(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 11 월 15 일 (15.11.2012)

WIPO | PCT

(10) 국제공개번호
WO 2012/153913 A1

(51) 국제특허분류:
H04L 12/22 (2006.01) *H04L 12/56* (2006.01)

(21) 국제출원번호: PCT/KR2012/001714

(22) 국제출원일: 2012 년 3 월 8 일 (08.03.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0044667 2011 년 5 월 12 일 (12.05.2011) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **주식회사 이스트소프트 (ESTSOFT CORP.)** [KR/KR]; 서울시 서초구 반포대로 3 (서초동. 이스트빌딩), 137-070 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **김준섭 (KIM, Jun Seob)** [KR/KR]; 서울시 강동구 상일동 173 번지 삼성빌라 3 동 305 호, 134-090 Seoul (KR). **정우영 (JUNG, Woo Young)** [KR/KR]; 서울시 동작구 사당동 1140 삼성아파트 101 동 208 호, 156-090 Seoul (KR).

(74) 대리인: **박기원 (PARK, Ki-won)**; 경기도 안양시 동안구 관양동 1597-1 한솔 3 차 205 호, 431-815 Gyeonggi-do (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

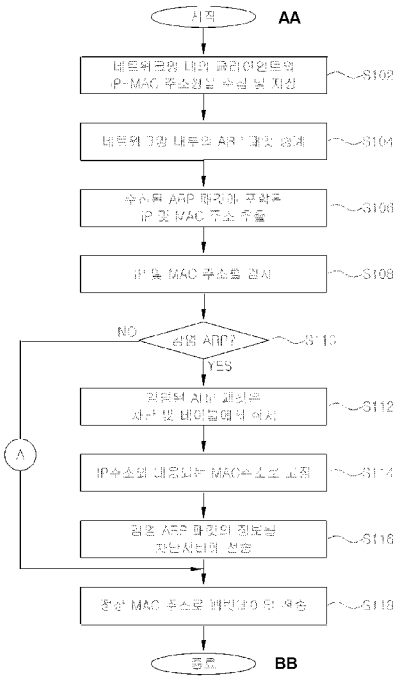
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) **Title**: METHOD OF DEFENDING AGAINST A SPOOFING ATTACK BY USING A BLOCKING SERVER

(54) **발명의 명칭** : 차단서버를 이용한 스푸핑 공격 방어방법

[Fig. 4]



S102 ... Collect and store an IP-MAC address pair for a client in a network
S104 ... Relay an ARP packet in a network
S106 ... Extract an IP and MAC address included in the received ARP packet
S108 ... Inspect the IP and MAC address
S110 ... Infected ARP?
S112 ... Block the infected ARP packet and delete from a table
S114 ... Fix as a MAC address corresponding to the IP address
S116 ... Transmit information on the infected ARP packet to a blocking server
S118 ... Transmit packet data using a legitimate MAC address
AA ... Start
BB ... End

(57) **Abstract**: The present invention relates to a method of defending against a spoofing attack using a blocking server, and more particularly, to a method of defending against a spoofing attack using a blocking server, which is characterized in that it involves inspecting an IP and MAC address included in an ARP packet received by a client in a network,

[다음 쪽 계속]

WO 2012/153913 A1

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

— 청구범위 보정서 및 설명서와 함께 (조약 제 19 조(1))

and changing the addresses to a legitimate IP address and to a corresponding MAC address when the addresses are found to be used in a spoofing attack. According to the present invention, in the blocking of a spoofing attack against a network, an IP address and a MAC address for legitimate hardware connected to the network may be prestored and monitored, so as to exhibit the effect of an accurate defense being enabled in a short time.

(57) 요약서: 본 발명은 차단서버를 이용한 스푸핑 공격 방어방법에 관한 것으로서, 보다 상세하게는 네트워크망 내부의 클라이언트에 수신되는 ARP 패킷에 포함된 IP 및 MAC 주소를 검사하여 스푸핑 공격에 이용되는 것으로 확인되면 정상적인 IP 주소와 대응되는 MAC 주소로 변경하는 것을 특징으로 하는 차단서버를 이용한 스푸핑 공격 방어방법에 관한 것이다. 본 발명에 따르면 네트워크망에 대한 스푸핑 공격을 차단함에 있어서 네트워크망에 연결된 정상 하드웨어에 대한 IP 주소 및 MAC 주소를 미리 저장하여 감시할 수 있으므로, 빠른 시간안에 정확한 방어가 가능해지는 효과가 있다.

명세서

발명의 명칭: 차단서버를 이용한 스푸핑 공격 방어방법

기술분야

[1] 본 발명은 차단서버를 이용한 스푸핑 공격 방어방법에 관한 것으로서, 보다 상세하게는 네트워크망 내부의 클라이언트에 수신되는 ARP 패킷에 포함된 IP 및 MAC 주소를 검사하여 스푸핑 공격에 이용되는 것으로 확인되면 정상적인 IP 주소와 대응되는 MAC 주소로 변경하는 것을 특징으로 하는 차단서버를 이용한 스푸핑 공격 방어방법에 관한 것이다.

배경기술

[2] 인터넷의 사용이 날로 증가함에 따라 해킹의 기술 또한 증가하고 있으며, 현재에 이르러서는 해킹 프로그램 등이 네트워크 상에 산재하는 상황에까지 이르게 됨으로써 이제 전문가가 아닌 일반인도 해커가 될 수 있는 상황에 이르렀다.

[3] 이와 같이, DoS, DDoS, Sniffing 또는 Hijacking 과 같은 해킹을 위해 사용되는 근본적인 수단이 ARP 또는 IP 스푸핑(Spoofing)이다. 이 중 ARP(Address Resolution Protocol) 스푸핑은 발신자(Sender) 하드웨어 주소와 발신자 IP 주소를 조작하는 것으로서, 로컬 네트워크에서 다른 시스템의 IP 주소에 대해서 공격 시스템의 MAC 주소를 ARP Reply 패킷의 소스 정보로 사용하여 로컬 네트워크 내의 다른 라우터나 스위치, 호스트들의 ARP 테이블을 변경함으로써, 공격 시스템의 IP 주소가 아닌 패킷을 공격 시스템의 MAC 주소를 달고 공격 시스템으로 전달되게 만드는 공격 기법이다.

[4] 또한, IP 스푸핑은 자신의 소스 IP를 변경하여 다른 시스템에게 자신이 누군지 모르게 또는 다른 시스템으로 오인하도록 만드는 공격을 위한 수단으로 사용된다.

[5] 현재, ARP나 IP 스푸핑 공격으로 인한 피해는 해킹 피해의 대부분을 차지한다고 볼 수 있으며, 누구나 인터넷에서 돌아다니는 스푸핑 툴을 이용하여 특정 호스트를 공격하거나 망 내에서 돌아다니는 정보를 훔쳐 봄으로써 보안이 유지되어야 할 개인 정보들이 쉽게 도용되는 일이 빈번한 실정이다.

[6] 예를 들면, ARP 스푸핑을 통하여 동일한 내부 네트워크에 연결된 다른 호스트에서 행하여지는 여러 가지 IP 패킷들을 훔쳐 봄으로써 개인 정보가 유출될 수 있고, 심지어 금융정보까지도 노출되는 위험이 있으며, 특정 서버의 관리자 레벨의 ID와 패스워드를 훔쳐 봄으로써 서버 정보를 마음대로 조작하는 것이 가능한 게 현실이다. 더 나아가, IP 스푸핑을 하여 외부 네트워크 상에서 행하여지는 온라인 작업을 훔쳐 볼 경우 더 많은 시스템이 공격에 쉽게 노출되게 된다.

[7] 이러한 스푸핑을 방지하기 위하여 현재 사용되고 있는 기법으로는, 필터링

기능이 있는 라우터를 사용하여 외부망으로부터 들어오는 IP 패킷에 대해서 각각의 포트에 연결된 호스트들에 대한 개별적인 IP 주소를 이용하지 않고 로컬 네트워크에 할당된 IP 네트워크 주소와 마스크를 이용하여 필터링하는 방법이 있다. 그러나, 상기 방법은, 필터링에 각 호스트의 개별적인 IP 주소가 아니라 로컬 네트워크 주소를 사용함으로 인해 공격자가 임의의 로컬 네트워크의 다른 주소를 이용한 스푸핑을 할 경우 이를 잡아내지 못할 뿐만 아니라, ARP 스푸핑에 대해서는 전혀 대처하지 못하는 문제점이 있었다.

발명의 상세한 설명

기술적 과제

[8] 전술한 문제점을 해결하기 위한 본 발명은 각 클라이언트 PC가 차단서버로부터 얻은 네트워크망 내 모든 클라이언트 PC의 유효한 IP-MAC 주소정보를 담고 있는 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록을 이용해 ARP 테이블과 ARP 패킷을 검사함으로써 ARP 스푸핑 공격에 실시간으로 또는 사후에 대응할 수 있도록 하는 차단서버를 이용한 스푸핑 공격 방어방법을 제공하는 것을 목적으로 한다.

[9] 또한 본 발명은 허용 IP-MAC 주소 목록과 차단 IP-MAC 주소 목록을 차단서버 또는 각 클라이언트에 저장하여 차단서버나 클라이언트가 독자적으로 스푸핑 공격을 감시 및 차단할 수 있도록 하는 차단서버를 이용한 스푸핑 공격 방어방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

[10] 전술한 문제점을 해결하기 위해 안출된 본 발명은 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서, 차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와; 상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 허용주소DB(108-3)에 저장하는 제2단계와; 상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 차단주소DB(108-4)에 저장하는 제3단계와; 상기 클라이언트(106)에 ARP 패킷이 유입되면, 상기 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 상기 차단서버(108)로 전송하면서 스푸핑 공격 여부에 대한 검사를 요청하는 제4단계와; 차단서버(108)의 주소검사부(108-2)의 검사 결과, 상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단주소DB(108-4)에 저장된 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 패킷이 감염 ARP 패킷이라는

것을 상기 차단서버(108)가 상기 클라이언트(106)에 통보하는 제5단계와; 상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송수신을 차단하는 제6단계;를 포함한다.

[11] 상기 제5단계는 상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함되어 있지 않은 경우, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 없거나, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 맵핑되어 주소쌍으로 저장되어 있는 허용 IP-MAC 주소의 구성과 다르다면 상기 ARP 패킷을 의심 ARP 패킷으로 정의하는 제5-1단계와; 상기 주소검사부(108-2)가 단위시간 동안 상기 클라이언트(106)에 유입된 ARP 패킷 중에서 상기 의심 ARP 패킷에 포함된 송신자의 MAC 주소와 동일한 송신자 MAC 주소를 가지는 ARP 패킷의 전송 개수를 누적하는 제5-2단계와; 일정한 시간 동안 누적된 전송 개수가 임계치를 넘는 경우, 상기 의심 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5-3단계;를 추가로 포함한다.

[12] 다른 실시예에 따른 본 발명은 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서, 차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와; 상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 허용주소DB(108-3)에 저장하는 제2단계와; 상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 차단주소DB(108-4)에 저장하는 제3단계와; 상기 클라이언트(106)의 ARP 테이블보호부(106-1b)가 상기 클라이언트(106)의 ARP 테이블에 포함된 ARP 엔트리의 IP 주소와 MAC 주소를 추출하여 상기 차단서버(108)로 전송하면서 스푸핑 공격 여부에 대한 검사를 요청하는 제4단계와; 차단서버(108)의 주소검사부(108-2)의 검사 결과, 상기 제4단계에서 추출된 MAC 주소가 상기 차단주소DB(108-4)에 저장된 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 엔트리가 감염 ARP 엔트리라는 것을 상기 차단서버(108)가 상기 클라이언트(106)에 통보하는 제5단계와; 상기 ARP 테이블보호부(106-1b)가 상기 감염 ARP 엔트리에 포함된 IP 주소를 추출하고, 상기 추출된 IP 주소와 대응하여 저장된 정상 MAC 주소를 상기 허용 IP-MAC 주소 목록에서 조회하는 제6단계와; 상기 ARP 테이블보호부(106-1b)가 상기 감염 ARP 엔트리의 MAC 주소를 상기 조회된 정상 MAC 주소로 변경시키는 제7단계;를 포함한다.

[13] 또 다른 실시예에 따른 본 발명은 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이

이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서, 차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와; 상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 상기 클라이언트(106)의 허용주소DB(106-1d)에 저장하는 제2단계와; 상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 상기 클라이언트(106)의 차단주소DB(106-1e)에 저장하는 제3단계와; 상기 클라이언트(106)에 ARP 패킷이 유입되면, 상기 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 스푸핑 공격 여부를 검사하는 제4단계와; 상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 패킷처리부(106-1c)가 상기 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5단계와; 상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송수신을 차단하는 제6단계;를 포함한다.

[14] 상기 제5단계는 상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함되어 있지 않은 경우, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 없거나, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 맵핑되어 주소쌍으로 저장되어 있는 허용 IP-MAC 주소의 구성과 다르다면 상기 ARP 패킷을 의심 ARP 패킷으로 정의하는 제5-1단계와; 상기 ARP 패킷처리부(106-1c)가 단위시간 동안 상기 클라이언트(106)에 유입된 ARP 패킷 중에서 상기 의심 ARP 패킷에 포함된 송신자의 MAC 주소와 동일한 송신자 MAC 주소를 가지는 ARP 패킷의 전송 개수를 누적하는 제5-2단계와; 일정한 시간 동안 누적된 전송 개수가 임계치를 넘는 경우, 상기 의심 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5-3단계;를 추가로 포함한다.

[15] 또 다른 실시예에 따른 본 발명은 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서, 차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와; 상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 상기 클라이언트(106)의 허용주소DB(106-1d)에 저장하는 제2단계와; 상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에

대한 정보인 차단 MAC 주소 목록을 상기 클라이언트(106)의 차단주소DB(106-1e)에 저장하는 제3단계와; 상기 클라이언트(106)의 ARP 테이블보호부(106-1b)가 상기 클라이언트(106)의 ARP 테이블에 포함된 ARP 엔트리의 IP 주소와 MAC 주소를 추출하여 스푸핑 공격 여부를 검사하는 제4단계와; 상기 제4단계에서 추출된 MAC 주소가 상기 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 테이블보호부(106-1b)가 상기 ARP 엔트리를 감염 ARP 엔트리로 분류하는 제5단계와; 상기 ARP 테이블보호부(106-1b)가 상기 감염 ARP 엔트리에 포함된 IP 주소를 추출하고, 상기 추출된 IP 주소와 대응하여 저장된 정상 MAC 주소를 상기 허용 IP-MAC 주소 목록에서 조회하는 제6단계와; 상기 ARP 테이블보호부(106-1b)가 상기 감염 ARP 엔트리의 MAC 주소를 상기 조회된 정상 MAC 주소로 변경시키는 제7단계;를 포함한다.

[16] 또 다른 실시예에 따른 본 발명은 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서, 특정 클라이언트(106)에 설치되어 있는 장치들의 IP 주소와 MAC 주소를 수집하는 제1단계와; 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 로컬 IP-MAC 주소 목록을 상기 클라이언트(106)의 허용주소DB(106-1d)에 저장하는 제2단계와; 상기 특정 클라이언트(106)로부터 ARP 패킷이 송신될 때, 상기 특정 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 송신되는 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 스푸핑 공격 여부를 검사하는 제2단계와; 제2단계에서 추출된 송신자의 IP 주소가 상기 로컬 IP-MAC 주소 목록에 포함되어 있지 않거나, 추출된 송신자의 IP 주소와 동일한 IP 주소에 대응하여 저장된 MAC 주소가 상기 송신되는 ARP 패킷에 포함된 송신자의 MAC 주소와 다른 경우, 상기 ARP 패킷처리부(106-1c)가 상기 송신되는 ARP 패킷을 감염 ARP 패킷으로 분류하는 제3단계와; 상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송신을 차단하는 제4단계;를 포함한다.

발명의 효과

[17] 본 발명에 따르면 네트워크망에 대한 스푸핑 공격을 차단함에 있어서 네트워크망에 연결된 정상 하드웨어에 대한 IP 주소 및 MAC 주소를 미리 저장하여 감시할 수 있으므로, 빠른 시간 안에 정확한 방어가 가능해지는 효과가 있다.

[18] 또한 차단서버뿐만 아니라 각각의 클라이언트에도 허용 주소 목록과 차단 주소 목록을 저장하고, 각각의 클라이언트가 공격의 감지와 방어를 수행할 수 있으므로, 차단서버의 부하를 줄이고 공격에 대한 대응 시간을 단축시킬 수 있는 효과가 있다.

도면의 간단한 설명

[19] 도 1은 본 발명의 실시예에 따른 차단서버가 포함된 네트워크망의 구성요소를 나타낸 블럭도.

[20] 도 2는 도 1의 차단서버의 구성요소를 나타낸 블럭도.

[21] 도 3은 도 1의 클라이언트의 구성요소를 나타낸 블럭도.

[22] 도 4는 스푸핑 공격을 차단하는 과정을 나타낸 순서도.

[23] 도 5는 스푸핑 공격으로 의심되는 패킷을 감시하는 과정을 나타낸 순서도.

[24]

[25] 102 : 라우터 104 : L2스위치

[26] 106 : 클라이언트 108 : 차단서버

[27] 110 : 관리자단말기

발명의 실시를 위한 형태

[28] 이하에서 도면을 참조하여 본 발명의 실시예에 따른 "차단서버를 이용한 스푸핑 공격 방어방법"(이하, '방어방법'이라 함)을 설명한다.

[29] 도 1은 본 발명의 실시예에 따른 차단서버가 포함된 네트워크망의 구성요소를 나타낸 블럭도이며, 도 2는 도 1의 차단서버의 구성요소를 나타낸 블럭도, 도 3은 도 1의 클라이언트의 구성요소를 나타낸 블럭도이다.

[30] 본 발명의 실시예에 따른 스푸핑 공격 방어방법은 네트워크망에 포함된 L2스위치(104)의 하단에 연결된 클라이언트(106)와, 각각의 클라이언트(106)와 연결된 차단서버(108)와, 수동으로 차단 대상을 입력하는 관리자단말기(110)에 의하여 수행된다. 클라이언트(106)는 클라이언트1(106-1)부터 클라이언트N(106-N)까지 N개의 단말기로 구성되는 것으로 설명한다.

[31] 클라이언트1(106-1) 내지 클라이언트N(106-N)은 ARP를 통해 서로 IP 패킷을 주고받게 된다. 이를 위해 ARP 패킷에는 클라이언트1(106-1) 내지 클라이언트N(106-N)의 IP 주소와 맵핑(mapping)된 MAC 주소가 포함된다.

[32] 차단서버(108)는 IP-MAC 주소 목록 수집 절차를 통해 클라이언트(106) 또는 관리자단말기(110)로부터 유효한 IP-MAC 주소 목록을 전달받고, 이를 토대로 허용 IP-MAC 주소 목록을 구성한다. 차단서버(108)는 허용 IP-MAC 주소 목록을 가지고 있다가 L2스위치(104)를 통해 출입하는 ARP 패킷을 검사하여 스푸핑 공격인지를 판단한다.

[33] 차단서버(108)는 허용 IP-MAC 주소 목록을 각각의 클라이언트(106)에 전달하여 저장하도록 하고, 클라이언트(106)가 직접 스푸핑 공격을 감시하도록 할 수도 있다.

[34] 본 발명에서는 클라이언트(106)의 IP 주소와, 이에 대응하는 MAC 주소(각각의 클라이언트에 설치된 어댑터의 MAC 주소)를 결합하여 'IP-MAC 주소'라 한다.

[35] 클라이언트(106)는 ARP 스푸핑 공격 검사 단계에서 ARP 테이블보호부(106-1b)와 ARP 패킷처리부(106-1c)를 통해 ARP 테이블의 감염 여부를 검사하고, 클라이언트(106)를 통해 출입하는 ARP 패킷을 검사한다.

[36] ARP 테이블보호부(106-1b)는 클라이언트(106)에 구성된 ARP 테이블의 모든 ARP 엔트리를 파악한다. ARP 엔트리의 파악은 주기적으로 이루어질 수도 있고, 차단 주소에 대한 정보가 업데이트될때마다 할 수도 있다. ARP 엔트리 중에서 감염 ARP 엔트리가 있는 경우에는 공격 차단 과정이 진행된다.

[37] ARP 패킷처리부(106-1c)는 ARP 패킷이 클라이언트(106)에 들어올때마다 ARP 의 감염 여부를 검사한다.

[38] 검사 과정에서 발견된 감염 ARP 엔트리 혹은 감염 ARP 패킷은 차단서버(108)에 의해 ARP 스푸핑 공격 차단 단계에서 처리되고,(도 4 참조) 의심 ARP 엔트리 혹은 의심 ARP 패킷은 의심 MAC 주소 확인 요청 단계에서 처리된다.(도 5 참조)

[39] 도 4는 스푸핑 공격을 차단하는 과정을 나타낸 순서도이며, 도 5는 스푸핑 공격으로 의심되는 패킷을 감시하는 과정을 나타낸 순서도이다.

[40] 이하에서 도 1 내지 5를 참조하여 본 발명의 실시예에 따른 차단서버(108)의 동작과정을 설명한다.

[41] 차단서버(108)는 네트워크망 내부의 모든 클라이언트(106)의 IP-MAC 주소 목록을 수집하여 저장한다.(S102) 차단서버(108)가 수집하는 대상은 로컬 네트워크를 구성하는 모든 단말기를 포함하는 것으로서, 하나의 라우터(102)의 하부에 연결된 모든 L2스위치(104)와 클라이언트(106)를 의미한다.

[42] 이를 위해 네트워크망에 포함된 클라이언트(106)는 자신의 IP 주소와 모든 어댑터(하드웨어)의 MAC 주소를 수집해 차단서버(108)에 전송한다.

[43] IP-MAC 주소의 수집과 전송은 자동으로(주기적으로) 이루어질 수도 있고, 장비의 교체나 추가와 같은 일정한 이벤트가 발생했을 때, 이루어질 수도 있다.

[44] 클라이언트(106)는 새로운 어댑터를 추가하거나 기존 어댑터를 제거함으로써 어댑터 정보의 변경이 감지되는 경우에 변경된 최근 IP-MAC 주소를 차단서버(108)로 전송한다.

[45] IP-MAC 주소의 수집은 관리자에 의해 수동으로 이루어질 수도 있는데, 네트워크망에 대한 관리자는 네트워크망에 연결된 1대 이상의 개별 클라이언트(106-1 내지 106-N)에 대한 IP-MAC 주소를 수집해 관리자단말기(110)를 통해 차단서버(108)에 수동으로 입력한다.

[46] 클라이언트(106)에 의해 자동으로 수집되거나 관리자에 의해 수동으로 입력된 IP-MAC 주소 정보는 차단서버(108)에 저장된다. 주소수집부(108-1)는 클라이언트(106) 또는 관리자단말기(110)로부터 입력되는 유효한 IP-MAC 주소 목록을 전송받는다.

[47] 차단서버(108)에 저장되는 IP-MAC 주소 정보는 네트워크망에 포함되어 있는 장치(스위치, 클라이언트)들에 대한 유효한 주소 정보이므로, 데이터 패킷의 교환이 허용되는 화이트리스트(white list)가 된다.

[48] 본 발명에서는 왜곡되지 않은 진정한 IP-MAC 주소 목록을 허용 IP-MAC 주소 목록이라고 정의하며, 허용 IP-MAC 주소 목록 중에서 특정 클라이언트(106)에

설치되어 있는 장치들에 대한 주소 정보를 해당하는 클라이언트(106)의 로컬 IP-MAC 주소 목록이라고 지칭한다.

[49] 로컬 IP-MAC 주소 목록은 주로 특정 클라이언트(106)에 의해 자동으로 생성되어 차단서버(108)에 보내진다. 허용 IP-MAC 주소 목록 중에서 로컬 IP-MAC 주소 목록을 제외한 나머지 목록은 관리자가 수동으로 입력하거나, 클라이언트(106)가 공격 감시 과정에서 획득하여 입력하거나, 외부 기관의 보안시스템으로부터 입수하여 저장된다.

[50] 로컬 IP-MAC 주소 목록을 특별히 따로 보관하는 것은 클라이언트(106)에서 나가는 ARP 패킷의 감염 여부를 확인하기 위해서이다. 클라이언트(106) 자신의 모든 장치들에 대한 MAC 주소를 가지고 있는 상황에서 클라이언트(106)가 다른 호스트를 향해서 ARP 패킷을 송신할 때, 송신되는 ARP 패킷에 포함된 송신자의 IP 주소가 로컬 IP-MAC 주소 목록에 포함되어 있지 않거나, 송신자의 IP 주소와 동일한 IP 주소에 대응하여 저장된 MAC 주소가 송신되는 ARP 패킷에 포함된 송신자의 MAC 주소와 다른 경우에는 클라이언트(106) 자신이 이미 스푸핑 공격을 받아서 IP 주소와 MAC 주소의 변경이 이루어져 있는 것으로 볼 수 있다. 이때에는 즉시 ARP 패킷의 송신을 차단하여야 하는데, 이를 위해 로컬 IP-MAC 주소 목록을 따로 관리하는 것이 바람직하다.

[51] 허용 IP-MAC 주소 목록의 IP주소와 MAC 주소 관계는 1:N 관계이다. 즉, 하나의 IP 주소를 갖는 클라이언트(106)에 독립적인 MAC 주소를 갖는 다수의 어댑터가 설치될 수 있으므로, 하나의 IP 주소와 다수의 MAC 주소가 각각의 주소쌍으로 저장될 수 있다.

[52] 차단서버(108)는 허용 IP-MAC 주소 목록을 관리하기 위해 자동으로 클라이언트(106)에 허용 IP-MAC 주소 목록을 요청하여 전송받거나, 관리자가 수동으로 허용 IP-MAC 주소 목록을 입력하면 이를 저장하는 방식을 모두 지원할 수 있다.

[53] 한편, L2스위치(104)를 통해 중계되는 ARP 패킷의 이더넷 헤더에 기록된 출발지(송신자)의 MAC 주소가 스푸핑 공격에 이용되는 것일 경우에는 차단 MAC 주소 목록에 추가함으로써 앞으로의 추가 공격을 막을 수 있다.

[54] 스푸핑 공격을 시도하는 단말기는 네트워크망에 포함된 클라이언트(106) 중의 하나일 것이며, 본 발명에서 지칭하는 차단 MAC 주소 목록은 공격자가 사용하는 클라이언트(106)의 하드웨어 주소를 의미한다. 차단 MAC 주소 목록은 차단서버(108)에 의한 지속적인 감시와 관리자의 입력 등의 방식으로 생성 및 추가가 가능하다.

[55] IP 주소와 이에 대응하는 MAC 주소를 쌍으로 대응시켜 저장하는 허용 IP-MAC 주소 목록과 달리 차단 MAC 주소 목록에는 패킷 전달이 차단되는 MAC 주소만 기재된다. 이것은 공격자가 IP 주소를 임의로 변조하여 ARP 패킷에 포함시키는 경우에도 동일한 MAC 주소를 가진 L2스위치(104)로 데이터가 전송되어 스푸핑 공격이 이루어지므로, 이를 방지하기 위하여 IP 주소에 관계없이 동일한 MAC

주소를 가진 L2스위치(104)로 데이터 패킷이 전해지지 않도록 하기 위한 것이다.

[56] 차단서버(108)는 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록을 각각 허용주소DB(108-3)와 차단주소DB(108-4)에 저장한다. 차단서버(108)는 두 개의 DB(108-3, 108-4)에 저장된 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록을 바탕으로 네트워크망을 출입하는 ARP 패킷의 감염여부를 확인한다.

[57] 그리고 차단서버(108)는 특정 클라이언트(106)가 네트워크망에 연결되는 시점을 통지받는 즉시 해당 클라이언트(106)로 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록을 전송한다.

[58] 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록에 변동이 발생되면 차단서버(108)는 네트워크망에 포함된 모든 클라이언트(106)에게 변동된 허용 IP-MAC 주소 목록과 차단 IP-MAC 주소 목록을 전송한다.

[59] 클라이언트(106)에게 전송된 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록은 클라이언트(106) 내부에 존재하는 허용주소DB(106-1d)와 차단주소DB(106-1e)에 각각 저장된다. 클라이언트(106)에 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록을 전송하여 저장하도록 하는 것은 선택적으로 채택할 수 있는 정책이며, 클라이언트(106)가 이러한 주소 목록을 가지고 있는 경우에는 자신에게 입력되는 ARP 패킷을 스스로 검사하여 스푸핑 공격 여부를 판단할 수 있다. 만약 정책적인 선택에 의해 각각의 클라이언트(106)에는 주소 목록을 전송하지 않는 것으로 설정한다면, ARP 패킷이 입력될 때마다 차단서버(108)가 공격 여부를 판단하게 될 것이다.

[60] ARP 테이블보호부(106-1b)는 새로운 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록이 전송될 때마다 클라이언트(106)의 ARP 테이블에 포함된 ARP 엔트리를 검사하여 감염 여부를 검사한다.

[61]

[62] <u>차단서버에만 허용 주소 목록이 저장된 경우</u>

[63] 먼저, 차단서버(108)만 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록을 가지고 있는 경우의 검사과정을 설명한다.

[64] L2스위치(104)는 네트워크망 내부에서 오고가는 모든 ARP 패킷을 중계(수신 및 송신)한다.(S104)

[65] 클라이언트(106)에 설치된 네트워크 필터 드라이버는 클라이언트(106)를 통해 들어오고 나가는 ARP 패킷을 실시간으로 검사한다. 여기서 ARP 패킷은 ARP 요청(Request)과 ARP 응답(Reply)을 포함한 모든 Operation 타입의 ARP 패킷을 지칭한다.

[66] ARP 패킷을 수신한 클라이언트(106)의 ARP 패킷처리부(106-1c)는 수신된 ARP 패킷에 포함된 출발지(송신자)의 IP 주소와 MAC 주소를 추출하여 차단서버(108)로 전송함으로써 스푸핑 공격 여부에 대한 검사를 요청한다.(S106) 또한 ARP 테이블보호부(106-1b)는 ARP 테이블에 포함된 ARP 엔트리의 출발지의 IP 주소와 MAC 주소를 추출하여 차단서버(108)로 전송한다.

[67] 검사요청은 일정한 시간을 주기로 이루어질 수도 있고, ARP 패킷이 입력될 때마다 또는 허용 또는 차단 주소 목록이 변경될 때마다 이루어질 수도 있다.

[68] 주소검사부(108-2)는 추출된 IP-MAC 주소를 DB(108-3, 108-4)에 저장된 주소 목록과 비교하여 스푸핑 공격 여부를 검사한다.(S108)

[69] 주소검사부(108-2)는 먼저 전송된 ARP 패킷 또는 ARP 엔트리의 출발지의 MAC 주소와 동일한 주소가 차단주소DB(108-4)에 저장되어 있는지를 검사한다.

[70] 공격자가 사용하는 클라이언트(106)로부터 전송된 ARP 패킷 또는 ARP 엔트리의 출발지의 MAC 주소가 차단주소DB(108-4)에 저장된 IP-MAC 주소 목록의 MAC 주소와 동일하다면, 이 ARP 패킷은 변조된 MAC 주소로 패킷 데이터를 가로채려는 스푸핑 공격에 사용되는 것으로 판단할 수 있으며, 이를 감염 ARP 패킷이라고 지칭한다.

[71] 예를 들어 클라이언트1(106-1)이 공격자의 단말기이고, 클라이언트2(106-2)와 클라이언트3(106-3) 사이를 오고가는 패킷을 가로채려고 한다고 가정한다.

[72] 클라이언트1(106-1)은 클라이언트2(106-2)와 클라이언트3(106-3)에 감염 ARP 패킷을 보내서 자신의 MAC 주소를 정상적인 수신자의 주소인 것처럼 속인다. 즉, 클라이언트2(106-2)의 ARP 테이블에서 클라이언트3(106-3)의 MAC 주소를 기록하는 곳에 클라이언트1(106-1)의 MAC 주소가 기재되도록 하며, 클라이언트3(106-3)의 ARP 테이블에서 클라이언트2(106-2)의 MAC 주소를 기록하는 곳에 클라이언트1(106-1)의 MAC 주소가 기재되도록 하는 것이다.

[73] 이렇게 감염이 되면, 클라이언트2(106-2)가 클라이언트3(106-3)에게 보내는 패킷과, 클라이언트3(106-3)이 클라이언트2(106-2)에게 보내는 패킷이 모두 클라이언트1(106-1)에게 전달된다. 클라이언트1(106-1)은 클라이언트2(106-2)와 클라이언트3(106-3)으로부터 입력되는 패킷을 캡처하여 저장한 후 다시 정상적인 목적지로 보내거나, 패킷의 전달을 차단하여 정상적인 통신이 이루어지지 않도록 한다.

[74] 차단서버(108)는 미리 저장한 모든 클라이언트(106)의 IP-MAC 주소쌍과 새로 입력되는 ARP 패킷 또는 ARP 엔트리에 포함된 IP-MAC 주소쌍을 비교하여 정상적인 MAC 주소를 가진 것인지를 판단한다.

[75] 공격자 클라이언트(106)로부터 입력된 감염 ARP 패킷은 차단서버(108)에 의해 수신자의 MAC 주소를 갖는 클라이언트(106)로 전송되지 않도록 차단(드롭)되며, 클라이언트(106)의 ARP 테이블은 정상적인 장치의 MAC 주소로 변경된다.

[76] 전송된 ARP 패킷 또는 ARP 엔트리의 송신자(출발지)의 MAC 주소와 동일한 주소가 차단주소DB(108-4)에 포함되어 있지 않다면, 주소검사부(108-2)는 허용주소DB(108-3)를 검사하여 이와 동일한 MAC 주소가 있는지를 판단한다.

[77] 만약 송신자의 IP 주소와 MAC 주소의 조합이 허용 IP-MAC 주소 목록에 저장된 조합의 내용과 동일하다면, 이 ARP 패킷은 정상적인 장치에서 보낸 것이므로 스푸핑 공격과 무관한 것이라고 볼 수 있다. 따라서 ARP 패킷에 포함된

목적지의 IP-MAC 주소에 해당하는 클라이언트(106)로 데이터 패킷을 전송하여야 하는데, 그 전에 의심 패킷에 대한 검사단계를 거친다.

[78] 두 개의 DB(108-3, 108-4)에 저장된 주소 중에서 송신자의 MAC 주소와 동일한 주소를 찾을 수 없거나, 송신자의 MAC 주소가 차단 MAC 주소 목록에는 없지만 IP 주소와 MAC 주소의 조합이 허용 IP-MAC 주소 목록에 저장된 조합의 내용과 다르다면 아직 최종적으로 안전한 패킷인지 감염된 패킷인지를 확정할 수 없는 상태이다. 이때에는 의심 ARP 패킷으로 분류하여 별도의 검사과정(도 4의 A 단계로서 도 5에 도시)을 거치도록 한다.

[79] 유입된 ARP 패킷의 송신자의 MAC 주소가 차단 MAC 주소 목록에 없다면 감염 패킷이 아닐 가능성이 크지만, 추가적인 두 가지 조건의 충족 여부를 확인한 후 의심 ARP 패킷으로 분류한다.

[80] 첫 번째는 송신자의 IP 주소와 MAC 주소가 허용 IP-MAC 주소 목록에 없는 경우이다. 다시 말해서 차단 목록에도 없지만 허용 목록에도 없다면 그 송신자로부터는 처음으로 들어온 패킷일 가능성이 크므로, 의심 ARP 패킷으로 분류한다.

[81] 두 번째는 송신자의 IP 주소와 MAC 주소가 허용 IP-MAC 주소 목록에 개별적으로 포함되어 있기는 하지만, 허용 IP-MAC 주소 목록에 저장된 조합과는 다른 경우이다. 예를 들어서 클라이언트1(106-1)과 클라이언트2(106-2)의 IP-MAC 주소가 [A-a]와 [B-b]로 각각 맵핑되어 허용 IP-MAC 주소 목록에 주소쌍으로 저장되어 있는데, 특정 클라이언트(106)에 들어온 ARP 패킷의 송신자의 IP-MAC 주소쌍이 [A-b] 또는 [B-a]인 경우를 말한다. 각각의 IP 주소인 A, B와, MAC 주소인 a, b가 허용 목록에 있기는 하지만 맵핑된 주소쌍의 구성요소가 달라진 경우이므로, 스푸핑 공격에 의해 주소가 변질된 것으로 의심해 볼 수 있다.

[82] 허용 IP-MAC 주소 목록에 저장된 주소쌍의 내용과 정확히 일치하지 않는 경우에는 바로 감염 ARP 패킷으로 분류하여 차단시킬 수도 있지만, 네트워크망 내부의 통신 상황에 따라서 MAC 주소를 변경하는 경우도 생길 수 있으므로, 최종적인 확인을 위해서 일단은 의심 패킷으로 분류한다.

[83] 의심 ARP 패킷에 대해서는 주소검사부(108-2)가 단위시간 동안 해당 의심 ARP 패킷의 출발지 MAC 주소와 동일한 출발지 MAC 주소를 가지는 ARP 패킷의 전송 개수를 누적한다.(S202)

[84] 일정한 시간동안 누적된 개수가 특정한 임계치를 넘는 경우에는 네트워크망에 대해서 지속적으로 과도한 ARP 패킷을 발송하는 것이므로, 스푸핑 공격을 시도하는 것으로 간주하는 것이 안전하다.(S204) 통상적으로는 1초당 20회 이상의 ARP 패킷의 발송이 이루어지는 경우에 스푸핑 공격이 시도되고 있는 것으로 판단하도록 하지만, 이 수치는 네트워크의 상태에 따라서 달라질 수 있다. 이후에는 의심 ARP 패킷을 감염 ARP 패킷으로 분류하여 차단과정이 진행된다.

[85] 한편, 어느 하나의 클라이언트(106)로부터 다른 클라이언트(106)로 나가는 ARP 패킷에 대해서도 동일한 방법으로 스푸핑 공격 감염 여부를 판단할 수 있다.

[86] 주소검사부(108-2)는 L2스위치(104)를 경유해서 다른 클라이언트(106)로 향하는 ARP 패킷의 이더넷 헤더의 출발지 IP 주소와 출발지 MAC 주소가 로컬 IP-MAC 주소 목록에 포함되는지를 검사한다. 로컬 IP-MAC 주소 목록은 네트워크망에 포함된 특정 클라이언트(106)의 모든 하드웨어에 대한 주소 정보를 가지고 있으므로, 특정 클라이언트(106)에서 나가는 ARP 패킷의 출발지 주소가 로컬 IP-MAC 주소 목록과 다르다면 해당하는 특정 클라이언트(106)는 이미 스푸핑 공격에 의해 감염이 된 것으로 볼 수 있다.

[87] 따라서 ARP 패킷의 이더넷 헤더의 출발지 IP 주소와 출발지 MAC 주소가 로컬 IP-MAC 주소 목록에 포함되지 않는 ARP 패킷은 감염 ARP 패킷으로 판단하여 차단과정을 진행한다. 송신되는 ARP 패킷에서 출발지 IP 주소 및 MAC 주소를 추출하고, 추출된 IP 주소가 로컬 IP-MAC 주소 목록에 없으면 감염 ARP 패킷이다.

[88] 또한 추출된 IP 주소와 동일한 IP 주소가 로컬 IP-MAC 주소 목록에 포함되어 있는지를 조회한다. 조회 결과 동일한 IP 주소가 발견되고, 이와 대응하여 저장된 MAC 주소가 있다면 이를 조회한다. 송신되는 ARP 패킷의 출발지의 MAC 주소와 로컬 IP-MAC 주소 목록에서 조회한 MAC 주소가 동일하지 않다면 이 역시 감염 ARP 패킷이다.

[89] 이와 같은 모든 검사과정을 거쳐서 안전한 ARP 패킷인 것으로 인정되는 경우에는 지정된 목적지로 ARP 패킷의 송수신이 진행된다.(S118)

[90]

[91] <u>클라이언트에도 허용 주소 목록이 저장된 경우</u>

[92] 개별 클라이언트(106)의 허용주소DB(106-1d)와 차단주소DB(106-1e)에 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록이 저장되어 있는 경우에는 L2스위치(104)를 거쳐서 각 클라이언트(106)에 ARP 패킷이 입력되었을 때 또는 허용주소DB(106-1d)와 차단주소DB(106-1e)가 업데이트될 때마다 클라이언트(106)의 ARP 테이블보호부(106-1b)와 ARP 패킷처리부(106-1c)가 자체적으로 스푸핑 공격 여부를 검사한다. 이때에는 차단서버(108)에 감염 여부의 검사를 요청하지 않고 클라이언트(106)가 직접 수행한다.

[93] 이 경우에도 전술한 바와 같이 출발지의 MAC 주소가 DB(106-1d, 106-1e)에 저장된 주소 목록과 동일한지를 판단한다. ARP 테이블보호부(106-1b)는 차단서버(108)가 수집하여 생성한 허용 IP-MAC 주소 목록과 차단 MAC 주소 목록을 주기적으로 또는 특정 이벤트가 발생했을 때마다 수신함으로써 허용주소DB(106-1d)와 차단주소DB(106-1e)가 항상 업데이트된 상태가 되도록 한다.

[94] ARP 테이블보호부(106-1b)는 주기적으로 ARP 엔트리를 검사하여 추출된 IP-MAC 주소를 DB(106-1d, 106-1e)에 저장된 주소 목록과 비교하여 감염 여부를

판단한다. 그리고 ARP 패킷처리부(106-1c)는 ARP 패킷이 들어오거나 나갈 때마다 IP-MAC 주소를 추출하여 감염 여부를 판단한다.

[95] 만약 출발지의 MAC 주소가 차단 IP-MAC 주소 목록에 저장된 MAC 주소와 동일하다면 ARP 패킷처리부(106-1c)가 해당 ARP 패킷을 차단시키거나, ARP 테이블보호부(106-1b)가 ARP 엔트리의 MAC 주소를 변경한다.

[96] 또한 의심 ARP 패킷에 대해서도 앞에서와 동일하게 일정한 시간 동안 동일한 MAC 주소를 갖는 ARP 패킷이 유입되는지를 감시하고, 특정한 임계치를 넘는 경우에는 감염 ARP 패킷으로 분류한다.

[97] 또한 클라이언트(106)로부터 나가는 ARP 패킷의 출발지 IP-MAC 주소가 로컬 IP-MAC 주소 목록에 저장된 정보와 다를 경우에 감염 ARP 패킷으로 분류한다.

[98]

[99] <u>스푸핑 공격 차단 과정</u>

[100] 차단서버(108) 또는 클라이언트(106)에 의해 감염 ARP 패킷으로 밝혀진 경우, 해당 ARP 패킷이 네트워크망 내부를 돌아다니지 않도록 해야 한다.

[101] 이를 위해 먼저 감염된 ARP 패킷의 송수신을 차단하고, ARP 테이블에서 해당 IP-MAC 주소를 수정한다.(S112) ARP 패킷처리부(106-1c)는 차단서버(108)로부터 ARP 패킷이 스푸핑 공격에 사용되고 있다는 검사결과를 통보받으면 해당 감염 ARP 패킷의 송수신을 차단시킨다.

[102] 그리고 ARP 테이블보호부(106-1b)는 ARP 엔트리가 스푸핑 공격에 사용되고 있다는 검사결과를 통보받으면 해당 감염 ARP 엔트리에 포함된 IP-MAC 주소 중에서 IP 주소를 추출하고, 추출된 IP 주소와 대응하여 저장된 정상 MAC 주소를 차단서버(108)의 DB(108-3, 108-4)나 클라이언트(106)의 DB(106-1d, 106-1e)에서 조회한다. 정상 MAC 주소가 조회되면, 감염 ARP 엔트리의 출발지(송신자) 주소를 저장된 정상 MAC 주소로 고정(static) 설정한다.(S114) 향후에는 해당 IP 주소를 가진 ARP 패킷이 들어왔을 때, 고정으로 설정된 정상 MAC 주소를 가진 클라이언트(106)로만 향하게 된다.

[103] ARP 테이블보호부(106-1b)와 ARP 패킷처리부(106-1c)는 차단된 패킷의 Operation 타입, 출발지 IP 주소, 출발지 MAC 주소, 대상지 IP 주소, 대상지 MAC 주소, 패킷 발신 프로세스 등의 정보를 차단서버(108)로 전송한다.(S116) 차단서버(108)의 주소수집부(108-1)는 ARP 테이블보호부(106-1b)와 ARP 패킷처리부(106-1c)가 전송한 데이터를 수신하여 차단주소DB(108-4)를 업데이트한다.

[104] 이상 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명하였지만, 상술한 본 발명의 기술적 구성은 본 발명이 속하는 기술 분야의 당업자가 본 발명의 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로서 이해되어야 하고, 본 발명의 범위는 상기 상세한 설명보다는 후술하는

특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 등가 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

청구범위

[청구항 1] 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서,
차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와;
상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 허용주소DB(108-3)에 저장하는 제2단계와;
상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 차단주소DB(108-4)에 저장하는 제3단계와;
상기 클라이언트(106)에 ARP 패킷이 유입되면, 상기 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 상기 차단서버(108)로 전송하면서 스푸핑 공격 여부에 대한 검사를 요청하는 제4단계와;
차단서버(108)의 주소검사부(108-2)의 검사 결과, 상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단주소DB(108-4)에 저장된 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 패킷이 감염 ARP 패킷이라는 것을 상기 차단서버(108)가 상기 클라이언트(106)에 통보하는 제5단계와;
상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송수신을 차단하는 제6단계;를 포함하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 2] 제1항에 있어서,
상기 제5단계는
상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함되어 있지 않은 경우, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 없거나, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 맵핑되어 주소쌍으로 저장되어 있는 허용 IP-MAC 주소의 구성과 다르다면 상기 ARP 패킷을 의심 ARP 패킷으로 정의하는

제5-1단계와;
상기 주소검사부(108-2)가 단위시간 동안 상기 클라이언트(106)에 유입된 ARP 패킷 중에서 상기 의심 ARP 패킷에 포함된 송신자의 MAC 주소와 동일한 송신자 MAC 주소를 가지는 ARP 패킷의 전송 개수를 누적하는 제5-2단계와;
일정한 시간 동안 누적된 전송 개수가 임계치를 넘는 경우, 상기 의심 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5-3단계;를 추가로 포함하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 3] 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서,
차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와;
상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 허용주소DB(108-3)에 저장하는 제2단계와;
상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 차단주소DB(108-4)에 저장하는 제3단계와;
상기 클라이언트(106)의 ARP 테이블보호부(106-1b)가 상기 클라이언트(106)의 ARP 테이블에 포함된 ARP 엔트리의 IP 주소와 MAC 주소를 추출하여 상기 차단서버(108)로 전송하면서 스푸핑 공격 여부에 대한 검사를 요청하는 제4단계와;
차단서버(108)의 주소검사부(108-2)의 검사 결과, 상기 제4단계에서 추출된 MAC 주소가 상기 차단주소DB(108-4)에 저장된 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 엔트리가 감염 ARP 엔트리라는 것을 상기 차단서버(108)가 상기 클라이언트(106)에 통보하는 제5단계와;
상기 ARP 테이블보호부(106-1b)가 상기 감염 ARP 엔트리에 포함된 IP 주소를 추출하고, 상기 추출된 IP 주소와 대응하여 저장된 정상 MAC 주소를 상기 허용 IP-MAC 주소 목록에서 조회하는 제6단계와;
상기 ARP 테이블보호부(106-1b)가 상기 감염 ARP 엔트리의 MAC 주소를 상기 조회된 정상 MAC 주소로 변경시키는 제7단계;를

포함하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 4] 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서,
차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와;
상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 상기 클라이언트(106)의 허용주소DB(106-1d)에 저장하는 제2단계와;
상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 상기 클라이언트(106)의 차단주소DB(106-1e)에 저장하는 제3단계와;
상기 클라이언트(106)에 ARP 패킷이 유입되면, 상기 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 스푸핑 공격 여부를 검사하는 제4단계와;
상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 패킷처리부(106-1c)가 상기 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5단계와;
상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송수신을 차단하는 제6단계;를 포함하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 5] 제4항에 있어서,
상기 제5단계는
상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함되어 있지 않은 경우, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 없거나, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 맵핑되어 주소쌍으로 저장되어 있는 허용 IP-MAC 주소의 구성과 다르다면 상기 ARP 패킷을 의심 ARP 패킷으로 정의하는 제5-1단계와;
상기 ARP 패킷처리부(106-1c)가 단위시간 동안 상기 클라이언트(106)에 유입된 ARP 패킷 중에서 상기 의심 ARP

패킷에 포함된 송신자의 MAC 주소와 동일한 송신자 MAC 주소를 가지는 ARP 패킷의 전송 개수를 누적하는 제5-2단계와;
일정한 시간 동안 누적된 전송 개수가 임계치를 넘는 경우, 상기 의심 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5-3단계;를 추가로 포함하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 6] 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서,
차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와;
상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 상기 클라이언트(106)의 허용주소DB(106-1d)에 저장하는 제2단계와;
상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 상기 클라이언트(106)의 차단주소DB(106-1e)에 저장하는 제3단계와;
상기 클라이언트(106)의 ARP 테이블보호부(106-1b)가 상기 클라이언트(106)의 ARP 테이블에 포함된 ARP 엔트리의 IP 주소와 MAC 주소를 추출하여 스푸핑 공격 여부를 검사하는 제4단계와;
상기 제4단계에서 추출된 MAC 주소가 상기 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 테이블보호부(106-1b)가 상기 ARP 엔트리를 감염 ARP 엔트리로 분류하는 제5단계와;
상기 ARP 테이블보호부(106-1b)가 상기 감염 ARP 엔트리에 포함된 IP 주소를 추출하고, 상기 추출된 IP 주소와 대응하여 저장된 정상 MAC 주소를 상기 허용 IP-MAC 주소 목록에서 조회하는 제6단계와;
상기 ARP 테이블보호부(106-1b)가 상기 감염 ARP 엔트리의 MAC 주소를 상기 조회된 정상 MAC 주소로 변경시키는 제7단계;를 포함하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 7] 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서,

특정 클라이언트(106)에 설치되어 있는 장치들의 IP 주소와 MAC 주소를 수집하는 제1단계와;
제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 로컬 IP-MAC 주소 목록을 상기 클라이언트(106)의 허용주소DB(106-1d)에 저장하는 제2단계와;
상기 특정 클라이언트(106)로부터 ARP 패킷이 송신될 때, 상기 특정 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 송신되는 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 스푸핑 공격 여부를 검사하는 제2단계와;
제2단계에서 추출된 송신자의 IP 주소가 상기 로컬 IP-MAC 주소 목록에 포함되어 있지 않거나, 추출된 송신자의 IP 주소와 동일한 IP 주소에 대응하여 저장된 MAC 주소가 상기 송신되는 ARP 패킷에 포함된 송신자의 MAC 주소와 다른 경우, 상기 ARP 패킷처리부(106-1c)가 상기 송신되는 ARP 패킷을 감염 ARP 패킷으로 분류하는 제3단계와;
상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송신을 차단하는 제4단계;를 포함하는, 차단서버를 이용한 스푸핑 공격 방어방법.

청구범위 보정서
국제사무국 접수일: 2012 년 10 월 19 일 (19.10.2012)

청구범위

[청구항 1] 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서,
차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와;
상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 허용주소DB(108-3)에 저장하는 제2단계와;
상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 차단주소DB(108-4)에 저장하는 제3단계와;
상기 클라이언트(106)에 ARP 패킷이 유입되면, 상기 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 상기 차단서버(108)로 전송하면서 스푸핑 공격 여부에 대한 검사를 요청하는 제4단계와;
차단서버(108)의 주소검사부(108-2)의 검사 결과, 상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단주소DB(108-4)에 저장된 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 패킷이 감염 ARP 패킷이라는 것을 상기 차단서버(108)가 상기 클라이언트(106)에 통보하는 제5단계와;
상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송수신을 차단하는 제6단계;를 포함하며,
상기 제5단계는
상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함되어 있지 않은 경우, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 없거나, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 맵핑되어 주소쌍으로 저장되어 있는 허용 IP-MAC 주소의 구성과 다르다면 상기 ARP 패킷을 의심 ARP 패킷으로 정의하는 제5-1단계와;
상기 주소검사부(108-2)가 단위시간 동안 상기 클라이언트(106)에

유입된 ARP 패킷 중에서 상기 의심 ARP 패킷에 포함된 송신자의 MAC 주소와 동일한 송신자 MAC 주소를 가지는 ARP 패킷의 전송 개수를 누적하는 제5-2단계와;
일정한 시간 동안 누적된 전송 개수가 임계치를 넘는 경우, 상기 의심 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5-3단계;로 이루어지는 것을 특징으로 하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 2] 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서,
차단서버(108)의 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106)의 IP 주소와 MAC 주소를 수집하는 제1단계와;
상기 주소수집부(108-1)가 상기 제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 허용 IP-MAC 주소 목록을 생성하고, 상기 허용 IP-MAC 주소 목록을 상기 클라이언트(106)의 허용주소DB(106-1d)에 저장하는 제2단계와;
상기 주소수집부(108-1)가 상기 네트워크망 내부에 연결된 클라이언트(106) 중에서 스푸핑 공격을 하는 공격자가 사용하는 클라이언트(106)의 MAC 주소에 대한 정보인 차단 MAC 주소 목록을 상기 클라이언트(106)의 차단주소DB(106-1e)에 저장하는 제3단계와;
상기 클라이언트(106)에 ARP 패킷이 유입되면, 상기 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 스푸핑 공격 여부를 검사하는 제4단계와;
상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함된 경우, 상기 ARP 패킷처리부(106-1c)가 상기 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5단계와;
상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송수신을 차단하는 제6단계;를 포함하며,
상기 제5단계는
상기 제4단계에서 추출된 송신자의 MAC 주소가 상기 차단 MAC 주소 목록에 포함되어 있지 않은 경우, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 없거나, 상기 송신자의 IP 주소와 MAC 주소가 상기 허용 IP-MAC 주소 목록에 맵핑되어 주소쌍으로 저장되어 있는 허용 IP-MAC 주소의 구성과

다르다면 상기 ARP 패킷을 의심 ARP 패킷으로 정의하는 제5-1단계와;
상기 ARP 패킷처리부(106-1c)가 단위시간 동안 상기 클라이언트(106)에 유입된 ARP 패킷 중에서 상기 의심 ARP 패킷에 포함된 송신자의 MAC 주소와 동일한 송신자 MAC 주소를 가지는 ARP 패킷의 전송 개수를 누적하는 제5-2단계와;
일정한 시간 동안 누적된 전송 개수가 임계치를 넘는 경우, 상기 의심 ARP 패킷을 감염 ARP 패킷으로 분류하는 제5-3단계;로 이루어지는 것을 특징으로 하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 3] 네트워크망 내부의 L2스위치(104)를 통해 중계되는 ARP 패킷에 포함된 IP 주소와 MAC 주소를 검사하여 스푸핑 공격이 이루어지고 있는 것으로 판단되면, 상기 ARP 패킷의 전송을 차단시키는 방어방법으로서,
특정 클라이언트(106)에 설치되어 있는 장치들의 IP 주소와 MAC 주소를 수집하는 제1단계와;
제1단계에서 수집한 상기 IP 주소와 상기 MAC 주소를 서로 대응시킨 로컬 IP-MAC 주소 목록을 상기 클라이언트(106)의 허용주소DB(106-1d)에 저장하는 제2단계와;
상기 특정 클라이언트(106)로부터 ARP 패킷이 송신될 때, 상기 특정 클라이언트(106)의 ARP 패킷처리부(106-1c)는 상기 송신되는 ARP 패킷에 포함된 송신자의 IP 주소와 MAC 주소를 추출하여 스푸핑 공격 여부를 검사하는 제2단계와;
제2단계에서 추출된 송신자의 IP 주소가 상기 로컬 IP-MAC 주소 목록에 포함되어 있지 않거나, 추출된 송신자의 IP 주소와 동일한 IP 주소에 대응하여 저장된 MAC 주소가 상기 송신되는 ARP 패킷에 포함된 송신자의 MAC 주소와 다른 경우, 상기 ARP 패킷처리부(106-1c)가 상기 송신되는 ARP 패킷을 감염 ARP 패킷으로 분류하는 제3단계와;
상기 ARP 패킷처리부(106-1c)가 상기 감염 ARP 패킷의 송신을 차단하는 제4단계;를 포함하는, 차단서버를 이용한 스푸핑 공격 방어방법.

[청구항 4] (취소됨)

[청구항 5] (취소됨)

[청구항 6] (취소됨)

[청구항 7] (취소됨)

조약 제19조(1) 규정의 설명서

[1] 출원의 경과

본 PCT 국제출원 PCT/KR2012/001714 는 2011년 5월 12일자 대한민국 특허출원을 기초로 하여 2012년 3월 8일자로 출원되었고, 2012년 9월 28일자로 국제조사보고서가 송부되었습니다.

출원인은 특허협력조약 제19조와 조약의 규칙 제46조에 따라서 본 출원의 청구범위에 대하여 보정서를 제출합니다.

[2] 청구범위의 보정

본 출원에 대한 보정서에서는 종전 청구범위 제1항과 제2항을 병합하여 새로운 제1항으로 기재하였고, 종전 청구범위 제4항과 제5항을 병합하여 새로운 제2항으로 기재하였으며, 종전 청구범위 제7항을 새로운 제3항으로 기재하였습니다. 이 과정에서 제3항과 제6항은 삭제하는 보정을 하였습니다.

[3] 보정의 내용

본 출원에 대한 국제조사보고서에 따르면 종전 제1항과 제3항, 제4항, 제6항에 기재된 발명은 인용참증1(KR 10-0807933 B1)의 기재로부터 당업자가 용이하게 도출할 수 있는 발명이어서 신규성이 없다는 판단을 받았습니다.

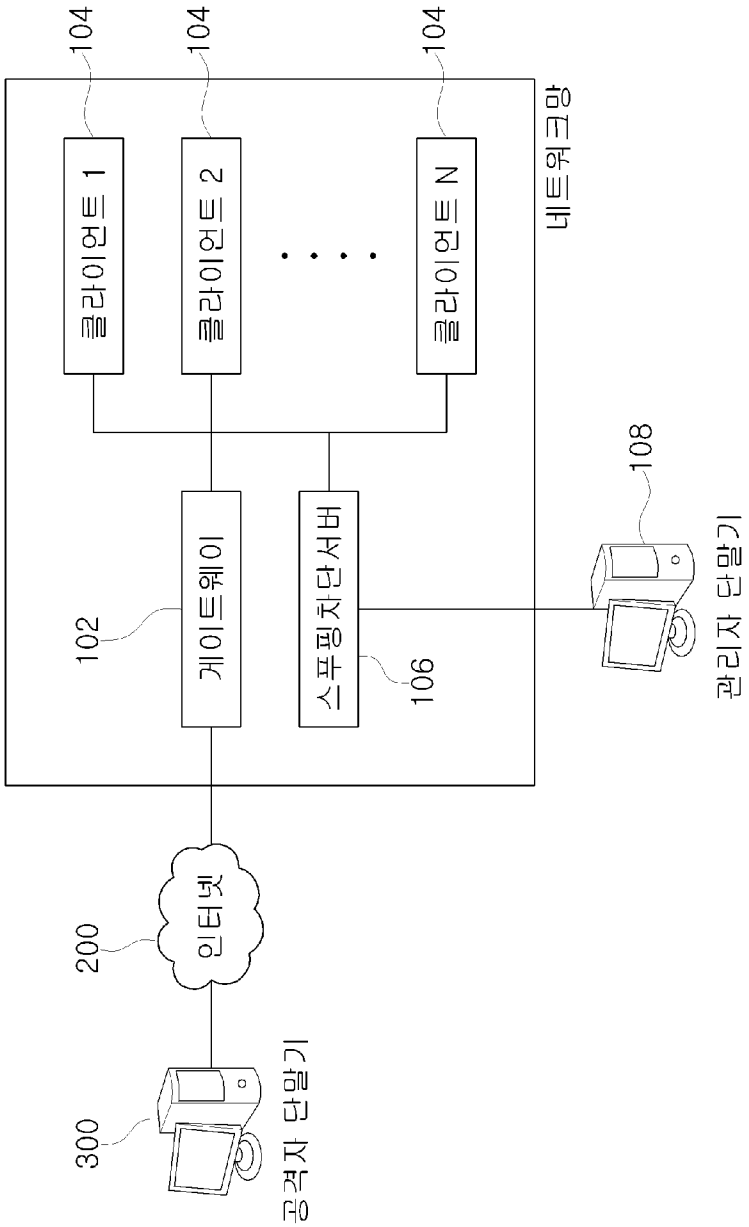
이러한 보고서의 견해에 따라 신규성 및 진보성이 없는 것으로 판단되는 제1

항, 제3항, 제4항, 제6항을 삭제하고, 제2항, 제5항, 제7항의 내용을 독립항에 통합 한정함으로써, 본 출원의 기술 내용은 인용참증1과는 다른 것으로 볼 수 있습니다.

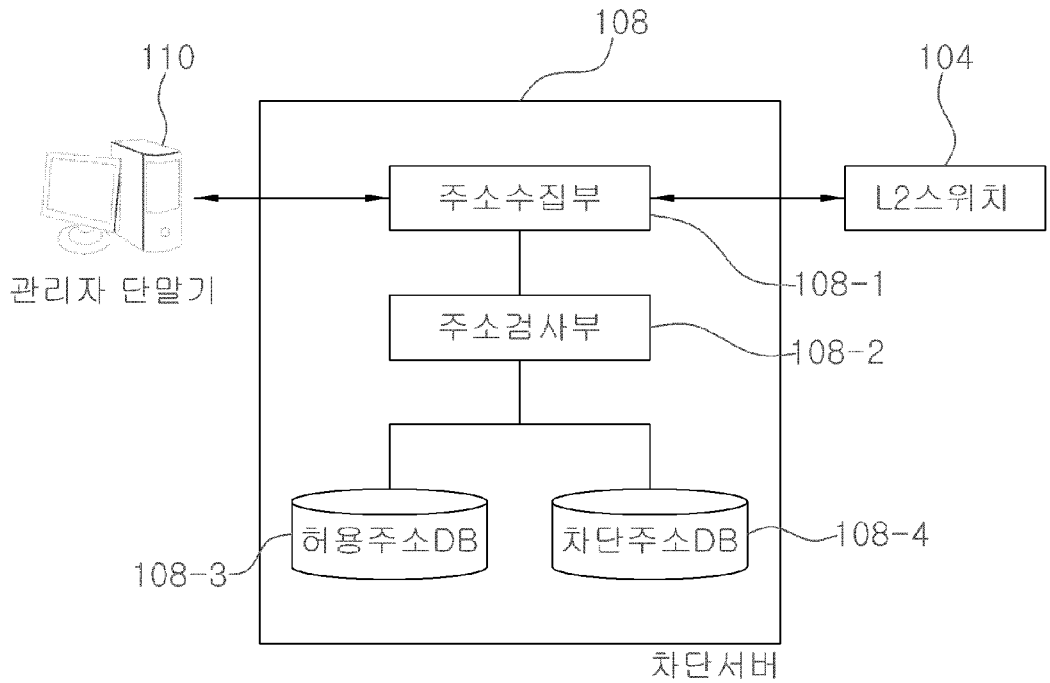
[4] 결론

본 출원에 대하여 국제사무국에 제출하는 대체용지에 기재된 보정 내용에 따르면 본 출원은 인용참증으로부터 당업자가 용이하게 발명할 수 없는 기술입니다.

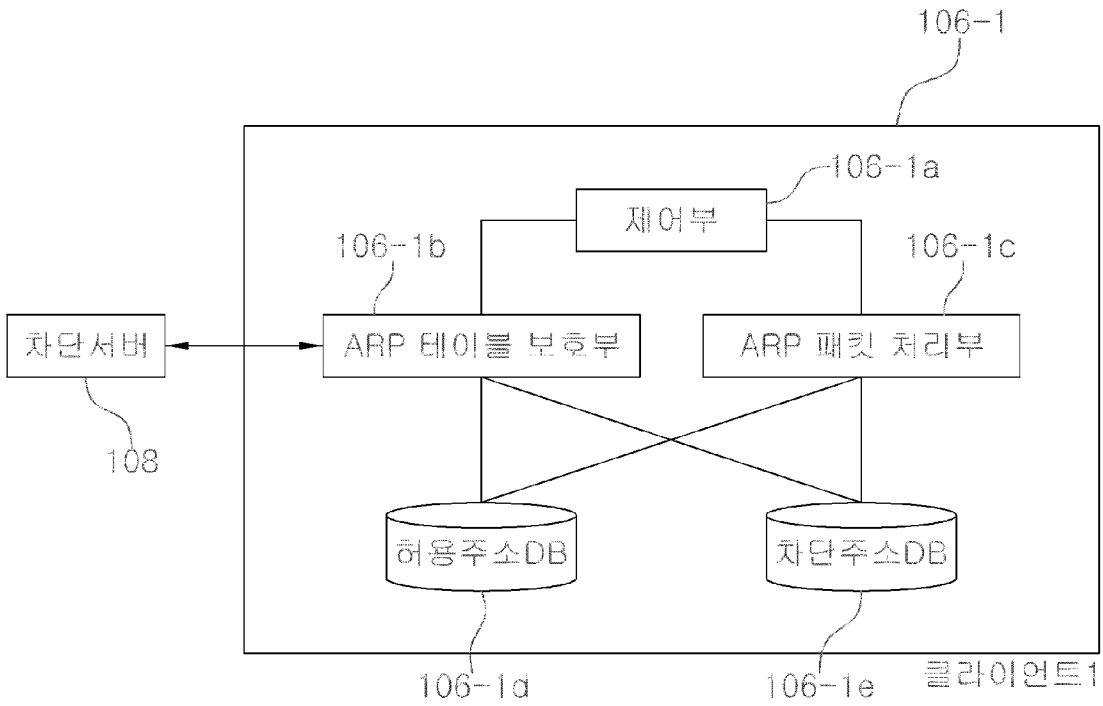
[Fig. 1]


104
104
104
클라이언트 1
클라이언트 2
클라이언트 N
네트워크망
102
게이트웨이
스푸핑차단서버
106
108
관리자 단말기
200
인터넷
300
공격자 단말기

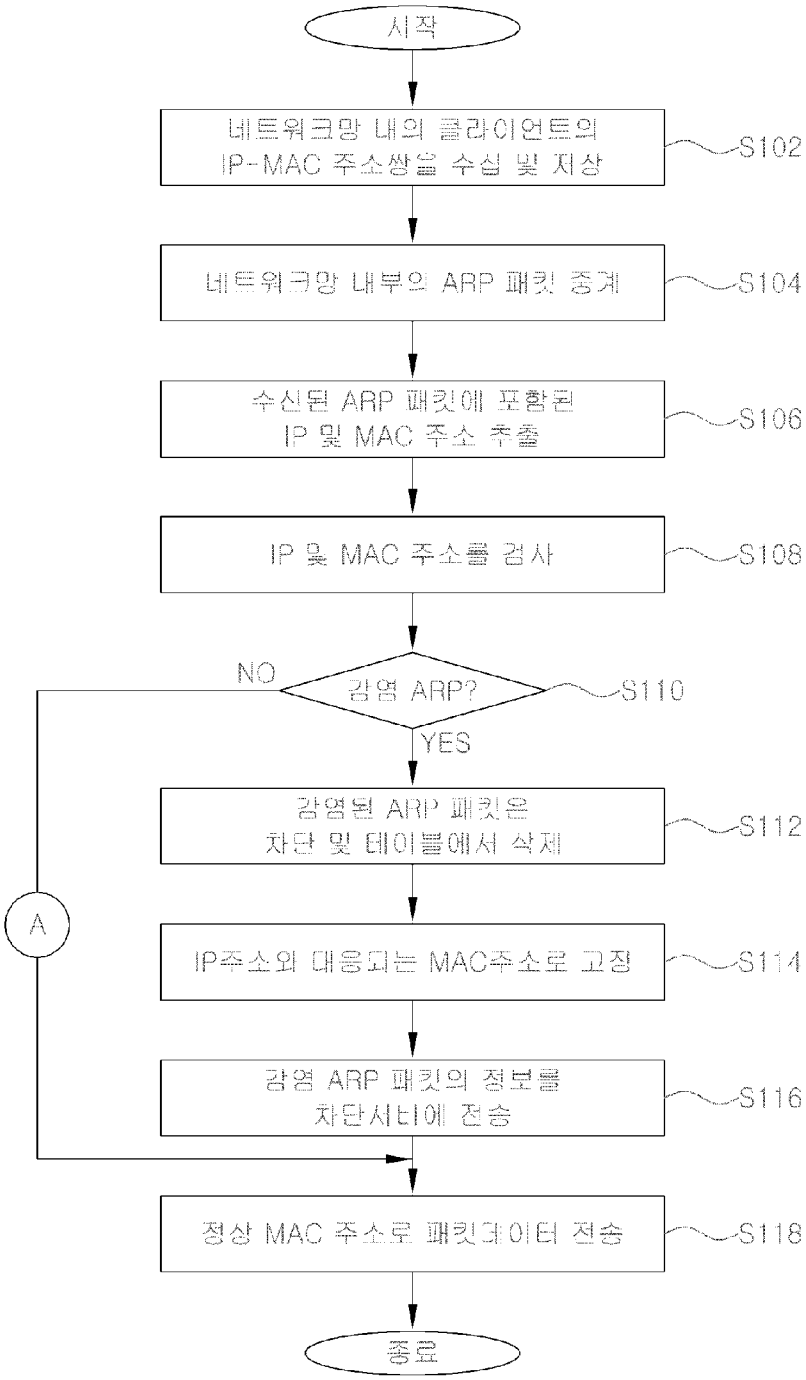
[Fig. 2]


108
110
104
주소수집부
L2스위치
관리자 단말기
108-1
주소검사부
108-2
허용주소DB
차단주소DB
108-3
108-4
차단서버

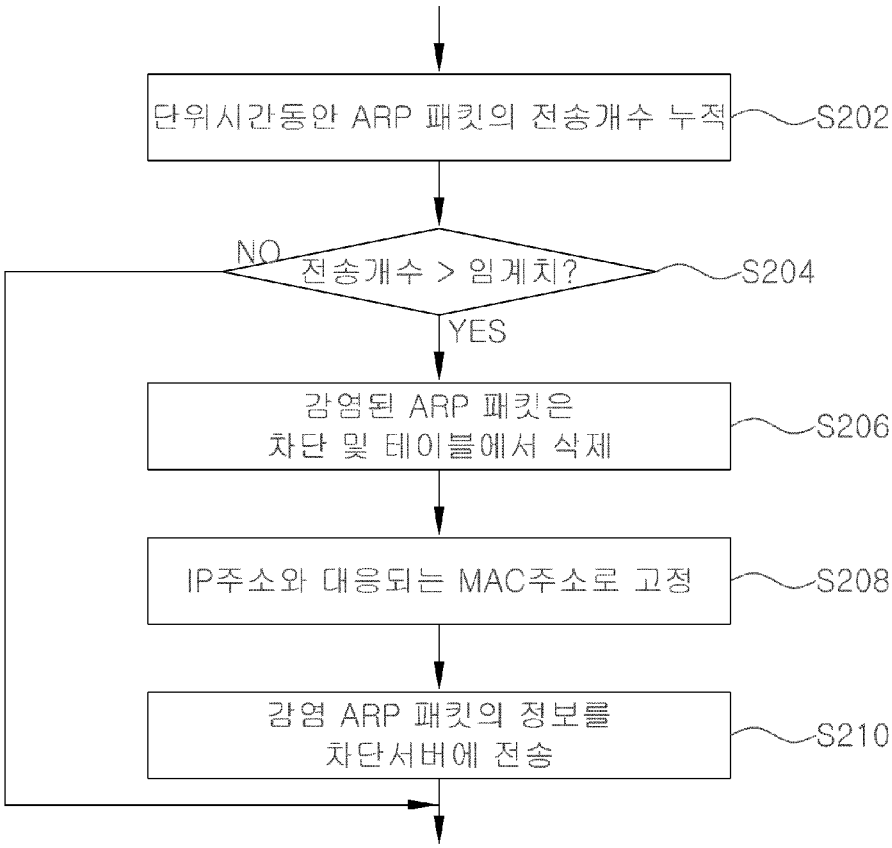
[Fig. 3]


106-1
106-1a
제어부
106-1b
106-1c
차단서버
ARP 테이블 보호부
ARP 패킷 처리부
108
허용주소DB
차단주소DB
106-1d
106-1e
클라이언트1

[Fig. 4]


시작
네트워크망 내의 클라이언트의 IP-MAC 주소쌍을 수집 및 저장
S102
네트워크망 내부의 ARP 패킷 중계
S104
수신된 ARP 패킷에 포함된 IP 및 MAC 주소 추출
S106
IP 및 MAC 주소를 검사
S108
NO
감염 ARP?
S110
YES
감염된 ARP 패킷은 차단 및 테이블에서 삭제
S112
A
IP주소와 대응되는 MAC주소로 고정
S114
감염 ARP 패킷의 정보를 차단서버에 전송
S116
정상 MAC 주소로 패킷데이터 전송
S118
종료

[Fig. 5]


단위시간동안 ARP 패킷의 전송개수 누적
S202
NO
전송개수 > 임계치?
S204
YES
감염된 ARP 패킷은
차단 및 테이블에서 삭제
S206
IP주소와 대응되는 MAC주소로 고정
S208
감염 ARP 패킷의 정보를
차단서버에 전송
S210

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2012/001714

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/22(2006.01)i, H04L 12/56(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/22; H04L 9/32; H04L 9/00; H04L 12/28; H04L 12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: spoofing, blocking, address, attack

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	KR 10-0807933 B1 (ERICSSON-LG CO., LTD.) 03 March 2008 Abstract; claims 1,2,4,7,8,10; paragraphs [0038], [0039], [0041], 0046].	1,3,4,6 2,5,7
A	KR 10-2004-0109985 A (INTIGATE INC.) 29 December 2004 Abstract; claims 1,2,9,10.	1-7
A	KR 10-2006-0064450 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 13 June 2006 Abstract; claims 1,3-6,8,10-13.	1-7
A	KR 10-2008-0107599 A (KT CORPORATION) 11 December 2008 Abstract; claims 1-3.	1-7

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 SEPTEMBER 2012 (27.09.2012)	**28 SEPTEMBER 2012 (28.09.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2012/001714

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-0807933 B1	03.03.2008	NONE	
KR 10-2004-0109985 A	29.12.2004	NONE	
KR 10-2006-0064450 A	13.06.2006	NONE	
KR 10-2008-0107599 A	11.12.2008	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2012/001714

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 12/22(2006.01)i, H04L 12/56(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 12/22; H04L 9/32; H04L 9/00; H04L 12/28; H04L 12/56

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드:스푸핑,차단,주소,공격

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X A	KR 10-0807933 B1 (엘지노텔 주식회사) 2008.03.03 요약; 청구항 1,2,4,7,8,10; 단락 [0038],[0039],[0041],[0046].	1,3,4,6 2,5,7
A	KR 10-2004-0109985 A (주식회사 인티게이트) 2004.12.29 요약; 청구항 1,2,9,10.	1-7
A	KR 10-2006-0064450 A (한국전자통신연구원) 2006.06.13 요약; 청구항 1,3-6,8,10-13.	1-7
A	KR 10-2008-0107599 A (주식회사 케이티) 2008.12.11 요약; 청구항 1-3	1-7

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2012년 09월 27일 (27.09.2012)	**2012년 09월 28일 (28.09.2012)**

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 82-42-472-7140

심사관
양찬호
전화번호 82-42-481-5689

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2012/001714

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-0807933 B1	2008.03.03	없음	
KR 10-2004-0109985 A	2004.12.29	없음	
KR 10-2006-0064450 A	2006.06.13	없음	
KR 10-2008-0107599 A	2008.12.11	없음	