(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0019457
(43) 공개일자 2018년02월26일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 21/55* (2013.01)
G06F 21/60 (2013.01)
(52) CPC특허분류
H04L 63/1483 (2013.01)
G06F 21/55 (2013.01)
(21) 출원번호 10-2016-0103838
(22) 출원일자 2016년08월16일
심사청구일자 없음

(71) 출원인
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
이종석
서울특별시 광진구 아차산로58길 78, 108호 (자양동)
이동훈
경기도 가평군 청평면 강변로 125
(74) 대리인
유미특허법인

전체 청구항 수 : 총 17 항

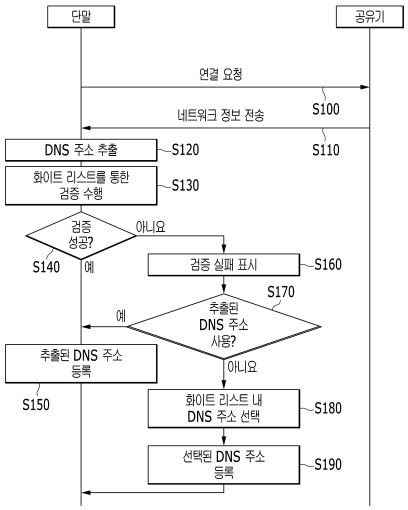
(54) 발명의 명칭 **공유기의 DNS 주소 변조를 통한 파밍 공격 방지 방법 및 단말**

(57) 요 약

공유기의 DNS 주소 변조를 통한 파밍 공격 방지 방법 및 단말이 개시된다.

이 방법에서 단말은 공유기로부터 DNS 주소를 포함하는 네트워크 정보를 수신한다. 그 후, 상기 네트워크 정보로부터 DNS 주소를 추출하여 검증을 수행하고, 상기 검증이 성공된 DNS 주소를 등록하여 사용한다. 상기 단말은 ISP 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있는 화이트 리스트를 포함한다. 구체적으로, 상기 단말은 상기 네트워크 정보로부터 추출된 DNS 주소와 상기 화이트 리스트에 등록되어 있는 DNS 주소를 비교하고, 상기 추출된 DNS 주소와 동일한 DNS 주소가 상기 화이트 리스트 내에 등록되어 있는 경우 상기 검증이 성공인 것으로 판단하며, 상기 추출된 DNS 주소와 동일한 DNS 주소가 상기 화이트 리스트 내에 등록되어 있지 않은 경우 상기 검증이 실패인 것으로 판단한다.

대 표 도 - 도2



(52) CPC특허분류
G06F 21/604 (2013.01)

명 세 서

청구범위

청구항 1

단말이 공유기의 DNS(Domain Name System) 주소 변조를 통한 파밍 공격을 방지하기 위한 방법으로서,

공유기로부터 DNS 주소를 포함하는 네트워크 정보를 수신하는 단계;

상기 네트워크 정보로부터 DNS 주소를 추출하여 검증을 수행하는 단계; 및

상기 검증이 성공된 DNS 주소를 등록하여 사용하는 단계

를 포함하는 파밍 공격 방지 방법.

청구항 2

제1항에 있어서,

상기 단말은 ISP(Internet Service Provider) 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있는 화이트 리스트(White List)를 포함하고,

상기 검증을 수행하는 단계는,

상기 네트워크 정보로부터 추출된 DNS 주소와 상기 화이트 리스트에 등록되어 있는 DNS 주소를 비교하는 단계;

상기 추출된 DNS 주소와 동일한 DNS 주소가 상기 화이트 리스트 내에 등록되어 있는 경우 상기 검증이 성공인 것으로 판단하는 단계; 및

상기 추출된 DNS 주소와 동일한 DNS 주소가 상기 화이트 리스트 내에 등록되어 있지 않은 경우 상기 검증이 실패인 것으로 판단하는 단계

를 포함하는, 파밍 공격 방지 방법.

청구항 3

제2항에 있어서,

상기 방법은,

상기 검증이 실패한 경우, 상기 화이트 리스트 내에 등록되어 있는 DNS 중에서 하나의 DNS 주소를 선택하여 등록하는 단계

를 더 포함하는 파밍 공격 방지 방법.

청구항 4

제3항에 있어서,

상기 하나의 DNS 주소를 선택하여 등록하는 단계는,

상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 상기 단말의 위치를 기반으로 필터링을 수행하는 단계; 및

상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 상기 필터링이 수행된 DNS 주소의 DNS 서버 각각에게 샘플 쿼리(sample query)를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 선택하여 등록하는 단계

를 포함하는, 파밍 공격 방지 방법.

청구항 5

제2항에 있어서,

상기 방법은,

상기 검증이 실패한 경우, 상기 추출된 DNS 주소의 검증 실패를 표시하는 단계;

상기 추출된 DNS 주소의 사용 여부를 문의하는 단계; 및

사용자의 지시에 따라 상기 추출된 DNS 주소를 등록하여 사용하는 단계

를 더 포함하는 파밍 공격 방지 방법.

청구항 6

제2항에 있어서,

상기 방법은,

외부의 DNS DB 서버로부터 상기 화이트 리스트의 업데이트 알림 메시지를 수신하는 단계; 및

사용자의 지시에 따라 상기 DNS DB 서버에 접속하여 상기 화이트 리스트의 업데이트를 수행하는 단계

를 더 포함하는, 파밍 공격 방지 방법.

청구항 7

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 DNS 주소는 NIC(Network Interface Card)에 등록하여 사용되도록 하는,

파밍 공격 방지 방법.

청구항 8

공유기의 DNS(Domain Name System) 주소 변조를 통한 파밍 공격을 방지하기 위한 단말로서,

공유기로부터 DNS 주소를 포함하는 네트워크 정보를 수신하는 제1 통신부; 및

상기 제1 통신부를 통해 수신되는 네트워크 정보로부터 DNS 주소를 추출하여 검증을 수행하고, 상기 검증이 성공된 DNS 주소를 등록하여 사용하는 처리부

를 포함하는 단말.

청구항 9

제8항에 있어서,

상기 처리부는,

ISP 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있는 화이트 리스트 DB;

상기 네트워크 정보로부터 DNS 주소를 추출하는 주소 추출부;

상기 DNS 주소 추출부에 의해 추출된 DNS 주소와 상기 화이트 리스트 DB에 등록되어 있는 DNS 주소를 비교하여 상기 추출된 DNS 주소의 검증을 수행하는 주소 검증부; 및

상기 주소 검증부에 의해 검증된 DNS 주소를 사용할 수 있도록 등록하는 주소 등록부

를 포함하는, 단말.

청구항 10

제9항에 있어서,

상기 단말은,

셀룰라 이동통신을 통해 외부의 서버에 접속되도록 통신을 수행하는 제2 통신부

를 더 포함하고,

상기 처리부는,

상기 제1 통신부를 통해 상기 공유기에 대한 접속을 수행하는 공유기 접속 수행부; 및

상기 제2 통신부를 통해 DNS DB 서버로부터 화이트 리스트의 업데이트 알림 메시지를 수신하는 경우, 상기 제2 통신부를 통해 상기 DNS DB 서버에 접속하여 상기 화이트 리스트 DB에 대한 업데이트를 수행하는 업데이트 처리부

를 더 포함하는, 단말.

청구항 11

제9항에 있어서,

상기 주소 등록부는, 상기 주소 검증부에 의해 상기 추출된 DNS 주소의 검증이 실패로 판단되는 경우, 상기 화이트 리스트 DB 내에 등록되어 있는 DNS 주소 중에서 하나의 DNS 주소를 선택하여 등록하는, 단말.

청구항 12

제11항에 있어서,

상기 처리부는,

상기 단말의 위치를 확인하여 제공하는 위치 확인부; 및

DNS 주소의 서버에게 쿼리를 전송하여 응답 시간을 측정하는 쿼리 발신부

를 더 포함하며,

상기 주소 등록부는, 상기 화이트 리스트 DB 내에 등록되어 있는 DNS 주소 중에서 상기 위치 확인부를 통해 확인되는 상기 단말의 위치를 기반으로 필터링을 수행하고, 필터링된 DNS 주소의 DNS 서버 각각에게 상기 쿼리 발신부를 통해 샘플 쿼리(sample query)를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 확인하여 등록하는,

단말.

청구항 13

제9항에 있어서,

상기 주소 등록부는, 상기 주소 검증부에 의해 상기 추출된 DNS 주소의 검증이 실패로 판단되는 경우, 상기 추출된 DNS 주소의 검증 실패를 사용자에게 표시하고, 사용자의 지시에 따라 상기 추출된 DNS 주소를 등록하는,

단말.

청구항 14

공유기의 DNS(Domain Name System) 주소 변조를 통한 파밍 공격을 방지하기 위한 단말로서,

제1 통신부, 메모리 및 프로세서를 포함하며,

상기 제1 통신부는 공유기로부터 DNS 주소를 포함하는 네트워크 정보를 수신하고,

상기 메모리는 상기 제1 통신부가 상기 공유기와 접속을 수행하도록 하는 프로그램, 및 상기 공유기의 DNS 주소 변조를 통한 파밍 공격을 방지하기 위한 프로그램을 저장하며,

상기 프로세서는 상기 메모리에 저장된 프로그램을 호출하여, 상기 제1 통신부를 통해 상기 공유기로부터 수신되는 네트워크 정보로부터 DNS 주소를 추출하고, 추출된 DNS 정보에 대한 검증을 수행하며, 상기 검증이 성공된 DNS 주소를 사용할 수 있도록 등록하는,

단말.

청구항 15

제14항에 있어서,

상기 메모리에는, ISP 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있는 화이트 리스트가 더 저장되며,

상기 프로세서는,

상기 화이트 리스트에 등록된 DNS 주소를 기반으로 상기 추출된 DNS 주소의 검증을 수행하고,

상기 추출된 DNS 주소의 검증이 성공인 경우 상기 추출된 DNS 주소를 등록하며,

상기 추출된 DNS 주소의 검증이 실패인 경우, 사용자의 지시에 따라서, 상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 하나의 DNS 주소를 선택하여 등록하거나, 또는 상기 추출된 DNS 주소를 등록하는,

단말.

청구항 16

제14항에 있어서,

상기 단말은,

셀룰라 이동통신을 통해 DNS DB 서버에 접속되도록 통신을 수행하는 제2 통신부

를 더 포함하고,

상기 프로세서는, 상기 제2 통신부를 통해 상기 DNS DB 서버로부터 화이트 리스트의 업데이트 알림 메시지를 수신한 후, 상기 제2 통신부를 통해 상기 DNS DB 서버에 접속하여 상기 화이트 리스트에 대한 업데이트를 수행하는,

단말.

청구항 17

제15항에 있어서,

상기 프로세서가 상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 하나의 DNS 주소를 선택하여 등록하는 경우, 상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 상기 단말의 위치를 기반으로 필터링을 수행하고, 필터링된 DNS 주소의 DNS 서버 각각에게 샘플 쿼리(sample query)를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 하나의 DNS 주소로 선택하여 등록하는,

단말.

발명의 설명

기 술 분 야

[0001] 본 발명은 공유기의 DNS 주소 변조를 통한 파밍 공격 방지 방법 및 단말에 관한 것이다.

배 경 기 술

[0002] 파밍이란 주소창의 URL(Uniform Resource Locator)은 정상이지만, 공격자(해커)가 만들어 놓은 가짜 사이트로 연결되도록 하는 악성 기법이다. 이러한 파밍에는 다양한 수법이 있으며 점차 교묘하게 진화하고 있다. 특히, 보안이 취약한 유/무선 공유기의 DNS(Domain Name System) 주소 변조를 통한 파밍 공격은 와이파이(WIFI)를 사용하려는 많은 사용자에게 피해를 준다.

[0003] 상기한 바와 같은 파밍 공격으로 인해 유/무선 공유기의 DNS 주소가 변조된 경우, 사용자가 유/무선 공유기에 연결할 때 공유기의 DHCP(Dynamic Host Configuration Protocol) 서버로부터 네트워크 정보를 수신하는데, 이 정보 중 DNS 주소가 해커로부터 변조되어 있어 결과적으로 변조된 DNS 주소를 사용하는 사용자는 공격자가 의도한 가짜 사이트 등으로로 연결하게 된다.

[0004] 따라서, 사용자가 접속을 원하는 유/무선 공유기가 공격자에 의해 해킹되어 DNS 주소가 변조된 상황에서도 사용자가 안전하게 네트워크를 이용할 수 있게 하기 위한 방법이 요구되고 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 이루고자 하는 기술적 과제는 공유기의 DNS 변조를 통한 파밍을 방지할 수 있는 파밍 공격 방지 방법 및 단말을 제공한다.

과제의 해결 수단

[0006] 본 발명의 한 특징에 따른 파밍 공격 방지 방법은,

[0007] 단말이 공유기의 DNS(Domain Name System) 주소 변조를 통한 파밍 공격을 방지하기 위한 방법으로서, 공유기로부터 DNS 주소를 포함하는 네트워크 정보를 수신하는 단계; 상기 네트워크 정보로부터 DNS 주소를 추출하여 검증을 수행하는 단계; 및 상기 검증이 성공된 DNS 주소를 등록하여 사용하는 단계를 포함한다.

[0008] 여기서, 상기 단말은 ISP(Internet Service Provider) 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있는 화이트 리스트(White List)를 포함하고, 상기 검증을 수행하는 단계는, 상기 네트워크 정보로부터 추출된 DNS 주소와 상기 화이트 리스트에 등록되어 있는 DNS 주소를 비교하는 단계; 상기 추출된 DNS 주소와 동일한 DNS 주소가 상기 화이트 리스트 내에 등록되어 있는 경우 상기 검증이 성공인 것으로 판단하는 단계; 및 상기 추출된 DNS 주소와 동일한 DNS 주소가 상기 화이트 리스트 내에 등록되어 있지 않은 경우 상기 검증이 실패인 것으로 판단하는 단계를 포함한다.

[0009] 또한, 상기 방법은, 상기 검증이 실패한 경우, 상기 화이트 리스트 내에 등록되어 있는 DNS 중에서 하나의 DNS 주소를 선택하여 등록하는 단계를 더 포함한다.

[0010] 또한, 상기 하나의 DNS 주소를 선택하여 등록하는 단계는, 상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 상기 단말의 위치를 기반으로 필터링을 수행하는 단계; 및 상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 상기 필터링이 수행된 DNS 주소의 DNS 서버 각각에게 샘플 쿼리(sample query)를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 선택하여 등록하는 단계를 포함한다.

[0011] 또한, 상기 방법은, 상기 검증이 실패한 경우, 상기 추출된 DNS 주소의 검증 실패를 표시하는 단계; 상기 추출된 DNS 주소의 사용 여부를 문의하는 단계; 및 사용자의 지시에 따라 상기 추출된 DNS 주소를 등록하여 사용하는 단계를 더 포함한다.

[0012] 또한, 상기 방법은, 외부의 DNS DB 서버로부터 상기 화이트 리스트의 업데이트 알림 메시지를 수신하는 단계; 및 사용자의 지시에 따라 상기 DNS DB 서버에 접속하여 상기 화이트 리스트의 업데이트를 수행하는 단계를 더 포함한다.

[0013] 또한, 상기 DNS 주소는 NIC(Network Interface Card)에 등록하여 사용되도록 한다.

[0014] 본 발명의 다른 특징에 따른 단말은,

[0015] 공유기의 DNS(Domain Name System) 주소 변조를 통한 파밍 공격을 방지하기 위한 단말로서, 공유기로부터 DNS 주소를 포함하는 네트워크 정보를 수신하는 제1 통신부; 및 상기 제1 통신부를 통해 수신되는 네트워크 정보로부터 DNS 주소를 추출하여 검증을 수행하고, 상기 검증이 성공된 DNS 주소를 등록하여 사용하는 처리부를 포함한다.

[0016] 여기서, 상기 처리부는, ISP 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있는 화이트 리스트 DB; 상기 네트워크 정보로부터 DNS 주소를 추출하는 주소 추출부; 상기 DNS 주소 추출부에 의해 추출된 DNS 주소와 상기 화이트 리스트 DB에 등록되어 있는 DNS 주소를 비교하여 상기 추출된 DNS 주소의 검증을 수행하는 주소 검증부; 및 상기 주소 검증부에 의해 검증된 DNS 주소를 사용할 수 있도록 등록하는 주소 등록부를 포함한다.

[0017] 또한, 상기 단말은, 셀룰라 이동통신을 통해 외부의 서버에 접속되도록 통신을 수행하는 제2 통신부를 더 포함하고, 상기 처리부는, 상기 제1 통신부를 통해 상기 공유기에 대한 접속을 수행하는 공유기 접속 수행부; 및 상기 제2 통신부를 통해 DNS DB 서버로부터 화이트 리스트의 업데이트 알림 메시지를 수신하는 경우, 상기 제2 통신부를 통해 상기 DNS DB 서버에 접속하여 상기 화이트 리스트 DB에 대한 업데이트를 수행하는 업데이트 처리부를 더 포함한다.

[0018] 또한, 상기 주소 등록부는, 상기 주소 검증부에 의해 상기 추출된 DNS 주소의 검증이 실패로 판단되는 경우, 상기 화이트 리스트 DB 내에 등록되어 있는 DNS 주소 중에서 하나의 DNS 주소를 선택하여 등록한다.

[0019] 또한, 상기 처리부는, 상기 단말의 위치를 확인하여 제공하는 위치 확인부; 및 DNS 주소의 서버에게 쿼리를 전송하여 응답 시간을 측정하는 쿼리 발신부를 더 포함하며, 상기 주소 등록부는, 상기 화이트 리스트 DB 내에 등록되어 있는 DNS 주소 중에서 상기 위치 확인부를 통해 확인되는 상기 단말의 위치를 기반으로 필터링을 수행하고, 필터링된 DNS 주소의 DNS 서버 각각에게 상기 쿼리 발신부를 통해 샘플 쿼리(sample query)를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 확인하여 등록한다.

[0020] 또한, 상기 주소 등록부는, 상기 주소 검증부에 의해 상기 추출된 DNS 주소의 검증이 실패로 판단되는 경우, 상기 추출된 DNS 주소의 검증 실패를 사용자에게 표시하고, 사용자의 지시에 따라 상기 추출된 DNS 주소를 등록한다.

[0021] 본 발명의 또 다른 특징에 따른 단말은,

[0022] 공유기의 DNS(Domain Name System) 주소 변조를 통한 파밍 공격을 방지하기 위한 단말로서, 제1 통신부, 메모리 및 프로세서를 포함하며, 상기 제1 통신부는 공유기로부터 DNS 주소를 포함하는 네트워크 정보를 수신하고, 상기 메모리는 상기 제1 통신부가 상기 공유기와 접속을 수행하도록 하는 프로그램, 및 상기 공유기의 DNS 주소 변조를 통한 파밍 공격을 방지하기 위한 프로그램을 저장하며, 상기 프로세서는 상기 메모리에 저장된 프로그램을 호출하여, 상기 제1 통신부를 통해 상기 공유기로부터 수신되는 네트워크 정보로부터 DNS 주소를 추출하고, 추출된 DNS 정보에 대한 검증을 수행하며, 상기 검증이 성공된 DNS 주소를 사용할 수 있도록 등록한다.

[0023] 여기서, 상기 메모리에는, ISP 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있는 화이트 리스트가 더 저장되며, 상기 프로세서는, 상기 화이트 리스트에 등록된 DNS 주소를 기반으로 상기 추출된 DNS 주소의 검증을 수행하고, 상기 추출된 DNS 주소의 검증이 성공인 경우 상기 추출된 DNS 주소를 등록하며, 상기 추출된 DNS 주소의 검증이 실패인 경우, 사용자의 지시에 따라서, 상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 하나의 DNS 주소를 선택하여 등록하거나, 또는 상기 추출된 DNS 주소를 등록한다.

[0024] 또한, 상기 단말은, 셀룰라 이동통신을 통해 DNS DB 서버에 접속되도록 통신을 수행하는 제2 통신부를 더 포함하고, 상기 프로세서는, 상기 제2 통신부를 통해 상기 DNS DB 서버로부터 화이트 리스트의 업데이트 알림 메시지를 수신한 후, 상기 제2 통신부를 통해 상기 DNS DB 서버에 접속하여 상기 화이트 리스트에 대한 업데이트를 수행한다.

[0025] 또한, 상기 프로세서가 상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 하나의 DNS 주소를 선택하여 등록하는 경우, 상기 화이트 리스트 내에 등록되어 있는 DNS 주소 중에서 상기 단말의 위치를 기반으로 필터링을 수행하고, 필터링된 DNS 주소의 DNS 서버 각각에게 샘플 쿼리(sample query)를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 하나의 DNS 주소로 선택하여 등록한다.

발명의 효과

[0026] 본 발명에 따르면, 공격자로부터 해킹된 유/무선 공유기에 접속하여도 안전하게 네트워크를 이용할 수 있다.

[0027] 또한, DNS 변조를 통한 개인정보 유출, 악성코드 삽입 등의 피해를 예방할 수 있다.

[0028] 또한, 와이파이 사용률이 높은 해외에서도 안전하게 네트워크를 이용할 수 있다.

도면의 간단한 설명

[0029] 도 1은 본 발명의 실시예에 따른 파밍 공격 방지 시스템의 개략 구성도이다.

도 2는 본 발명의 실시예에 따른 파밍 공격 방지 방법의 개략 흐름도이다.

도 3은 본 발명의 실시예에 따른 단말의 개략적인 구성 블록도이다.

도 4는 도 3에 도시된 처리부의 구체적인 구성 블록도이다.

도 5는 도 3에 도시된 처리부의 다른 구성의 구체적인 구성 블록도이다.

도 6은 본 발명의 다른 실시예에 따른 단말의 개략적인 구성 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0030] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 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.

[0031] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0032] 이하, 도면을 참조하여 본 발명의 실시예에 따른 공유기의 DNS 주소 변조를 통한 파밍 공격 방지 방법 및 단말에 대해 설명한다.

[0033] 도 1은 본 발명의 실시예에 따른 파밍 공격 방지 방법이 적용되는 시스템의 개략 구성도이다.

[0034] 도 1에 도시된 바와 같이, 본 발명의 실시예에 따른 파밍 공격 방지 방법이 적용되는 시스템은 단말(100), 공유기(200) 및 DNS DB 서버(300)를 포함한다.

[0035] 단말(100)은 공유기(200)에 유/무선으로 접속하여 공유기(200)를 통해 데이터를 송수신할 수 있는 장치이다. 특히, 단말(100)은 공유기(200)를 통해 인터넷(400)에 접속되어 다양한 서버를 통해 인터넷 서비스를 제공받을 수 있는 단말이다. 이러한 단말(100)은 공유기(200)에 유/무선으로 접속 가능한 데스크톱 컴퓨터, 개인용 컴퓨터, 노트북, 스마트폰, 스마트패드 등을 포함할 수 있다.

[0036] 공유기(200)는 AP(Access Point)라고도 하며, 사무실이나 가정에서 1개의 회선을 사용하여 외부의 네트워크, 특히 인터넷을 이용할 수 있도록 해주는 장치이다. 이러한 공유기(200)는 초기에는 유선을 이용하여 각종의 단말에 접속되는 유선 공유기였으나, 최근 무선 기술의 발전으로 인해 무선을 이용하여 단말에 접속이 가능한 무선 공유기, 유/무선 모두 접속 가능한 유/무선 공유기 중 하나일 수 있다.

[0037] 공유기(200)는 공유기(200)에 접속하는 단말에게 통신을 수행하기 위한 네트워크 구성 파라미터, 특히 IP 주소를 동적으로 할당하는 DHCP 서버의 기능을 포함할 수 있다.

[0038] 따라서, 단말(100)이 와이파이 연결을 위해 공유기(200)에 접속을 시도할 때 공유기(200)의 DHCP 서버는 단말(100)에서 사용할 IP 주소, DNS 주소, 게이트웨이 주소 등의 네트워크 정보를 단말(100)에게 할당하여 단말(100)이 해당 네트워크 정보를 사용하여 공유기(200)를 통해 데이터를 송수신할 수 있도록 한다.

[0039] 한편, 단말(100)은 ISP(Internet Service Provider) 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있는 화이트 리스트(White List)를 포함한다. 구체적으로는, 단말(100)에서 구동되는 애플리케이션 내의 DB에 화이트 리스트로서 저장되어 있다.

[0040] 단말(100)은 공유기(200)와의 와이파이 연결을 위해 공유기(200)에 접속을 시도할 때 공유기(200)로부터 제공되는 네트워크 정보를 수신하며, 수신되는 네트워크 정보로부터 DNS 주소를 추출하여 화이트 리스트에 포함된 DNS 주소와의 비교를 통해 추출된 DNS 주소의 검증을 수행한다. 구체적으로, 단말(100)은 추출된 DNS 주소가 화이트 리스트 내에 포함되어 있는 DNS 주소와 일치하는 주소가 있는 경우 추출된 DNS 주소의 검증이 성공인 것으로 판단한다. 그러나, 단말(100)은 추출된 DNS 주소가 화이트 리스트 내에 포함되어 있는 DNS 주소와 일치하는 주소가 없는 경우 추출된 DNS 주소의 검증이 실패인 것으로 판단한다.

[0041] 단말(100)은 공유기(200)에서 제공한 네트워크 정보로부터 추출된 DNS 주소의 검증 결과에 따라 추출된 DNS 주소의 사용 여부를 결정할 수 있다. 구체적으로, 단말(100)은 추출된 DNS 주소의 검증이 성공인 것으로 판단되면 추출된 DNS 주소를 사용할 수 있도록 설정할 수 있다. 예를 들어, 단말(100)은 검증 결과가 성공인 추출된 DNS 주소를 NIC(Network Interface Card)에 등록하여 사용할 수 있다.

[0042] 선택적으로, 단말(100)은 추출된 DNS 주소의 검증 결과가 실패인 경우 검증 결과를 사용자에게 표시하고, 사용자로부터의 선택에 따라 추출된 DNS 주소의 사용 여부를 결정할 수 있다. 예를 들어, 사용자가 검증 결과가 실패임에도 불구하고 추출된 DNS 주소를 사용하는 것으로 선택하는 경우, 단말(100)은 추출된 DNS 주소를 사용할 수 있도록 설정할 수 있다. 그러나, 사용자가 추출된 DNS 주소를 사용하지 않는 것으로 선택하는 경우, 단말

(100)은 화이트 리스트 내에 포함되어 있는 DNS 주소 중 하나를 선택하여 사용할 수 있도록 설정할 수 있다. 즉, 단말(100)은 화이트 리스트 내에 포함되어 있는 DNS 주소 중 하나를 선택하여 NIC에 등록한다. 이 때, 단말(100)은 화이트 리스트 내에 포함되어 있는 DNS 주소 중에서 단말(100)이 위치한 국가를 기반으로 DNS 주소를 1차 필터링하고, 그 후, 필터링된 DNS 주소의 DNS 서버 각각에게 샘플 쿼리(sample Query)를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 선택하여 사용할 수 있도록 설정할 수 있다. 한편, 상기에서 사용자에 대한 표시는 단말(100)의 디스플레이에 팝업을 통해 경고 메시지 형태로 수행될 수 있다.

[0043] DNS DB 서버(300)는 국내외 ISP 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소를 저장하여 관리한다.

[0044] DNS DB 서버(300)는 DNS 서버의 추가시 또는 DNS 서버의 주소 변경시에 업데이트될 수 있으며, 이러한 업데이트가 발생하는 경우 DNS DB 서버(300)는 단말(100)내에 있는 화이트 리스트에서의 업데이트를 위해 단말(100)에게 푸시(push) 메시지의 전송 등을 통해 업데이트 알림을 수행한다.

[0045] 단말(100), 특히 단말(100) 내 애플리케이션은 DNS DB 서버(300)로부터의 업데이트 알림에 따라 업데이트 알림 메시지를 푸시 메시지를 통해 사용자에게 표시한 후, 사용자의 요청에 따라 화이트 리스트에 대한 업데이트를 수행한다. 이 때, 단말(100)은 DNS DB 서버(300)로부터 전송된 푸시 메시지를 통해 DNS DB 서버(300)와 무선 통신 연결을 통해서 단말(100) 내 화이트 리스트의 업데이트를 수행할 수 있다.

[0046] 선택적으로, 단말(100)은 화이트 리스트에 대한 업데이트를 자동으로 수행할 수 있다. 예를 들어, 단말(100) 내 애플리케이션은 DNS DB 서버(300)로부터의 업데이트 알림이 있는 경우 이벤트 처리를 통해 DNS DB 서버(300)에 접속하여 자동으로 화이트 리스트에 대한 업데이트를 수행할 수 있다. 이 경우, 단말(100) 내 애플리케이션은 화이트 리스트에 대한 자동 업데이트 진행에 대해 사용자가 알 수 있도록 푸시 메시지를 통해 표시할 수 있다.

[0047] 도 2는 본 발명의 실시예에 따른 파밍 공격 방지 방법의 개략 흐름도이다.

[0048] 도 2를 참조하면, 단말(100)이 공유기(200)에서 브로드캐스팅되는 비콘(Beacon) 프레임을 통해 공유기(200)를 인식하거나 또는 기존에 접속하였던 공유기(200)의 정보로서 저장한 프로파일(profile)을 통해 공유기(200)를 인식하여 공유기(200)에게 연결을 요청한다(S100).

[0049] 연결 요청을 수신한 공유기(200)는 연결 요청에 대응하여 단말(100)이 사용할 IP 주소, DNS 주소, 게이트웨이 주소 등의 네트워크 정보를 단말(100)에게 전송한다(S110). 이 때, 상기 S100 단계와 S110 단계 사이에는 공유기(200)가 단말(100)에 대한 인증을 수행하고, DHCP 서버 주소 등의 정보를 제공하는 과정이 더 수행되지만 이에 대해서는 본 기술분야의 통상의 당업자라면 잘 알고 있을 것이므로 설명의 편의를 위해 구체적인 설명을 생략한다.

[0050] 다음, 단말(100)은 공유기(200)로부터 전송되어 수신되는 네트워크 정보로부터 DNS 주소를 추출한다(S120). 이러한 추출은 단말(100) 내에 애플리케이션이 백 그라운드(back ground)로 동작하는 중에 공유기(200)로부터의 네트워크 정보 수신 이벤트가 발생하는 경우 수행될 수 있으며, 구체적인 내용이 잘 알려져 있으므로 여기에서는 해당 설명을 생략한다.

[0051] 그 후, 단말(100)은 상기 단계(S120)에서 추출된 DNS 주소와 단말(100) 내에 저장되어 있는 화이트 리스트 내에 등록되어 있는 DNS 주소의 비교를 통해 추출된 DNS 주소에 대한 검증을 수행한다(S130). 이 때, 화이트 리스트에는 ISP 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있으며, 최신의 DNS 주소 정보가 DNS DB 서버(300)를 통해 업데이트되어 있다.

[0052] 구체적으로, 단말(100)은 추출된 DNS 주소와 화이트 리스트 내에 등록되어 있는 DNS 주소들 하나하나를 비교하여 추출된 DNS 주소가 화이트 리스트 내에 포함되어 있는지를 판단함으로써 상기한 검증을 수행할 수 있다.

[0053] 검증 결과, 검증이 성공한 것으로 판단되는 경우(S140), 단말(100)은 추출된 DNS 주소를 단말(100)이 사용할 수 있도록 설정한다(S150). 예를 들어, 단말(100)은 추출된 DNS 주소를 NIC에 등록하여 사용할 수 있다.

[0054] 그러나, 상기 단계(S140)에서 검증이 실패한 것으로 판단되는 경우, 즉 추출된 DNS 주소가 화이트 리스트 내에 없는 경우, 단말(100)은 추출된 DNS 주소에 대한 검증이 실패한 것으로 사용자에게 경고 메시지를 표시하고(S160), 검증이 실패한 추출된 DNS 주소를 사용하는 대신에 화이트 리스트 내에 있는 검증된 DNS 주소를 사용할 것인지를 문의한다(S170).

[0055] 만약 사용자가 화이트 리스트 내에 있는 검증된 DNS 주소를 사용하는 것을 선택하는 경우, 단말(100)은 화이트 리스트 내에 등록되어 있는 DNS 주소 중 하나를 선택하고(S180), 선택된 DNS 주소를 사용할 수 있도록 설정한다(S190). 즉, 단말(100)은 화이트 리스트 내에 포함되어 있는 DNS 주소 중 하나를 선택하여 NIC에 등록한다. 이 때, 단말(100)은 화이트 리스트 내에 포함되어 있는 DNS 주소 중에서 단말(100)이 위치한 국가를 기반으로 DNS 주소를 1차 필터링하고, 그 후, 필터링된 DNS 주소의 DNS 서버 각각에게 샘플 쿼리를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 선택하여 사용할 수 있도록 설정할 수 있다.

[0056] 한편, 상기 단계(S170)에서, 사용자가 검증이 실패한 추출된 DNS 주소를 사용하는 것으로 선택하는 경우, 추출된 DNS 주소를 등록하는 상기 단계(S150)를 수행한다.

[0057] 그 후, 단말(100)이 공유기(200)로부터 전달된 네트워크 정보를 사용하여 공유기(200)와의 연결을 완료하는 과정이 더 수행될 수 있으나, 이러한 과정은 본 발명에서의 특징에 해당되지 않으며, 또한 통상의 당업자라면 쉽게 이해할 것이므로 여기에서는 구체적인 설명을 생략한다.

[0058] 한편, 상기 단계(S100) 전에, 단말(100)은 인터넷(400)에 접속되어 있는 DNS DB 서버(300)를 통해 화이트 리스트를 최신 상태로 업데이트한 것이 가정되어야 한다. 구체적으로, 단말(100)은 DNS DB 서버(300)에서 DNS 주소의 업데이트가 필요한 경우 전송되는 푸시 메시지를 수신하는 경우, DNS DB 서버(300)와 무선 통신 연결을 통해서 접속한 후 DNS 주소의 최신 상태로의 업데이트를 수행한다. 선택적으로, 단말(100)은 DNS DB 서버(300)로부터 푸시 메시지 후에 전송되는 업데이트를 위한 DNS 주소가 포함되어 있는 메시지를 수신하여 단말(100) 내 화이트 리스트의 업데이트를 수행할 수도 있다.

[0059] 이하, 본 발명의 실시예에 따른 단말(100)의 구성에 대해 설명한다.

[0060] 도 3은 본 발명의 실시예에 따른 단말(100)의 개략적인 구성 블록도이다. 도 3에서는 설명의 편의상 본 발명의 특징과 관련없는 단말(100)의 일반적인 구성 및 그 동작에 대한 설명은 생략하였다.

[0061] 도 3에 도시된 바와 같이, 본 발명의 실시예에 따른 단말(100)은 제1 통신부(110), 제2 통신부(120) 및 처리부(130)를 포함한다.

[0062] 제1 통신부(110)는 공유기(200)와 유/무선으로 접속되어 데이터를 송수신하는 통신을 수행한다. 예를 들어, 제1 통신부(110)는 유/무선 랜(Local Area Network, LAN) 통신을 통해서 공유기(200)와 데이터 송수신을 수행할 수 있다.

[0063] 제2 통신부(120)는 셀룰라 이동통신을 통해 인터넷(400)에 접속하여 각종의 서버와의 데이터 송수신을 수행한다. 예를 들어, 제2 통신부(120)는 LTE(Long Term Evolution), 3G(3 Generation) 등의 통신을 통해서 외부의 서버와 데이터 송수신을 수행할 수 있다. 구체적으로, 제2 통신부(120)는 인터넷(400)을 통해 DNS DB 서버(300)와 접속하여 화이트 리스트의 업데이트를 위한 데이터를 송수신할 수 있다.

[0064] 처리부(130)는 제1 통신부(110)를 통해 공유기(200)에 접속할 때 공유기(200)로부터 전송되는 네트워크 정보를 수신하고, 수신되는 네트워크 정보로부터 DNS 주소를 추출한다. 그 후, 처리부(130)는 추출된 DNS 주소와 화이트 리스트 내에 있는 DNS 주소를 비교하여 추출된 DNS 주소를 검증한 후, 추출된 DNS 주소가 검증되면 시스템에 등록한다.

[0065] 처리부(130)는 추출된 DNS 주소의 검증이 실패하면 사용자의 선택에 따라서 추출된 DNS 주소를 등록하여 사용하거나, 또는 화이트 리스트 내에 있는 DNS 주소 중 하나를 선택하여 등록할 수 있다.

[0066] 또한, 처리부(130)는 제2 통신부(120)를 통해 DNS DB 서버(300)로부터 화이트 리스트의 업데이트를 위한 푸시 메시지를 수신하고, 사용자의 선택에 따라서 제2 통신부(120)를 통해 DNS DB 서버(300)에 접속하여 화이트 리스트에 대한 업데이트를 수행할 수 있다.

[0067] 상기한 동작을 위해 처리부(130)는 도 4와 같이 구성될 수 있다.

[0068] 도 4는 도 3에 도시된 처리부(130)의 구체적인 구성 블록도이다.

[0069] 도 4에 도시된 바와 같이, 처리부(130)는 화이트 리스트 DB(131), 공유기 접속 수행부(132), DNS 주소 추출부(133), DNS 주소 검증부(134), DNS 주소 등록부(135) 및 업데이트 처리부(136)를 포함한다.

[0070] 화이트 리스트 DB(131)에는 ISP 회사의 공식 DNS 서버의 주소와 국내외에서 검증된 주요 DNS 서버의 주소가 등록되어 있다. 이러한 화이트 리스트 DB(131)는 추후 설명되는 업데이트 처리부(136)를 통해 DNS DB 서버(300)

에서 관리되고 있는 최신의 DNS 주소를 등록하고 있도록 관리된다.

[0071] 공유기 접속 수행부(132)는 제1 통신부(110)를 사용하여 공유기(200)와 데이터 송수신을 위해 공유기(200)에 대한 유/무선 접속을 수행한다. 공유기(200)에 대한 접속은 일반적인 방식을 사용하여 수행되므로 여기에서는 구체적인 설명을 생략한다.

[0072] DNS 주소 추출부(133)는 공유기 접속 수행부(132)에 의해 단말(100)이 공유기(200)에 접속될 때 공유기(200)로부터 전송되는 네트워크 정보에서 DNS 주소를 추출한다.

[0073] DNS 주소 검증부(134)는 DNS 주소 추출부(133)에서 추출된 DNS 주소와 화이트 리스트 DB(131)에 등록되어 있는 DNS 주소를 비교하여 추출된 DNS 주소의 검증을 수행한다. 즉, DNS 주소 검증부(134)는 추출된 DNS 주소와 동일한 DNS 주소가 화이트 리스트 DB(131) 내에 등록되어 있는지를 판단하여 추출된 DNS 주소의 검증을 수행할 수 있다. 검증 결과 추출된 DNS 주소가 화이트 리스트 DB(131) 내에 등록되어 있으면 검증이 성공인 것으로 판단하고, 등록되어 있지 않으면 실패인 것으로 판단한다. 검증이 실패인 경우에는 공유기(200)의 DNS 주소가 파밍 공격에 의해 변조된 것으로 판단하게 되는 것이다.

[0074] DNS 주소 등록부(135)는 DNS 주소 검증부(134)에 의한 검증 결과에 따라 선택되는 DNS 주소를 등록한다. 예를 들어, DNS 주소 등록부(135)는 DNS 주소 검증부(134)에 의한 검증 결과가 성공인 경우 DNS 주소 추출부(133)에 의해 추출된 DNS 주소를 NIC에 등록할 수 있다. 또한, DNS 주소 등록부(135)는 DNS 주소 검증부(134)에 의한 검증 결과가 실패인 경우 사용자의 선택에 따라 추출된 DNS 주소를 등록하거나 또는 화이트 리스트 DB(131) 내에 등록되어 있는 DNS 주소 중에서 하나를 선택하여 등록할 수 있다.

[0075] 업데이트 처리부(136)는 제2 통신부(120)를 통해 DNS DB 서버(300)로부터 화이트 리스트 업데이트를 위한 푸시 메시지를 수신하고, 사용자의 선택에 따라서 제2 통신부(120)를 통해 DNS DB 서버(300)에 접속하여 최신의 DNS 주소로서 화이트 리스트 DB(131)를 업데이트할 수 있다.

[0076] 한편, 도 5에 도시된 바와 같이, DNS 주소 등록부(135)가 추출된 DNS 주소의 검증 실패로 인해 화이트 리스트 DB(131) 내에 등록되어 있는 DNS 주소 중에서 하나를 선택하는 경우, DNS 주소 중에서 단말(100)이 위치한 국가를 기반으로 DNS 주소를 1차 필터링하고, 필터링된 DNS 주소의 DNS 서버 각각에게 샘플 쿼리를 전송하여 가장 빠른 응답이 오는 DNS 서버의 DNS 주소를 선택하여 등록할 수 있다. 이를 위해, 처리부(130)는 단말의 위치를 확인할 수 있는 위치 확인부(137)와 DNS 주소의 서버에게 샘플 쿼리를 전송하여 응답 시간을 측정할 수 있는 쿼리 발신부(138)를 더 포함한다. 여기서, 위치 확인부(137)는 GPS(Global Positioning System)를 통해 단말(100)의 위치를 확인할 수 있다.

[0077] 도 6은 본 발명의 다른 실시예에 따른 단말(100)의 개략적인 구성 블록도이다.

[0078] 도 6에 도시된 바와 같이, 본 발명의 다른 실시예에 따른 단말(100)은 제1 통신부(110), 제2 통신부(120), 메모리(140) 및 프로세서(150)를 포함한다.

[0079] 제1 통신부(110) 및 제2 통신부(120)는 도 3에서 설명한 바와 동일한 기능을 수행하므로 여기에서는 중복하여 설명하지 않는다.

[0080] 메모리(140)는 본 발명의 실시예에 따른 공유기의 DNS 주소 변조를 통한 파밍 공격 방지를 위해 사용되는 애플리케이션의 프로그램 코드를 저장한다. 이 외에 메모리(140)는 단말(100)이 동작을 수행하는데 필요한 각종의 프로그램 코드 및 임시 메모리 공간을 제공할 수 있다. 이에 대해서는 잘 알려져 있으므로 구체적인 설명을 생략한다.

[0081] 프로세서(150)는 메모리(140)에 저장된 프로그램을 호출하여, 도 2를 참조하여 설명한 바와 같은 본 발명의 실시예에서 제안한 방법을 구현하도록 구성될 수 있다. 즉, 프로세서(150)는 제1 통신부(110)를 통해 공유기(200)에 접속할 때 공유기(200)로부터 전송되는 네트워크 정보를 수신하고, 수신되는 네트워크 정보로부터 DNS 주소를 추출한다. 그 후, 프로세서(150)는 추출된 DNS 주소와 화이트 리스트 내에 있는 DNS 주소를 비교하여 추출된 DNS 주소를 검증한 후, 추출된 DNS 주소가 검증되면 시스템에 등록한다. 또한, 프로세서(150)는 추출된 DNS 주소의 검증이 실패하면 사용자의 선택에 따라서 추출된 DNS 주소를 등록하여 사용하거나, 또는 화이트 리스트 내에 있는 DNS 주소 중 하나를 선택하여 등록할 수 있다. 또한, 프로세서(150)는 제2 통신부(120)를 통해 DNS DB 서버(300)로부터 화이트 리스트의 업데이트를 위한 푸시 메시지를 수신하고, 사용자의 선택에 따라서 제2 통신부(120)를 통해 DNS DB 서버(300)에 접속하여 화이트 리스트에 대한 업데이트를 수행할 수 있다.

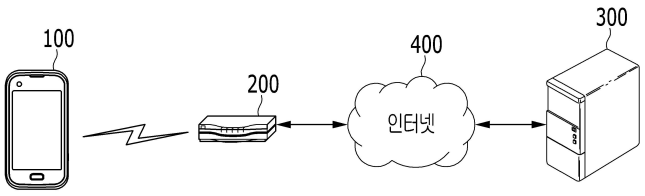
[0082] 이러한 프로세서(630)는 컨트롤러(controller), 마이크로 컨트롤러(microcontroller), 마이크로 프로세서

(microprocessor), 마이크로 컴퓨터(microcomputer) 등으로도 호칭될 수 있다. 또한, 프로세서(630)는 하드웨어(hardware) 또는 펌웨어(firmware), 소프트웨어, 또는 이들의 결합에 의해 구현될 수 있다.

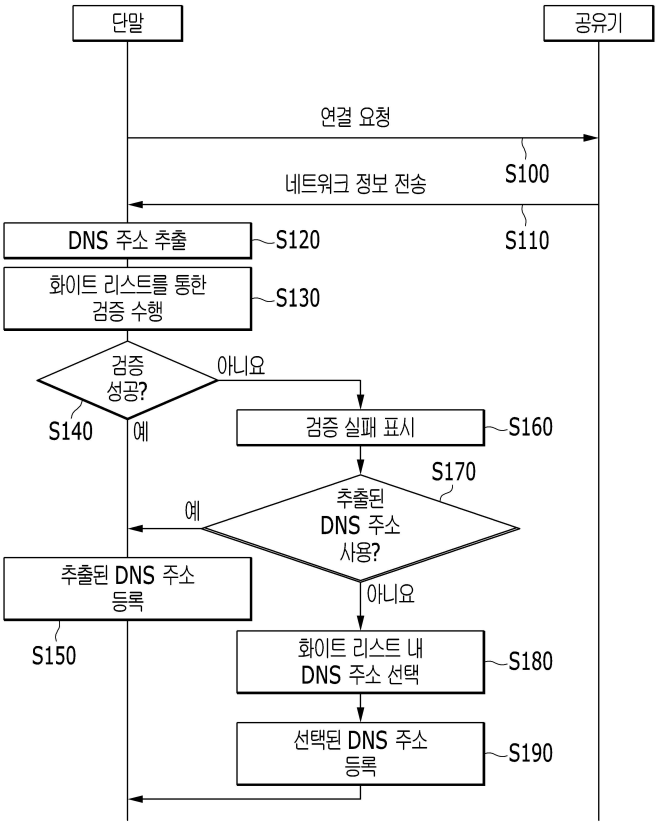
[0083] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

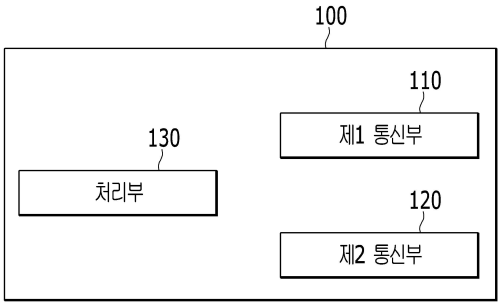
도면1



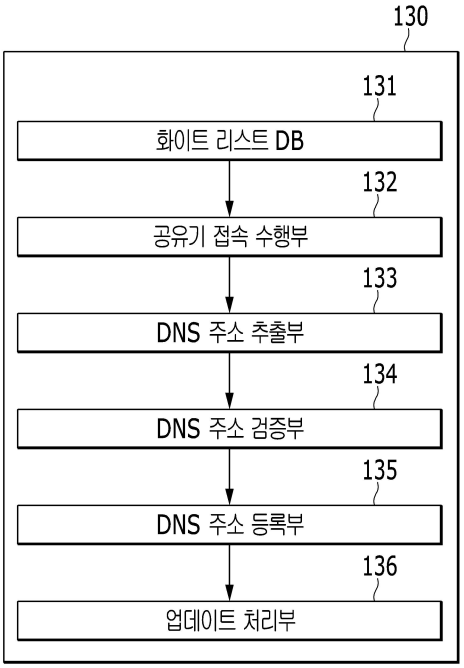
도면2



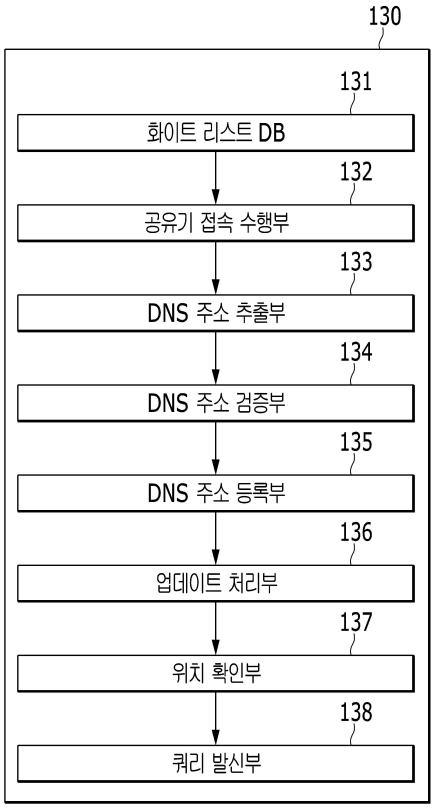
도면3


100
110
제1 통신부
130
처리부
120
제2 통신부

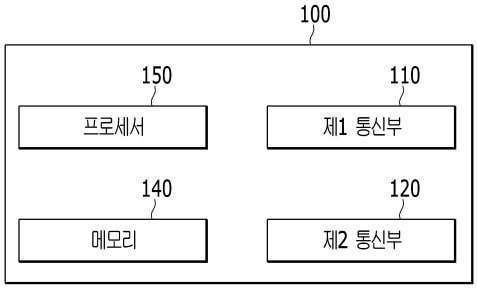
도면4


130
131
화이트 리스트 DB
132
공유기 접속 수행부
133
DNS 주소 추출부
134
DNS 주소 검증부
135
DNS 주소 등록부
136
업데이트 처리부

도면5


130
131
화이트 리스트 DB
132
공유기 접속 수행부
133
DNS 주소 추출부
134
DNS 주소 검증부
135
DNS 주소 등록부
136
업데이트 처리부
137
위치 확인부
138
쿼리 발신부

도면6


100
150
프로세서
110
제1 통신부
140
메모리
120
제2 통신부