Theoretical), 혹은 실제적(Practical)으로 가능한 attack은 이미 밝혀져 있다[4, 5].

2.3 IPSec/VPN

IPSec/VPN은 현재 널리 사용되고 있는 보안 아키텍처(Security Architecture)로써 WEP의 취약성을 해결하기 위해 802.11 Wireless LAN에서 WEP과 함께 사용할 경우 보안 메커니즘의 향상을 가져올 수 있다. 2.2절에서 상술한 바와 같이, Wireless LAN에서는 STA와 AP사이의 보안 문제를 해결하기 위해 WEP을 사용한다. 그러나, 단지 WEP만을 사용할 경우 AirSnort[8], WEPCrack[9] 등의 유틸리티를 이용한 공격에 대해 매우 취약함으로 이러한 취약성을 해결하기 위해 대부분의 회사(Company)에서는 VPN과 WEP를 함께 사용한다[5, 6]. VPN은 OSI(Open System Interconnection) 계층 2(layer 2)에서의 데이터 암호화와 인증과는 독립적으로 OSI 계층 3(layer 3)에서 IPSec/VPN tunnel를 통한 보안 서비스를 한다. 따라서 IPSec/VPN을 WEP과 함께 사용할 경우



(그림 1) 802.11 network에서 IPSec/VPN과 WEP이 함께 사용되는 솔루션

보다 강력한 인증 메커니즘(Authentication Mechanism)를 제공할 수 있다.

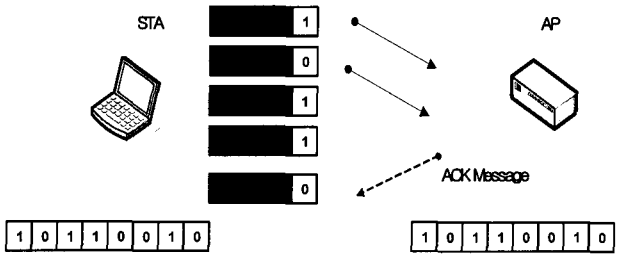
(그림 1)은 통상적인 IPSec/VPN과 WEP이 함께 사용되었을 때의 기본적인 네트워크 구성을 나타내고 있다. STA와 AP는 동일한 비밀키와 암호화 알고리즘을 가지고 있으며, VPN 서버는 STA와 IPSec/VPN tunnel를 지원하는 종단(End Point)이다. (그림 1)에서, STA가 전송한 패킷이 AP에서 인증 받기 위해서는 STA는 AP와 동일한 비밀키와 암호화 알고리즘을 사용하여 패킷을 암호화하게 되고 AP는 동일한 비밀키와 암호화 알고리즘을 가지고 패킷을 복호화 할 수 있다. 또한, STA는 VPN 서버와 종단간 보안(End-to-End Security)을 지원하기 위해 IPSec/VPN tunnel를 이용하여 패킷을 암호화하게 된다.

위와 같은 구성에서 STA는 패킷에 대해 두 번의 암호화를 수행해야 하며, 이로 인해 STA는 컴퓨터 자원(Computing Resource)를 낭비하게 된다[7].

2.4 A One-bit Identity Authentication Protocol

H.Johnson[3]은 IPSec/VPN과 WEP을 함께 사용할 경우에 발생하는 패킷 암호화의 중복(Redundancy)을 해결하기 위해 1-bit를 이용한 패킷 인증 메커니즘인 SOLA를 제안하였다. SOLA는 STA와 AP사이의 접근 제어 및 패킷 인증을 위해 WEP을 사용하는 대신, 단지 1-bit를 인증 비트로 사용하여 MAC(Media Access Control) 헤더(header)에 삽입함으로써 패킷 암호화의 오버헤드(Overhead)를 줄이고 무선 대역폭 자원(Wireless bandwidth Resource)를 보호하는 방안이다. SOLA의 기본 메커니즘은 다음과 같다.

기본 서비스 영역내의 모든 STA와 AP사이에는 특별한 랜덤 비트 스트림(PRBS, Particular Random Bit Stream)를 생성하는 인증 스트림 생성기(ASG, Authentication Stream Generator)라는 모듈(Module)을 가지게 된다. 따라서, STA와 AP사이에는 동일한 PRBS의 첫 번째 bit를 가리키게 된다. (그림 2)에서와 같이, STA는 AP로 패킷을 전송할 때, ASG가 생성한 PRBS의 1-bit를 MAC 헤더에 삽입하여 전송하게 된다. 패킷의 손실(Packet Loss)이나 보안 공격(Security Attack)이 없다면, STA가 패킷에 삽입한 1-bit와 AP가 현재 가리키고 있는 PRBS의 1-bit는 일치하게 됨으로 패킷은 AP에서 인증되고 서비스된다. STA는 패킷의 전송마다 PRBS의



(그림 2) SOLA에서 1-bit를 이용한 패킷 인증의 예

인덱스(Index)를 증가시키면서 새로운 bit를 MAC 헤더에 삽입하여 전송하게 된다. AP에서는 STA가 전송된 패킷을 서비스한 후, ACK(Acknowledge) 메시지를 STA에게 전송하여 패킷이 인증되었음을 통지하게 된다.

이러한 1-bit를 이용한 인증 메커니즘에서는 attacker가 ASG가 생성한 올바른 PRBS를 가지고 있지 않다면, STA가 전송한 패킷된 삽입된 인증 비트를 연속적으로 추측할 확률은 매우 낮다. 즉 연속적으로 n 번의 패킷에 삽입된 인증 비트를 올바르게 추측할 확률(2^{-n})은 매우 낮기 때문에, attacker가 올바른 PRBS의 인증 비트를 인지하기 전에서는 MAC address를 속이는 방법등으로 패킷을 AP에 전송하여 서비스를 받을 수 없다.

또한, SOLA에서는 패킷 손실에 의해 STA와 AP사이의 PRBS의 동기화가 깨어졌을 때, PRBS의 인덱스를 동기화하는 알고리즘을 제안하고 있다(그림 3). 802.11 Wireless LAN은 신뢰할 수 없는 통신 링크(Unreliable Communication Link)를 가지고 있기 때문에, SOLA에서 제안하고 있는 1-bit를 이용한 인증 메커니즘은 PRBS의 인덱스의 동기화가 매우 중요하다. 즉, 무선 채널에서는 잡음(Noise)에 의한 변질(Corruput)등으로 패킷 손실이 발생할 수 있기 때문에 STA와 AP사이의 PRBS 인덱스 동기화가 깨어질 수 있기 때문이다.

(그림 3)에서 α, β는 각각 STA와 AP의 현재 PRBS의 인덱스가 가리키고 있는 인증 비트를 나타내고 있다. 먼저, AP

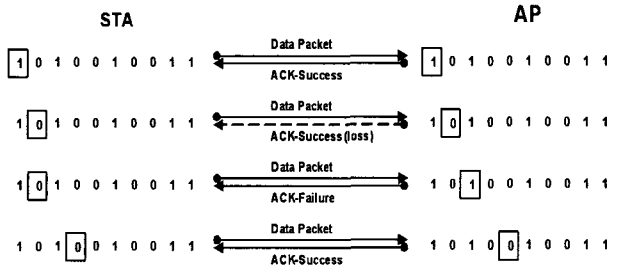
```
        Algorithm for AP
// AP receives data packet with Bit[α]
      if  Bit[α] == Bit[β] then
        β ++
        AP -) MN:Packet [ ACK-Success ]
      else if  Bit[α] ≠ Bit[β] then
        β = pointer of to next opposite bit + 1
        AP -) MN:Packet [ ACK-Failure]

      Algorithm for STA
// MN receives ACK packet with success or failure from AP
      If  ACK == ACK-Success then
        α ++
      else If  ACK == ACK-Failure then
        α = pointer of to next opposite bit + 1
```

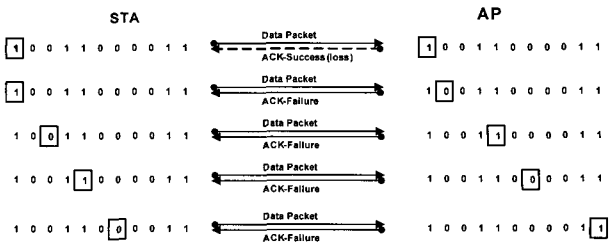
(그림 3) SOLA에서의 동기화 알고리즘

에서는 STA에서 전송된 패킷의 MAC 헤더의 인증 비트(bit[α])와 자신의 현재 인증 비트(bit[β])를 비교한다. 만약, bit[α] == bit[β]이면 AP에서 STA가 전송한 패킷은 인증하고 서비스한다. 또한, β = β+1로 증가시키며 AP는 ACK-Success 메시지를 STA에게 전송하여 전송된 패킷이 올바르게 서비스되었음을 통지하게 된다. 그러나, bit[α] ≠ bit[β]이면 STA으로부터 전송된 패킷은 AP에서 드롭되고, β = pointer of to next opposite bit + 1 로 증가된다. 또한, AP는 ACK-Failure 메시지를 STA에게 전송함으로써 패킷이 드롭되었음을 STA에게 통지하게 된다. 여기서, pointer of to next opposite bit는 현재 PRBS의 인덱스가 가리키고 있는 값과 반대의 값을 가지는 가장 가까운 bit의 index를 의미한다. STA에서도 AP와 유사한 방법으로 동기화 알고리즘을 수행한다. 즉, STA이 AP로부터 ACK-Success 메시지를 받을 경우, α = α+1로 증가하게 되며, ACK-Failure 메시지를 받을 경우, α = pointer of to next opposite bit +1로 증가하게 된다.

이러한 동기화 알고리즘은 데이터 패킷의 손실시에는 STA와 AP사이의 PRBS의 인덱스의 동기화에 영향을 주지 않기 때문에 ACK 메시지의 손실에 대해서만 동기화 알고리즘을 고려하고 있다. (그림 4)에서 이러한 동기화 과정의 예시를 나타내고 있다. 즉 ACK-Success 메시지의 손실로 인해 PRBS의 인덱스가 서로 맞지 않는 상황이 발생하였을 경우, AP는 ACK-Failure 메시지를 보내면서 자신의 PRBS 인덱스를 pointer of to next opposite bit + 1로 증가시킨다. ACK Failure 메시지를 받은 STA는 마찬가지로 자신의 PRBS 인덱스를 pointer of to next opposite bit +1로 증가시킨다. (그림 4)의 마지막에서 동기화 알고리즘을 한번 거치더라도 PRBS 인덱스 차이가 없어지지 않는 것을 볼 수 있다. 동기화 알고리즘의 문제점을 좀더 확실히 보기 위해 (그림 5)에서의 경우를 생각해 보면, STA와 AP의 ASG 모듈에서 생성한 PRBS는 10011000011이다. STA는 첫 번째 패킷에 대하여 MAC 헤더에 인증 비트인 1을 삽입하여 AP에게 전송하게 된다. AP가 패킷을 제대로 전송 받은 후 자신의 인증 비트와 STA가 전송한 패킷의 인증 비트가 일치할 경우, AP는 ACK-Success 메시지를 STA에게 보내게 된다. (그림 5)에서와 같이, 만약 AP가 전송한 ACK-Success 메시지가 손실될 경우 STA는 타임아웃(Timeout)시간 동안 ACK 메시지를 받지 못했기 때문에 같은 패킷을 AP에 재 전송하게 된다. 그러나, 동기화 알고리즘에 의해 AP의 PRBS의 인덱스는 증가하



(그림 4) SOLA에서 동기화 알고리즘의 수행 예



(그림 5) SOLA에서 ACK 메시지의 손실에 의한 비동기화 문제의 예

게 됨으로 인증 비트는 0으로 변했기 때문에, 재 전송된 패킷은 AP에서 인증을 받지 못하고 드롭된다. 따라서 SOLA에서 제안하고 있는 동기화 알고리즘은 오랜 시간동안 STA와 AP의 인증 비트가 동기화되기 못하는 상황이 발생하기 때문에, 이로 인한 Wireless LAN에서의 성능 저하를 일으킬 수 있는 원인이 된다.

2.5 Wang의 방식

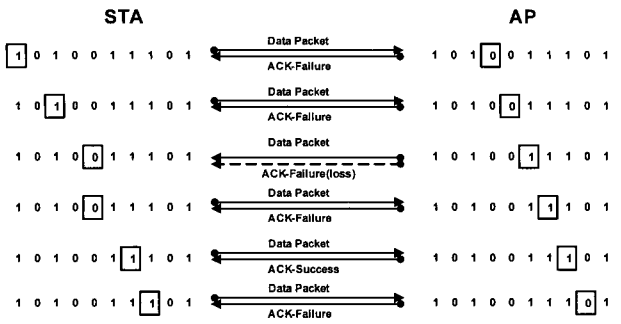
Wang[7]은 SOLA에서 제안한 동기화 알고리즘의 문제점을 해결하기 위한 수정된 동기화 알고리즘을 제안하고 있다.

무선 채널의 오류로 인한 ACK-Success 메시지의 손실은 STA와 AP사이의 인증 비트의 동기화가 깨어지는데 직접적인 영향을 미치게 된다. 따라서 ACK-Success 메시지가 손실되었을 때 발생하는 동기화 알고리즘의 문제점을 해결하기 위해 (그림 6)과 같이 수정된 동기화 알고리즘을 제안하고 있다. 이 알고리즘은 H.Johnson[3]이 제안한 SOLA 알고리즘에서 AP쪽의 인덱스 증가를 패킷 하나당 1로 고정시킨 알고리즘이다. 그러나, 이러한 수정된 동기화 알고리즘에서도 STA와 AP사이의 인증 비트의 비동기화 gap (NSI, Non-Synchronization Index) 만큼의 동기화 알고리즘이 수행되어야 하며, 이로 인해 동일한 패킷을 재전송해야 하는 문제점은 여전히 발생하게 된다. 또한, (그림 7)에서와 같이 ACK-Failure 메시지의 손실이 발생할 경우, Wang이 제안하고 있는 동기화 알고리즘을 통해서는 NSI만큼의 동기화 알고리즘의 수행을 통해 STA와 AP의 인증 비트를 동기화 할 수 없는 문제점을 가지고 있다.

```
        Algorithm for AP
// AP receives data packet with Bit[α]
        if  Bit[α] == Bit[β]  then
          β ++
          AP -> MN : Packet [ ACK-Success ]
        else if  Bit[α] ≠  Bit[β] then
          β ++
          AP -> MN : Packet [ ACK-Failure]

        Algorithm for STA
// MN receives ACK packet with success or failure from AP
        If  ACK == ACK-Success then
          α ++
        else If  ACK == ACK-Failure then
          α = pointer of to next opposite bit + 1
```

(그림 6) Wang 방식에서의 동기화 알고리즘



(그림 7) Wang 방식에서ACK 메시지의 손실에 의한 비동기화 문제의 예

3. The Proposed Scheme

이번 장에서는 1-bit를 인증 비트로 사용하여 STA와 AP 사이의 패킷 인증시에 발생되는 비효율적인 동기화 알고리즘을 개선하고자 하는 방안을 제안한다. 앞서 설명한 바와 같이, IPSec/VPN과 WEP이 함께 사용되는 Wireless LAN에서 불필요한 패킷 암호화의 중복을 해결하기 위해 제안된 1-bit를 인증 비트로 사용하는 인증 메커니즘에서는 ACK 메시지의 손실이 발생하게 되면 불필요한 패킷의 재 전송이 발생하게 되고, 또한 STA와 AP사이의 인증 비트를 동기화하는데 오랜 지연 시간이 발생하게 됨으로 Wireless LAN의 성능을 저하시킨다. 이러한 문제점을 해결하기 위해 제안하는 방안에서는 AP에서 STA가 전송한 각 패킷의 수신에 대한 카운트(Count)를 기록하여 ACK 메시지에 피기백(Piggyback)한다. 이러한 카운트 정보를 이용하여 STA는 ACK 메시지를 수신하였을 때 한번의 동기화 알고리즘의 수행을 통해 STA와 AP의 인증 비트를 동기화 할 수 있다. 따라서, 제안하는 방안에서는 STA와 AP사이에서 발생하는 인증 비트의 비동기화 문제를 해결하고, 동일한 패킷을 재 전송하지 않으므로 더 높은 성능 향상을 얻을 수 있다.

3.1 STA와 AP에서의 Random Bit Stream의 생성 및 패킷 인증 과정

기존 제안[3]과 마찬가지로 기본 서비스 영역내의 모든 STA와 AP는 PRBS를 생성하는 ASG 모듈을 가지게 된다. AP는 기본 서비스 영역내의 모든 STA에 대한 MAC address와 ASG 모듈에서 PRBS를 생성하는데 사용되는 seed의 페어(pair)를 관리하게 된다. Seed는 각각의 STA에 대해 상이한 값을 가지게 되며 STA는 AP에서 관리하고 있는 seed와 일치된 값을 저장하고 있다. 따라서, 기본 서비스 영역내의 각각의 STA와 AP사이에서는 동일한 PRBS가 생성되게 되며 PRBS의 인증 비트를 가리키는 인덱스는 첫 번째 bit로 초기화된다.

STA와 AP에서의 동일한 PRBS가 생성된 후 STA는 AP로 패킷을 전송할 때, ASG에서 생성된 PRBS의 1-bit를 MAC header에 삽입하여 전송한다. STA가 MAC header에서 삽입한 1-bit는 AP에서 패킷 인증을 위한 인증 비트로 사용되며 AP에서 PRBS의 인덱스가 가리키고 있는 1-bit와 일치할 경우, 전송된 패킷은 AP에 의해 인증되고 서비스되어진다. 또한, AP는 ACK-Success 메시지를 STA에게 전송하여 패킷이 올바르게 서비스되었음을 STA에게 통지하게 된다. 이에 반해, 패킷에 삽입된 인증 비트와 AP가 가리키고 있는 PRBS 인덱스의 1-bit가 일치되지 않을 경우, 패킷은 드롭되고 AP는 ACK-Failure 메시지를 STA에게 전송하여 패킷이 드롭되었음을 통지하게 된다.

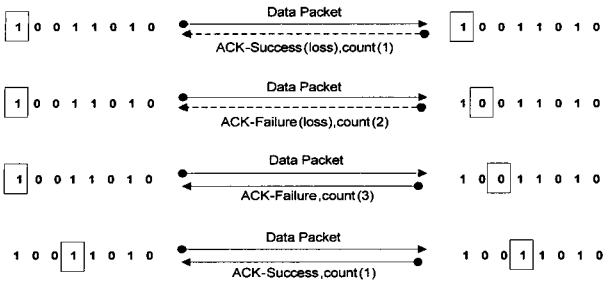
3.2 STA와 AP에서의 인증 비트의 동기화 과정

2장에서 설명한 바와 같이, ACK 메시지의 손실은 PRBS의 인증 비트의 비동기화 및 AP에서 하나의 패킷을 인증하는데 오랜 시간이 소요되는 문제점을 야기한다. 인증 비트를 동기화하는데 소요되는 지연을 최소화하기 위해서 AP에서는 동일한 패킷을 몇 번 수신했는지에 대한 카운트 정보(Dup-Packet-Count)를 ACK 메시지에 피기백(Piggyback)하여 STA에게 보내게 된다. 예를 들어 새로운 패킷을 받았을 경우 카운트 정보는 1이 되고, 동일한 패킷이 세 번 AP에 수신된 경우 카운트 값은 3이 된다. STA이 ACK 메시지(ACK-Success 메시지나 ACK-Failure 메시지)를 받게 되면, STA에서는 AP에서 동일한 패킷을 몇 번 받았음을 알게 되기 때문에, 그 카운트만큼 인덱스를 증가시켜서 AP와 PRBS의 인증 비트를 동기화 할 수 있다. 이렇게 하면 AP에서 매 새로운 패킷의 첫번째 수신은 PRBS의 인증 비트와 일치한다. 따라서 STA가 ACK-Failure를 수신할 경우에 있어서도 STA는 동일한 패킷을 재 전송할 필요가 없게 된다. 또한, STA에서 ACK 메시지를 수신하게 되면 동기화 알고리즘을 한 번만 수행하여 STA와 AP사이의 PRBS의 인증 비트를 동기화 할 수 있다.

```
        Algorithm for AP
// AP receives data packet with Bit[α], sequence number k
    if   k == sequence number of previous received packet
         Dup-Packet-Count ++
    else if  k ≠ sequence number of previous received packet
         Dup-Packet-Count  = 1

    if   Bit[α] == Bit[β]  then
         β ++
         AP -) MN:Packet [ ACK-Success, Dup-Packet-Count ]
    else if   Bit[α] ≠  Bit[β] then
         β ++
         AP -) MN:Packet [ ACK-Failure, Dup-Packet-Count]
        Algorithm for STA
// MN receives ACK packet with success or failure from AP
    If  ACK == ACK-Success then
         α = α + Dup-Packet-Count
    else If  ACK == ACK-Failure then
         α = α + Dup-Packet-Count
```

(그림 8) 제안하는 동기화 알고리즘

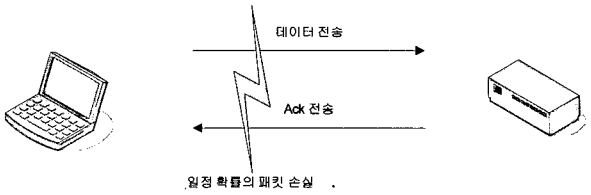


(그림 9) 제안하는 방안에서의 동기화 알고리즘의 수행 예

(그림 8)에서와 같이, AP는 수신된 각 패킷에 대한 카운트를 계산하게 된다. ACK 메시지의 손실로 인한 동일한 패킷의 재 전송을 AP에서 카운트함으로써 STA에 처음으로 도착하는 ACK 메시지에 의해 새로운 패킷을 전송할 수 있으며 한번의 동기화 알고리즘을 통해 STA와 AP사이의 PRBS의 인증 비트를 동기화 할 수 있다. 왜냐하면 ACK 메시지에 피기백 되어 있는 카운트 값은 곧 AP와 STA사이에 존재하는 PRBS 인덱스 차이를 의미하기 때문이다. (그림 9)에서와 같이, STA는 PRBS의 첫 번째 비트를 인증 비트로 선택하여 패킷의 MAC 헤더에 삽입하여 AP에게 전송하게 된다. AP에서 PRBS의 인덱스가 가리키는 인증 비트는 STA에서 전송된 패킷의 인증 비트와 같으므로, 패킷을 인증하고 서비스하게 된다. 또한 AP는 제안하고 있는 동기화 알고리즘에 의해 PRBS의 인덱스를 증가시키고, ACK-Success 메시지에 전송된 패킷의 카운트를 피기백하여 전송하게 된다. AP가 전송한 ACK-Success 메시지가 손실되었을 때, STA는 타임아웃 동안 ACK 메시지가 도착하지 않음으로 AP에게 동일한 패킷을 재 전송하게 되고 AP는 이전 패킷과 동일한 패킷을 수신하게 된다. (그림 8)에서 제안된 알고리즘에 의해 이미 AP의 PRBS의 인덱스가 증가되었기 때문에 AP가 수신한 패킷의 인증 비트와 AP의 인증 비트는 일치하기 않는다. 따라서 AP는 STA에게 ACK-Failure 메시지에 패킷의 카운트를 피기백하여 전송한다. ACK-Failure 메시지 역시 손실 되었을 경우, STA는 다시 타임아웃 이후에 패킷을 재전송 하게 된다. 이 패킷도 인증 비트가 일치하지 않기 때문에 AP는 다시 ACK-Failure를 보내게 된다. STA가 ACK-Failure 메시지를 수신하게 되면, ACK-Failure 메시지의 카운트 정보를 통해 AP에서는 이미 동일한 패킷을 세 번 받았음을 알게 된다. 따라서, STA가 이전에 전송한 패킷은 이미 AP에 의해 서비스 되었음을 알게 되며 STA는 시퀀스 번호(Sequence Number)를 증가시켜 새로운 패킷을 AP에게 전송할 수 있다. 또한, STA는 한 번의 ACK 메시지(여기서는 ACK-Failure 메시지)를 수신하고 이때 알게 된 카운트 값만큼 PRBS의 인덱스를 증가시켜서 AP의 인증 비트와 동기화 할 수 있다.

4. 성능 평가

제안된 동기화 알고리즘에서는 한번의 ACK 메시지의 전송 성공으로 동기화가 완료된다. 즉 기존 방식들에 비해 동기화에 관한 성능은 탁월하다고 할 수 있다. 본 장에서는 제안하는 동기화 알고리즘의 성능을 평가하기 위하여 실제 이 동기화 방식을 사용하면 접속제어나 PRBS 관리에 얼마나 유용한지를 모의 실험을 통해 평가하고자 한다. 모의 실험 환경은 AP에 하나의 STA이 접속해 있는 형태로 (그림 10)과 같다.



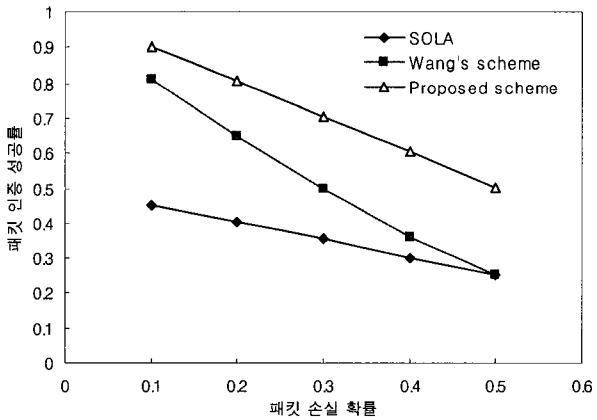
(그림 10) 모의 실험 환경

PRBS는 STA과 AP사이에 무한히 공유 되어 있고 동일한 패킷의 길이를 가정하여 패킷 손실 확률(Packet Loss Rate)은 패킷에 관계없이 일정하다고 하였다. 제안된 방안을 SOLA , Wang의 방식과 비교하여 실험하였다.

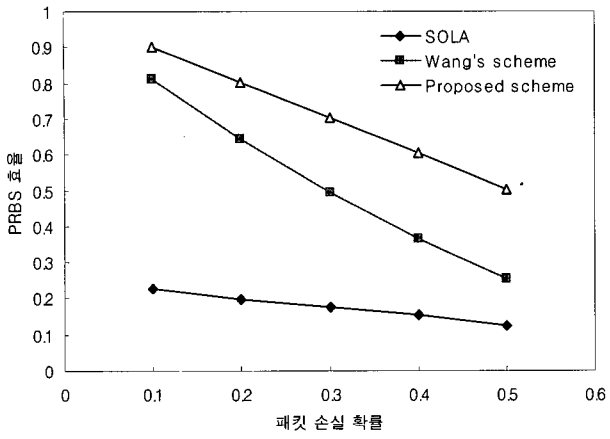
4.1 패킷 인증 성공률

AP는 일정기간 패킷을 관찰하면서 패킷 인증 성공률 (인증에 성공하는 패킷의 개수와 총 전송 시도되는 패킷의 비율)을 계산할 수 있고 이 값은 접속제어를 진행하는 기초가 된다. 즉 패킷 인증 성공률이 높을수록 PRBS의 동기화가 더 잘 된 상태이고 실제 PRBS를 공유하고 있을 확률이 높다고 생각할 수 있다. (그림 11)에서는 각 알고리즘을 사용하였을 때의 패킷 인증 성공률을 패킷 손실률(Packet Loss Rate)에 따라 나타내었다. 각각 10,000번의 전송이 시도될 때까지 실험을 진행하였다.

(그림 11)에서 볼 수 있듯이 제안된 방식은 SOLA, Wang의 방식에 비해서 월등히 높은 인증 성공률을 보임으로써, 패킷 인증 성공률을 기반으로 한 접속제어에 더 좋은 성능을 나타낼 수 있으며 패킷 재 전송으로 인한 무선 채널의 대역폭의 낭비를 줄일 수 있다. Wang의 방식에 비해 패킷 손실 확률이 0.1일 때는 11%의 성능 증가를 보이고 0.5일 때는 98%의 성능 향상을 보인다.



(그림 11) 패킷 손실 확률에 따른 패킷 인증 성공률



(그림 12) 패킷 손실 확률에 따른 PRBS 효율

4.2 Utilization of PRBS with changing loss rate of ACK message

동기화 알고리즘에서 PRBS의 효율이 성능에서 중요한 부분을 차지 하게 된다. PRBS 효율이란 패킷의 인증에 사용된 비트수와 PRBS에서 진행된 비트수의 비율을 말하는데 예를 들어, 총 10개의 패킷이 인증에 성공하였고, PRBS에서 100개의 비트가 진행되었을 때의 효율은 0.1이다. PRBS의 효율이 좋지 못하다는 말은 PRBS가 그만큼 많이 생성되어있어야 한다는 뜻이기 때문에 동기화 알고리즘은 PRBS의 효율이 좋아야 한다. (그림 12)에서는 각 알고리즘을 사용할 경우 패킷 손실 확률에 따른 PRBS 효율을 나타내었다. 측정을 위해서 PRBS의 크기로 각각 20000bit를 사용하였다.

(그림 12)에서 SOLA나 Wang의 방식에 비해서 제안한 알고리즘의 PRBS효율이 훨씬 좋다는 것을 알 수 있다. Wang의 방식에 비해서 패킷 손실 확률 0.1에서는 11%의 효율 향상을 보이고, 손실 확률 0.5에서는 97%의 효율 향상을 보인다. SOLA나 Wang의 방식에서는 동기화를 맞추는 과정에서 한번에 많은 PRBS 비트를 이동하여 PRBS의 낭비가 초래되지만 제안한 방식에서는 한 비트씩만 이동하기 때문에 PRBS의 bit가 절약되기 때문이다. 즉 제안한 방식에서는 한번 생성한 일정한 크기의 PRBS를 가지고 인증할 수 있는 패킷의 수가 SOLA나 Wang의 방식에 비해서 많다.

4.3 제안된 방식의 오버헤드

제안된 방식을 사용하기 위해서는 AP에서 패킷을 수신할 때 마다 이전 패킷과 동일한 패킷인지를 검사해야 한다. 이 과정은 패킷의 시퀀스 넘버만을 단순 비교함으로써 간단히 해결할 수 있다. 또한 제안된 방식에서는 ACK에 카운트 정보를 저장하는 부분이 필요하게 된다. 5bit를 카운트 정보에 할당한다고 하면 32까지의 카운트를 표현할 수 있는데 카운트가 이 값을 초과 하려면 연속적인 32번의 ACK 손실이 있어야 하므로 이 값은 충분하다고 할 수 있겠다. ACK 패킷에 추가적으로 5bit를 더함으로써 생기는 손실이 존재하지만 이 값은 일반적인 데이터 패킷의 크기에 비해서 크지 않다고 생각된다. 그에 반해 (그림 11)에서처럼 패킷 인증 성공률이 높기 때문에 동기화 실패로 인한 패킷 재전송이 줄어 든다. 즉 패킷 인증 성공률이 10% 증가한다면 전체 goodput이 10% 증가 한다고 볼 수 있기 때문에 ACK 패킷의 크기가 커지는 데에 따르는 성능 저하는 무시된다고 생각할 수 있다.

5. 결 론

무선랜이 VPN등과 같은 다른 계층의 보안 기술과 같이 사용되는 경우, 802.11의 MAC 계층에서 제공하는 기존의 보안 기술을 사용하면 두 가지 보안 메커니즘을 동시에 적용하는 결과가 되어 컴퓨팅 자원의 낭비가 초래된다. 이런 경우 간단한 인증 기능만을 위해 1-bit를 인증 비트로 사용하는 light weight authentication 방법을 사용할 수 있다. 본 논문에서는 이러한 light weight authentication방법을 사용하는 절차상의 동기화 과정에서 발생할 수 있는 문제점을 분석하였고, 이러한 문제점을 해결하기 위해 카운트를 이용한 새로운 동기화 알고리즘을 제시하였다. 또한 새로운 동기화 알고리즘이 패킷 인증 성공률과 비트 스트림 효율을 최대 90% 이상까지 증가 시킬 수 있음을 검증하였다.

References

[1] "LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification", IEEE Standard 802.11, 1997 Edition, 1997.

[2] "IEEE 802.11i Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6 : Medium Access Control (MAC) Security Enhancements", IEEE Standard, 2004.

[3] Henric Johnson, Arne Nilsson, Judy Fu, S.Felix Wu, Albert Chen and He Huang "SOLA : A One-bit Identity Authentication protocol for Access Control in IEEE 802.11", Globecom 2002.

[4] J. Walker, "unsafe at any key size : an analysis of WEP encapsulation", Tech. Rep. 03628E, IEEE 802.11 committee, March, 2000.

[5] Hea Suk Jo and Hee Yong Youn "A New Synchronization Protocol for Authentication in Wireless LAN Environment", ICCSA 2004.

[6] "VPN and WEP Wireless 802.11b security in a corporate environment", Intel white paper, March, 2003.

[7] Haoli Wang, Aravind Velayutham, Yong Guan "A Lightweight Authentication Protocol for Access Control in IEEE 802.11", Globecom 2003.

[8] http://airsnort.shmoo.com

[9] http://wepcrack.sourceforge.net

이 성 렬

e-mail : srlee@popeye.snu.ac.kr
2001년 서강대학교 컴퓨터학과(학사)
2003년 서강대학교(공학석사)
2004년~현재 서울대학교 전기, 컴퓨터공학부 박사과정
관심분야 : Wireless LAN, Sensor Network, Security, 등

강 지 명

e-mail : jmkang@popeye.snu.ac.kr
2004년 서울대학교 컴퓨터공학부(학사)
2004년~현재 서울대학교 전기, 컴퓨터공학부 석사과정
관심분야 : Wireless LAN, 차세대 인터넷, 이동통신 등

문 호 건

e-mail : hkmoon@kt.co.kr
1987년 중앙대학교 전자공학과(석사)
2005년 부산대학교 전자공학과(박사)
1987년~2004년 KT 차세대 통신망연구소 보안기술연구실장
2005년~현재 KT 정보보호단 기술개발 1부장
관심분야 : 위험분석, 위험관리, 네트워크 보안

이 명 수

e-mail : msrhee@kt.co.kr
1989년 연세대학교 전자공학과(박사)
1990년~2004년 KT 네트워크 보안연구팀장
2004년~정보보호학회 무임 소이사
2005년~현재 KT 정보보호기술팀장
관심분야 : 개인 정보보안 및 네트워크 보안

김 종 권

e-mail : ckim@popeye.snu.ac.kr
1981년 서울대학교 산업공학과(학사)
1982년 미국 조지아 공대(공학석사)
1987년 미국 일리노이대학(공학박사)
1984년~1987년 IBM 산 호세 연구소 연구조원
1987년~1991년 미국 벨 통신 연구소 연구원
1991년~현재 서울대학교 전기, 컴퓨터공학부 교수
관심분야 : 차세대 인터넷, 초고속 라우터, 이동통신 등