(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0060005
(43) 공개일자 2017년05월31일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *H04L 12/26* (2006.01)
(52) CPC특허분류
H04L 67/1093 (2013.01)
H04L 43/065 (2013.01)
(21) 출원번호 10-2017-7007330
(22) 출원일자(국제) 2015년09월17일
심사청구일자 없음
(85) 번역문제출일자 2017년03월16일
(86) 국제출원번호 PCT/EP2015/071286
(87) 국제공개번호 WO 2016/042058
국제공개일자 2016년03월24일
(30) 우선권주장
14306449.1 2014년09월19일
유럽특허청(EPO)(EP)

(71) 출원인
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 잔 다르크 뤼 1-5
(72) 발명자
르 메레, 에르완
프랑스 35576 쎄쏭 쎄비녜 쎄에스 176 16 자크 데샹 블랑 975 아브뉘 데 샹 블랑 떼끄니꼴로르 에르 에 데 프랑스
르 스쿠아넥, 니꼴라
프랑스 35576 쎄쏭 쎄비녜 쎄에스 176 16 자크 데샹 블랑 975 아브뉘 데 샹 블랑 떼끄니꼴로르 에르 에 데 프랑스
뤼디나흐, 로마릭
프랑스 35042 헨느 세덱스 껑뿌스 위니베시테흐 드 보리우 앙스티튀 나시오날 드 흐세쉬 앙 앙포마띠끄 에 오토마띠끄 앙리아
(74) 대리인
양영준, 전경석, 백만기

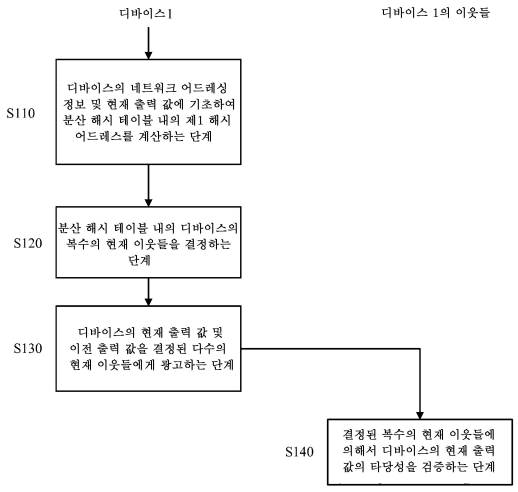
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **네트워크 시스템 및 네트워크 시스템 내의 디바이스에 의해 리턴되는 값의 타당성을 검증하는 방법**

(57) 요 약

디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법이 제공된다. 이것은 현재 시간 인스턴트에서의 디바이스의 이웃에 의해 디바이스의 현재 출력 값 및 이전 출력 값을 수신하는 단계(S410)와, 디바이스의 이웃에 의해 디바이스의 현재 출력 값 및 과거 출력 값 사이의 값 진화가 값 진화에 따라 타당성 없는지를 결정하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 43/10 (2013.01)
H04L 43/16 (2013.01)
H04L 67/125 (2013.01)

명 세 서

청구범위

청구항 1

디바이스로부터 수신된 값의 타당성(plausibility)을 검증하기 위한 방법으로서,

상기 디바이스의 이웃에 의해, 현재 시간 인스턴트에서 상기 디바이스의 현재 출력 값 및 이전 출력 값을 수신하는 단계(S410); 및

상기 디바이스의 상기 이웃에 의해, 상기 디바이스의 상기 현재 출력 값과 상기 이전 출력 값 사이의 값 진화(value evolution)가 상기 값 진화에 따라 타당성 없다고 결정하는 단계

를 포함하는 것을 특징으로 하는, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 2

제1항에 있어서,

상기 디바이스의 상기 이웃에 의해, 상기 디바이스로부터 이전 시간 인스턴트에서의 상기 디바이스의 이전 이웃들의 네트워크 어드레싱 정보 및 이전 출력 값들을 수신하는 단계(S610);

상기 디바이스의 상기 이웃에 의해, 상기 이전 이웃들 각각과 접촉하는 단계(S620);

상기 디바이스의 상기 이웃에 의해, 상기 이전 이웃들로부터 확인 응답들(acknowledges)을 수신하는 단계(S630); 및

상기 이전 이웃들로부터 수신된 긍정적인 확인 응답들의 수가 확인 응답 임계치(acknowledge threshold)에 도달하지 못하는 경우, 상기 디바이스의 상기 이웃에 의해, 상기 디바이스가 거짓말한다고 결정하는 단계(S650)

를 더 포함하는, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 3

제1항에 있어서,

상기 네트워크 어드레싱 정보는 IP 어드레스를 포함하거나, IP 어드레스 및 포트 번호를 포함하거나, 디바이스 ID, IP 어드레스 및 포트 번호를 포함하는, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 디바이스 및 상기 디바이스의 상기 이웃은 GPS 디바이스이고, 상기 디바이스의 상기 현재 출력 값은 현재 시간 인스턴트에서의 GPS 위치 값이며, 상기 디바이스의 상기 이전 출력 값은 이전 시간 인스턴트에서의 GPS 위치 값이고; 또는

상기 디바이스 및 상기 디바이스의 상기 이웃은 홈 게이트웨이이고, 상기 디바이스의 상기 현재 출력 값은 현재 시간 인스턴트에서의 평균 평가점(mean opinion score)이며, 상기 디바이스의 상기 이전 출력 값은 이전 시간 인스턴트에서의 평균 평가점인, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 5

디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법으로서,

상기 디바이스에 의해, 상기 디바이스의 네트워크 어드레싱 정보 및 현재 출력 값에 기초하여 분산 해시 테이블(distributed hash table) 내의 제1 해시 어드레스를 계산하는 단계(S110);

상기 디바이스에 의해, 상기 분산 해시 테이블 내의 복수의 현재 이웃들을 결정하는 단계(S120); 및

상기 디바이스에 의해, 상기 디바이스의 상기 현재 출력 값 및 상기 디바이스의 이전 출력 값을 결정된 복수의

현재 이웃들에게 광고하는 단계(S130)

를 포함하며,

상기 현재 출력 값 및 상기 이전 출력 값은 상기 디바이스의 상기 현재 출력 값의 타당성을 결정하기 위해 이용되는 것을 특징으로 하는, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 6

제5항에 있어서,

상기 결정된 복수의 현재 이웃들 각각에 의해, 상기 디바이스의 상기 현재 출력 값의 상기 타당성을 검증하는 것은,

상기 결정된 다수의 현재 이웃들 각각에 의해, 광고된 현재 출력 값과 광고된 이전 출력 값 사이의 값 진화가 값 진화 임계치보다 큰지 여부를 판단하는 단계(S430); 및

상기 값 진화가 상기 값 진화 임계치보다 큰 경우, 상기 결정된 복수의 현재 이웃들 각각에 의해, 상기 디바이스의 상기 값 진화가 타당성 없다고 결정하고 보고하는 단계(S440)

를 포함하는, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 7

제5항에 있어서,

상기 디바이스에 의해, 상기 디바이스의 이전 이웃들의 네트워크 어드레싱 정보를 상기 결정된 복수의 현재 이웃들에게 광고하는 단계

를 더 포함하며,

상기 결정된 복수의 현재 이웃들 각각에 의해, 상기 디바이스의 상기 현재 출력 값의 상기 타당성을 검증하는 것은,

상기 결정된 복수의 현재 이웃들 각각에 의해, 상기 이전 이웃들 각각과 접촉하는 단계;

상기 결정된 복수의 현재 이웃들 각각에 의해, 상기 이전 이웃 디바이스로부터 수신된 긍정적인 확인 응답의 수가 확인 응답 임계치에 도달하는지 여부를 판단하는 단계; 및

상기 이전 이웃 디바이스로부터 수신된 긍정적인 확인 응답들의 수가 상기 확인 응답 임계치에 도달하지 못하는 경우, 상기 결정된 복수의 현재 이웃들 각각에 의해, 상기 디바이스가 거짓말한다고 결정하고 보고하는 단계

를 더 포함하는, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 8

제5항에 있어서,

상기 네트워크 어드레싱 정보는 IP 어드레스를 포함하거나, IP 어드레스 및 포트 번호를 포함하거나, 디바이스 ID, IP 어드레스 및 포트 번호를 포함하는, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 9

제5항 내지 제8항 중 어느 한 항에 있어서,

상기 디바이스 및 상기 디바이스의 상기 이웃은 GPS 디바이스이고, 상기 디바이스의 상기 현재 출력 값은 현재 시간 인스턴트에서의 GPS 위치 값이며, 상기 디바이스의 상기 이전 출력 값은 이전 시간 인스턴트에서의 GPS 위치 값이고; 또는

상기 디바이스 및 상기 디바이스의 상기 이웃은 홈 게이트웨이이고, 상기 디바이스의 상기 현재 출력 값은 현재 시간 인스턴트에서의 평균 평가점이며, 상기 디바이스의 상기 이전 출력 값은 이전 시간 인스턴트에서의 평균 평가점인, 디바이스로부터 수신된 값의 타당성을 검증하기 위한 방법.

청구항 10

디바이스로부터 수신된 값의 타당성을 검증하기 위한 검증 디바이스로서,

상기 검증 디바이스는 현재 시간 인스턴트에서 상기 디바이스의 이웃이고, 상기 검증 디바이스는,

상기 디바이스의 현재 출력 값 및 이전 출력 값을 수신하기 위한 수신 모듈; 및

상기 디바이스의 상기 현재 출력 값과 상기 이전 출력 값 사이의 값 진화가 상기 값 진화에 따라 타당성 없다고 결정하기 위한 프로세서

를 포함하는 검증 디바이스.

청구항 11

제10항에 있어서,

상기 수신 모듈은, 상기 디바이스로부터 이전 시간 인스턴트에서의 상기 디바이스의 이전 이웃들의 네트워크 어드레싱 정보 및 이전 출력 값들을 더 수신하고, 상기 디바이스의 이전 이웃들로부터 확인 응답을 더 수신하기 위한 것이고,

상기 프로세서는, 상기 이전 이웃들로부터 수신된 긍정적인 확인 응답의 수가 확인 응답 임계치에 도달하지 못하는 경우, 상기 디바이스가 거짓말한다고 더 결정하기 위한 것인, 검증 디바이스.

청구항 12

통신 네트워크로부터 다운로드 가능하고 및/또는 컴퓨터에 의해 판독 가능한 매체 상에 기록되고 및/또는 프로세서에 의해 실행 가능한 컴퓨터 프로그램 제품(computer program product)으로서,

제1항 내지 9항 중 어느 한 항에 따른 방법의 단계들을 구현하기 위한 프로그램 코드 명령어들을 포함하는 것을 특징으로 하는 컴퓨터 프로그램 제품.

청구항 13

비일시적인 컴퓨터 판독 가능한 매체(non-transitory computer-readable medium)로서,

상기 컴퓨터 판독 가능한 매체 상에 기록되며, 프로세서에 의해 실행될 수 있고, 제1항 내지 9항 중 어느 한 항에 따른 방법의 단계들을 구현하기 위한 프로그램 코드 명령어들을 포함하는 컴퓨터 프로그램 제품(computer program product)

을 포함하는 컴퓨터 판독 가능한 매체.

발명의 설명

기 술 분 야

[0001] 본 개시 내용은 네트워크 내의 디바이스 관리에 관한 것이고, 구체적으로는 네트워크 시스템 내의 디바이스에 의해 리턴되는 값의 타당성(plausibility)을 검증(checking)하기 위한 네트워크 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 네트워크에는, 흔히 대규모 세트의 자율 디바이스들(autonomous devices)이 있으며, 자율 디바이스들 또는 자율 디바이스들 내의 특별한 어플리케이션들은 모니터링되는 서비스의 정상적인 동작을 보장하기 위해서 모니터링된다. 이러한 모니터링 컨텍스트(monitoring context)에서, 오퍼레이터(operator)는 모니터링되는 디바이스들로부터 신뢰할 수 있는 정보를 획득할 필요가 있고, 그 결과, 오퍼레이터는 발생하고 있는 문제들, 예를 들면, 전형적으로는 자율 디바이스가 예를 들어 홈 게이트웨일 때의 서비스 저하와 같은 것을 식별할 수 있다.

[0003] 그러나, 몇몇 특별한 모니터링되는 어플리케이션들이나 디바이스들은 신뢰될 수 없다. 예를 들어, 만족(gratification)이 보상되도록 하기 위해서, 그러한 어플리케이션이나 디바이스의 이용자는, 오퍼레이터에게 리턴되는 값(들)에 관해 거짓말을 하도록 어플리케이션이나 디바이스를 제어할 수 있다.

[0004] 예를 들어, 피어-투-피어(P2P) 네트워크에서, 특정 어플리케이션이나 디바이스는 그것이 항상 동작(operating) 중(또는 업)임을 나타내도록 오퍼레이터에게 값을 리턴하지만, 특정 어플리케이션이나 디바이스는, 예를 들면,

전기/대역폭을 절약하기 위해서, 실제로는 슬리핑(sleeping) 중(또는 다운)이다. 거짓말의 결과, 특정 어플리케이션이나 디바이스가 심지어 P2P 서비스에 참여하지 않는다는 사실에도 불구하고, P2P 서비스에 액세스 할 수 있을 것이다.

[0005] 오퍼레이터에게 리턴되는 값(들)에 관해 특정 어플리케이션이나 특정 디바이스가 거짓말을 하는지 여부를 인지하기 위해서, 논문 "AVMON : 분산 네트워크 시스템에 대한 일관된 이용 가능성 모니터링 오버레이들의 최적 및 확장 가능한 발견(Optimal and Scalable Discovery of Consistent Availability Monitoring Overlays for Distributed network systems)(IEEE TPDS 2009)"에는, P2P 네트워크 내의 어플리케이션들이 그들의 실제 이용 가능성(availability)에 대해서 거짓말하는 것을 회피하기 위한, 모니터링 접근법(monitoring approach)이 제안되었다. 이 논문에서, P2P 네트워크 내의 특정 P2P 네트워크 노드(즉, 어플리케이션 또는 디바이스)에 대해, P2P 네트워크 노드들(즉, P2P 어플리케이션들 또는 디바이스들)의 서브셋이 먼저 무작위로 선택되고, 후속적으로, 특정 P2P 네트워크 노드의 (PING을 사용하여) 측정 가능한 실제의 이용 가능성을 모니터링할 것을 요청받는다. 다시 말하면, 모든 P2P 네트워크 노드는 몇몇의 다른 P2P 네트워크 노드들에 의해 감독되고, 그 결과, P2P 네트워크 노드는 그것의 실제 이용 가능성에 관해 거짓말을 할 수 없다. 이러한 모니터링 접근법에서, 모니터링되는 값(여기서는, 노드 이용 가능성)은 외부적으로, 그리고 구체적으로는 PING 툴로 측정할 수 있어야 한다.

[0006] 그럼에도 불구하고, 외부적으로 측정될 수 없는, 모니터링되어야하는 광범위한 값들이 있다. 예를 들면, 이것은 Waze와 같은 협력 네비게이션 어플리케이션들(collaborative navigation applications)의 경우이고, 여기서, 스마트폰에 설치된 Waze 어플리케이션은 수시로 이용자의 GPS 위치(GPS position)를 제공한다. 이것은 또한 홈 게이트웨이들(home gateways) 내의 QoS (또는 QoE)에 대한 경우인데, 이 QoS는 게이트웨이 내의 많은 매개 변수(지터(jitter), 패킷 손실(packet loss), 소프트웨어 구성(software configuration) 등)의 복잡한 상호 작용으로 인하여 발생하고, 따라서 오퍼레이터에 의해 외부로부터 각각의 게이트웨이를 관찰하는 것에 의해서 외부적으로 평가될 수 없기 때문이다.

[0007] 특정 어플리케이션 또는 디바이스에서 특정 이득을 최대화하기 위해, 어플리케이션 또는 디바이스의 이용자는 잘못된 값들(false values)을 제공하는 것에 동기(incentive)를 가질 수 있다. 예를 들어, Waze 어플리케이션에서, 이용자의 GPS 장소(GPS location)가 아직 관찰되지 않은(yet-non-observed) 거리 또는 도로 상에 있다면 이용자는 크레딧(credit)을 얻고, 이것은 이용자가 그의 실제 위치에 관해 거짓말할 동기를 제공한다.

[0008] 따라서, 외부적으로 측정할 수는 없지만 특정 어플리케이션들이나 디바이스들에 의해 리턴되는 값들이 실제로 옳은지(또는 유효한지) 여부를 평가할 필요가 있고, 그렇지 않으면, 오퍼레이터는 값을 리턴하는 디바이스나 어플리케이션을 신뢰하도록 강요되고, 이는 전체 서비스의 오작동을 야기할 수 있다.

발명의 내용

[0009] 본 개시 내용의 실시예들의 일 양태에 따르면, 디바이스에 의해 리턴되는 값의 타당성을 검증하는 방법이 제공되고, 이 방법은 디바이스에 의해 네트워크 어드레싱 정보(예를 들어, IP 어드레스, 및 디바이스의 포트) 및 디바이스의 현재 출력 값에 기초하여 분산 해시 테이블(distributed hash table) 내의 제1 해시 어드레스를 계산하는 단계; 디바이스에 의해 분산 해시 테이블 내의 복수의 현재 이웃들을 결정하는 단계; 디바이스에 의해 디바이스의 현재 출력 값 및 디바이스의 이전 출력 값을 결정된 복수의 현재 이웃들에게 광고하는 단계; 및 결정된 복수의 현재 이웃들 각각에 의해 디바이스의 현재 출력 값의 타당성을 검증하는 단계를 포함한다.

[0010] 본 개시 내용의 실시예들의 다른 양태에 따르면, 디바이스에 의해 리턴되는 현재 출력 값의 타당성을 검증하는 방법이 제공되고, 이 방법은 디바이스의 이웃에 의해 현재 시간 인스턴트(time instant)에서 디바이스의 현재 출력 값 및 이전 출력 값을 수신하는 단계; 디바이스의 이웃에 의해 디바이스의 현재 출력 값과 이전 출력 값 사이의 값 진화(value evolution)가 미리 정의된 값 진화 임계치(predefined value evolution threshold)보다 큰지 여부를 판단하는 단계; 및 값 진화가 미리 정의된 값 진화 임계치보다 크면, 디바이스의 이웃에 의해 디바이스의 값 진화가 타당성 없는 것으로 결정하고 보고하는 단계를 포함한다.

[0011] 본 개시 내용의 실시예들의 다른 양태에 따르면, 복수의 모니터링되는 디바이스들을 포함하는 네트워크 시스템이 제공된다. 모니터링되는 디바이스들 각각에 대해, 모니터링되는 디바이스는 모니터링되는 디바이스의 네트워크 어드레싱 정보 및 현재 출력 값에 기초하여 분산 해시 테이블 내의 제1 해시 어드레스를 계산하고; 분산 해시 테이블 내의 복수의 모니터링되는 디바이스들 중에서, 모니터링되는 디바이스의 미리 정의된 수의 현재 이웃하는 모니터링되는 이웃들을 결정하고; 모니터링되는 디바이스의 현재 출력 값 및 이전 출력 값을 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스들에게 광고하며; 모니터 디바이스의 미리 정의된 수의 현재 이웃

하는 모니터링되는 디바이스들 각각에 대해, 현재 이웃하는 모니터링되는 디바이스는 모니터링되는 디바이스에 의해 리턴되는 현재 출력 값의 타당성을 검증한다.

[0012] 본 개시 내용의 실시들예의 다른 양태에 따르면, 통신 네트워크로부터 다운로드 가능하고 및/또는 컴퓨터에 의해 판독 가능한 매체(medium) 상에 기록되고 및/또는 프로세서에 의해 실행 가능한 컴퓨터 프로그램 제품(computer program product)이 더 제공되며, 이 컴퓨터 프로그램 제품은 위의 방법들 중 어느 하나의 단계들을 구현하기 위한 프로그램 코드 명령어들(program code instructions)을 포함한다.

[0013] 본 개시 내용의 실시예들의 다른 양태에 따르면, 디바이스에 의해 리턴되는 값의 타당성을 검증하기 위한 검증 디바이스(checking device)가 더 제공되며, 여기서 검증 디바이스는 현재 시간 인스턴트에서 디바이스의 이웃이고, 검증 디바이스는 디바이스의 현재 출력 값 및 이전 출력 값을 수신하기 위한 수신 모듈과; 디바이스의 현재 출력 값과 이전 출력 값 사이의 값 진화가 미리 정의된 값 진화 임계치보다 큰지 여부를 판단하고; 값 진화가 미리 정의된 값 진화 임계치보다 크면 디바이스의 값 진화가 타당성 없는 것으로 결정하고 보고하기 위한 프로세서를 포함한다.

[0014] 본 개시 내용의 실시예들의 다른 양태에 따르면, 프로세서에 의해 실행될 수 있는 컴퓨터 프로그램 제품이 기록되어 있는 비일시적인 컴퓨터 판독 가능한 매체(non-transitory computer-readable medium)가 더 제공되며, 이 컴퓨터 프로그램 제품은 위의 방법들 중 어느 하나의 단계들을 구현하기 위한 프로그램 코드 명령어들을 포함한다.

[0015] 본 개시 내용의 실시예들의 다른 양태에 따르면, 공격 디바이스(attacking device)(거짓말하는 디바이스(lying device))에 의한 리턴된 값을 통한 공격들은 공격 디바이스의 자원들을 소진시킬 수 있고, 보안 해시 함수(secure hash function)(예를 들어, SHA, MD5)의 이용에 의해 보장되는 분산 해시 테이블 내의 디바이스 위치의 무작위성(randomness)은, 공격 디바이스(거짓말하는 디바이스)가 잘못된 값에 대해 옳다는 평가를 얻기 위해 다른 거짓말쟁이들과 공모할 수 없다는 것을 보장하도록 영향력을 미친다(leveraged).

도면의 간단한 설명

[0016] 본 개시 내용의 실시예 또는 종래 기술의 기술적 해결 방안을 보다 명확하게 설명하기 위해서, 본 개시 내용의 실시예 또는 종래 기술의 설명에 필요한 도면들이 다음과 같이 간단히 소개된다. 다음의 설명되는 도면들은 단지 본 개시 내용의 몇몇 실시예를 설명할 뿐이고, 다른 도면들이 임의의 창의적 노력을 들이지 않고 이러한 도면들에 따라 획득될 수 있음은 본 기술분야의 통상의 기술자들에게 명백할 것이다.

도 1은 본 개시 내용의 실시예들에 따라 네트워크 내의 디바이스에 의해 리턴된 값의 타당성을 검증하기 위한 방법의 개략적인 흐름도이다.

도 2는 본 개시 내용의 실시예에 따른 분산 해시 테이블의 개략도이다.

도 3a 내지 도 3d는 본 개시 내용의 실시예들에 따라 네트워크 내의 디바이스에 의해 리턴된 값의 타당성을 검증하기 위한 방법의 단계들의 개략도이다.

도 4는 본 개시 내용의 실시예들에 따라 디바이스의 이웃에 의해 수행되는, 디바이스에 의해 리턴된 값의 타당성을 검증하는 방법의 개략적인 흐름도이다.

도 5a는 본 개시 내용의 실시예들에 따른 거짓말하는 디바이스의 타당성 없는(implausible) 이동의 개략도이다.

도 5b는 본 개시 내용의 실시예들에 따른 디바이스의 유효한 이동 순서(sequence)의 개략도이다.

도 6은 본 개시 내용의 실시예들에 따라 디바이스의 이웃에 의해 수행되는, 디바이스에 의해 리턴되는 값의 타당성을 검증하기 위한 방법의 다른 개략적인 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 개시 내용의 실시예의 기술적 해결 방안들을 명백히 그리고 충분히 설명하기 위하여, 이하에서, 첨부 도면들과 관련하여 본 개시 내용의 실시예들에 대해 상세한 설명이 이루어질 것이다. 명백히, 설명되는 실시예들은 본 개시 내용의 실시예들의 일부일 뿐이며, 본 개시 내용의 모든 실시예가 아니다. 어떠한 창의적 노력도 들이지 않고 본 개시 내용의 실시예들에 기초하여 본 기술분야의 통상의 기술자들에 의해 획득되는 모든 다른 실시예들은 본 개시 내용의 보호에 속한다.

[0018] 본 개시 내용에서, 우리는 분산 해시 테이블(distributed hash table)의 널리 공지된 개념을 통신 계층(communication layer)으로서 사용한다. 논문 "코드(Chord) : 인터넷 어플리케이션들을 위한 확장 가능한 P2P 조회 서비스(a scalable P2P lookup service for Internet applications)"에서, 분산 해시 테이블이 소개되어 있고, 그것은 P2P 네트워크 내의 각각의 디바이스가 소수의 다른 디바이스들에 접속하도록 허용하고 메시지들이 P2P 네트워크 내의 한 디바이스에서 다른 디바이스들로 라우팅되도록 허용한다. 흔히, P2P 네트워크 내의 각각의 네트워크 노드(즉, 어플리케이션 또는 디바이스)는 분산 해시 테이블 내에서 그의 위치를 얻기 위해 네트워크 어드레싱 정보(network addressing information)를 해시한다(hash). 네트워크 어드레싱 정보는 IP 어드레스, 또는 IP 어드레스와 포트 번호의 조합, 또는 디바이스 ID, IP 어드레스와 포트 번호의 조합, 또는 그 밖에 유사한 것을 포함할 수 있다. 또한, 포트 번호는 UDP 포트 번호 일 수 있다.

[0019] 본 출원의 실시예들에 따라 네트워크 내의 디바이스에 의해 리턴된 값의 타당성을 검증하기 위한 방법을 구체적으로 설명하기 전에, 디바이스(X)가 처음으로 새로운 노드로서 네트워크에 참여하는 경우에 수행되는 특정 프로토콜이 설명될 것이며, 구체적으로, 디바이스(X)는 코드 프로토콜(Chord protocol)을 통해서, 가입 명령(JOIN command)을 통하여 DHT의 라우팅 테이블들(routing tables) 내에 삽입되려고 시도한다.

[0020] DHT 내의 디바이스(X)의 최초 삽입을 위하여, 디바이스(X)는 중앙 서버에 접촉해야 한다. 비상실성 토큰(unforgettable token)이, 네트워크 오퍼레이터에 의해 제어되는 그 중앙 서버에 의해, 네트워크에 처음으로 새로 참여한 디바이스(X)에게 주어진다. 이 토큰은, 디바이스(X)에 의해 주장된 초기 값이 (초기의 것으로) 타당하고 디바이스(X)가 시스템 내에서 정말 새로운 것이라는 (디바이스(X)의 하드웨어 특성(예를 들면, 고유한 식별자)을 검증한 것에 의한) 중앙 서버에 의한 평가이다.

[0021] 후속적으로, 디바이스(X)가 네트워크에 새로운 것이며 그 증거는 이 주어진 토큰임을 선언하기 위해서, 이 토큰은 새로 참여된 디바이스(X)에 의해 DHT 내의 그의 새로운 이웃들에게 주어져야만 한다. 후속적으로, 디바이스(X)가 정말로 처음으로 네트워크에 참여하고 있는지 여부를 확인하기 위해 이러한 이웃들은 그 토큰을 갖고 중앙 서버에 직접 접촉할 수 있다. 디바이스(X)가 정말로 처음으로 네트워크에 참여하고 있다면 토큰은 유효하고, 그렇지 않으면, 토큰은 유효하지 않거나 이미 사용되었고 따라서 디바이스(X)는 거짓말을 하고 있는 것이다.

[0022] 유효한 토큰의 경우에, 주장된 초기 값은 이웃들에 의해 수용된다. 즉, 유효한 토큰의 경우에, 이웃들은 다른 부가적인 검사(verification)를 수행하지 않고 디바이스(X)의 주장된 초기 값을 수용한다.

[0023] 중앙 서버에 의해 주어진 토큰의 도움으로, 디바이스(X)가 자신이 지금 막 네트워크에 참여하였기에 이전 이웃들 및 값들을 갖지 않는다는 거짓말을 하는 것을 효과적으로 회피할 수 있다.

[0024] 도 1은 본 개시 내용의 실시예들에 따라 네트워크 내의 디바이스에 의해서 리턴되는 값의 타당성을 검증하기 위한 방법의 개략적인 흐름도이다.

[0025] 네트워크에는, 복수의 네트워크 노드들(즉, 어플리케이션들 또는 디바이스들)이 있으며, 이러한 네트워크 노드 각각은 네트워크 노드의 상태를 나타내기 위해 적어도 하나의 출력 값을 오퍼레이터에게 리턴하지만, 네트워크 노드의 적어도 하나의 출력 값의 적어도 일부는 네트워크 내의 다른 네트워크 노드들에 의해서 외부적으로 측정될 수 없거나 모니터링될 수 없다.

[0026] 먼저, 단계 S110에서, 디바이스의 네트워크 어드레싱 정보를 해싱(h(<네트워크 어드레싱 정보>))하는 대신에, 디바이스(디바이스1)는 디바이스의 네트워크 어드레싱 정보와 디바이스의 현재 출력 값, 즉 h(<네트워크 어드레싱 정보, 출력 값>)에 기초하여 분산 해시 테이블(DHT) 내의 제1 해시 어드레스(hash address)를 계산한다.

[0027] 본 개시 내용에서 출력 값의 단수형 형태(singular form)는 대응하는 복수형 형태(plural form)를 포함할 수 있다. 즉, 디바이스의 출력 값은 단일의 모니터링되는 출력 값일 수 있거나 복수의 모니터링되는 출력 값들의 조합일 수 있다.

[0028] 시간은 본 개시 내용의 실시예에서 이산화된다(discretized). 각각의 이산 시간 인스턴트(discretized time instant)에서, 분산 해시 테이블(DHT)은 각각의 디바이스 내에서 업데이트되고 라운드(round)에 의해 나타내어진다.

[0029] 도 2에 나타난 바와 같이, 특정 시간 인스턴트(time instant)(또는 시점(time point)이라고 지칭됨)에서, 디바이스(X)는 h(<IP, 포트, X의 값>)에 의해 정의된 위치를 갖고, 디바이스(Y)는 h(<IP, 포트, Y의 값>)에 의해 정의된 위치를 갖는다.

[0030] 단계 S120에서, 디바이스(디바이스1)는 분산 해시 테이블 내의 디바이스의 복수의 현재 이웃들(디바이스1의 이웃들)을 결정한다.

[0031] 본 개시 내용의 실시예에 따르면, DHT 내 디바이스 위치의 무작위성(randomness)은 디바이스의 네트워크 어드레싱 정보 및 출력 값에 대한 보안 해시 함수(예를 들어, SHA, MD5)의 이용에 의해 보장되고, 즉, 거짓말하는 노드가 잘못된 값에 대해 옳다는 평가를 얻기 위하여 다른 거짓말쟁이들과 공모할 수 없음이 보장될 수 있다.

[0032] 단계 S130에서, 디바이스는 디바이스의 현재 출력 값 및 이전 출력 값을 결정된 복수의 현재 이웃들(디바이스1의 이웃들)에게 광고한다.

[0033] 단계 S140에서, 결정된 복수의 현재 이웃들(디바이스1의 이웃들)은 디바이스(디바이스1)에 의해 리턴된 현재 출력 값의 타당성을 검증한다.

[0034] 다음으로, 본 개시 내용의 실시예들에 따라 디바이스에 의해 리턴된 현재 출력 값의 타당성을 검증하기 위한 방법의 동작들이 상세하게 설명될 것이다.

[0035] 도 3a 내지 3d는 본 개시 내용의 실시예들에 따라 네트워크 내의 디바이스에 의해 리턴된 현재 출력 값의 타당성을 검증하기 위한 방법의 단계들의 개략도이다.

[0036] 시간 인스턴트(t1)에서, 디바이스(X)는 출력 값(값1)을 가지고, 시간 인스턴트(t1)에서의 DHT 내의 디바이스(X)의 위치는, 해시 함수 h(<IP, 포트, X의 값1>)에 의해 정의된다. 도 3a에서, 시간 인스턴트(t1)에서의 DHT 내의 디바이스(X)의 위치는 검은색 원에 의해 나타내진다.

[0037] 시간 인스턴트(t1)의 바로 다음의 또 다른 시간 인스턴트(t2)에서, 디바이스(X)는 출력 값(값2)을 가지고, 시간 인스턴트(t2)에서의 DHT 내의 디바이스(X)의 위치는 해시 함수 h(<IP, 포트, X의 값2>)에 의해 정의된다. 도 3b에서, 시간 인스턴트(t1)에서의 DHT 내의 디바이스(X)의 위치는 점선 원(dash circle)에 의해 표현되고, 시간 인스턴트(t2)에서의 DHT 내의 디바이스(X)의 위치는 검은색 원에 의해 표현되며, 시간 인스턴트(t1)에서의 위치로부터 시간 인스턴트(t2)에서의 위치로의 이동은 점선 곡선(dash curve)에 의해 보여진다.

[0038] 즉, 디바이스(X)가 시간 인스턴트(t1)와 시간 인스턴트(t2) 사이에서 값1에서 값2로의 값 변화(value change)를 경험할 때, 디바이스(X)는 DHT 내의 h(<IP, 포트, X의 값>) 어드레스(위치)에 머물러야 하기 때문에, 따라서 DHT 내의 디바이스(X)의 장소(위치)는 변한다. 후속적으로, 디바이스(X)는 그에 따라 자신의 위치를 변경한다.

[0039] 점선 원(dash circle)에 의해 표현된 시간 인스턴트(t1)에서의 DHT 내의 디바이스(X)의 위치는, 도 3b에 나타난 시간 인스턴트(t2)의 라운드(round) 내에 실제로 존재하지 않음이 명백해야 하고, 점선 원은 단지 검은색 원으로 표현된 시간 인스턴트(t2)에서의 디바이스(X)의 위치와 비교하기 위해 보여진다. 마찬가지로, 점선 원은 도 3c 및 도 3d에 나타난 시간 인스턴트(t2)의 라운드 내에 실제로 존재하지 않는다.

[0040] 도 2, 도 3a, 및 도 3b에서는 네트워크 어드레싱 정보가 IP 어드레스(IP)와 포트 번호(Port)에 의해 표현되지만, 본 개시 내용의 실시예들은 이와 같이 제한되지 않는다.

[0041] 디바이스(X)가 시간 인스턴트(t2)에서 DHT 내의 자신의 새로운 위치를 계산할 때, 디바이스(X)는 시간 인스턴트(t2)에서 DHT 내의 자신의 인접한(immediate) 이웃들을 결정한다.

[0042] 여기서, N 개의 노드들(즉, 디바이스들)을 포함하는 네트워크에 대하여, 디바이스(X)는 시간 인스턴트(t2)에서 DHT 내의 자신의 인접한 O(logN) 개의 이웃들을 결정할 수 있다. 예를 들어, N=10000일 때, 디바이스(X)는 자신의 인접한 O(log(10000)) 개의 이웃들을 결정하고, 이는 소수의 유닛들(units)정도로 적은 것부터, 도 2c에 나타난 바와 같이 십이 약간 넘는 수(very few tens)의 이웃일 수 있다. 실제로, O(logN)은 이러한 프로토콜이 전개될(deployed)때 일단 고정될 필요가 있는 지시 값(indicating value)이다. 예를 들어, O(logN)는 실제로는 5*logN이 될 수 있다.

[0043] DHT 내의 O(logN) 개의 인접한 이웃들을 결정한 이후에, 디바이스(X)는 O(logN) 개의 인접한 이웃들에게 시간 인스턴트(t2)에서의 자신의 현재 출력 값(값2)과 시간 인스턴트(t1)에서의 자신의 이전 출력 값(값1)을 알린다.

[0044] 후속적으로, O(logN) 개의 인접한 이웃들은, 디바이스(X)의 현재 출력 값(값2)과 이전 출력 값(값1)에 기초하여, 디바이스(X)에 의해 리턴되는 현재 출력 값의 타당성을 검증한다.

[0045] 상술한 바와 같이, 기존의 DHT 방법에서 해시 어드레스(hash address)가 네트워크 어드레싱 정보에 기초하여 계산되는 것을 대신에, 새로운 파라미터(즉, 출력 값)가 보안 해시 함수(secure hash function)에 도입된다. 여

기서, 새로운 파라미터는 단일 파라미터일 뿐만 아니라, 두 개 이상의 파라미터의 조합일 수 있다. 즉, 출력 값은 디바이스(X)의 적어도 하나의 출력 값일 수 있다.

[0046] 이러한 방식에서, 디바이스(X)의 출력 값이 시간에 따라 변화되면, DHT 내의 디바이스(X)의 위치(장소) 또한 변화된다. 결과적으로, 디바이스(X)의 이웃들 또한 변화될 수 있고, 거짓말하는 노드가 잘못된 값에 대해 옳다는 평가를 얻기 위해 변경된 이웃들과 공모하는 것은 가능하지 않다.

[0047] 이제, 디바이스(X)의 임의의 하나의 이웃을 예로 들어서, 도 4 내지 도 6을 참조하여 디바이스(X)의 이웃들의 동작이 설명될 것이다.

[0048] 도 4는 본 개시 내용의 실시예들에 따라 디바이스의 이웃에 의해 수행되는, 디바이스에 의해 리턴된 현재 출력 값의 타당성을 검증하기 위한 방법의 개략적인 흐름도이다.

[0049] 단계 S410에서, 디바이스(X)의 이웃은, 디바이스(X)의 시간 인스턴트(t2)에서의 현재 출력 값(값2) 및 시간 인스턴트(t1)에서의 이전 출력 값(값1)을 수신한다.

[0050] 단계 S420에서, 디바이스(X)의 이웃은, 디바이스(X)의 시간 인스턴트(t2)에서의 현재 출력 값(제2 값)과 시간 인스턴트(t1)에서의 이전 출력 값(제1 값) 사이의 값 진화(value evolution)를 계산한다.

[0051] 단계 S430에서, 디바이스(X)의 이웃은, 값 진화가 미리 정의된 값 진화 임계치(predefined value evolution threshold)보다 큰지 여부를 판단한다.

[0052] 디바이스(X)의 시간 인스턴트(t2)에서의 현재 출력 값(값2)과 시간 인스턴트(t1)에서의 이전 출력 값(값1) 사이의 값 진화가 미리 정의된 값 진화 임계치보다 크다고 판단되면, 단계 S440에서, 디바이스(X)의 이웃은 디바이스(X)가 자신의 출력 값에 관하여 거짓말한다고 결정할 수 있다. 즉, 디바이스(X)는 타당성 없는 값 진화(implausible value evolution)를 보인다.

[0053] 디바이스(X)의 이웃이 디바이스(X)가 자신의 출력 값에 관하여 거짓말한다고 결정할 때, 디바이스(X)의 이웃은 또한 단계 S440에서, 디바이스(X)가 출력 값에 관하여 거짓말한다는 것을 오퍼레이터에게 보고할 수 있다.

[0054] 도 4에 나타난 바와 같이, 디바이스(X)의 이웃에 의해 수행되는, 디바이스(X)의 현재 출력 값의 타당성을 검증하기 위한 방법은, 현재 시간 인스턴트(t2)와 이전 시간 인스턴트(t1) 사이의 값 진화의 타당성에 의존한다.

[0055] 예를 들면, 만일 게이트웨이들 구역의 오퍼레이터(operator of a park of gateways)가 주어진 서비스(예를 들어, VoIP)의 하드웨어/소프트웨어 구현으로부터, 평균 평가점(MOS; mean opinion score)이 1분 미만에 3단위([1,…,5] 범위 내)를 초과하여 떨어질 수 없다는 것을 알아내고, 만일 게이트웨이가 4의 값을 보고한다면, 보고된 값이 거짓임을 아는 것은 대수롭지 않다. 마찬가지로, 만일 GPS 가능 추적 디바이스(GPS-enabled tracked device)가 현실적이지 않은 (물리적으로 너무 빠른) 위치 진화(position evolution)를 보고한다면, 보고된 위치 진화는 아마도 거짓일 것이다. 협력 네비게이션 어플리케이션을 고찰해 보면, 만일 이용자가 자신의 위치가 몇 분 전에 리턴된 자신의 이전 장소로부터 100 km에 있다고 주장한다면, 이 새롭게 리턴된 GPS 값이 잘못되었고 디바이스가 보상들(rewards)을 얻기 위해서 어플리케이션의 해킹을 시도한다는 것은 명백하다.

[0056] 만일 이전 시간 인스턴트(t1)로부터 현재 시간 인스턴트(t2)까지의 값 진화가 미리 정의된 값 진화 임계치를 초과한다면, 예를 들어, 상술한 게이트웨이의 값 진화가 1분 내에 미리 정의된 값 진화 임계치인 3을 초과했거나, 상술한 GPS 가능 추적 디바이스의 값 진화가 1분 내에 미리 정의된 값 진화 임계치인 10 km를 초과했다면, 이러한 값 진화는 모니터링된 값의 타당성 없는 진화(implausible evolution)라고 불려진다. 도 5a는 값 범위(value range) 내에서의 모니터링된 값의 타당성 없는 진화를 나타낸다.

[0057] 타당성 없는 값 진화와는 달리, 이전 시간 인스턴트(t1)에서의 이전 출력 값과 현재 시간 인스턴트(t2)에서의 현재 출력 값 사이의 타당한 값 진화(plausible value evolution)는 미리 정의된 값 진화 임계치보다 작아야 한다. 디바이스의 실제 문제(real problem) 또는 적당한 이동(legitimate movement)으로부터 유래하는 가장 개연성 있는 타당한 값 진화 순서(most probable plausible value evolution sequence)(즉, 유효한 이동 순서)가 도 5b에 나타나있다.

[0058] 도 4에 나타난 디바이스(X)의 이웃에 의해 수행되는, 디바이스(X)의 현재 출력 값의 타당성을 검증하기 위한 방법이, 값 진화가 모니터링되는 값의 타당성 없는 진화라고 판단할 때는, 모니터링되는 디바이스가 모니터링되는 값에 관하여 거짓말을 한다고 결정될 수 있다. 반대로, 도 3에 나타난 디바이스(X)의 이웃에 의해 수행되는, 디바이스(X)의 현재 출력 값의 타당성을 검증하는 방법이, 값 진화가 모니터링되는 값의 타당한 진화라고 판단

할 때는, 우리는 모니터링되는 디바이스가 모니터링되는 값에 관하여 거짓말을 하지 않는다고 결정할 수는 없다.

[0059] 따라서, 도 4에 나타난 방법은 공격 디바이스(attacking device)에 의해 리턴되는 값을 통한 공격들이 공격 디바이스(거짓말하는 디바이스)의 리소스들을 고갈시키도록 만드는 것을 보장한다. 그러나, 도 4에 나타난 방법은 도 5b에 나타난 (멀티-홉 및 순차적인) 순서(sequence)가 공격 디바이스(거짓말하는 디바이스)에 의해 생성되지 않는다는 것을 보증할 수는 없다.

[0060] 실제로, 공격자(공격 디바이스 또는 거짓말하는 디바이스)가 값 공간(value space) 내에서 이러한 일련의 값 진화들(시간 인스턴트(t1)에서의 초기 값으로부터 시간 인스턴트(tk)에서의 목표 값까지)을 모방하도록 강제하는 것은, 공격자의 리소스(예를 들면, 시간, 계산)를 소모시켜, 이러한 공격들의 확률이 상당히 감소되게 하도록 의도된 것이다.

[0061] 이 간단하고 비방해적인(non-intrusive)(따라서 좀 더 일반적인) 모델에서, 우리가 디바이스를 제어하지는 않지만, 우리는 이러한 방법으로 값 진화를 미리 정의된 값 진화 임계치보다 작게 만들게 함으로써 공격의 확률을 낮게 만들 수 있다.

[0062] 도 6은 본 개시 내용의 실시예에 따라 디바이스의 이웃에 의해 수행되는, 디바이스의 현재 출력 값의 타당성을 검증하기 위한 방법의 다른 개략적인 흐름도이다.

[0063] 단계 S610에서, 디바이스(X)의 이웃은 디바이스(X)로부터 이전 시간 인스턴트(t1)에서의 디바이스(X)의 이전 이웃들의 네트워크 어드레싱 정보 및 이전 값들을 수신한다.

[0064] 단계 S620에서, 디바이스(X)의 이웃은 DHT 내의 디바이스(X)의 이전 이웃의 위치에 따라 이전 이웃들 각각과 접촉한다. 예를 들어, 디바이스(X)의 이전 이웃의 위치는 h(<IP-이전-이웃(IP-pre-neighbor), 포트-이전-이웃(Port-pre-neighbor), 값-이전-이웃(Value-pre-neighbor)>)에 대응할 수 있고, 여기서 IP-이전-이웃 및 포트-이전-이웃은 이전 시간 인스턴트(t1)에서의 한 이전 이웃의 네트워크 어드레싱 정보를 나타내고, 값-이전-이웃은 이전 시간 인스턴트(t1)에서의 이전 이웃의 이전 출력 값을 나타낸다. 즉, 현재 시간 인스턴트(t2)에서의 디바이스(X)의 이웃은 이제 시간 인스턴트(t1)에서의 디바이스(X)의 이전 이웃의 네트워크 어드레싱 정보 및 이전 출력 값을 알기 때문에, 현재 시간 인스턴트(t2)에서의 디바이스(X)의 이웃은 이전 시간 인스턴트(t1)에서의 DHT 내의 디바이스(X)의 이전 위치의 O(logN) 개의 이웃들을 식별하고, 따라서 현재 시간 인스턴트(t1)에서의 디바이스(X)의 이전 이웃들 각각의 h(<IP-이전-이웃, 포트- 이전-이웃, 값-이전-이웃>)를 다시 계산할 수 있다.

[0065] 다시 말해서, 디바이스(X)가 값 변화(value change)를 가질 때, 디바이스(X)는 이전 시간 인스턴트(t1)에서의 자신의 이전 이웃들의 네트워크 어드레싱 정보를 전송할 뿐만 아니라, 이전 시간 인스턴트(t1)에서의 자신의 이전 이웃들의 이전 출력 값들을 현재 시간 인스턴트(t2)에서의 자신의 현재 이웃에게 전송한다. 따라서, 현재 시간 인스턴트(t2)에서의 디바이스(X)의 현재 이웃은, 네트워크 어드레싱 정보 (IP-이전-이웃 및 포트-이전-이웃)에 대응되는 이전 이웃이 실제로 여전히 이러한 계산된 장소(위치)에 있는지 여부를 검증하기 위해서, h(<IP-이전-이웃, 포트-이전-이웃, 값-이전-이웃>)를 계산할 수 있고, 후속적으로, t1에서 X가 주장하는 새로운 값이 정확한지를 알기 위해서, 이전 이웃에게 문의한다(interrogate). 이것은 t1에서의 X의 위치가 정확한지(즉, X가 t1에서 정말로 이러한 이웃 노드들의 이웃이었는지)를 평가함으로써 간단히 검증된다. 새로운 값을 주장하고 후속적으로 DHT 내의 새로운 어드레스를 얻는 노드는 자신의 새로운 이웃들에게 자신의 거짓말을 확인해줄 (실제로 공모하는) 노드들의 거짓 목록을 줄 수 없기 때문에, 이러한 이전 이웃들이 동일한 장소에 있다는 사실은, 공모하는 노드들(colluding nodes)을 방지한다. 따라서 프로토콜은, 노드들이 DHT 내에서 자신의 위치를 위조할 수 없고 후속적으로 자신들의 값들 또한 위조할 수 없다는 불변성(invariant)을 보존한다.

[0066] 단계 S630에서, 디바이스(X)의 이웃은 접촉된 이전 이웃들로부터 확인 응답(acknowledge)을 수신한다. 동시에, 디바이스의 이웃은 이전 시간 인스턴트(t1)에서 디바이스(X)의 이전 이웃들로부터 수신된 확인 응답을 카운트할 수 있다.

[0067] 단계 S640에서, 디바이스(X)의 이웃은, 이전 이웃들로부터 수신된 긍정적인 확인 응답들(positive acknowledges)의 수가 시스템의 역학(dynamics)(오래된 이웃들은 또한 그들의 이전 위치로부터 이동했을 수 있음), 및 시스템 내의 가능한 공모자들(colluders)의 수에 대한 경계에 의존하는 미리 정의된 확인 응답 임계치(predefined acknowledge threshold)에 도달했는지 여부를 판단한다.

[0068] 만일 이전 이웃들로부터 수신된 긍정적인 확인 응답들의 수가 미리 정의된 확인 응답 임계치에 도달하지 않는다고 결정되면, 단계 S650에서 디바이스(X)의 이웃은 디바이스(X)가 자신의 이전 이웃들에 관하여 거짓말한다고

결정할 수 있다. 디바이스(X)의 이웃이 디바이스(X)가 디바이스(X)의 이전 이웃들에 관하여 거짓말한다고 결정할 때, 디바이스(X)의 이웃은 또한 단계 S650에서 디바이스(X)가 이용 가능하지 않음을 오퍼레이터에게 보고한다.

[0069] 여기서, 미리 정의된 확인 응답 임계치는, 접촉된 이전 이웃들로부터의 대다수의 긍정적인 응답(a majority of positive answers)을 보장할 수 있거나, 대다수 마이너스 엡실론(ε)(majority minus epsilon (ε))일 수 있는데, 여기서 엡실론(ε)은 디바이스가 네트워크에서 사라지거나 접속이 끊어질 수 있거나 그들의 현재 출력 값에서의 변화로 인하여 이동할 수 있을 때의 네트워크 내의 디바이스들의 이탈(churn)에 의존하여 설정된다.

[0070] 이 방법에서, 네트워크 내의 디바이스들은 각각의 이동 또는 진화 단계에서 서로를 확장 가능한 방식(scalable fashion)으로 관찰하거나 모니터링할 수 있고, 디바이스(X)는 DHT 내의 자신의 현재의 인접한 O(logN) 개(또는 방법의 확장성을 보장하는 임의의 다른 수량)의 이웃들에게 이전 시간 인스턴트(t1)에서의 자신의 출력 값을 알려야 하고, DHT 내의 이전 시간 인스턴트(t1)에서 자신의 이전 이웃들에 대한 네트워크 질의(network querying)를 수행해야 한다. 우리는 디바이스를 직접 신뢰할 수 없기 때문에, 현재 시간 인스턴트(t2)에서의 디바이스(X)의 현재 이웃들은, 이전 시간 인스턴트(t1)에서의 디바이스(X)의 이전 이웃들이 디바이스(X)에 의해 알려진 값이 옳은지를 정말로 알고 있는지를 묻기 위해서, 이전 시간 인스턴트(t1)에서의 디바이스(X)의 이전 이웃들과 접촉해야 한다.

[0071] 상술한 방법에서, DHT에 의해 사용되는 해시 함수는 오버레이(overlay) 내의 각각의 단일 디바이스의 위치 무작위성(position randomness)을 보장하고 이에 따라 디바이스를 관찰/모니터링하는 디바이스의 이웃들의 무작위성을 보장한다.

[0072] 상술한 방법에서, 모니터링되는 네트워크 내의 모든 디바이스들은, 심지어 거짓말하는 노드들(디바이스들)이 존재하더라도, 값 진화(value evolution)를 평가하기 위해 협력한다. 상술한 방법은 모니터링되는 디바이스들의 세트에 걸쳐 분산되고, 후속적으로, 오퍼레이터들에게 저렴하다. 동등한 동작이 클라우드 유사 환경에서 중앙 집중식으로 이루어질 수 있으나, 이러한 탄력적인 서비스를 실행하는 데는 비용이 매우 많이 들 수 있다.

[0073] 부가적으로, 본 개시 내용의 다른 실시예들에서, 디바이스(X)의 위치의 주기적인 입증이 요구될 수 있다. 예를 들어, GPS 추적(tracking)의 경우에, 디바이스(X)는 디바이스(X)가 자신의 이웃의 Wifi 신호를 알고 있음을 입증할 필요가 있다. 디바이스(X)의 신뢰도는 각 라운드마다 느리게 감소하고, 디바이스(X)가 그의 위치에 대한 증거를 제공할 때마다 완전히 신뢰되도록 재설정된다.

[0074] 부가적으로, 본 개시 내용의 다른 실시예들에서, 디바이스(X)의 현재 이웃들은 이전 이웃들에 직접 접촉하는 대신에, 이전 이웃들에 의해 서명된(signed) 이전 위치의 증거들(evidences)을 사용할 수 있다.

[0075] 부가적으로, 몇몇 통신을 절약(save)하기 위해서, 검증(checking)은 확률에 의거할 수 있다.

[0076] 또한, 상술한 방법은 간단한 비방해적(non-intrusive) 소프트웨어 프로토콜에 기초하고, 이는 전문적인 하드웨어 또는 더 복잡한 암호화 프로토콜들을 도입할 필요없이도 거짓말하는 디바이스들을 금지하기에 충분하다.

[0077] 상술한 방법은 어플리케이션들/디바이스들의 값들의 진화의 타당성을 평가하기 위해 어플리케이션들/디바이스들의 값들을 정기적으로 체크포인트한다(checkpoint). 이 체크포인팅에서, 어플리케이션들/디바이스들은 분산 방식으로 자체 평가되고(self-evaluated), 이는 오퍼레이터가 계산 비용이 청구되며 후속적으로 비용이 거대해지는 클라우드와 같은 중앙 지점상에서 각각의 디바이스에 대해 많은 메트릭 진화(metric evolution)를 계산해야만하는 것을 방지한다.

[0078] 요약하면, 상술한 방법은 포괄적이고, 오퍼레이터 또는 관리 지점(management point)이 하나 또는 다수의 값들의 진화에 관한 정보를 도출하기 위해서(모니터링, 추적(tracing), 기록(logging)), 하나 또는 다수의 값들이 디바이스들 또는 어플리케이션들에 의해서 전송되는 폭넓고 다양한 상황에서 사용될 수 있다. 특히, 거짓말하는 디바이스가 잘못된 값을 전송할 때 중앙 오퍼레이터와 포인트-투-포인트 네트워크 통신을 수행하지 않고서 그 거짓말하는 디바이스가 네트워크로부터 버려지는 것이 관찰될 수 있다면, 상술한 방법이 이 디바이스들에서 구현될 가능성이 크다.

[0079] 또한, 본 개시 내용의 실시예들에 따르면, 복수의 모니터링되는 디바이스들을 포함하는 네트워크 시스템이 더 제공된다.

[0080] 모니터링되는 디바이스들 각각에 대해, 모니터링되는 디바이스는 네트워크 어드레싱 정보 및 모니터링되는 디바이스의 현재 출력 값에 기초하여 분산 해시 테이블 내의 제1 해시 어드레스를 계산하고; 분산 해시 테이블 내에

서 복수의 모니터링되는 디바이스들 중의 모니터링되는 디바이스의 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스들을 결정하고; 모니터링되는 디바이스의 현재 출력 값 및 이전 출력 값을 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스들에게 광고한다.

[0081] 모니터 디바이스의 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스들 각각에 대해, 현재 이웃하는 모니터링되는 디바이스는 모니터링되는 디바이스의 이용 가능성을 검증한다.

[0082] 선택적으로, 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스들 각각은, 광고된 현재 출력 값과 광고된 이전 출력 값 사이의 값 진화가 미리 정의된 값 진화 임계치보다 큰지 여부를 판단할 수 있고; 값 진화가 미리 정의된 값 진화 임계치보다 크다면, 모니터링되는 디바이스가 이용 가능하지 않다는 것을 결정하고 보고한다.

[0083] 선택적으로, 모니터링되는 디바이스는, 모니터링되는 디바이스의 제1 해시 어드레스 및 네트워크 어드레싱 정보를 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스들에게 더 광고한다. 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스들 각각은 모니터링되는 디바이스의 네트워크 어드레싱 정보 및 현재 출력 값에 기초하여 분산 해시 테이블 내의 제2 해시 어드레스를 더 계산하고; 제2 해시 어드레스가 제1 해시 어드레스와 상이하다면 모니터링되는 디바이스가 이용 가능하지 않다는 것을 결정하고 보고한다.

[0084] 선택적으로, 모니터링되는 디바이스는 이전 이웃하는 모니터링되는 디바이스들의 네트워크 어드레싱 정보를 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스들에 더 알린다. 미리 정의된 수의 현재 이웃하는 모니터링되는 디바이스 각각은 이전 이웃하는 모니터링되는 디바이스들 각각과 접촉하고; 이전 이웃하는 모니터링되는 디바이스들로부터 수신된 긍정적인 확인 응답들의 수가 미리 정의된 확인 응답 임계치(predefined acknowledge threshold)에 도달하는지 여부를 판단하고; 이전 이웃하는 모니터링되는 디바이스들로부터 수신된 긍정적인 확인 응답의 수가 미리 정의된 확인 응답 임계치에 도달하지 못하면 디바이스가 이용 가능하지 않다는 것을 결정하고 보고한다.

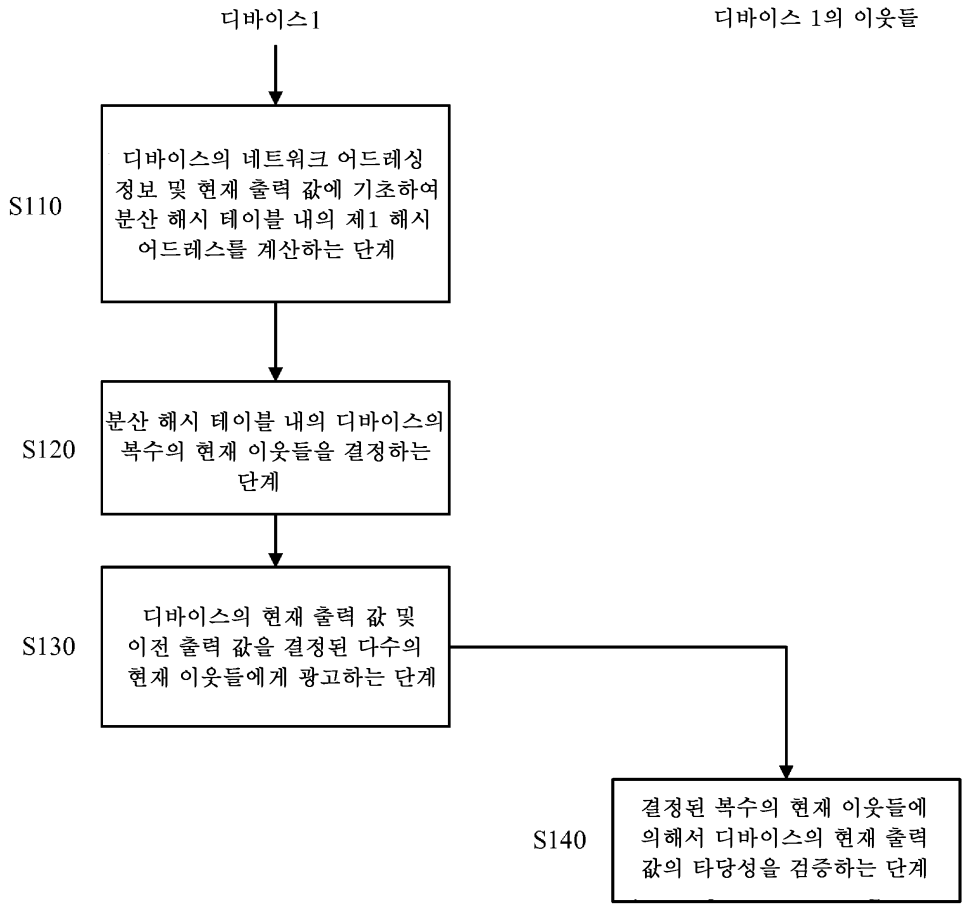
[0085] 구체적으로, 네트워크 시스템내의 복수의 모니터링되는 디바이스들의 수는 N이고, 이웃하는 모니터링되는 디바이스의 미리 정의된 수는 O(logN)이다.

[0086] 또한, 본 개시 내용의 실시예들에 따르면, 통신 네트워크로부터 다운로드 가능하고 및/또는 컴퓨터에 의해 판독 가능한 매체 상에 기록되고 및/또는 프로세서에 의해 실행 가능한 컴퓨터 프로그램 제품이 더 제공되며, 컴퓨터 프로그램 제품은 도 1, 도 4, 및 도 6 중 어느 하나를 참조하여 설명된 방법의 단계들을 구현하기 위한 프로그램 코드 명령어들을 포함한다.

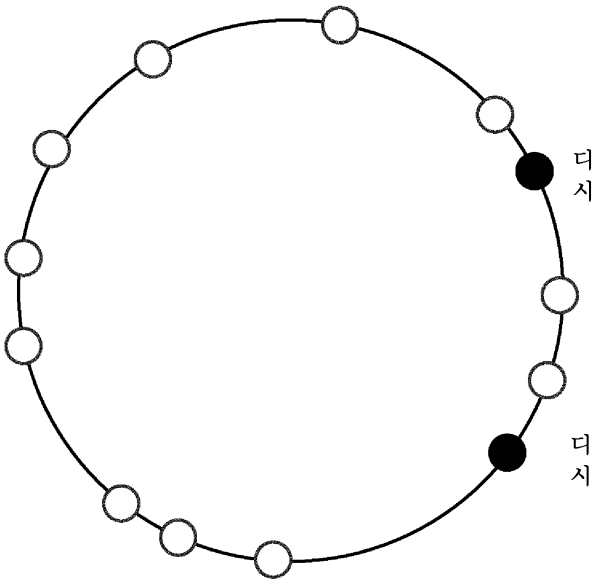
[0087] 또한, 본 개시 내용의 실시예들에 따르면, 프로세서에 의해 실행될 수 있는 컴퓨터 프로그램 제품이 기록되어 있는 비일시적인 컴퓨터-판독 가능한 매체가 더 제공되며, 이 컴퓨터 프로그램 제품은 도 1, 도 4, 및 도 6 중 어느 하나를 참조하여 설명된 방법의 단계들을 구현하기 위한 프로그램 코드 명령어들을 포함한다. 위의 실시예들은 본 개시 내용의 원리를 설명하기 위한 것일 뿐이며, 본 개시 내용의 범위를 결코 제한하지 않는다. 본 기술분야의 통상의 기술자들은 후속하는 청구항들에 의해 정의된 바와 같은 본 개시 내용의 범위를 벗어나지 않고 위의 실시예들에 대한 수정들, 변형들 및 등가물을 만들 수 있음은 명백할 것이다. 이러한 변형들 및 수정들은 본 개시 내용의 범위 내에 포함되는 것으로 의도된다.

도면

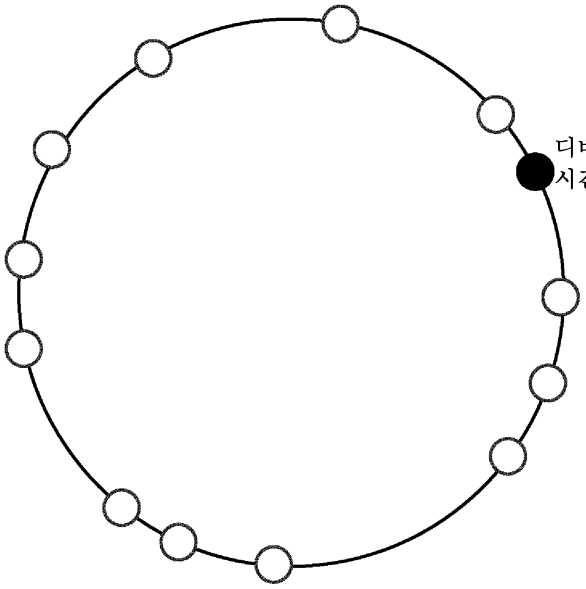
도면1


디바이스1
디바이스 1의 이웃들
S110
디바이스의 네트워크 어드레싱 정보 및 현재 출력 값에 기초하여 분산 해시 테이블 내의 제1 해시 어드레스를 계산하는 단계
S120
분산 해시 테이블 내의 디바이스의 복수의 현재 이웃들을 결정하는 단계
S130
디바이스의 현재 출력 값 및 이전 출력 값을 결정된 다수의 현재 이웃들에게 광고하는 단계
S140
결정된 복수의 현재 이웃들에 의해서 디바이스의 현재 출력 값의 타당성을 검증하는 단계

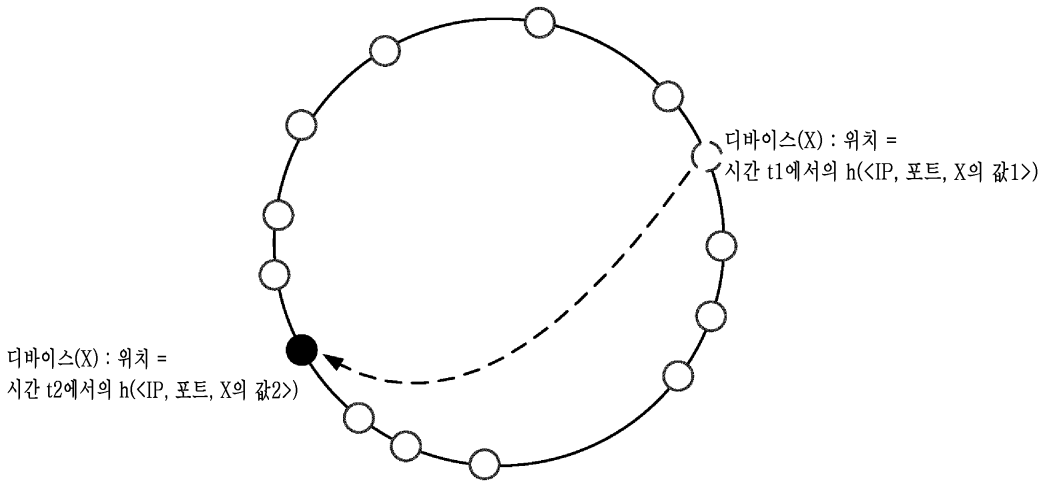
도면2


디바이스(X) : 위치 =
시간 t1에서의 h(<IP, 포트, X의 값>)
디바이스(Y) : 위치 =
시간 t1에서의 h(<IP, 포트, Y의 값>)

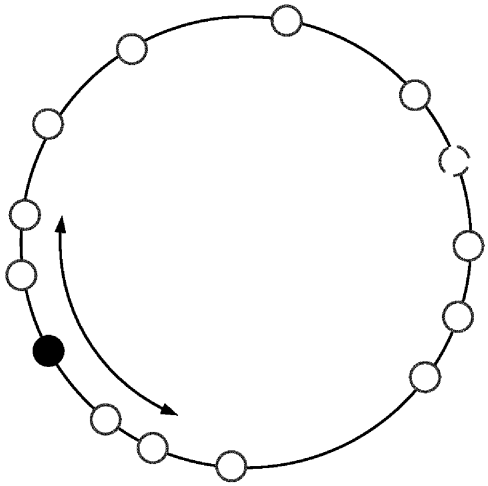
도면3a


디바이스(X) : 위치 =
시간 t1에서의 h(<IP, 포트, X의 값1>)

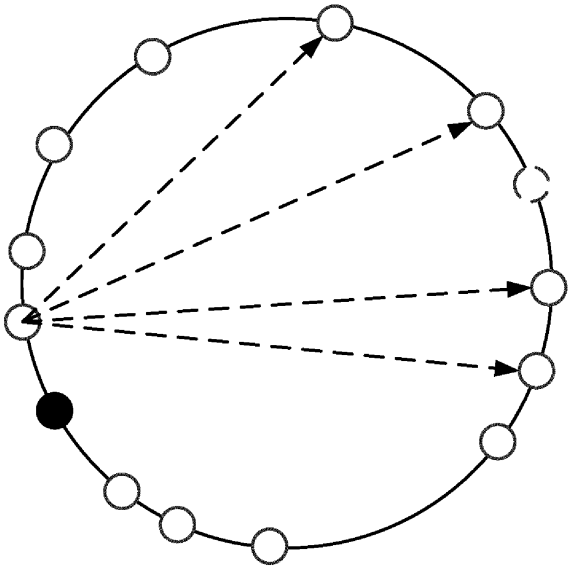
도면3b



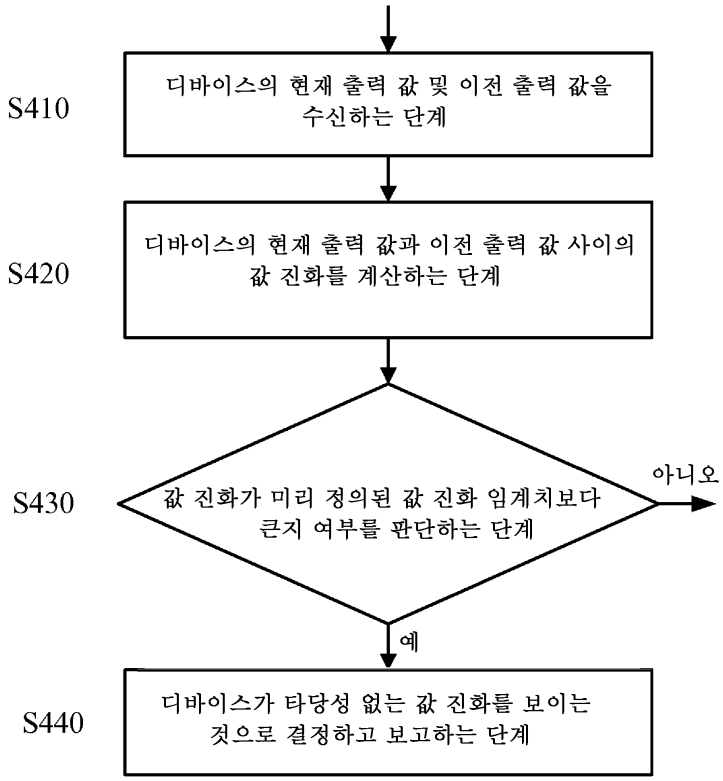
도면3c



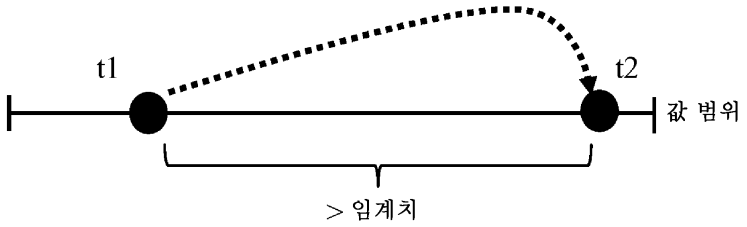
도면3d



도면4

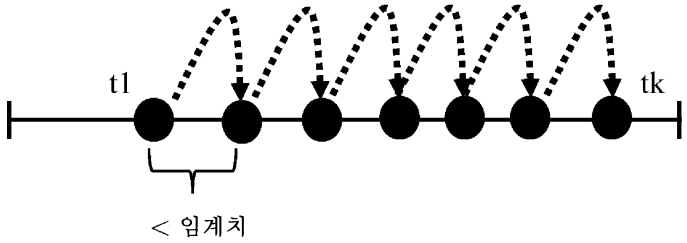

S410
디바이스의 현재 출력 값 및 이전 출력 값을 수신하는 단계
S420
디바이스의 현재 출력 값과 이전 출력 값 사이의 값 진화를 계산하는 단계
S430
값 진화가 미리 정의된 값 진화 임계치보다 큰지 여부를 판단하는 단계
아니오
예
S440
디바이스가 타당성 없는 값 진화를 보이는 것으로 결정하고 보고하는 단계

도면5a



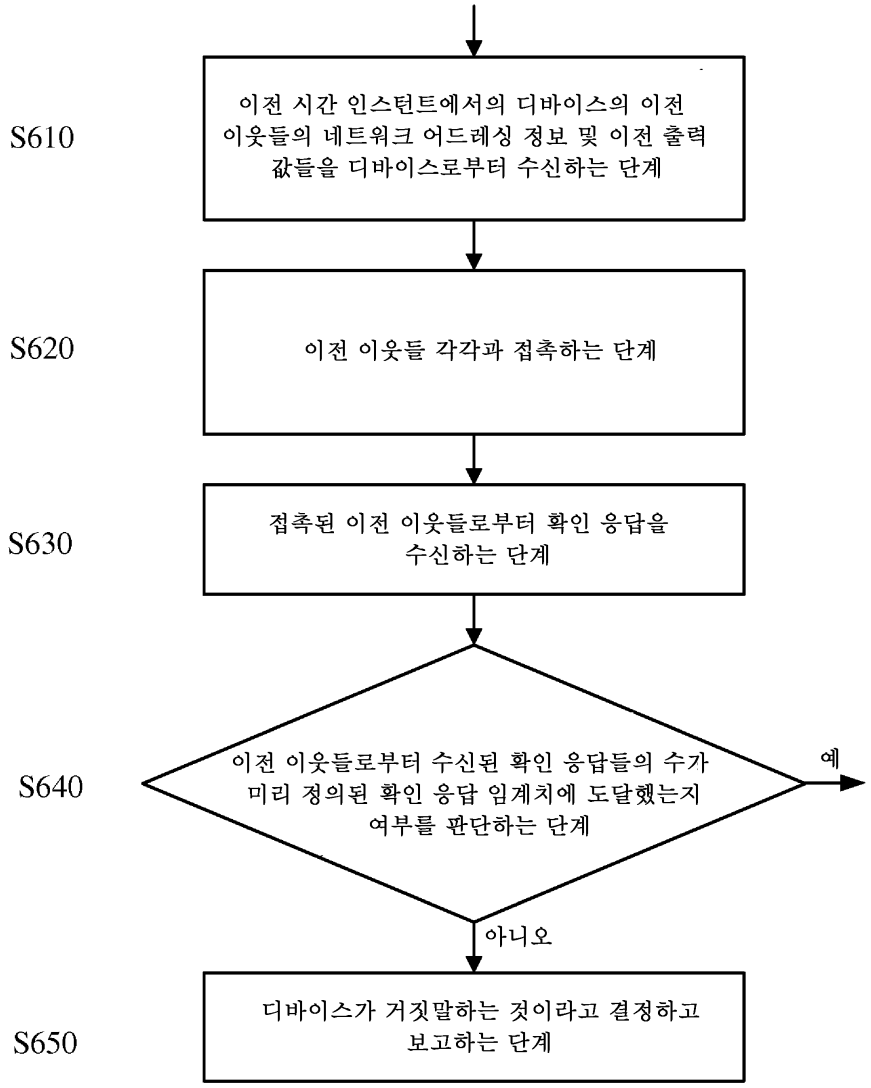
타당성 없는 이동, 디바이스의 거짓말

도면5b



유효한 이동 순서

도면6


S610
이전 시간 인스턴트에서의 디바이스의 이전 이웃들의 네트워크 어드레싱 정보 및 이전 출력 값들을 디바이스로부터 수신하는 단계
S620
이전 이웃들 각각과 접촉하는 단계
S630
접촉된 이전 이웃들로부터 확인 응답을 수신하는 단계
S640
이전 이웃들로부터 수신된 확인 응답들의 수가 미리 정의된 확인 응답 임계치에 도달했는지 여부를 판단하는 단계
예
아니오
S650
디바이스가 거짓말하는 것이라고 결정하고 보고하는 단계