무선랜 환경에서 TKIP를 이용한 DoS 공격 대응 메커니즘

강명수° 홍충선
경희대학교 컴퓨터공학과
mskang@networking.khu.ac.kr°, cshong@khu.ac.kr

A Prevention Mechanism against DoS Attack Using the TKIP in Wireless LAN Environment

Myung Soo Kang° Choong Seon Hong
Dept, of Computer Engineering, Kyung Hee University.

요 약

IEEE 802.11 기술이 상용화된 이후 여러 가지 보안에 관련된 취약점들이 드러났다. 이를 보완하기 위하여 802.11i 그룹이 802.11보안 관련 표준안을 제시하였다. 그러나 802.11에서 문제가 되었던 여러 종류의 DoS 공격들 중 몇 개의 공격들은 802.11i에서 아직 유효하다. Deauthe- ntication, Disassociation 메시지를 이용한 공격이 802.11i에서도 유효한 대표적인 공격 중 하나이다. 이 공격은 802.11i에서의 관리 프레임에 802.11과 같은 수준의 데이터 암호화가 적용되기 때문에 가능한 것이다. 본 논문에서는 이러한 취약점을 TKIP를 이용해 제안된 state value 를 암호화하여 이를 예상 값과 비교한 후 Deauthentication, Disassociation 공격을 판단하는 메커니즘을 제시 하였다.

1. 서 론

최근에 무선 네트워크가 주목받고 있는 가운데 무선 네트워크의 보안 문제가 이슈로 떠오르고 있다. 무선 네트워크 중 802.11로 대표되는 무선랜 환경에서도 예외는 아니다. 802.11은 상용화 단계에서 벌써 DoS(Denial of Service) 공격에 관한 취약점과 WEP[1]의 취약점 등 수많은 보안 취약점을 가지고 있었다. 이러한 취약점은 802.11i 그룹을 생겨나게 했고 802.11i 그룹은 이러한 이슈들을 보완한 표준안을 제시하였다. 802.11과 802.11i의 차이점 중 하나는 802.11i가 상호키(Pairwise Key)를 이용한 강력한 데이터 무결성 및 기밀성을 제공한다는 것이다. 기존 802.11에서 WEP만을 이용하여 데이터를 암호화했던 것과는 달리 802.11i에서는 TKIP[2]또는 CCMP[2]를 이용한 강력한 데이터 암호화를 제공한다. 또한 802.11i에서는 인증서버(Authentication Server)를 이용하여 서플리컨트(supplicant) 네트워크에 들어오는 과정을 더욱 엄격하게 만들었다. 위와 같은 방법으로 802.11의 보안취약점을 보완한 802.11i에서도 몇몇 취약점들이 대두 되고 있다.

본 논문에서는 802.11i에서 대두되고 있는 보안 취약점 중 Deauthentication, Disassociation 메시지를 이용한 DoS 공격[3][4][5] 예방 메커니즘을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 802.11i를 간단히 소개하고 3장에서는 논문에서 제시하는 Deauthentication, Disassociation 메시지를 이용한 DoS 공격 예방 메커니즘을 자세하게 소개한다. 마지막 4장에서는 제안한 메커니즘에 대한 결론을 맺고 향후 연구 계획에 대해 기술한다.

2. 관련 연구

802.11i는 서플리컨트(Supplicant), AP(authenticator), 인증서버(authentication server)라는 3개의 컴포넌트로 구성되어 있다.

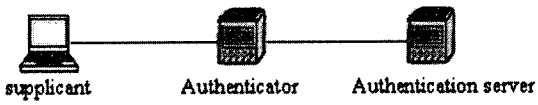

그림1. 802.11i의 3가지 컴포넌트

기존의 802.11에서는 정의되지 않았던 인증서버 기능이 추가됨에 따라 서플리컨트가 네트워크로 접근하는 과정에 4-Way Handshake[6]와 같은 새로운 절차가 추가되었고 데이터 암호화 또한 TKIP를 사용함으로써 보안이 강력해졌다. 그러나 TKIP를 사용한 데이터 암호화는 관리 프레임에 있어서는 예외적이다.

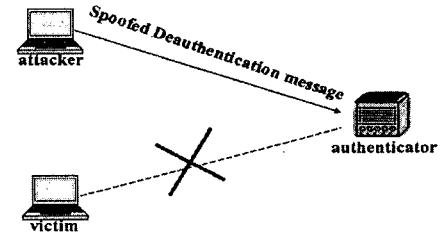

그림2. Deauthentication 공격 과정

This work was supported by MIC

관리 프레임은 802.11과 마찬가지로 데이터 암호화를 위해서 WEP만이 사용된다. 이러한 이유로 802.11의 대표적인 DoS 공격인 Deauthentication, Disassociation 공격이 802.11i에서도 그대로 이루어 질 수 있다. 그림2와 같은 Deauthentication 공격이 이루어지면 피해자의 상태가 그림3에서 State3, 또는 State2 상태에서 State1의 상태가 된다. 이 공격은 피해자가 authentication, association과정을 다시 수행하게 만든다.

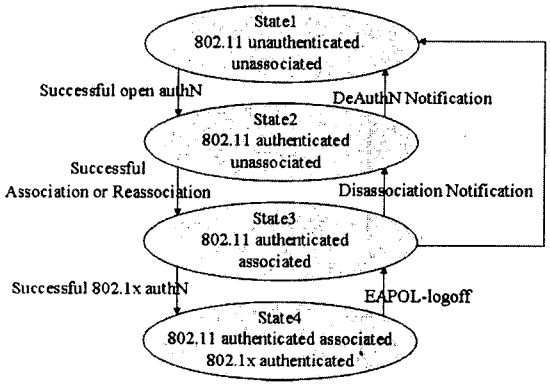

그림3. 802.11i 상태 천이도

3. 제안사항

본 논문에서 제안하는 예방 메커니즘을 위해서는 서플리컨트가 State Value라는 고유의 값을 가지고 있어야 한다. 그리고 메커니즘의 구조는 Packet Analysis Engine과 Spoofing Detection Engine으로 구별된다.

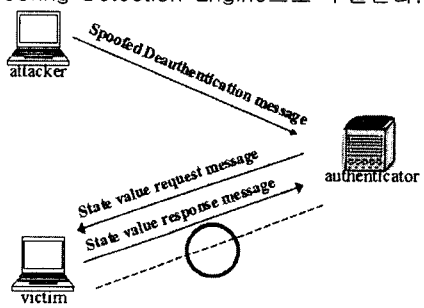

그림4. Deauthentication 공격을 예방 하는 과정

그림4는 Deauthentication 공격이 들어왔을 때 메커니즘이 어떻게 동작하는 지를 보여주고 있다. 처음 들어오는 Deauthentication 메시지에 대해서 AP는 이 메시지가 정당한 메시지인지 공격인지를 알지 못한다. 이를 알기 위해서 AP는 받은 Deauthentication 메시지의 Source MAC 주소로 State value 요청 메시지를 보내게 되고 이를 받은 서플리컨트는 자신의 State Value를 State Value 응답 메시지에 넣어 서플리컨트로 보내게 된다. SDE는 자신이 예상한 값과 서플리컨트에게서 받은 값을 비교하여 공격 여부를 판단하게 되고 공격이 아닐 경우에 패킷을 처리 하고 공격일 경우에는 패킷을 폐기한다.

그림5는 메커니즘 동작과정에서 메시지들이 전달되는 형태를 보여 준다. Deauthentication 메시지는 관리 프레임이므로 WEP을 사용하여 암호화되고 나머지 두 개의 메시지들은 데이터 프레임이므로 TKIP를 이용하여 암호화된다.

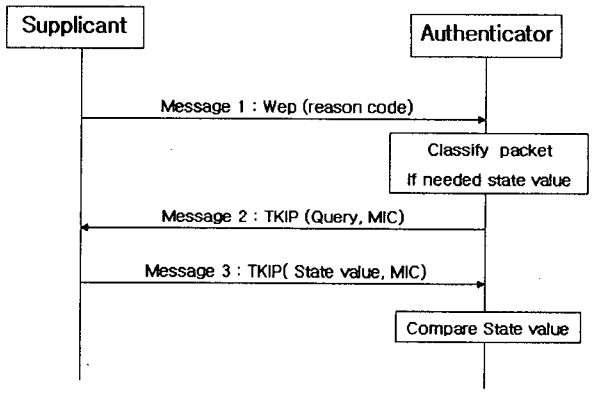

그림5. 메커니즘의 메시지 전달

3.1 State Value

State Value는 SDE에서 패킷의 진위 여부를 판단하는데 쓰이는 값이다. 이 값은 서플리컨트에 저장되어 있고 자신의 State변화를 위한 메시지(ex. Authentication 요청 메시지, Association 요청 메시지, EAPOL start 메시지, EAPOL 로그오프(logoff) 메시지, disassociation 요청 메시지, Deauthentication 요청 메시지)를 보낸 후에 스스로 업데이트한다. 표1은 State Value의 값과 그에 따른 상태에 관한 도표이다.

표1. State Value Table

State Value	서플리컨트의 상태
000	Authentication 요청 메시지를 보낸 후
001	Association또는Reassociation 요청 메시지를 보낸후.
010	EAPOL start 메시지를 보낸 후
011	EAPOL logoff 메시지를 보낸 후
100	Disassociation 요청 메시지를 보낸 후
101	Deauthentication 요청 메시지를 보낸 후

3.2 DoS 공격 예방 메커니즘

DoS 공격 예방 메커니즘은 Packet Analysis Engine (PAE)과 Spoofing Detection Engine(SDE)으로 구성된다.

3.2.1 Packet Analysis Engine

PAE는 받은 패킷 중 Deauthentication 메시지와 Disassociation 메시지만을 SDE에 보내주고 나머지 패킷들은 Authenticator에게 보내 주는 역할을 한다. 프레임 제어 필드(Frame control field)의 타입(Type)과 서브타입(Subtype)값을 보고 패킷이 Deauthentication 메시지인지 Disassociation 메시지인지 판별하게 된다. PAE를 두

는 이유는 모든 패킷에 관해서 요청 메시지와 응답 메시지를 주고받는 동작을 하게 되면 이에 따른 부하가 크기 때문이다.

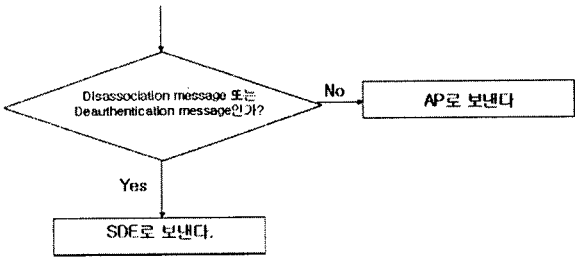

그림6. PAE 동작과정

3.2.2 Spoofing Detection Engine

SDE에서 DoS 예방 메커니즘의 가장 주요한 일들이 이루어진다. PAE로부터 패킷을 받으면 SDE에서 받은 패킷의 Source MAC 주소로 State Value 요청 메시지를 보내고 이에 관한 응답 메시지를 받는다. 이렇게 받은 응답 메시지에는 위에서 언급한 State Value 값이 들어 있다. 이 값을 자신이 예상한 값과 비교하여 같으면 PAE로부터 받은 메시지를 AP로 전달하고, 같지 않으면 폐기처리한다. 예를 들면 Deauthentication 메시지를 보낸 후에 서플리컨트의 State Value는 '101' 이어야 하는데 응답 메시지에 담겨진 State Value 값이 '010' 이라면 이는 위조된 Deauthentication 메시지라고 판단하여 폐기처분하게 된다. 그림7은 이러한 SDE의 동작과정을 흐름도로 나타낸 것이다.

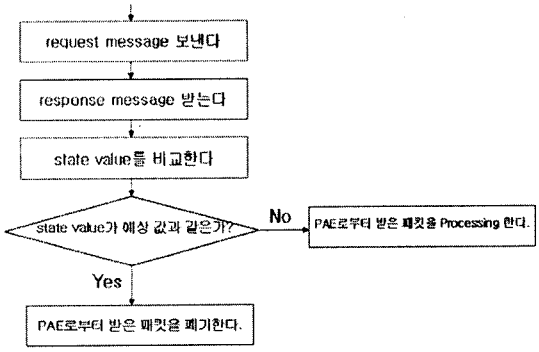

그림7. SDE동작과정 흐름도

요청메시지와 응답메시지는 그림8과 그림9에서 보여주듯이 데이터 프레임이고 각각의 서브 시퀀스 필드(sub sequence field) 값은 사용하지 않는 1000과 1001로 정의 한다. 요청 메시지에는 의미를 가지는 값이 포함되지 않지만 응답메시지에는 State Value 값이 포함된다.

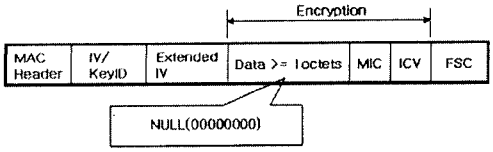

그림8. State request 메시지

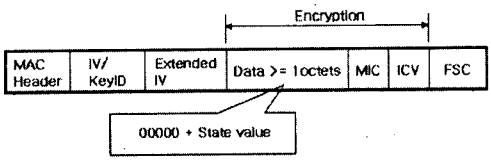

그림9. State response 메시지

4. 결론

본 논문에서는 802.11i에서 Deauthentication 공격과 Disassociation 공격을 예방하는 메커니즘을 제시하였다. 이 메커니즘에서는 모든 패킷에 관한 예방을 하는 것이 아니라 Deauthentication request 메시지와 Disassociation request 메시지에 관해서만 예방함으로써 오버헤드를 줄였고 또한 예방 알고리즘 또한 복잡하지 않다. 이 논문에서 제안한 State Value를 이용하여 스푸핑(Spoofing)된 MAC를 이용한 공격에 관한 다른 예방책을 제안할 수 있을 것이다.

향후 과제는 State Value를 이용한 다른 종류의 DoS 공격에 관한 예방 알고리즘 개발과 현제 802.11에서 사용되고 있는 다른 예방 메커니즘을 수용한 발전적인 예방 메커니즘 개발 그리고 논문에서 제안된 메커니즘을 구현하여 검증하는 것이다.

참 고 문 헌

[1]IEEE Standard 802.11-2003. Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11:Wireless LAN Medium Access Control and Physical Layer Specifications. 2004.

[2]IEEE Standard 802.11i-2004. Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11:Wireless LAN Medium Access Control and Physical Layer Specifications. 2004.

[3]Ding, P.Q. Holliday, J.N. Celik, "A Improving the security of wireless LANs by managing 802.1x disassociation" CCNC 2004, Page(s):53 - 58, Jan.2004.

[4]Changhua He and John C. Mitchell. "Security analysis and improvements of IEEE 802.11i. NDSS05", Feb. 2005.

[5]Joshua Wright, "Detecting Wireless LAN MAC Address Spoofing", CCNA, jun.2003

[6]Changhua He and John C. Mitchell, "Analysis of 802.11i 4-Way Handshake", WiSe04, Oct. 2004.