(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년11월04일
(11) 등록번호 10-1079736
(24) 등록일자 2011년10월28일

(51) Int. Cl.
H04L 12/22 (2006.01) *H04L 9/32* (2006.01)
H04L 12/26 (2006.01)
(21) 출원번호 10-2010-0044844
(22) 출원일자 2010년05월13일
심사청구일자 2010년05월13일
(56) 선행기술조사문헌
KR1020060022861 A*
US06606709 B1*
KR1020080001216 A
KR1020100033626 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
이우기
인천광역시 남구 용현4동 인하대학교 산업공학과
박순형
서울특별시 양천구 신정6동 신시가지8단지아파트 810동 706호
임차성
인천광역시 남구 학익2동 신동아아파트 8차 101동 1602호
(74) 대리인
유완식, 이은철

전체 청구항 수 : 총 12 항 심사관 : 양찬호

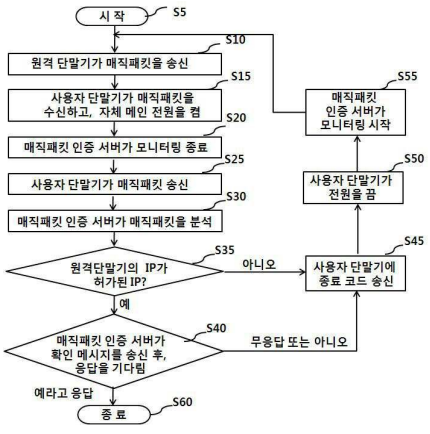
(54) 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템 및 그 방법

(57) 요 약

본 발명에 따르면, 해당 컴퓨터에 접근하는 모든 패킷을 모니터링하는 서버를 만들어 허가되지 않은 매직패킷에 대해 보안을 강화할 수 있다. 또한, IPv4에서 확장되어 IPv6의 경우에도 컴퓨터를 포함한 모든 전자 기기에 대해 허가되지 않은 매직패킷에 대해 보안을 강화할 수 있다.

본 발명의 바람직한 일실시예는, 원격 단말기가 사용자 단말기의 원격에서의 제어를 위해 매직패킷을 상기 사용자 단말기로 송신하는 단계; 상기 사용자 단말기가 상기 매직패킷을 수신하고, 자체의 메인 전원을 켜는 단계; 상기 사용자 단말기가 매직패킷 인증 서버로 상기 매직패킷을 송신하는 단계; 상기 매직패킷 인증 서버가 상기 매직패킷을 수신하여 분석하는 단계; 상기 매직패킷 인증 서버가 상기 매직패킷의 분석 결과, 상기 원격 단말기의 IP가 허가된 IP인 경우, 상기 매직패킷 인증 서버가 상기 사용자 단말기로 확인 메시지를 송신하는 단계: 및 상기 사용자 단말기가 상기 확인 메시지에 대해 응답을 상기 매직패킷 인증 서버로 송신하는 단계;를 포함한다.

대 표 도 - 도3



특허청구의 범위

청구항 1

허가되지 않은 WOL 보안 방법에 있어서,

(a) 원격 단말기가 사용자 단말기의 원격에서의 제어를 위해 매직패킷을 상기 사용자 단말기로 송신하는 단계;

(b) 상기 사용자 단말기가 상기 매직패킷을 수신하고, 자체의 메인 전원을 켜는 단계;

(c) 상기 사용자 단말기가 매직패킷 인증 서버로 상기 매직패킷을 송신하는 단계;

(d) 상기 매직패킷 인증 서버가 상기 매직패킷을 수신하여 분석하는 단계;

(e) 상기 매직패킷 인증 서버가 상기 매직패킷의 분석 결과, 상기 원격 단말기의 IP가 허가된 IP인 경우, 상기 매직패킷 인증 서버가 상기 사용자 단말기로 확인 메시지를 송신하는 단계: 및

(f) 상기 매직패킷 인증 서버가 상기 확인 메시지에 대한 응답을 수신한 경우 대기하고, 상기 매직패킷 인증 서버가 상기 확인 메시지에 대한 응답을 수신하지 않거나 '아니오'라는 응답을 수신한 경우 사용자 단말기로 종료 코드를 송신하는 단계;를 포함하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 방법.

청구항 2

제1항에 있어서,

상기 (b) 단계에서 상기 사용자 단말기의 메인 전원이 켜지는 경우 상기 매직패킷 인증 서버가 상기 사용자 단말기에 대한 모니터링을 종료하는 단계;를 더 포함하는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 방법.

청구항 3

제1항에 있어서,

상기 (d) 단계의 매직 패킷을 분석한 결과, 상기 원격 단말기의 IP가 허가되지 않은 IP인 경우,

(d-1) 상기 매직패킷 인증 서버가 상기 사용자 단말기로 종료 코드를 송신하는 단계;

(d-2) 상기 사용자 단말기가 자체의 메인 전원을 끄는 단계; 및

(d-3) 상기 매직패킷 인증 서버가 상기 사용자 단말기에 대한 모니터링을 다시 시작하는 단계;를 더 포함하는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 방법.

청구항 4

제1항에 있어서,

상기 (f) 단계에서 상기 사용자 단말기가 응답을 상기 매직패킷 인증 서버로 송신하지 않는 경우,

(f-1) 상기 매직패킷 인증 서버가 상기 사용자 단말기로 종료 코드를 송신하는 단계;

(f-2) 상기 사용자 단말기가 자체의 메인 전원을 끄는 단계; 및

(f-3) 상기 매직패킷 인증 서버가 상기 사용자 단말기에 대한 모니터링을 다시 시작하는 단계;를 더 포함하는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 방법.

청구항 5

허가되지 않은 WOL 보안 시스템에 있어서,

원격 단말기로부터 원격에서의 제어를 위한 매직패킷을 수신하여 자체의 메인 전원를 켜고, 매직패킷 인증 서버로 상기 매직패킷을 송신하는 사용자 단말기;

상기 매직패킷을 수신하여 분석하는 매직패킷 인증 서버;를 포함하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템.

청구항 6

제5항에 있어서, 상기 매직패킷 인증 서버는,

상기 사용자 단말기의 메인 전원이 켜지는 경우, 상기 사용자 단말기에 대한 모니터링을 종료하는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템.

청구항 7

제5항 또는 제6항에 있어서, 상기 매직패킷 인증 서버는,

상기 매직패킷의 분석 결과, 상기 원격 단말기의 IP가 허가된 IP인 경우, 상기 사용자 단말기로 확인 메시지를 송신하고, 상기 사용자 단말기로부터 상기 확인 메시지에 대한 응답을 수신하는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템.

청구항 8

제7항에 있어서, 상기 매직패킷 인증 서버는,

상기 사용자 단말기로부터 상기 확인 메시지에 대한 응답을 수신하지 못하는 경우, 상기 사용자 단말기로 종료 코드를 송신하고, 상기 사용자 단말기에 대한 모니터링을 다시 시작하는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템.

청구항 9

제8항에 있어서, 상기 사용자 단말기는,

상기 종료 코드를 수신하고, 자체의 메인 전원을 끄는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템.

청구항 10

제5항 또는 제6항에 있어서, 상기 매직패킷 인증 서버는,

상기 매직패킷의 분석 결과, 상기 원격 단말기의 IP가 허가되지 않은 IP인 경우, 상기 사용자 단말기로 종료 코드를 송신하고, 상기 사용자 단말기에 대한 모니터링을 다시 시작하는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템.

청구항 11

제10항에 있어서, 상기 사용자 단말기는,

상기 종료 코드를 수신하고, 자체의 메인 전원을 끄는 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템.

청구항 12

제5항에 있어서, 상기 매직패킷 인증 서버는,

상기 사용자 단말기가 속해 있는 네트워크 그룹의 관리자 서버와 동일한 것을 특징으로 하는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 허가되지 않은 WOL 보안 시스템 및 그 방법에 관한 것으로, 더욱 상세하게는 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 원격 부팅에 대한 관심이 점점 더 높아지고 있다. 이 기술은 'Wake-On-Lan'(WOL)이라 불리는 기능으로 예전에는 고급 사양으로 인식되어 일부 고가의 시스템에만 탑재되었으나, 현재는 출시되는 모든 컴퓨터의 메인보드에 WOL 기능이 추가되어, 해당 컴퓨터의 원격 부팅과 원격 조정을 할 수 있게 되었다.

[0003] 이러한 원격 부팅으로 얻을 수 있는 효과는 매우 크다. 집과 사무실에서 인터넷에 연결되어 있는 것만으로 누구의 도움 없이 컴퓨터를 켤 수 있으며, 원격으로 조정할 수 있는 것이다. 이 기능은 스마트폰을 통해서도 이용되고 있으며, IPv6 기술이 더욱 발전 되어 모든 기기가 네트워크 주소를 가지게 된다면 WOL 기능에 의해 모든 기기들을 켜는 것을 통제할 수 있게 될 것이다.

[0004] 다만, 상기와 같은 시스템에는 문제가 있다. 즉, 같은 네트워크망 안에 있는 컴퓨터 사용자가 이 원리를 안다면 누구나 다른 사람의 컴퓨터나 기기를 켤 수 있게 되는 것이다. 해당 컴퓨터가 켜져 있는 상태에서 해킹 가능한 수준의 악의적인 사용자라면 그 컴퓨터를 공격하거나, 개인 정보 등을 비롯한 중요한 정보를 빼내오는 것이 그리 어려운 일이 아닐 것이다.

[0005] 이를 위해 일부 장치에 보안 기능을 탑재하여 매직패킷의 정보 마지막에 패스워드를 붙여야만 인증되는 것도 있지만, 이는 고가의 상품이어서 모든 컴퓨터가 이러한 장비를 구입하는 것에는 무리가 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 전술한 바와 같은 기술적 과제를 해결하는 데 목적이 있는 발명으로서, 해당 컴퓨터에 접근하는 모든 패킷을 모니터링하는 서버를 만들어 허가되지 않은 매직패킷에 대해 보안을 강화하는 것에 그 목적이 있다.

[0007] 또한, IPv4에서 확장되어 IPv6의 경우에도 컴퓨터를 포함한 모든 전자 기기에 대해 허가되지 않은 매직패킷에 대해 보안을 강화하는 것에도 그 목적이 있다.

과제의 해결 수단

[0008] 본 발명의 일실시예에 따른 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 방법은, (a) 원격 단말기가 사용자 단말기의 원격에서의 제어를 위해 매직패킷을 상기 사용자 단말기로 송신하는 단계; (b) 상기 사용자 단말기가 상기 매직패킷을 수신하고, 자체의 메인 전원을 켜는 단계; (c) 상기 사용자 단말기가 매직패킷 인증 서버로 상기 매직패킷을 송신하는 단계; (d) 상기 매직패킷 인증 서버가 상기 매직패킷을 수신하여 분석하는 단계; (e) 상기 매직패킷 인증 서버가 상기 매직패킷의 분석 결과, 상기 원격 단말기의 IP가 허가된 IP인 경우, 상기 매직패킷 인증 서버가 상기 사용자 단말기로 확인 메시지를 송신하는 단계: 및 (f) 상기 사용자 단말기가 상기 확인 메시지에 대해 응답을 상기 매직패킷 인증 서버로 송신하는 단계;를 포함한다.

[0009] 또한, 상기 (b) 단계에서 상기 사용자 단말기의 메인 전원이 켜지는 경우 상기 매직패킷 인증 서버가 상기 사용

자 단말기에 대한 모니터링을 종료하는 단계;를 더 포함하는 것이 바람직하다.

[0010] 아울러 상기 (d) 단계의 매직 패킷을 분석한 결과, 상기 원격 단말기의 IP가 허가되지 않은 IP인 경우, (d-1) 상기 매직패킷 인증 서버가 상기 사용자 단말기로 종료 코드를 송신하는 단계; (d-2) 상기 사용자 단말기가 자체의 메인 전원을 끄는 단계; 및 (d-3) 상기 매직패킷 인증 서버가 상기 사용자 단말기에 대한 모니터링을 다시 시작하는 단계;를 포함하는 것을 특징으로 한다.

[0011] 또한, 상기 (f) 단계에서 상기 사용자 단말기가 응답을 상기 매직패킷 인증 서버로 송신하지 않는 경우, (f-1) 상기 매직패킷 인증 서버가 상기 사용자 단말기로 종료 코드를 송신하는 단계; (f-2) 상기 사용자 단말기가 자체의 메인 전원을 끄는 단계; 및 (f-3) 상기 매직패킷 인증 서버가 상기 사용자 단말기에 대한 모니터링을 다시 시작하는 단계;를 더 포함하는 것이 바람직하다.

[0012] 본 발명의 바람직한 일실시예에 따른 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템은, 원격 단말기로부터 원격에서의 제어를 위한 매직패킷을 수신하여 자체의 메인 전원를 켜고, 매직패킷 인증 서버로 상기 매직패킷을 송신하는 사용자 단말기; 상기 매직패킷을 수신하여 분석하는 매직패킷 인증 서버;를 포함한다.

[0013] 또한 상기 매직패킷 인증 서버는, 상기 사용자 단말기의 메인 전원이 켜지는 경우, 상기 사용자 단말기에 대한 모니터링을 종료하는 것이 바람직하다.

[0014] 아울러, 상기 매직패킷 인증 서버는, 상기 매직패킷의 분석 결과, 상기 원격 단말기의 IP가 허가된 IP인 경우, 상기 사용자 단말기로 확인 메시지를 송신하고, 상기 사용자 단말기로부터 상기 확인 메시지에 대한 응답을 수신하는 것을 특징으로 한다.

[0015] 또한 상기 매직패킷 인증 서버는, 상기 사용자 단말기로부터 상기 확인 메시지에 대한 응답을 수신하지 못하는 경우, 상기 사용자 단말기로 종료 코드를 송신하고, 상기 사용자 단말기에 대한 모니터링을 다시 시작한다.

[0016] 아울러 상기 사용자 단말기는,상기 종료 코드를 수신하고, 자체의 메인 전원을 끄는 것을 특징으로 한다.

[0017] 구체적으로 상기 매직패킷 인증 서버는 상기 매직패킷의 분석 결과, 상기 원격 단말기의 IP가 허가되지 않은 IP인 경우, 상기 사용자 단말기로 종료 코드를 송신하고, 상기 사용자 단말기에 대한 모니터링을 다시 시작하는 것을 특징으로 한다. 또한, 상기 사용자 단말기는, 상기 종료 코드를 수신하고, 자체의 메인 전원을 끄는 것이 바람직하다.

[0018] 바람직한 일실시예에 따른 상기 매직패킷 인증 서버는, 상기 사용자 단말기가 속해 있는 네트워크 그룹의 관리자 서버와 동일한 것을 특징으로 한다.

발명의 효과

[0019] 본 발명의 매직패킷 인증 서버를 통한 허가되지 않은 WOL 보안 시스템 및 그 방법에 따르면, 해당 컴퓨터에 접근하는 모든 패킷을 모니터링하는 서버를 만들어 허가되지 않은 매직패킷에 대해 보안을 강화할 수 있다.

[0020] 또한, IPv4에서 확장되어 IPv6의 경우에도 컴퓨터를 포함한 모든 전자 기기에 대해 허가되지 않은 매직패킷에 대해 보안을 강화할 수 있다.

도면의 간단한 설명

[0021] 도 1은 매직패킷의 분석도이다.

도 2는 본 발명의 바람직한 일실시예에 따른 WOL 보안 시스템의 네트워크 상에서의 구조를 나타낸다.

도 3은 본 발명의 바람직한 일실시예에 따른 흐름도를 나타낸다.

도 4는 원격 단말기가 허가된 IP를 사용하는 인증된 단말기가 아닌 경우의 흐름도를 나타낸다.

도 5는 원격 단말기가 허가된 IP를 사용하는 인증된 단말기인 경우의 흐름도를 나타낸다.

도 6은 허가되지 않은 IP를 사용하는 원격 단말기가 헤더 파일의 변조를 통해 사용자 단말기에 접근하는 경우의 흐름도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하, 첨부된 도면을 참조하면서 본 발명의 일실시예에 따른 허가되지 않은 WOL 보안 시스템 및 그 방법에 대해 상세히 설명하기로 한다.

[0023] 본 발명의 하기의 실시예는 본 발명을 구체화하기 위한 것일 뿐 본 발명의 권리범위를 제한하거나 이를 한정하는 것이 아님은 물론이다. 본 발명의 상세한 설명 및 실시예로부터 본 발명이 속하는 기술분야의 전문가가 용이하게 유추할 수 있는 것은 본 발명의 권리범위에 속하는 것으로 해석된다.

[0024] 매직패킷이라는 신호는 데이터 링크 구간, 즉 OSI-LAYER 2를 통해서 발송된다. 이 부분은 브로드캐스트 되도록 되어 있어서 해당 네트워크 안에 있는 모든 기기들은 이러한 신호를 받게 된다. 구체적으로 매직패킷은 UDP 헤더 부분, FF-FF-FF-FF-FF-FF라는 부분 및 해당 기기의 16개의 맥(MAC) 어드레스의 구조로 되어 있다.

[0025] 도 1에 매직패킷을 분석해 놓았다.

[0026] 즉, 도 1은 맥 어드레스가 00-E0-4C-31-03-AC인 기기를 켜기 위해 발생시키는 매직패킷을 분석해 놓은 예시도이다. 도 1로부터 알 수 있는 바와 같이 2008년 1월 28일 3:01:11에 192.168.1.4라는 IP를 가진 컴퓨터에서 목적지 IP 192.168.1.255(브로드캐스트 주소)로 FF-FF-FF-FF-FF-FF와 16개의 00-E0-4C-31-03-AC의 구조를 가진 신호를 보내고 있다. 마지막에 00-00-00-00-00-00이 포함되어 있는 이유는 현재 이 기기가 Secure-On 기능이 있어서 패스워드 00-00-00-00-00-00이 있는 신호만을 받아들이기 때문이다.

[0027] 상기와 같은 매직패킷 신호를 활용하면 네트워크 안에 있는 모든 기기 중에서 맥 어드레스가 00-E0-4C-31-03-AC인 기기만이 켜지게 된다. 물론 맥 어드레스가 다른 나머지 기기들은 아무런 동작도 하지 않는다.

[0028] WOL에 쓰이는 신호, 예를 들면, 매직패킷의 특성상 네트워크 안에 있는 모든 기기는 신호를 받기 때문에 해당 네트워크 안에 신호 인증 서버를 둔다면 이러한 인증서버는 매직패킷을 받아서 분석할 수 있다.

[0029] 본 발명에서는 그 중 헤더 파일을 분석하여, 소스(Source) IP가 허가된 사용자인지 확인을 함으로써, 의도된 신호인지 확인을 수행한다.

[0030] 먼저, 도 2로부터 본 발명의 일실시예에 따른 허가되지 않은 WOL 보안 시스템의 네트워크 상에서의 구조를 알 수 있다.

[0031] 즉, 본 발명의 바람직한 일실시예에 따른 WOL 보안 시스템은, 라우터와 백본스위치에 의해 외부 네트워크와 연결된 네트워크 그룹에 위치한 사용자 단말기(10)와 매직패킷 인증 서버(20)를 포함한다.

[0032] 상기 사용자 단말기(10)는 컴퓨터, 휴대전화 등을 예로 들 수 있을 것이며, 다수의 사용자 단말기(10a, 10b, 10c)를 포함하며, 상기 매직패킷 인증 서버(20)는 상기 사용자 단말기(10)가 속해 있는 네트워크 그룹의 관리자 서버와 동일한 것(20b)일 수도 있고, 관리자 서버와는 별도(20a)로 구비될 수도 있다.

[0033] 도 3에 본 발명에 의한 바람직한 일실시예에 따른 흐름도를 나타내었다.

[0034] 도 3의 흐름도에 의해 본 발명에 대해 보다 구체적으로 설명하기로 한다.

[0035] 먼저, 원격 단말기가 사용자 단말기(10)의 원격에서의 제어를 위해 매직패킷을 상기 사용자 단말기(10)로 송신한다(S10). 상기 사용자 단말기(10)가 상기 매직패킷을 수신하고, 상기 사용자 단말기(10) 자체의 메인 전원을 켠다(S15).

[0036] 또한, 상기 사용자 단말기(10)의 메인 전원이 켜진 것을 상기 매직패킷 인증 서버(20)가 확인하면, 상기 매직패킷 인증 서버(20)의 상기 사용자 단말기(10)에 대한 모니터링이 종료되게 된다(S20).

[0037] 다음으로, 상기 사용자 단말기(10)가 매직패킷 인증 서버(20)로 상기 매직패킷을 송신하고(S25), 상기 매직패킷 인증 서버(20)가 상기 매직패킷을 수신하여 분석을 하게 된다(S30).

[0038] 상기 매직패킷 인증 서버(20)가 상기 매직패킷의 분석 결과, 상기 원격 단말기의 IP가 허가된 IP인지를 판단하고(S35), 허가된 IP인 경우 상기 매직패킷 인증 서버(20)가 상기 사용자 단말기(10)로 확인 메시지를 송신하고 상기 사용자 단말기(10)의 응답을 기다린다(S40). 만약 상기 사용자 단말기(10)가 상기 확인 메시지에 대해 응답을 상기 매직패킷 인증 서버(20)로 송신하면, 상기 매직패킷 인증 서버(20)는 아무런 후속 조치를 취하지 않는다(S60).

[0039] 만약, S35 단계에서 원격 단말기가 허가된 IP가 아니거나, S40 단계에서 상기 사용자 단말기(10)의 응답이 없거나 '아니오'라는 응답의 경우는 다음의 단계가 수행된다.

[0040] 즉, 상기 매직패킷 인증 서버(20)가 상기 사용자 단말기(10)로 종료 코드를 송신하고(S45), 상기 사용자 단말기(10)가 종료 코드에 의해 자체의 메인 전원을 끄게 된다(S50). 또한, 상기 매직패킷 인증 서버(20)가 상기 사용자 단말기(10)에 대한 모니터링을 재개하게 된다(S55).

[0041] S15 단계와 같이 상기 사용자 단말기(10)가 매직패킷을 송신하기 위해서는, 상기 사용자 단말기(10)의 메인 전원은 꺼져 있더라도, 네트워크 카드는 켜져 있는 상태로 있어야 한다는 것이 전제되어야 한다. 과거에는 네트워크 카드와 메인 보드가 분리되어 나왔기 때문에 3핀이라는 것을 통해 연결이 되어야만 사용이 가능하였다.

[0042] 하지만 최근 들어 네트워크 카드와 마더보드가 붙어 있는 일체형으로 나오고 있고, 게다가 그러한 장치는 대부분 WOL 기능을 내장하고 있다. 이와 같이 마더 보드와 네트워크 카드에서 WOL 기능을 지원한다면 CMOS 설정 단계에서 해당 관련 항목을 'ENABLE'로 바꾸어 주고, 네트워크 카드의 속성 중에서 매직 신호 기능을 체크 해주면 WOL 기능을 사용할 수도 있는 것이다. 이와 같이 관련된 설정이 완료 되었다면, 네트워크 안에 있는 해당 기기에 설정이 되어 있는 신호를 보내는 것만으로 간단히 작동이 가능해진다.

[0043] S20 단계와 같이 상기 사용자 단말기(10)의 메인 전원이 켜졌을 때, 상기 매직패킷 인증 서버(20)가 모니터링을 종료하는 것은 상기 사용자 단말기(10)가 켜져 있는 동안에는 많은 신호를 받기 때문에 상기 매직패킷 인증 서버(20)에서 그러한 모든 신호를 분석하다가 올 수 있는 과부하 현상을 방지하기 위한 것이다.

[0044] 도 4에 도 3의 흐름도에 대해 원격 단말기가 허가된 IP가 아닌 경우에 대한 흐름도만을 좀 더 자세히 나타내었다.

[0045] 즉, 도 4는 원격 단말기가 허가되지 않은 IP를 사용하여 헤더 파일의 변조 없이 상기 사용자 단말기(10)의 원격 제어를 시도하는 경우이다. 이 경우에는 S40 단계는 필요로 하지 않는다.

[0046] 그러나, 악의적인 사용자가 매직패킷의 헤더 파일을 변조하는 것에 의해, 헤더 파일의 IP를 관리자나 허가된 IP로 바꾸어 신호를 보낼 수도 있다. 이러한 공격을 막기 위하여 S40 단계와 같이 상기 사용자 단말기(10)의 확인 메시지에 대한 응답의 절차를 만든다. 즉, 관리자나 허가된 IP로부터 자신이 보냈다는 응답이 오면 올바른 과정이므로 별도의 조치를 취할 필요가 없고, 만약 그렇지 않다면 이는 악의적 사용자 혹은 인증받지 못한 접근 시도이므로 종료 코드를 보내는 것이다(S45). 이를 통해 매직패킷 신호의 변조 여부를 확인하고 이에 대한 대응조치를 취할 수 있는 것이다.

[0047] 도 5에 원격 단말기가 허가된 IP를 사용하는 인증된 단말기인 경우 및 도 6에 원격 단말기가 허가되지 않은 IP를 사용하되 헤더 파일의 변조를 통해 상기 사용자 단말기(10)에 접근하는 예제에 대해 좀 더 자세히 나타내었

다.

[0048] 도 5 및 도 6의 비교를 통해 알 수 있는 바와 같이 상기 S40 단계의 확인메시지를 보내고, 상기 사용자 단말기(10)의 응답을 송신 받는 절차에 의해 해당 매직패킷 신호의 헤더 파일이 변조의 방지가 가능하다.

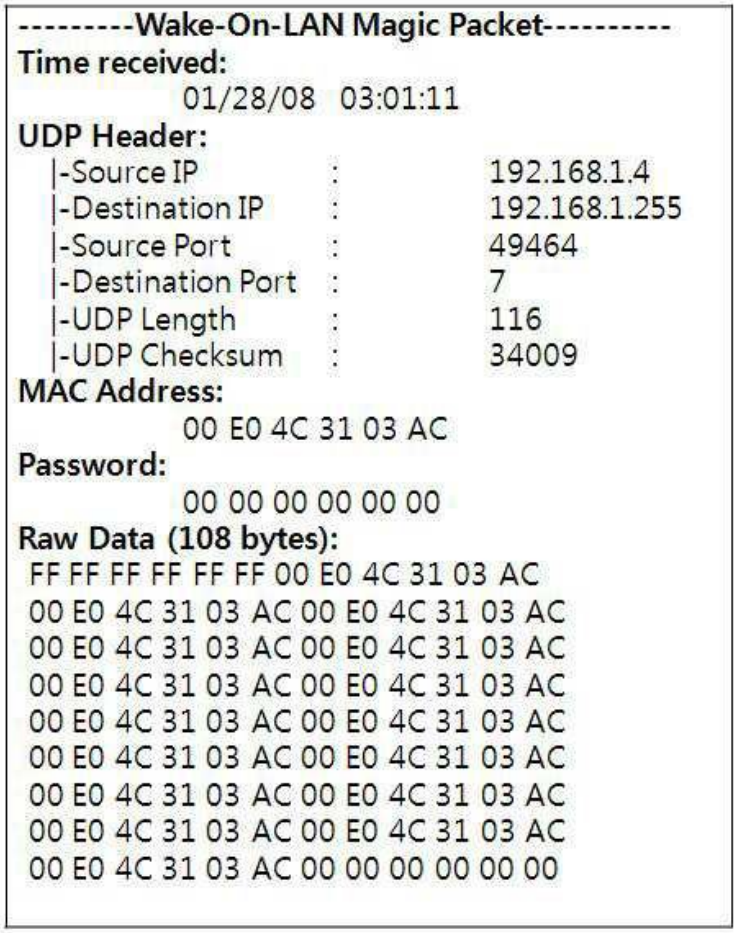
부호의 설명

[0049] 10, 10a, 10b, 10c : 사용자 단말기

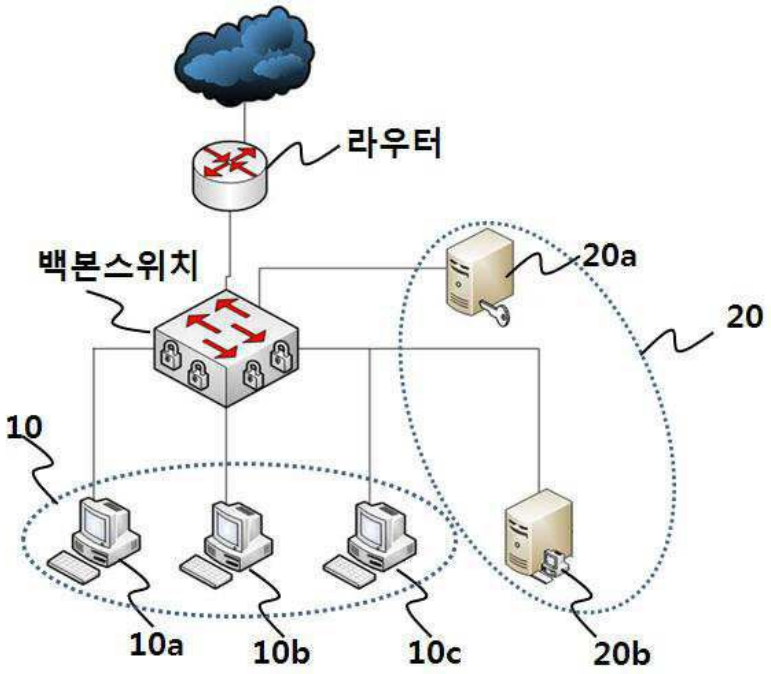
20, 20a, 20b : 매직패킷 인증 서버

도면

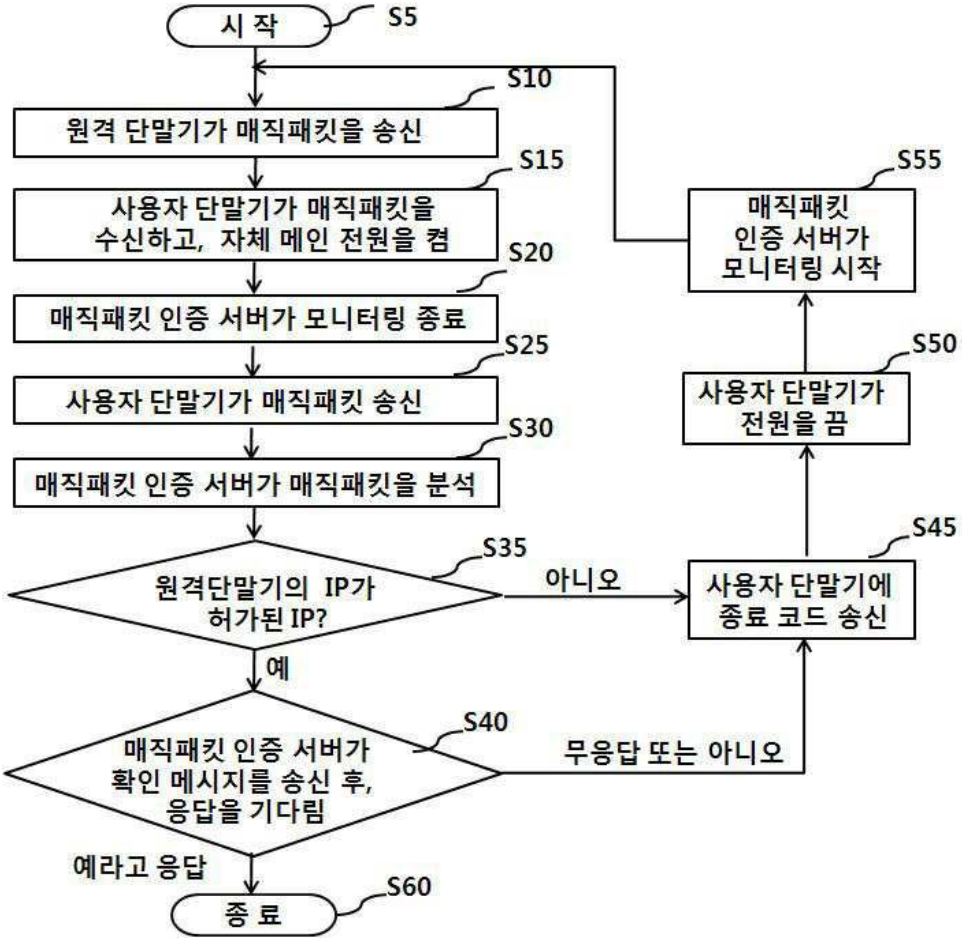
도면1



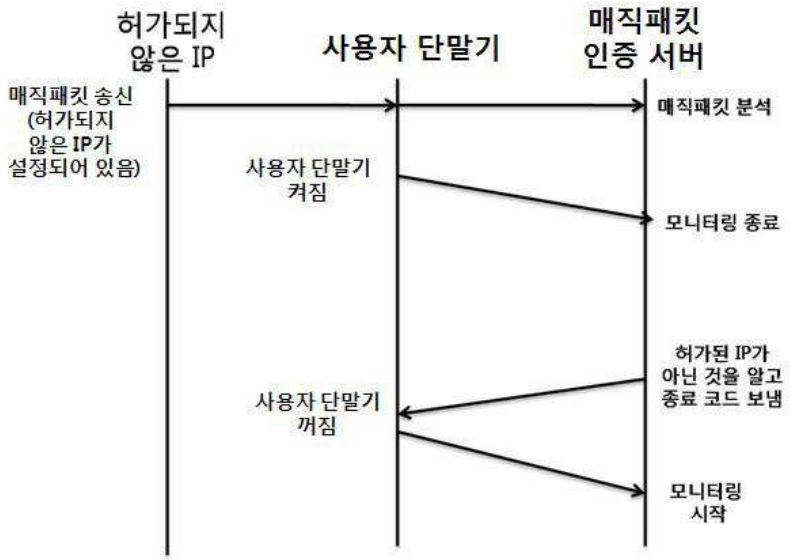
도면2


라우터
백본스위치
20a
20
10
10a
10b
10c
20b

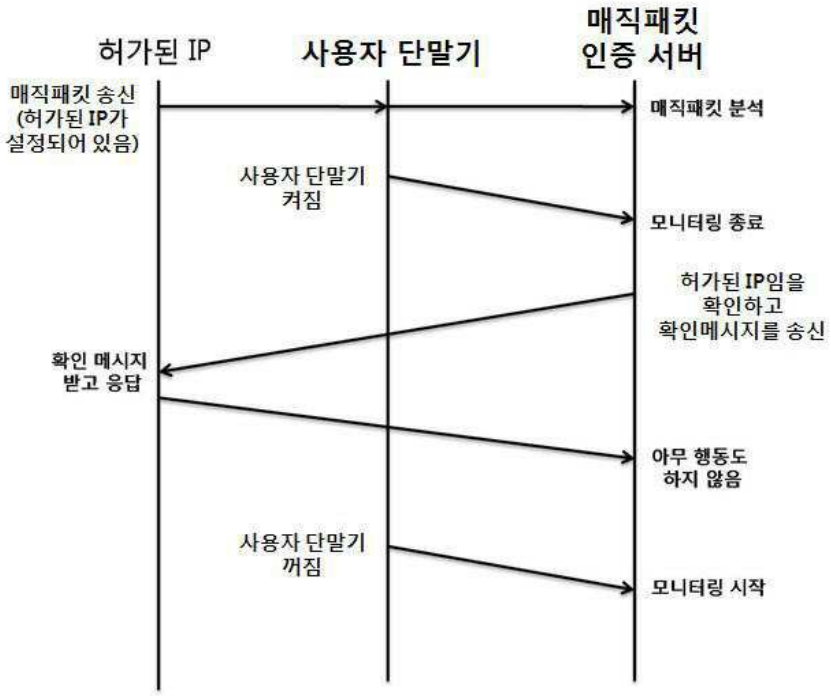
도면3


시 작
S5
S10
원격 단말기가 매직패킷을 송신
S15
사용자 단말기가 매직패킷을
수신하고, 자체 메인 전원을 켬
S20
매직패킷 인증 서버가 모니터링 종료
S25
사용자 단말기가 매직패킷 송신
S30
매직패킷 인증 서버가 매직패킷을 분석
S35
원격단말기의 IP가
허가된 IP?
아니오
예
S40
매직패킷 인증 서버가
확인 메시지를 송신 후,
응답을 기다림
무응답 또는 아니오
예라고 응답
종 료
S60
S45
사용자 단말기에
종료 코드 송신
S50
사용자 단말기가
전원을 끔
S55
매직패킷
인증 서버가
모니터링 시작

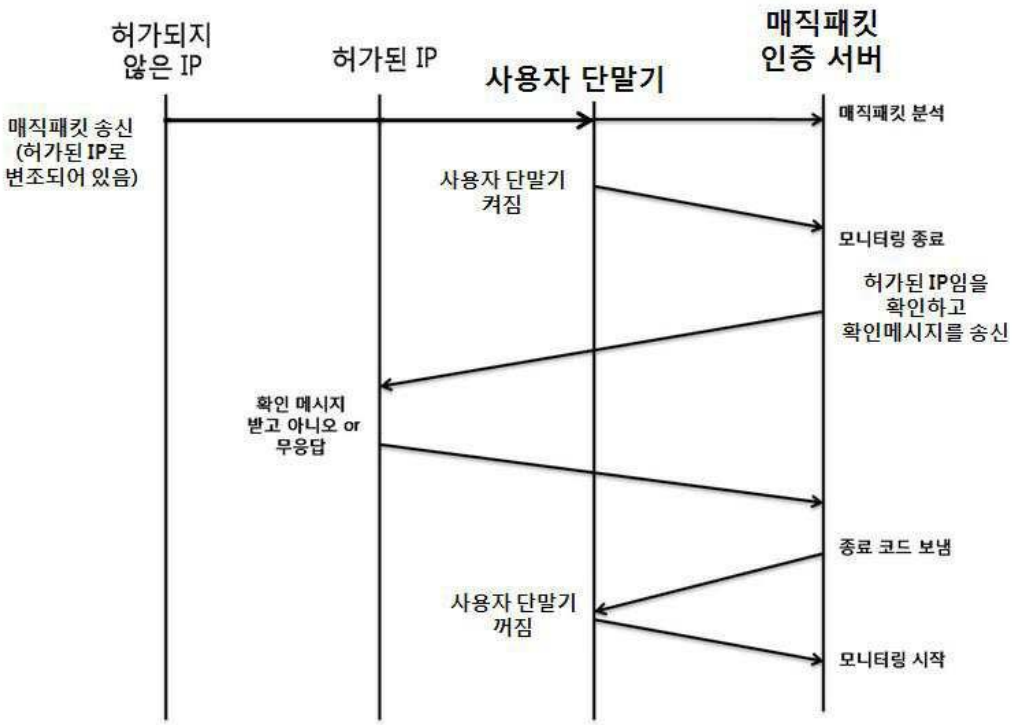
도면4


허가되지
않은 IP
사용자 단말기
매직패킷
인증 서버
매직패킷 송신
(허가되지
않은 IP가
설정되어 있음)
매직패킷 분석
사용자 단말기
켜짐
모니터링 종료
허가된 IP가
아닌 것을 알고
종료 코드 보냄
사용자 단말기
꺼짐
모니터링
시작

도면5


허가된 IP
사용자 단말기
매직패킷
인증 서버
매직패킷 송신
(허가된 IP가
설정되어 있음)
매직패킷 분석
사용자 단말기
켜짐
모니터링 종료
허가된 IP임을
확인하고
확인메시지를 송신
확인 메시지
받고 응답
아무 행동도
하지 않음
사용자 단말기
꺼짐
모니터링 시작

도면6


허가되지
않은 IP
허가된 IP
사용자 단말기
매직패킷
인증 서버
매직패킷 송신
(허가된 IP로
변조되어 있음)
매직패킷 분석
사용자 단말기
켜짐
모니터링 종료
허가된 IP임을
확인하고
확인메시지를 송신
확인 메시지
받고 아니오 or
무응답
종료 코드 보냄
사용자 단말기
꺼짐
모니터링 시작