(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년02월03일
(11) 등록번호 10-1489178
(24) 등록일자 2015년01월28일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) *H04L 12/26* (2006.01)
(21) 출원번호 10-2013-0109983
(22) 출원일자 2013년09월12일
심사청구일자 2013년09월12일
(56) 선행기술조사문헌
KR101091780 B1*
KR101174304 B1*
KR1020120090574 A
KR1020040109985 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
숭실대학교산학협력단
서울특별시 동작구 상도로 369 (상도동)
주식회사 안랩
경기도 성남시 분당구 판교역로 220 (삼평동)
(72) 발명자
정수환
서울특별시 동작구 상도로 369 숭실대학교 형남공학관 1105호
정승욱
서울특별시 동작구 상도로 369 숭실대학교 형남공학관 1102호
박정수
서울특별시 동작구 상도로 369 숭실대학교 형남공학관 1102호
(74) 대리인
특허법인엠에이피에스

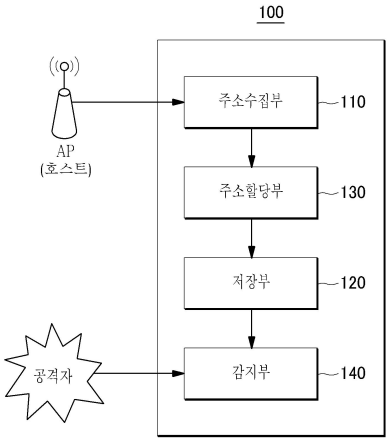
전체 청구항 수 : 총 6 항 심사관 : 장석환

(54) 발명의 명칭 **ARP스푸핑 감지단말 및 감지방법**

(57) 요 약

ARP스푸핑 감지단말은 서버로부터 인가된 호스트의 ARP정보를 수신하고, ARP정보로부터 맥 주소 및 아이피 주소를 수집하고, ARP테이블에 인가된 호스트의 맥 주소 및 아이피 주소를 정적 할당하고, 인가된 호스트와 동일한 아이피 주소에 대한 ARP응답 패킷을 수신한 경우, ARP스푸핑 공격으로 감지한다.

대 표 도 - 도2



이 발명을 지원한 국가연구개발사업
과제고유번호 1415128814
부처명 미래창조과학부
연구관리전문기관 정보통신산업진흥원
연구사업명 정보통신기술인력양성
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술개발 및 연구 인력양성
기 여 율 1/1
주관기관 숭실대학교산학협력단
연구기간 2013.01.01 ~ 2013.12.31

특허청구의 범위

청구항 1

ARP(Address Resolution Protocol) 스푸핑 감지단말에 있어서,

서버로부터 인가된 호스트의 ARP정보를 수신하고, 상기 ARP정보로부터 맥 주소 및 아이피 주소를 수집하는 주소수집부;

하나 이상의 호스트에 대한 맥 주소 및 아이피 주소가 할당된 ARP테이블이 저장된 저장부;

상기 ARP테이블에 상기 인가된 호스트의 맥 주소 및 아이피 주소를 정적 할당하는 주소할당부; 및

상기 인가된 호스트와 동일한 아이피 주소에 대한 ARP응답 패킷을 수신한 경우, ARP스푸핑 공격으로 감지하는 감지부를 포함하되,

상기 주소할당부는 상기 ARP테이블의 인가되지 않은 호스트의 맥 주소 및 아이피 주소를 동적 할당으로 관리하는 것인 ARP스푸핑 감지단말.

청구항 2

제 1 항에 있어서,

상기 인가된 호스트는 복수인 ARP스푸핑 감지단말.

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 감지부가 ARP스푸핑 공격을 감지한 경우 상기 ARP응답 패킷을 전송한 공격자의 아이피 주소 및 맥 주소를 상기 서버로 전송하는 ARP스푸핑 감지단말.

청구항 5

제 1 항 또는 제 2 항에 있어서,

상기 인가된 호스트 또는 상기 인가되지 않은 호스트는 무선랜 환경에서의 중계설비(Access Point, AP)인 ARP스푸핑 감지단말.

청구항 6

ARP스푸핑을 감지하는 방법에 있어서,

서버로부터 인가된 호스트에 대한 정보를 수신하고, 상기 ARP정보로부터 맥 주소 및 아이피 주소를 수집하는 단계;

상기 인가된 호스트의 맥 주소 및 아이피 주소를 ARP테이블에 정적 할당하는 단계; 및

상기 인가된 호스트와 동일한 아이피 주소에 대한 ARP응답 패킷을 수신한 경우, ARP스푸핑 공격으로 감지하는 단계를 포함하되,

상기 호스트의 맥 주소 및 아이피 주소를 ARP테이블에 정적 할당하는 단계는,

상기 서버로부터 인가되지 않은 호스트의 맥 주소 및 아이피 주소를 동적 할당으로 관리하는 단계를 포함하는 것인 ARP스푸핑 감지방법.

청구항 7

삭제

청구항 8

제 6 항에 있어서,

ARP스푸핑 공격을 감지한 경우 상기 ARP응답 패킷을 전송한 공격자의 아이피 주소 및 맥 주소를 상기 서버로 전송하는 단계를 더 포함하는 ARP스푸핑 감지방법.

명 세 서

기 술 분 야

[0001] 본 발명은ARP(Address Resolution Protocol)스푸핑 감지단말 및 감지방법에 관한 것이다.

배 경 기 술

[0002] ARP스푸핑이란 주소 결정 프로토콜(ARP) 캐쉬 메모리를 변조시켜 공격 대상의 맥(MAC) 주소를 자신의 컴퓨터의 맥 주소로 변경하여 모든 데이터가 공격자의 컴퓨터로 모니터링 되게 하는 공격기법을 의미한다.

[0003] 이때, ARP는 아이피(IP) 주소를 맥 주소와 연결시키는 프로토콜로서, ARP는 호스트가 아이피 주소를 이용하여 인터넷과 연결하면 내부 로컬 네트워크가 사용하는 물리적 주소인 맥 주소로 변환시켜준다.

[0004] 도 1은 도 1은 통상적으로 한 호스트(A)가 다른 호스트(C)에 패킷을 보내기 위하여 ARP프로토콜을 이용하는 프로세스의 도면이다.

[0005] 호스트(A)가 호스트(C)의 아이피 주소는 알고 있지만 맥 주소는 모르고 있는 상황이라면, 먼저 호스트(A)는 호스트(C)를 포함하여 자신과 같은 로컬 네트워크를 형성하고 있는 서브넷 호스트(B, C, D)들에게 ARP요청 패킷(Request)을 브로드캐스트한다. ARP요청 패킷(Request)은 패킷을 전송하는 호스트(A)의 맥 주소와 아이피 주소 및 호스트(C)의 아이피주소를 포함한다. ARP요청 패킷을 수신한 호스트(C)는 자신의 아이피 주소에 대한 패킷임을 감지하고 호스트(A)에 ARP응답 패킷을 전송한다. ARP응답 패킷은 호스트(C) 자신의 맥 주소와 아이피 주소, 및 호스트(A)의 맥 주소와 아이피 주소를 포함한다. ARP응답 패킷을 수신한 호스트(A)는 자신의 ARP테이블에 호스트(C)의 맥 주소를 할당한다.

[0006] 그러나, 이러한 ARP프로토콜은 ARP 응답 패킷을 보내는 호스트에 대한 인증 절차가 없어서, 외부의 공격자가 자신의 맥 주소 및 호스트(C)와 동일한 아이피 주소를 포함한 ARP응답 패킷을 호스트(A)에 전송한 경우, 호스트(A)는 자신의 ARP테이블에 공격자의 맥 주소 및 호스트(C)의 아이피 주소를 대응시켜 저장하고, 결국 공격자에게 패킷을 전송하게 되는 문제가 발생한다.

[0007] 이를 해결하기 위한 종래의 ARP스푸핑을 감지하는 장치는 모든 의심이 드는 장치에 악성코드를 포함한 실행파일이 존재하는지 확인해야 하였고, 해당 실행파일을 삭제하거나 프로세스의 실행을 중지시킴으로써 ARP공격을 중단시킬 수 있었다.

[0008] 이와 관련하여, 대한민국 공개특허공보 제10-2007-0081116호(발명의 명칭: 에이알피 스푸핑 자동 차단 장치 및 방법)에는 종래의 ARP스푸핑 방지 장치 및 방법에 대하여 기술되어있다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 서버로부터 인가된(허가된) 호스트에 대한 주소 정보를 수집해 ARP테이블에 주소 정보를 고정시킴으로써, 인가된 호스트에 대한 ARP스푸핑 공격을 감지하는 단말을 제안한다.

[0010] 또한, 본 발명은 이러한 ARP스푸핑 공격을 감지하는 단말을 이용하여 ARP스푸핑 공격을 감지하는 방법을 제안한다.

과제의 해결 수단

[0011] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 ARP스푸핑 감지단말은, 서버로부터 인가된 호스트의 ARP정보를 수신하고, ARP정보로부터 맥 주소 및 아이피 주소를 수집하는 주소수집부; 하나 이상의 AP에 대한 맥 주소 및 아이피 주소가 할당된 ARP테이블이 저장된 저장부; ARP테이블에 인가된 호스트의 맥 주소 및 아이피 주소를 정적 할당하는 주소할당부; 및 인가된 호스트와 동일한 아이피 주소에 대하여 ARP응답 패킷을 수신한 경우, ARP스푸핑 공격으로 감지하는 감지부를 포함한다.

[0012] 또한, 본 발명의 제 2 측면에 따른 ARP스푸핑 감지방법은, 서버로부터 인가된 호스트에 대한 ARP정보를 수신하고, ARP정보로부터 맥 주소 및 아이피 주소를 수집하는 단계; 인가된 호스트의 맥 주소 및 아이피 주소를 ARP테이블에 정적 할당하는 단계; 및 인가된 호스트와 동일한 아이피 주소에 대하여 ARP응답 패킷을 수신한 경우, ARP스푸핑 공격으로 감지하는 단계를 포함한다.

발명의 효과

[0013] 전술한 본 발명의 과제 해결 수단에 의한 ARP스푸핑 감지단말 및 감지방법은, 인가된 호스트에 대한 주소 정보를 ARP테이블에 고정시키고 해당 주소 정보에 대하여 동일한 아이피 주소를 갖고 상이한 맥 주소를 갖는 ARP응답을 수신하면 ARP스푸핑이 감지되도록 한다.

도면의 간단한 설명

[0014] 도 1은 통상적인 ARP프로토콜을 이용하는 프로세스의 도면이다.

도 2는 본 발명의 일 실시예에 따른 ARP스푸핑 감지단말의 블록도이다.

도 3은 ARP스푸핑 감지단말이 다른 호스트의 주소 정보를 할당하고, 공격자의 ARP스푸핑 공격을 감지하는 과정에 대한 도면이다.

도 4는 본 발명의 일 실시예에 따른 ARP스푸핑을 감지하는 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0016] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다.

[0017] 본원 명세서 전체에서, 어떤 부재가 다른 부재 "상에" 위치하고 있다고 할 때, 이는 어떤 부재가 다른 부재에 접해 있는 경우뿐 아니라 두 부재 사이에 또 다른 부재가 존재하는 경우도 포함한다.

[0018] 본원 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함" 한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다. 본원 명세서 전체에서 사용되는 정도의 용어 "~(하는) 단계" 또는 "~의 단계"는 "~ 를 위한 단계"를 의미하지 않는다.

[0019] 본원 명세서 전체에서 "호스트"는, 인터넷 네트워크에 접속되어 다른 인터넷 호스트와 통신할 수 있는 컴퓨터 또는 단말을 의미한다. 호스트는 패킷을 전송할 수 있고 수신할 수 있으며, 서버, 클라이언트, 및 네트워크와 클라언트 간의 중계설비(Access point, AP)를 포함할 수 있다. 각 호스트는 인터넷 주소에 의해 식별되고, 인터넷 상에서 한 호스트에서 다른 호스트로 데이터를 보내는 데에 쓰이는 주소로서 아이피(IP) 주소 및 이더넷의 물리적인 주소로서 맥(MAC) 주소를 가지고 있다.

[0020] 네트워크는 근거리 통신망(Local Area Network; LAN), 광역 통신망(Wide Area Network; WAN) 또는 부가가치 통신망(Value Added Network; VAN) 등과 같은 유선 네트워크나 이동 통신망(mobile radio communication network) 또는 위성 통신망 등과 같은 모든 종류의 무선 네트워크로 구현될 수 있다.

[0021] 도 2는 본 발명의 일 실시예에 따른 ARP스푸핑 감지단말의 블록도이고, 도 3은 이러한 ARP스푸핑 감지단말이 다른 호스트의 주소 정보를 할당하는 과정을 도시한다.

[0022] 도 2에 따르면, ARP스푸핑 감지단말(100)은 주소수집부(110), 저장부(120), 주소할당부(130), 및 감지부(140)를 포함한다.

[0023] ARP스푸핑 감지단말(100)은 서버로부터 수신한 인가된 다른 호스트의 아이피 주소 및 맥 주소를 미리 저장하여, 동일한 아이피 주소를 갖고 상이한 맥 주소를 갖는 ARP응답 패킷을 수신한 경우 ARP스푸핑으로 감지하는 호스트이다. 이러한 ARP스푸핑 감지단말(100)은 네트워크를 통해 다른 호스트에 접속할 수 있는 컴퓨터나 휴대용 단말기로 구현될 수 있는데, 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop), 태블릿 PC, 슬레이트 PC 등을 포함하고, 휴대용 단말기는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), WiBro(Wireless Broadband Internet) 단말, 스마트 폰(Smart Phone), 스마트패드(Smart Pad) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.

[0024] 우선, 주소수집부(110)는 서버로부터 인가된(또는, 허가된) 호스트(예를 들어, AP)의 ARP정보를 수신한다. 그리고 수신한 ARP정보로부터 인가된 호스트의 맥주소 및 아이피 주소를 수집한다.

[0025] 이때, 본 발명의 일 실시예에 따르면 인가된 호스트는 복수개 일 수 있다.

[0026] 저장부(120)는 각 호스트의 맥 주소 및 아이피 주소가 할당된 ARP테이블을 저장하고 있다. 각 호스트의 맥 주소 또는 아이피 주소는 정적 할당(STATIC)될 수 있고, 동적 할당(DYNAMIC)될 수도 있다.

[0027] 이때, 저장부(120)는 캐쉬, ROM(Read Only Memory), PROM(Programmable ROM), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM) 및 플래쉬 메모리(Flash memory)와 같은 비휘발성 메모리 소자 또는 RAM(Random Access Memory)과 같은 휘발성 메모리 소자 또는 하드디스크 드라이브(HDD, Hard Disk Drive), CD-ROM과 같은 저장 매체 중 적어도 하나로 구현될 수 있으나 이에 한정되지는 않는다.

[0028] 이어서, 주소할당부(130)는 저장부(120)에 저장된 ARP테이블에 각 호스트의 맥 주소 또는 아이피 주소를 할당한다.

[0029] 주소할당부(130)는 서버로부터 인가된 호스트의 맥 주소 및 아이피 주소를 수집한 경우, 아이피 주소 및 맥 주소를 ARP테이블에 정적 할당한다. 예를 들어, ARP테이블에 정적(STATIC) 할당하는 방법으로써, arp-s "IP Address" "MAC Address"와 같은 명령을 이용할 수 있다. 해당 호스트의 주소에 대하여 공격자로부터 스푸핑 공격이 발생한 경우 이를 감지하기 위함이다.

[0030] 한편 본 발명의 다른 실시예에 따르면, 주소할당부(130)는 인가되지 않은 호스트의 맥 주소 및 아이피 주소를 ARP테이블에서 동적 할당으로 관리한다. 즉, 정적 할당되는 것과 달리, 새로 수집한 맥 주소에 의해서 자유롭게 바뀔 수 있음을 의미한다.

[0031] 감지부(140)는 인가된 호스트와 동일한 아이피 주소에 대하여 ARP응답을 수신한 경우, ARP스푸핑 공격으로 감지한다. 또한 본 발명의 일 실시예에 따르면 감지부(140)는 ARP스푸핑을 감지한 경우 ARP응답을 전송한 공격자의 맥 주소를 서버로 전송한다. 더욱 상세한 감지부(130)에 대한 설명은 ARP스푸핑 공격을 감지하는 방법과 관련하여 후술한다.

[0032] 도 3은 ARP스푸핑 감지단말이 다른 호스트의 주소 정보를 할당하고, 공격자의 ARP스푸핑 공격을 감지하는 과정에 대한 도면이다.

[0033] 상술한 바와 같이, ARP스푸핑 감지단말은 미리 서버로부터 인가된 AP(호스트)의 주소정보를 수집한다. 따라서, ARP스푸핑 감지단말의 ARP테이블에는 인가된 AP의 아이피 주소(192.168.0.1) 및 맥 주소(01-01-01-01-01-01)가 정적 할당(STATIC) 되어있다. 그러나, 인가되지 않은 AP의 아이피 주소및 맥 주소는 동적 할당(DYNAMIC)으로 관리 된다.

[0034] 주소 정보가 동적 할당으로 관리되는 인가되지 않은 AP의 경우, 인가된 AP와 달리 통신이 필요하지 않은 경우 주소 정보가 저장되지 않는다. 따라서 새롭게 인가되지 않은 AP와의 통신이 필요하면 ARP요청 패킷을 브로드캐스트한다. 인가되지 않은 AP로부터 ARP응답 패킷을 수신한 ARP스푸핑 감지단말은 해당 아이피 주소(192.168.0.2) 및 맥 주소(02-02-02-02-02-02)를 ARP테이블에 동적 할당하고, 해당 맥 주소를 이용하여 인가되

지 않은 AP와 통신한다.

[0035] 그러나 주소 정보가 정적 할당으로 관리되는 인가된 AP의 경우, 인가되지 않은 AP와 달리 통신이 필요하지 않은 경우에도 주소 정보를 저장하고 있으므로, ARP요청 패킷을 브로드캐스트할 필요가 없다.

[0036] 이때, ARP스푸핑 공격자가 인가된 AP와 동일한 아이피 주소(192.168.0.1) 및 상이한 맥 주소(05-05-05-05-05-05)를 갖는 ARP응답 패킷을 지속적으로 ARP스푸핑 감지단말에 전송하는 경우, ARP스푸핑 감지단말은 ARP스푸핑 공격을 감지하고, 더 나아가 공격자의 아이피 주소 및 맥 주소를 서버에 전송할 수 있다.

[0037] 도 4는 본 발명의 일 실시예에 따른 ARP스푸핑을 감지하는 방법의 순서도이다.

[0038] 먼저, ARP스푸핑 감지단말은 인가된 호스트에 대한 정보를 서버로부터 수신하고, 이 정보로부터 인가된 호스트의 맥 주소 및 아이피 주소를 수집한다(S510).

[0039] 이어서, ARP스푸핑 감지단말은 인가된 호스트의 맥 주소 및 아이피 주소를 ARP테이블에 정적 할당한다(S520). 그러나, 인가된 호스트 외의 다른 호스트에 대하여는 맥 주소 및 아이피 주소를 동적 할당으로 관리한다. 즉, 종래와 같이 ARP응답 패킷을 인가되지 않은 호스트로부터 수신한 경우, 해당 ARP응답 패킷에 포함된 주소 정보를 ARP테이블에 할당한다.

[0040] 이를 전제로 하여, 종래와 같이 ARP프로토콜을 동작시키다가, 정적 할당된 인가된 호스트의 아이피 주소 및 맥 주소와 동일한 아이피 주소 및 상이한 맥 주소를 포함한 ARP응답을 수신한 경우, 이를 ARP스푸핑 공격으로 감지한다(S530, S540). 그러나 주소가 동적 할당된 호스트의 아이피 주소 및 맥 주소에 대한 ARP응답을 수신한 경우(S530)에는 종래와 같이 ARP응답 패킷에 포함된 주소 정보로 ARP테이블을 변경한다.

[0041] 이때, ARP스푸핑 공격을 감지한 경우 ARP스푸핑 감지단말은 ARP응답 패킷을 전송한 공격자의 맥 주소를 서버로 전송함으로서 ARP스푸핑 공격에 대해 대응한다.

[0042] 이와 같이 ARP스푸핑 감지단말 및 감지방법은, 유무선 네트워크 서브넷 내에 별도의 관리시스템의 요구나 기존의 표준 ARP프로토콜의 변경 없이 사용자 단말에서 안전한 ARP테이블을 관리하고 스푸핑 공격에 의한 정보 유출을 방지할 수 있게 한다.

[0043] 참고로, 본 발명의 실시예에 따른 도 2에 도시된 구성 요소들은 소프트웨어 또는 FPGA(Field Programmable Gate Array) 또는 ASIC(Application Specific Integrated Circuit)와 같은 하드웨어 구성 요소를 의미하며, 소정의 역할들을 수행한다.

[0044] 그렇지만 '구성 요소들'은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 각 구성 요소는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.

[0045] 따라서, 일 예로서 구성 요소는 소프트웨어 구성 요소들, 객체지향 소프트웨어 구성 요소들, 클래스 구성 요소들 및 태스크 구성 요소들과 같은 구성 요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다.

[0046] 구성 요소들과 해당 구성 요소들 안에서 제공되는 기능은 더 작은 수의 구성 요소들로 결합되거나 추가적인 구성 요소들로 더 분리될 수 있다.

[0047] 한편, 도 2 에서 도시된 각각의 구성요소는 일종의 '모듈'로 구성될 수 있다. 상기 '모듈'은 소프트웨어 또는 Field Programmable Gate Array(FPGA) 또는 주문형 반도체(ASIC, Application Specific Integrated Circuit)과 같은 하드웨어 구성요소를 의미하며, 모듈은 어떤 역할들을 수행한다. 그렇지만 모듈은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. 모듈은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 실행시키도록 구성될 수도 있다. 구성요소들과 모듈들에서 제공되는 기능은 더 작은 수의 구성요소들 및 모듈들로 결합되거나 추가적인 구성요소들과 모듈들로 더 분리될 수 있다.

[0048] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령

어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0049] 상술한 본 발명에 따른 ARP스푸핑 감지방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체로는 컴퓨터 시스템에 의하여 해독될 수 있는 데이터가 저장된 모든 종류의 기록 매체를 포함한다. 예를 들어, ROM(Read Only Memory), RAM(Random Access Memory), 자기 테이프, 자기 디스크, 플래쉬 메모리, 광 데이터 저장장치 등이 있을 수 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 통신망으로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

[0050] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0051] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0052] 100: ARP스푸핑 감지단말

110: 주소수집부

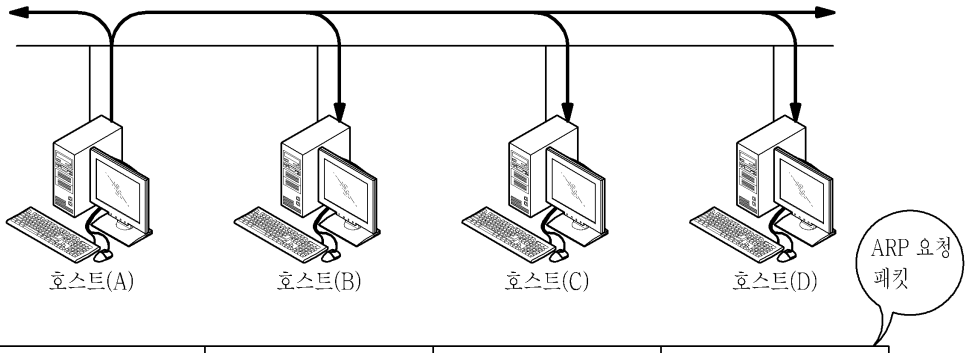
120: 저장부

130: 주소할당부

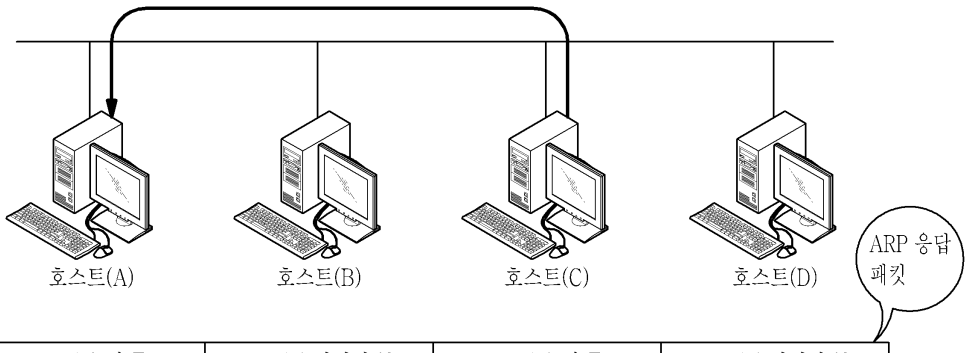
140: 감지부

도면

도면1

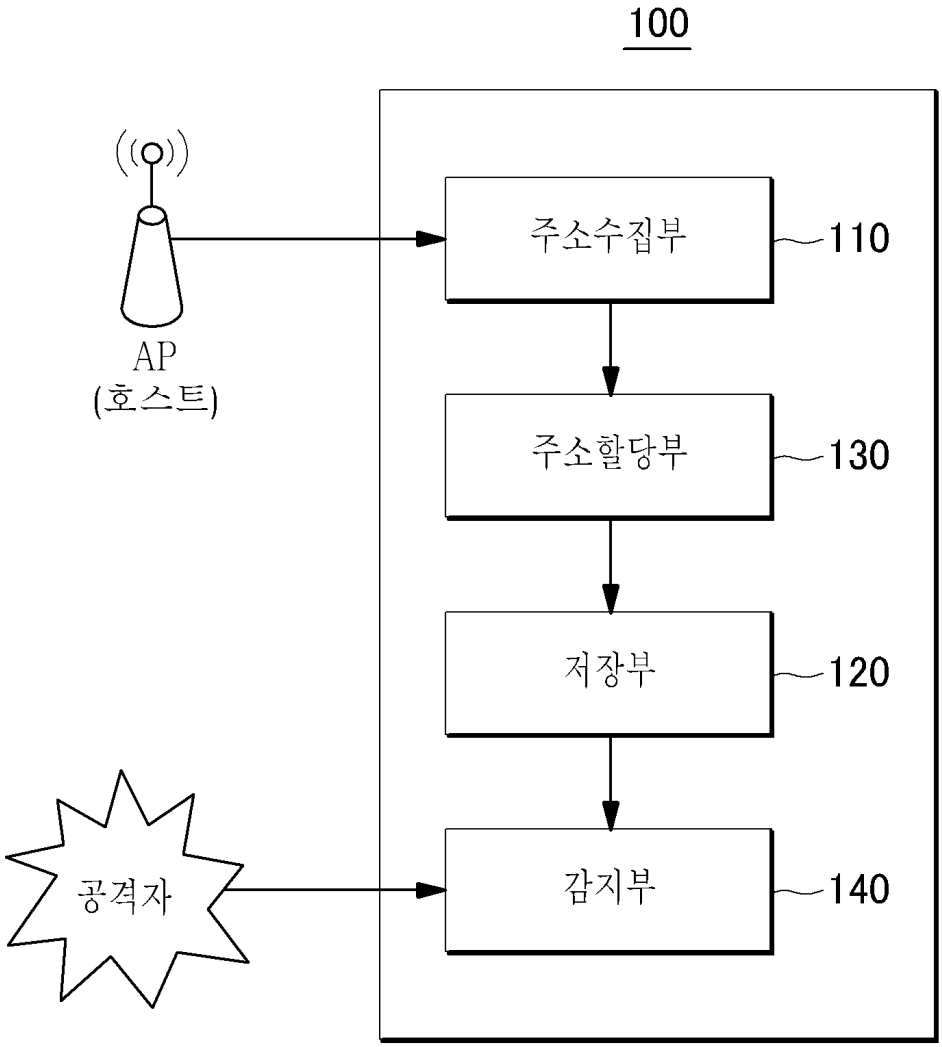


호스트(A) 맥 주소	호스트(A) 아이피 주소	호스트(C) 맥 주소	호스트(C) 아이피 주소
08-10-74-07-47-DA	10.0.0.1	FF-FF-FF-FF-FF-FF	10.0.0.2

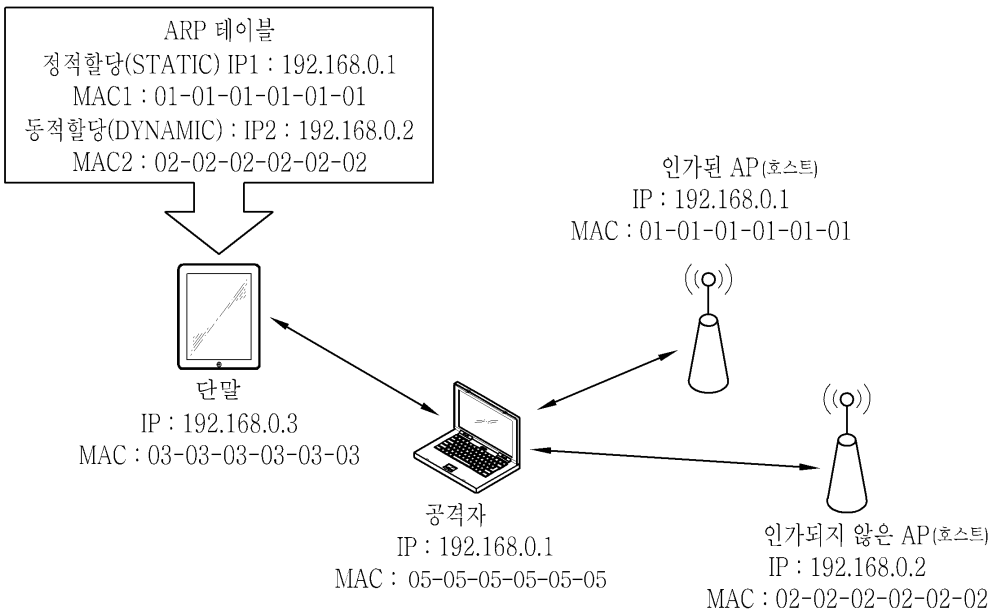


호스트(C) 맥 주소	호스트(C) 아이피 주소	호스트(A) 맥 주소	호스트(A) 아이피 주소
02-00-54-55-4E-01	10.0.0.2	08-10-74-07-47-DA	10.0.0.1

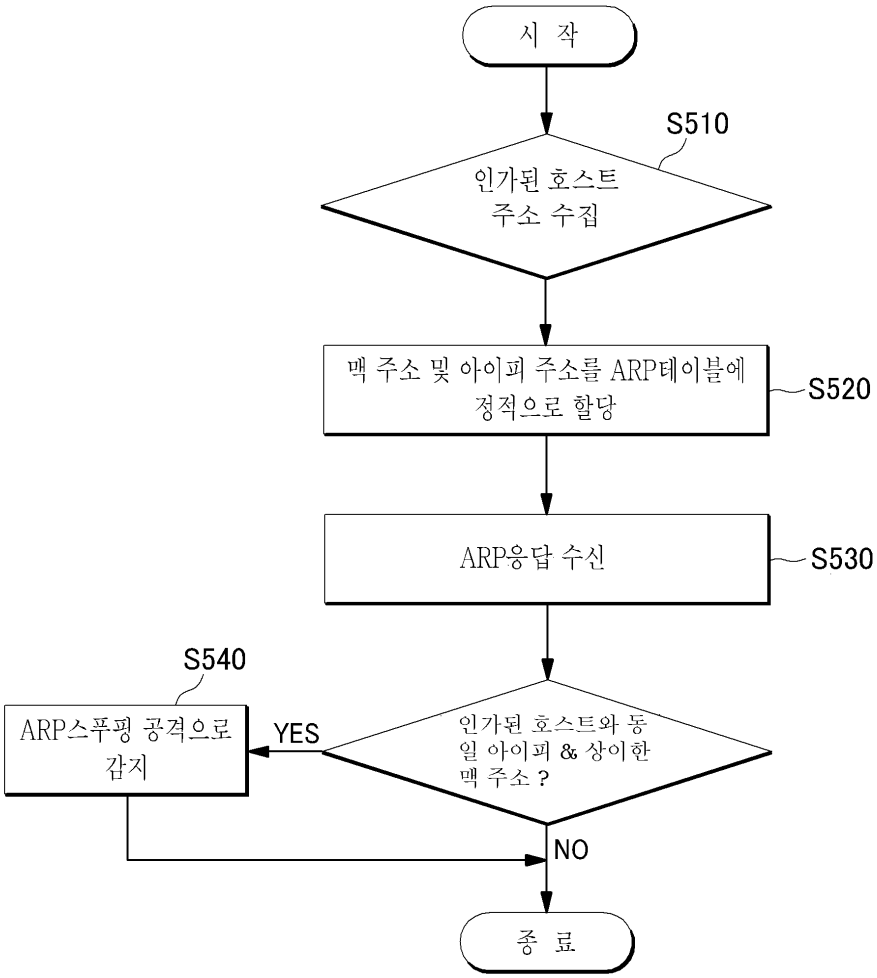
도면2



도면3


ARP 테이블
정적할당(STATIC) IP1 : 192.168.0.1
MAC1 : 01-01-01-01-01-01
동적할당(DYNAMIC) : IP2 : 192.168.0.2
MAC2 : 02-02-02-02-02-02
인가된 AP(호스트)
IP : 192.168.0.1
MAC : 01-01-01-01-01-01
단말
IP : 192.168.0.3
MAC : 03-03-03-03-03-03
공격자
IP : 192.168.0.1
MAC : 05-05-05-05-05-05
인가되지 않은 AP(호스트)
IP : 192.168.0.2
MAC : 02-02-02-02-02-02

도면4


시 작
S510
인가된 호스트 주소 수집
맥 주소 및 아이피 주소를 ARP테이블에 정적으로 할당
S520
ARP응답 수신
S530
S540
ARP스푸핑 공격으로 감지
YES
인가된 호스트와 동일 아이피 & 상이한 맥 주소 ?
NO
종 료