(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년05월12일
(11) 등록번호 10-1393180
(24) 등록일자 2014년04월30일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) *H04L 9/00* (2006.01)
H04L 12/70 (2013.01) *H04L 12/22* (2006.01)
(21) 출원번호 10-2012-0096999
(22) 출원일자 2012년09월03일
심사청구일자 2012년09월03일
(65) 공개번호 10-2014-0046495
(43) 공개일자 2014년04월21일
(56) 선행기술조사문헌
KR1020040022073 A*
논문:(2002.10)
JP2012039437 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대헌
서울 서초구 서초중앙로 200, 13동 1407호 (서초동, 삼풍아파트)
강전일
인천광역시 남구 용현동 인하대학교 253 하이테크센터 307호
(뒷면에 계속)
(74) 대리인
양성보

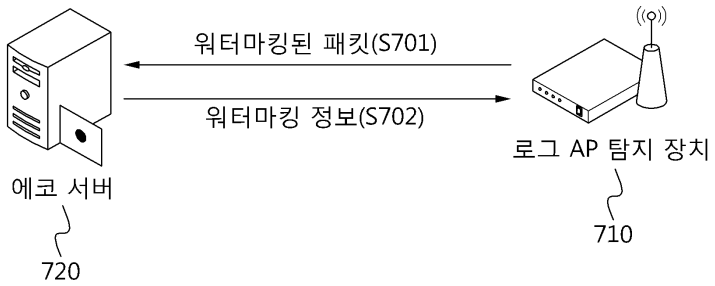
전체 청구항 수 : 총 10 항 심사관 : 전용해

(54) 발명의 명칭 **패킷 워터마킹을 통한 로그 AP 탐지 방법 및 시스템**

(57) 요 약

본 발명은 패킷 워터마킹을 이용하여 로그 AP(Access Point)를 탐지하는 방법과 그 시스템에 관한 것이다. 로그 무선 접속 장치(Access Point, AP)를 탐지하는 방법에 있어서, 로그 AP 탐지 장치가 에코 서버로 워터마킹된 패킷을 전송하는 단계; 및 로그 AP 탐지 장치가 접속되어 있는 무선 랜 네트워크에 워터마킹된 패킷이 전송되는지 확인하는 단계를 포함하는 로그 AP 탐지 방법이 제공될 수 있다.

대 표 도 - 도7



(72) 발명자

신동오

서울 강서구 남부순환로5길 26, 3층 (공항동)

변제성

전남 순천시 연향1로 12, (연향동)

특허청구의 범위

청구항 1

로그 무선 접속 장치(Access Point, AP)를 탐지하는 방법에 있어서,

로그 AP 탐지 장치가 에코 서버로 워터마킹된 패킷을 전송하는 단계; 및

상기 로그 AP 탐지 장치가 접속되어 있는 무선 랜 네트워크에 상기 워터마킹된 패킷이 전송되는지 확인하는 단계

를 포함하고,

상기 에코 서버로 워터마킹된 패킷을 전송하는 단계는

복수의 패킷들 각각의 전송 시간 간격이 얼마나 긴지 여부를 워터마크로 사용하는 방식 또는 특정 시간에서 상기 복수의 패킷들이 전송되는지 여부를 워터마크로 사용하는 방식 중 어느 하나의 방식을 이용하여 워터마킹된 패킷을 생성하는 단계

를 포함하는 로그 AP 탐지 방법.

청구항 2

제1항에 있어서,

상기 워터마킹된 패킷을 전송하는 단계는

상기 에코 서버가 수신한 상기 워터마킹된 패킷에 대한 정보를 다시 상기 AP 로그 탐지 장치로 전송하는 단계를 포함하며,

상기 패킷에 대한 정보는 암호학적 방법을 통해 데이터의 무결성을 보장하는 것으로, 메시지 인증 코드(Message Authentication Code, MAC)나 전자 서명(Digital Signature)에 해당하는 것

을 특징으로 하는 로그 AP 탐지 방법.

청구항 3

제2항에 있어서,

상기 워터마킹된 패킷이 전송되는지 확인하는 단계는

상기 패킷이 상기 로그 AP 탐지 장치와 상기 에코 서버를 오가는 동안 상기 로그 AP 탐지 장치가 접속되어 있는 무선 랜을 계속적으로 모니터링하고,

전송된 패킷과 동일한 워터마킹된 패킷을 찾아낸다면 상기 로그 AP 탐지 장치가 접속해 있는 AP가 로그 AP라고 판단하는 것

을 특징으로 하는 로그 AP 탐지 방법.

청구항 4

제1항에 있어서,

상기 워터마킹된 패킷의 데이터에는 송신하고자 하는 값, 또는 워터마킹 값 자체가 중복되어 저장되거나, 에러 교정 코드를 저장하고 있는 것

을 특징으로 하는 로그 AP 탐지 방법.

청구항 5

삭제

청구항 6

로그 무선 접속 장치(Access Point, AP)를 탐지하는 방법에 있어서,

에코 서버로부터 수신하는 패킷의 워터마킹을 예측할 수 있는 로그 AP 탐지 장치는 상기 로그 AP 탐지 장치가 접속하고 있는 무선 랜에 상기 예측된 워터마킹된 패킷이 존재하는지 확인하는 단계

상기 워터마킹된 패킷은

복수의 패킷들 각각의 **전송 시간 간격이 얼마나** 긴지 여부를 워터마크로 사용하는 방식 또는 특정 시간에서 상기 복수의 패킷들이 전송되는지 여부를 워터마크로 사용하는 방식 중 어느 하나의 방식을 이용하여 생성되는 로그 AP 탐지 방법.

청구항 7

제6항에 있어서,

상기 로그 AP 탐지 장치에서 워터마킹을 지정해 상기 에코 서버로 알리거나, 상기 에코 서버가 무작위로 워터마킹을 결정하여 상기 로그 AP 탐지 장치로 전송하는 패킷을 통해 알림으로써,

상기 로그 AP 탐지 장치가 상기 에코 서버로부터 수신하는 패킷의 워터마킹을 예측하는 것

을 특징으로 하는 로그 AP 탐지 방법.

청구항 8

제6항에 있어서,

상기 로그 AP 탐지 장치와 상기 에코 서버 사이에 공유 비밀키가 존재하여, 상기 공유 비밀키를 이용하여 워터마킹을 결정하거나,

상기 로그 AP 탐지 장치나 상기 에코 서버가 선택한 난수를 암호화하여 공유하여 워터마킹을 결정함으로써,

상기 로그 AP 탐지 장치가 상기 에코 서버로부터 수신하는 패킷의 워터마킹을 예측하는 것

을 특징으로 하는 로그 AP 탐지 방법.

청구항 9

제6항에 있어서,

상기 에코서버에서 상기 로그 AP 탐지 장치로 전송되는 패킷은

워터마킹의 무결성을 보장하기 위해 메시지 인증 코드나 전자 서명을 포함하는 것

을 특징으로 하는 로그 AP 탐지 방법.

청구항 10

로그 AP 탐지 장치; 및

에코 서버

를 포함하고,

상기 로그 AP 탐지 장치가 상기 에코 서버로 워터마킹된 패킷을 전송하며,

상기 로그 AP 탐지 장치가 접속되어 있는 무선 랜 네트워크에 상기 워터마킹된 패킷이 전송되는지 확인하고,

상기 워터마킹된 패킷은

복수의 패킷들 각각의 **전송 시간 간격이 얼마나** 긴지 여부를 워터마크로 사용하는 방식 또는 특정 시간에서 상기 복수의 패킷들이 전송되는지 여부를 워터마크로 사용하는 방식 중 어느 하나의 방식을 이용하여 생성되는 것

을 특징으로 하는 로그 AP 탐지 시스템.

청구항 11

로그 AP 탐지 장치; 및

에코 서버

를 포함하고,

상기 에코 서버로부터 수신하는 패킷의 워터마킹을 예측할 수 있는 상기 로그 AP 탐지 장치는 상기 로그 AP 탐지 장치가 접속하고 있는 무선 랜에 상기 예측된 워터마킹된 패킷이 존재하는지 확인하고,

상기 워터마킹된 패킷은

복수의 패킷들 각각의 **전송 시간 간격이 얼마나** 긴지 여부를 워터마크로 사용하는 방식 또는 특정 시간에서 상기 복수의 패킷들이 전송되는지 여부를 워터마크로 사용하는 방식 중 어느 하나의 방식을 이용하여 생성되는 것

을 특징으로 하는 로그 AP 탐지 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 패킷 워터마킹을 이용하여 로그 AP(Access Point)를 탐지하는 방법과 그 시스템에 관한 것이다.

배 경 기 술

[0002] 기존의 많은 로그 AP(Access Point, 무선 접속 장치) 탐지 기법은 실제 인터넷을 포함한 외부 네트워크에 접속하고자 하는 무선 랜 장치에 의해서 이루어졌다. 일반적인 무선 랜 장치는 하드웨어적인 제한 사항으로 인하여, 무선 링크에서 이루어지는 외부의 모든 통신에 대해서 모니터링 하는 능력이 제한되기 때문에, 이러한 기법들은 자신에게 주어진 정보만을 이용할 수밖에 없다.

[0003] 이에, AP의 하드웨어 주소라든지 AP로부터 보내진 데이터를 근거로 AP가 사용하는 스택을 파악하는 방법들이 바로 그것이다. 또는 메시지를 보내고 돌아오는 시간을 보고 네트워크의 상태 등을 파악하거나 이상 유무를 감별하는 방법들이 사용되기도 하였다.

[0004] 이러한 방법들은 사용자의 입장에서 적극적으로 로그 AP에 대항하는 방법으로써 충분히 가치 있는 일이지만, AP에 접속하는 모든 무선 랜 장치에 탑재되어야 할 뿐만 아니라, 오류의 발생 빈도가 높다는 문제도 존재한다.

발명의 내용

해결하려는 과제

[0005] 본 발명에서는 로그 AP 탐지 장치(Rogue AP detector)와 에코 서버(echo server)를 이용하여 로그 AP를 찾아내고, 로그 AP로의 접속을 차단하기 위한 방법을 제공하고자 한다.

[0006] 로그 AP 탐지 장치는 무선 랜 서비스 지역에 설치되어 동작하므로, 무선 랜 장치들은 기존과 동일하게 로그 AP에 신경 쓰지 않고 무선 랜 서비스를 이용할 수 있게 한다. 따라서, 기존의 무선 침입 방지 시스템(Wireless Intrusion Prevention System, WIPS)에 탑재되어 동작될 수 있는 로그 AP 탐지 장치를 제공하고자 한다.

과제의 해결 수단

[0007] 로그 무선 접속 장치(Access Point, AP)를 탐지하는 방법에 있어서, 로그 AP 탐지 장치가 에코 서버로 워터마킹된 패킷을 전송하는 단계; 및 로그 AP 탐지 장치가 접속되어 있는 무선 랜 네트워크에 워터마킹된 패킷이 전송되는지 확인하는 단계를 포함하는 로그 AP 탐지 방법이 제공될 수 있다.

[0008] 또 다른 측면에 있어서, 워터마킹된 패킷을 전송하는 단계는 에코 서버가 수신한 워터마킹된 패킷에 대한 정보를 다시 AP 로그 탐지 장치로 전송하는 단계를 포함하며, 패킷에 대한 정보는 암호학적 방법을 통해 데이터의 무결성을 보장하는 것으로, 메시지 인증 코드(Message Authentication Code, MAC)나 전자 서명(Digital Signature)에 해당할 수 있다.

[0009] 또 다른 측면에 있어서, 워터마킹된 패킷이 전송되는지 확인하는 단계는 패킷이 로그 AP 탐지 장치와 에코 서버를 오가는 동안 로그 AP 탐지 장치가 접속되어 있는 무선 랜을 계속적으로 모니터링하고, 전송된 패킷과 동일한

워터마킹된 패킷을 찾아낸다면 로그 AP 탐지 장치가 접속해 있는 AP가 로그 AP라고 판단할 수 있다.

[0010] 또 다른 측면에 있어서, 워터마킹된 패킷의 데이터에는 송신하고자 하는 값, 또는 워터마킹 값 자체가 중복되어 저장되거나, 에러 교정 코드를 저장할 수 있다.

[0011] 또 다른 측면에 있어서, 에코 서버로 전송되는 패킷은 패킷 전송 시간 또는 패킷 전송 시간 간격을 이용하여 워터마킹될 수 있다.

[0012] 로그 무선 접속 장치(Access Point, AP)를 탐지하는 방법에 있어서, 에코 서버로부터 수신하는 패킷의 워터마킹을 예측할 수 있는 로그 AP 탐지 장치는 로그 AP 탐지 장치가 접속하고 있는 무선 랜에 예측된 워터마킹된 패킷이 존재하는지 확인하는 단계를 포함하는 로그 AP 탐지 방법이 제공될 수 있다.

[0013] 또 다른 측면에 있어서, 로그 AP 탐지 장치에서 워터마킹을 지정해 에코 서버로 알리거나, 에코 서버가 무작위로 워터마킹을 결정하여 로그 AP 탐지 장치로 전송하는 패킷을 통해 알림으로써, 로그 AP 탐지 장치가 에코 서버로부터 수신하는 패킷의 워터마킹을 예측할 수 있다.

[0014] 또 다른 측면에 있어서, 로그 AP 탐지 장치와 에코 서버 사이에 공유 비밀키가 존재하여, 공유 비밀키를 이용하여 워터마킹을 결정하거나, 로그 AP 탐지 장치나 에코 서버가 선택한 난수를 암호화하여 공유하여 워터마킹을 결정함으로써, 로그 AP 탐지 장치가 에코 서버로부터 수신하는 패킷의 워터마킹을 예측할 수 있다.

[0015] 또 다른 측면에 있어서, 에코서버에서 로그 AP 탐지 장치로 전송되는 패킷은 워터마킹의 무결성을 보장하기 위해 메시지 인증 코드나 전자 서명을 포함할 수 있다.

[0016] 로그 AP 탐지 장치; 및 에코 서버를 포함하고, 로그 AP 탐지 장치가 에코 서버로 워터마킹된 패킷을 전송하며, 로그 AP 탐지 장치가 접속되어 있는 무선 랜 네트워크에 워터마킹된 패킷이 전송되는지 확인하는 것을 특징으로 하는 로그 AP 탐지 시스템이 제공될 수 있다.

[0017] 로그 AP 탐지 장치; 및 에코 서버를 포함하고, 에코 서버로부터 수신하는 패킷의 워터마킹을 예측할 수 있는 로그 AP 탐지 장치는 로그 AP 탐지 장치가 접속하고 있는 무선 랜에 예측된 워터마킹된 패킷이 존재하는지 확인하는 것을 특징으로 하는 로그 AP 탐지 시스템이 제공될 수 있다.

발명의 효과

[0018] 본 발명의 실시예를 통해, 무선 랜의 모든 패킷을 모니터링 할 수 있는 로그 AP 탐지 장치는 에코 서버에게 워터 마킹된 패킷을 보내고 무선 랜에 자신이 보냈던 패킷들이 전송되는지를 탐지하여 로그 AP를 가려내고, 로그 AP의 접속을 차단할 수 있다.

[0019] 또한, 기존의 무선 침입 방지 시스템(wireless intrusion prevention system, WIPS) 장치에 탑재되어 동작될 수 있는 로그 AP 탐지 장치를 제공하여, 로그 AP 탐지 장치를 위한 추가적인 비용을 필요로 하지 않게 된다.

도면의 간단한 설명

[0020] 도 1은 정상적으로 무선 랜을 이용하는 환경의 예시를 도시한 것이다.

도 2는 로그 AP로 인한 비정상적인 무선 랜 이용 환경의 예시를 도시한 것이다.

도 3은 로그 AP 탐지 장치가 탑재될 수 있는 무선침입 방비 시스템(WIPS)의 일례를 도시한 것이다.

도 4는 본 발명의 일실시예에 있어서, 로그 AP를 통해 로그 AP 탐지 장치가 에코 서버와 데이터를 송수신하는 것을 나타낸 것이다.

도 5는 본 발명의 일실시예에 있어서, 여러 가지 패킷 전달 방식과 패킷 워터마킹 방식의 일례를 도시한 것이다.

도 6은 본 발명의 일실시예에 있어서, 패킷의 워터마킹과 패킷의 데이터 사이의 관계를 설명하기 위한 도면이다.

도 7은 본 발명의 일실시예에 있어서, 로그 AP 탐지 장치에서 에코 서버로 워터마킹된 패킷이 전송되는 일례를 도시한 것이다.

도 8은 본 발명의 일실시예에 있어서, 에코 서버에서 로그 AP 탐지 장치로 워터마킹된 패킷이 전송되는 일례를

도시한 것이다.

발명을 실시하기 위한 구체적인 내용

[0021] 이하, 로그 AP를 탐지하는 방법과 그 시스템에 대해서 첨부된 도면을 참조하여 자세히 설명한다.

[0022] 정상적인 무선 랜 환경의 이용은 도 1과 같이 이루어질 수 있다. 실시예에 있어서, 로그 AP가 존재하지 않는 네트워크 시스템에서 무선 랜 장치는 AP를 통해 AP와 유선으로 연결된 외부의 네트워크에 접속하도록 할 수 있다. 사용자의 설정에 의해서 무선 연결 구간은 암호화되거나, 되지 않을 수 있다.

[0023] 본 발명의 실시예에 있어서, 탐지하고자 하는 로그 AP는 도 2와 같은 네트워크 시스템을 만드는 둘 이상의 무선 링크를 가지고 있는 로그 AP이다. 둘 이상의 무선 링크 중 최소 하나의 링크는 로그 AP가 아닌 AP를 통해 외부 네트워크에 연결하는 역할을 수행하며, 또 다른 최소 하나의 링크는 일반 무선 랜 장치들에게 정상적인 AP인 것처럼 연결을 유도하여 중간에서 일반 무선 랜 장치와 외부 네트워크 사이에서 송수신되는 메시지를 엿듣거나 데이터를 변조할 수 있다.

[0024] 이러한 로그 AP는 진짜 AP와 무선 랜 장치 사이의 무선 링크가 암호화되어 있다고 하더라도 접속을 유도하여 메시지의 내용을 볼 수 있다. 일반적으로 진짜 AP는 외부 네트워크로 통하는 유선 링크를 가지고 있는데, 로그 AP는 이러한 유선 링크를 쉽게 찾을 수 없으며, 공격자가 기존 AP의 유선 링크를 물리적으로 빼앗아 로그 AP에 접속하는 것은 공격자에게 위험 부담이 될 수 있다.

[0025] 또한, 이러한 로그 AP는 일반 노트북과 같은 장비에 무선 랜 카드를 하나 더 추가함으로써 쉽게 구성할 수 있다. 이러한 관점에서 생각하면, 3G나 4G 네트워크 망을 이용하여 무선 랜을 테더링하는 스마트 폰, WDS(Wireless Distribution System) 등의 서비스들도 잠재적인 로그 AP로 분류할 수 있다.

[0026] 본 발명은 상기 설명한 두 개 이상의 무선 링크를 가진 로그 AP(Access Point, 무선 접속 장치)를 패킷 워터마킹 기법을 이용하여 탐지하는 방법 및 그 시스템에 대한 것이다. 실시예에 있어서, 무선 랜의 모든 패킷을 모니터링 할 수 있는 로그 AP 탐지 장치는 에코 서버에게 워터마킹된 패킷을 보내고 무선 랜에 자신이 보냈던 패킷들이 전송되는지 탐지하여 로그 AP를 가려낼 수 있다.

[0027] 발명의 실시예에 있어서, 로그 AP 탐지 장치는 도 3에 도시된 무선 침입 방비 시스템의 내부에 탑재되어 동작할 수 있다. 로그 AP를 탐지하기 위해서 도 3과 같이 무선 침입 방비 시스템(Wireless Intrusion Prevention System, WIPS)을 통해서 무선 연결되는 구간에서 데이터 링크(MAC) 수준의 모든 데이터를 모니터링할 수 있고, 이러한 무선 침입 방비 시스템은 특정 AP와 데이터를 송수신할 수 있다.

[0028] 도 4는 로그 AP를 통하여 로그 AP 탐지 장치가 에코 서버에 데이터를 보내고 받는 절차의 예시를 나타낸 것이다.

[0029] 로그 AP 탐지 장치는 무선 랜 서비스가 지원되는 지역에 설치되어 무선 링크를 통한 모든 통신을 엿들을 수 있다. 에코 서버는 무선 랜 외부의 유선 네트워크에 고정적으로 설치되어 다수의 로그 AP 탐지 장치의 요청을 처리할 수 있다. 에코 서버는 개인키(Private key)를 이용하여 서명을 생성할 수 있으며 모든 로그 AP 탐지 장치는 이러한 에코 서버의 IP 주소와 공개키 인증서(Public key certificate)를 가지고 있다. 그렇지 않은 경우엔 로그 AP 탐지 장치는 에코 서버와의 사이에 비밀키(secret key)를 공유할 수 있다.

[0030] 로그 AP 탐지 장치와 에코 서버 사이의 패킷들은 워터마킹이 되어 있기 때문에 로그 AP가 패킷을 조작하면, 로그 AP 탐지 장치가 이를 발견해낼 수 있으며, 조작하지 않은 워터마킹된 패킷은 무선 랜 모니터링을 통해서 검출될 수 있다.

[0031] 이에 로그 AP 탐지 장치는 탐지가 가능한 범위 내에서 실시간으로 무선 랜을 모니터링할 수 있다. 패킷의 모니터링은 MAC 계층에서 이루어질 수 있는데, 본 발명에서 필요로 하는 패킷의 모니터링 수준은 MAC 계층에서 전달되는 패킷의 내용이 필요한 것이 아니라, 패킷이 담고 있는 워터마킹에 초점을 맞추고 있다. 따라서, 환경에 따라서 다르지만, 이상적인 환경에서는 패킷 워터마킹 모니터링은 전달 매체(공기)의 에너지 변화의 감지로써도 이루어질 수 있다.

[0032] 만약 도 4에서 로그 AP가 아닌 AP를 통하여 로그 AP 탐지 장치와 에코 서버가 네트워크 연결될 경우, AP와 로그 AP 탐지 장치가 직접적으로 연결되며, 이는 정상적인 연결이기 때문에 별도의 조치가 필요하지 않다.

[0033] 본 발명의 실시예에 있어서, 도 5는 여러 가지 패킷의 전달 방식과 패킷의 워터마킹 방식의 일례를 도시한 것이다. 그림 (a)를 기본적인 패킷 전달 방식이라 한다면, 그림 (b)는 상 변환 방식, 그림 (c)는 타임 슬롯 방식으

로 설명할 수 있다.

[0034] 로그 AP 탐지를 위해서 로그 AP 탐지 장치와 에코 서버는 일련의 패킷에 워터마킹을 하여 데이터를 송수신한다. 워터마킹은 패킷의 내용과는 상관없이 구성될 수 있다.

[0035] 예를 들어, 그림 (b)와 같이 패킷 간 전송 시간 간격이 짧거나 긴 것이 일련의 데이터를 표현하기 위해서 사용될 수 있다. 패킷이 무선 랜을 포함하여 네트워크를 통해 전송되는 동안 정상적인 경우 전송 시간 간격은 대체적으로 유지되므로, 고의적으로 수정하지 않는다면 패킷의 워터마킹 값은 유사한 값을 유지된다.

[0036] 또 다른 예로는 그림 (c)와 같이, 시간을 일정한 간격으로 나누고 특정 시간에 패킷을 전송하거나 전송하지 않음으로써 일련의 데이터를 표현할 수도 있을 것이다. 또한, 패킷 간 전송 시간 간격이 단순히 두 단계로 나누는 것이 아니라 여러 단계로 나누어 사용할 수도 있을 것이다.

[0037] 워터마킹된 패킷의 데이터에는 송신하고자 하는 값이 중복되어 저장되는 것 이외에도 워터마킹 값 자체가 중복되어 저장되거나 에러 교정 코드 등을 포함할 수 있다.

[0038] 도 6은 본 발명의 일실시예에 있어서, 워터마킹된 패킷과 패킷의 데이터 간의 관계를 설명하기 위한 도면이다. 실시예에 있어서, 주어진 데이터와 워터마킹 정보를 담은 패킷 시퀀스를 만드는 함수이다. 도 6의 실시예를 통해 패킷의 내용은 데이터로서, 패킷 간의 간격은 워터마킹 정보로서 저장된다. 예컨대, 도시된 도면과 같이 간격이 좁으면 0, 넓으면 1의 정보를 담을 수 있다.

[0039] 본 발명의 실시예에 있어서, 로그 AP 탐지 장치는 모니터링하고 있는 무선 랜 서비스 지역에 새로운 AP가 탐지되거나 기존에 알려진 AP가 접속중인 MAC 주소를 변경하거나, 채널을 변경하는 등의 중요한 이벤트가 발생하면 이에 대해 로그 AP 탐지 방법을 실시할 수 있다. 본 발명에서 제안하는 패킷의 워터마킹 로그 AP 탐지 방법은 두 가지 방법으로 이루어질 수 있다.

[0040] 도 7은 본 발명의 실시예에 있어서, 로그 AP 탐지 장치에서 에코 서버로 워터마킹된 패킷을 전송하여 로그 AP를 탐지하는 방법을 설명하기 위해 간략화된 도면이다. 이때, 로그 AP 탐지 장치(710)는 에코 서버(720) 사이에 패킷(데이터)이 송수신되는 동안 무선 랜을 계속 모니터링할 수 있다.

[0041] 로그 AP 탐지 장치(710)는 에코 서버(720)로 워터마킹된 패킷을 전송한다(S701). 여기서, 로그 AP 탐지 장치(710)와 에코 서버(720)가 접속되어 있는 무선 랜 네트워크에 로그 AP 탐지 장치(710)가 전송한 패킷과 동일한 워터마킹이 있는지 확인할 수 있다. 송수신되는 패킷의 내용과 상관없이, 만약 로그 AP 탐지 장치(710)가 동일한 워터마킹을 발견한다면, 로그 AP 탐지 장치(710)가 접속하고 있는 AP는 로그 AP일 가능성이 높다고 판단할 수 있다.

[0042] 여기서, 로그 AP가 패킷의 워터마킹을 삭제할 가능성이 존재하기 때문에, 에코 서버(720)는 수신한 워터마킹의 정보를 다시 로그 AP 탐지 장치(710)로 전송할 수 있다(S702). 워터마킹의 정보는 암호학적 방법을 통해 데이터의 무결성이 보장되어야 한다.

[0043] 일반적으로 데이터의 무결성의 보장을 위해서는 메시지 인증 코드(message authentication code, MAC)나 전자서명(Digital signature)이 사용될 수 있다. 메시지 인증 코드의 경우 에코 서버(720)와 로그 AP 탐지 장치(710) 사이에 공유 비밀키(Shared secret key)가 필요하게 되며, 전자 서명의 경우 로그 AP 탐지 장치(710)가 에코 서버(720)의 서명 확인키(Verifying key)를 알고 있어야 한다. 또한, 로그 AP 탐지 장치(710)의 공개키(Public key) 또는 공유 비밀키를 이용하여 암호화하고, 그 결과를 되돌려 줌으로써 패킷의 무결성을 확보할 수도 있다.

[0044] 또는, 로그 AP 탐지 장치(710)는 패킷의 데이터로 워터마킹 정보와 그에 대한 무결성 정보, 즉, 메시지 인증 코드나 전자 서명을 사용하여 에코 서버(720)에 보낼 수 있다. 에코 서버(720)는 로그 AP 탐지 장치(710)로부터 받은 패킷의 워터마킹과 패킷이 담고 있는 데이터의 워터마킹(무결성이 확보된)을 비교하여 올바른 정보를 받았는지 아닌지 판단하여 로그 AP 탐지 장치로 알려줄 수 있다. 물론, 이러한 정보 또한 메시지 인증 코드나 전자서명으로 무결성의 확보가 필요하다.

[0045] 또한, 도 8과 같이 도 7에 도시한 것과는 반대로, 에코 서버(820)가 로그 AP 탐지 장치로 보내는 패킷에 워터마킹이 될 수 있다(S802). 실시예에 있어서, 단계(S802)의 실시는 로그 AP 탐지 장치(810)가 만약 에코 서버(820)가 보낼 패킷들의 워터마킹을 예측할 수 있을 때 가능한데, 로그 AP 탐지 장치(810)는 에코 서버(820)로부터 수신하는 패킷들을 제외하고 무선 랜에 동일한 워터마킹이 되어 있는 패킷이 존재하는지 확인하여 로그 AP가

있는지 확인할 수 있다.

[0046] 로그 AP 탐지 장치(810)가 에코 서버(820)로부터 수신할 패킷들의 워터마킹을 미리 알 수 있는 방법은 다양하게 존재할 수 있다. 에코 서버(820)로 워터마킹의 정보를 전송할 수 있는데(S801), 예컨대 워터마킹을 지정하여 알려줄 수도 있으며, 두 장치(810, 820) 간의 약속을 통해서 워터마킹을 정할 수도 있다. 또는, 에코 서버(820)가 무작위로 워터마킹을 결정하고, 패킷에 이를 알려줄 수도 있다.

[0047] 단계(S801)를 실시하기 위해서, 로그 AP 탐지 장치(810)는 공유 비밀키를 이용하여 워터마킹의 메시지 인증 코드를 생성하거나 서명키를 이용하여 전자 서명을 생성하여 첨부할 수 있다. 또한, 공유 비밀키를 이용하여 워터마킹을 대칭키 암호화 기법을 통해 암호화한 이후에 전송할 수 있으며, 에코 서버의 공개키로 암호화하여 전송해주는 방식으로 워터마킹의 무결성을 확보할 수도 있다.

[0048] 실시예에 있어서, 장치 간의 약속을 통해 워터마킹을 결정하기 위해서는 로그 AP 탐지 장치(810)와 에코 서버(820) 사이에 공유 비밀키가 있어 공개적으로 주고받은 난수 이외에 이를 이용하여 워터마킹 값을 계산해 내거나, 로그 AP 탐지 장치(810) 또는 에코 서버(820)가 선택한 난수 중 하나 또는 둘 모두 대칭키 시스템이나 공개키 시스템을 통해 암호화되어 서로에게 전송되어야 한다.

[0049] 만약, 에코 서버(820)가 무작위로 선택하여 패킷에 워터마킹을 하는 경우, 로그 AP 탐지 장치(810)는 워터마킹에 대한 사전 정보가 없기 때문에 네트워크를 모니터링하는 과정에서는 탐지해낼 수 없지만, 데이터를 수신한 뒤에 저장되어 있는 과거에 모니터링한 내용을 검색하여 로그 AP가 있었는지 탐지해낼 수 있다. 이때, 에코 서버(820)가 워터마킹 값을 안전하게 로그 AP 탐지 장치(810)에게 전송해주기 위해서는 공유 비밀키나 서명키가 존재하여, 메시지 인증 코드나 전자 서명을 생성함으로써 데이터의 무결성을 보장해 주어야 한다.

[0050] 도 8의 실시예는 도 7과 마찬가지로, 에코 서버가 로그 AP 탐지 장치로 보내는 패킷은 워터마킹과 워터마킹의 무결성 정보, 즉 메시지 인증 코드나 전자 서명, 또는 암호 등을 포함할 수 있다.

[0051] 이상과 같이 패킷 워터마킹을 이용하여 로그 AP를 찾아내는 방법을 통해서 로그 AP가 패킷의 워터마킹을 삭제할 경우엔 에코 서버의 도움을 받아 탐지해낼 수 있으며, 패킷의 워터마킹을 삭제하지 않았을 경우, 무선 랜을 모니터링하고 있는 로그 AP 탐지 장치를 통해 탐지할 수 있다. 따라서, 결과적으로 본 발명의 실시예를 통해 무선 네트워크 망에서 로그 AP를 탐지할 수 있는 확률을 높일 수 있다.

[0052] 본 발명의 실시예에 있어서, 로그 AP 탐지 방법은 로그 AP 탐지 시스템을 통해서 실시 가능하다. 도 7과 도 8에 나타낸 바, 로그 AP 탐지 시스템은 로그 AP 탐지 장치(710, 810)와 에코 서버(720, 820)를 포함하여 구성되며, 도 7과 도 8에 나타낸 로그 AP 탐지 방법을 실시할 수 있는 시스템이 될 수 있다.

[0053] 본 발명의 실시예는 이 분야의 통상의 지식을 지닌 사람에 의해서 다양한 변형이 가능하다. 도 7의 실시예 혹은 도 8의 실시예 중 하나의 실시예를 선택할 수 있으며, 두 가지 이상의 방법이 조합될 수 있다.

[0054] 예컨대, 로그 AP 탐지 장치로부터 에코 서버로 무작위로 생성한 워터마킹을 포함하는 패킷에 에코 서버가 생성하는 워터마킹을 지정하여 보내고, 에코 서버는 자신이 받은 패킷의 워터마킹을 풀어 이에 대한 서명을 데이터로 하는 패킷을 로그 AP 탐지 장치가 지정한 워터마킹 값에 따라 워터마킹하여 로그 AP 탐지 장치에게 보내는 방법을 생각해볼 수 있다.

[0055] 상기의 경우 로그 AP 탐지 장치는 두 번의 무선 랜 모니터링 기회를 갖고 있기 때문에, 한 가지 실시예만 사용하는 경우보다 더 높은 정확도로 로그 AP를 찾아낼 수 있다.

[0056] 로그 AP 탐지 절차를 어떠한 순서로 사용하느냐는 발명자에 의해 얼마든지 변형이 가능하다. 하지만 아무렇게나 선택해서 사용하는 것보다는, 로그 AP 탐지 장치나 에코 서버가 가져야 하는 사전 지식과 이 두 장치의 연산처리량에 따라 선택되는 것이 바람직하다.

[0057] 예를 들어, 로그 AP 탐지 장치가 어떠한 비밀키도 소유하지 않도록 하기 위해서는 디지털 서명이나 공개키 암호화 방식으로 이루어진 기법들만을 사용해야만 한다. 어떠한 비밀키도 소유하지 않는 로그 AP 탐지 장치는 관리가 간단하며, 양산이 용이하다.

[0058] 실시예에 있어서, 로그 AP 탐지 장치는 탐지된 로그 AP의 MAC 주소와 BSSID(Basic Service Set Identifier, 기본서비스영역(BSS)을 식별하는 식별자 또는 네트워크 ID)를 이용하여 관리 메시지를 주변의 모든 무선 랜 장치로 지속적으로 전송함으로써, 로그 AP와의 접속을 차단할 수 있다.

[0059] 실시예에 따른 로그 AP의 탐지 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현

되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic media), CD-ROM, DVD와 같은 광기록 매체(Optical media), 플롭티컬 디스크(Floptical disk)와 같은 자기-광 매체(Magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0060] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등한 것들에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0061] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

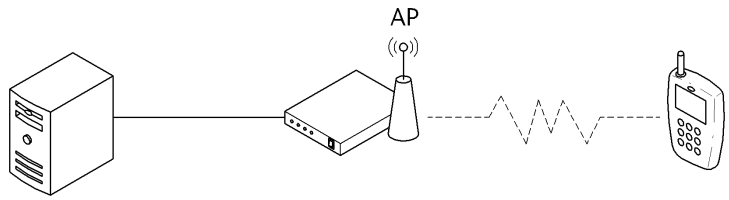
부호의 설명

[0062] 710, 810: 로그 AP 탐지 장치

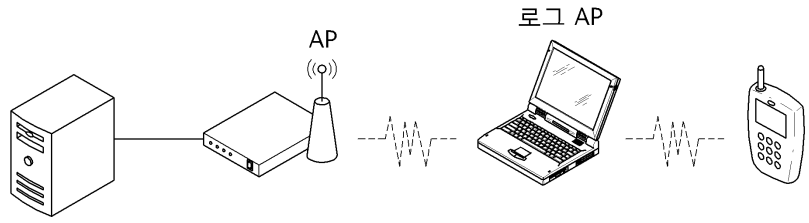
720, 820: 에코 서버

도면

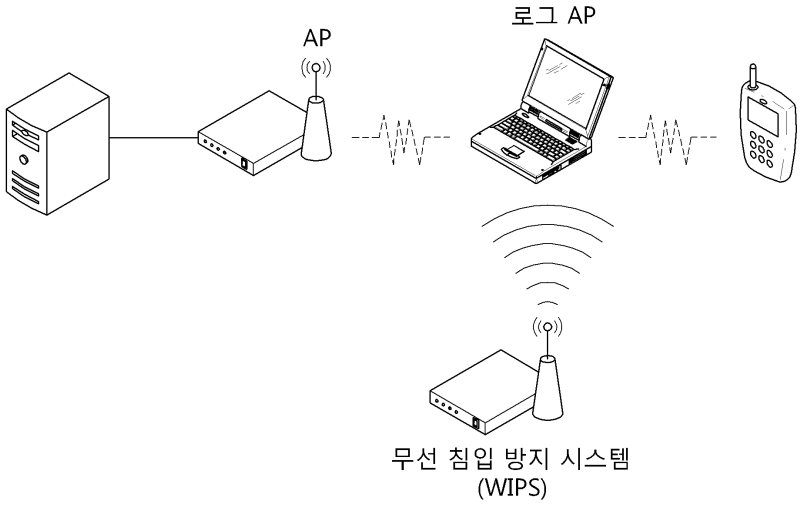
도면1



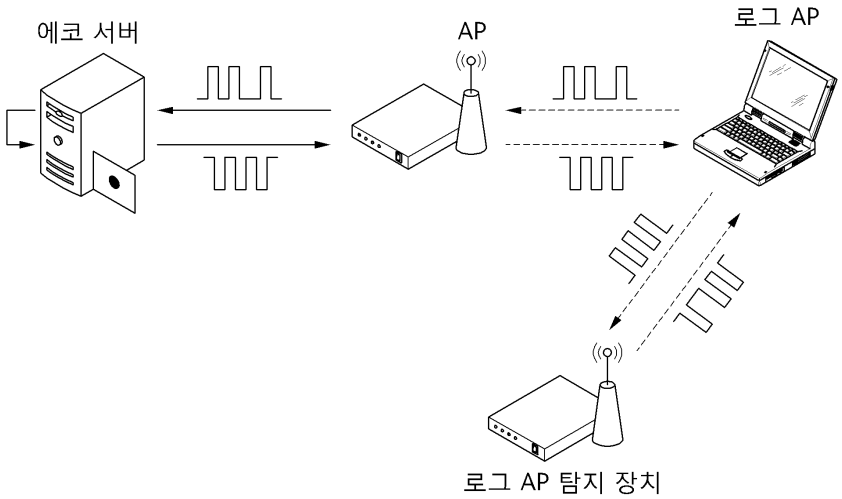
도면2



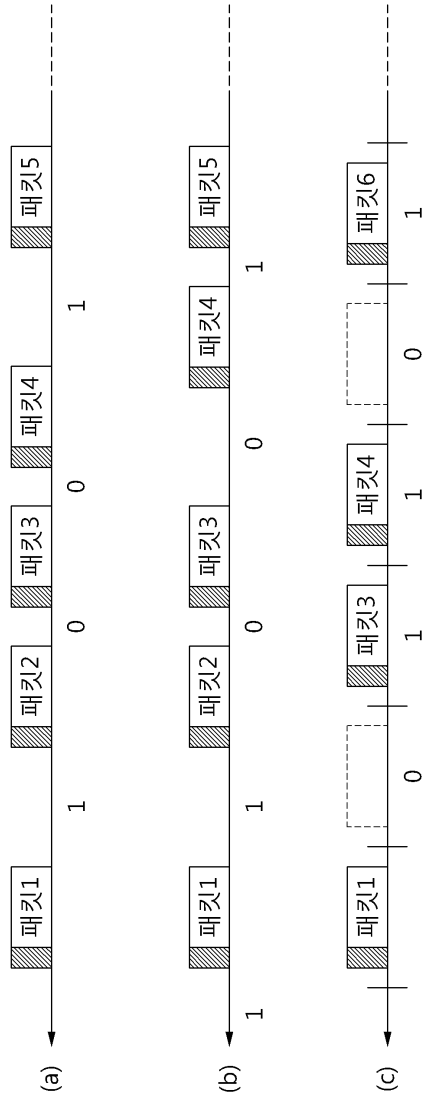
도면3



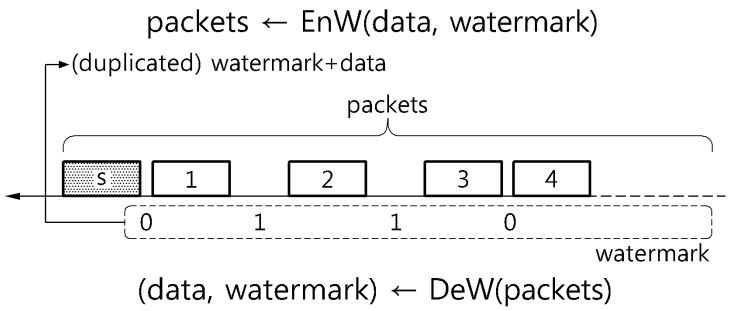
도면4



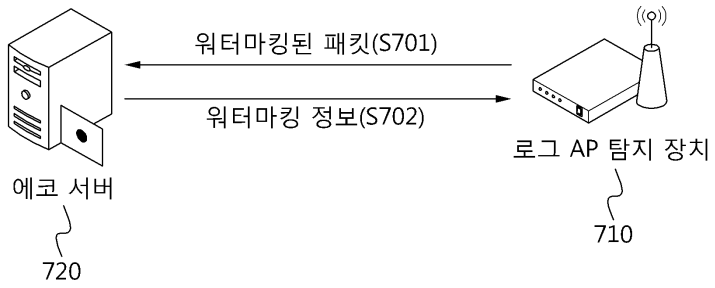
도면5


패킷1
패킷2
패킷3
패킷4
패킷5
패킷6
1
0
1
0
1
0
1
0
1
0
1
(a)
(b)
(c)

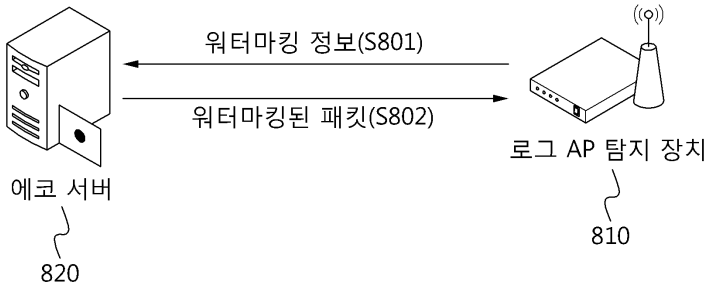
도면6


packets ← EnW(data, watermark)
(duplicated) watermark+data
packets
S
1
2
3
4
0
1
1
0
watermark
(data, watermark) ← DeW(packets)

도면7


워터마킹된 패킷(S701)
워터마킹 정보(S702)
에코 서버
720
로그 AP 탐지 장치
710

도면8


워터마킹 정보(S801)
워터마킹된 패킷(S802)
에코 서버
820
로그 AP 탐지 장치
810