(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년05월20일
(11) 등록번호 10-0959046
(24) 등록일자 2010년05월13일

(51) Int. Cl.
H04W 12/10 (2009.01) *G06F 11/36* (2006.01)
G06F 15/16 (2006.01)
(21) 출원번호 10-2008-7000970
(22) 출원일자(국제출원일자) 2006년06월13일
심사청구일자 2008년01월11일
(85) 번역문제출일자 2008년01월11일
(65) 공개번호 10-2008-0015940
(43) 공개일자 2008년02월20일
(86) 국제출원번호 PCT/US2006/023047
(87) 국제공개번호 WO 2006/135905
국제공개일자 2006년12월21일
(30) 우선권주장
11/303,156 2005년12월15일 미국(US)
60/690,209 2005년06월13일 미국(US)
(56) 선행기술조사문헌
US20030217193 A1
US20040198319 A1
US07246266 B2
US20040025036 A1
전체 청구항 수 : 총 45 항

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
자 산제이 케이
미국 92131 캘리포니아주 샌디에고 시카모어 리지 코트 12386
압디 베루즈 엘
미국 92011 캘리포니아주 칼스배드 피튜니아 플레이스 6563
(뒷면에 계속)
(74) 대리인
특허법인코리아나

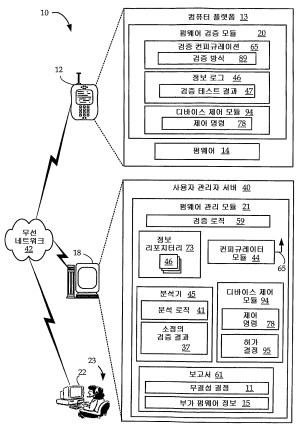
심사관 : 김견수

(54) 무선 디바이스 상의 펌웨어 검증을 관리하는 장치 및 방법

(57) 요 약

본 발명은 무선 디바이스 상의 펌웨어 무결성을 검증하는 장치, 방법, 프로세서 및 기계 판독가능 매체를 개시한다. 본 발명의 양태는 무선 디바이스 상의 펌웨어 무결성을 테스트하는 검증 방식을 생성하는 것 및 검증 방식을 무선 디바이스에 송신하는 것을 포함한다. 무선 디바이스는 검증 방식을 펌웨어에 적용하고, 검증 테스트 결과를 얻는데, 이 검증 테스트 결과는 분석을 위해 전송된다. 분석기는 생성된 검증 테스트 결과를 소정의 테스트 결과와 비교하여 펌웨어 무결성을 나타내는 무결성 결정을 얻는다. 몇몇 양태에서, 무선 디바이스의 동작 특성을 변경하라는 제어 명령은 무결성 결정에 기초하여 생성될 수도 있다.

대 표 도 - 도1



(72) 발명자

스콧 클리프턴 유진

미국 92127 캘리포니아주 샌디에고 아구아미엘 로드 17742

폭 케니

미국 92129 캘리포니아주 샌디에고 메사 크레스트 플레이스 13126

카세트 티아 매닝

미국 92130 캘리포니아주 샌디에고 페어포트 웨이 4817

황 지현

미국 92126 캘리포니아주 샌디에고 골드 코스트 드라이브 9505넘버121

특허청구의 범위

청구항 1

무선 통신 디바이스로서,

펌웨어를 갖는 컴퓨터 플랫폼; 및

검증 컨피규레이션 (configuration) 을 실행하여 펌웨어 정보를 수집하도록 동작 가능한 펌웨어 검증 모듈을 포함하고,

상기 펌웨어 정보는 펌웨어 무결성을 나타내고,

상기 검증 컨피규레이션은 하나 이상의 검증 방식을 포함하며,

상기 펌웨어 검증 모듈은 상기 펌웨어를 조각 (segment) 내고 상기 펌웨어의 하나 이상의 소정의 세그먼트에 상기 하나 이상의 검증 방식을 적용하도록 동작 가능한, 무선 통신 디바이스.

청구항 2

제 1 항에 있어서,

상기 펌웨어 검증 모듈은 또한 상기 펌웨어 상에서 상기 하나 이상의 검증 방식을 실행하여 검증 테스트 결과를 생성하도록 동작 가능하고,

상기 검증 테스트 결과는 상기 펌웨어 무결성을 나타내는, 무선 통신 디바이스.

청구항 3

제 2 항에 있어서,

상기 펌웨어 검증 모듈은 소정의 검증 결과를 더 포함하고, 상기 펌웨어 검증 모듈은 상기 소정의 검증 결과를 상기 생성된 검증 테스트 결과와 비교하여 상기 펌웨어 무결성을 결정하도록 동작 가능한, 무선 통신 디바이스.

청구항 4

제 2 항에 있어서,

상기 펌웨어 검증 모듈은 상기 생성된 검증 테스트 결과를 다른 디바이스에 송신하여 상기 펌웨어 무결성을 결정하도록 동작 가능한, 무선 통신 디바이스.

청구항 5

제 4 항에 있어서,

상기 펌웨어 검증 모듈은 무선 네트워크를 가로질러 상기 생성된 검증 테스트 결과를 송신하도록 동작 가능한, 무선 통신 디바이스.

청구항 6

제 2 항에 있어서,

상기 하나 이상의 검증 방식은 중복 검사, 상기 펌웨어 내의 소정의 위치에 있는 소정의 값에 대한 테스트, 펌웨어 서명 정보의 검사, 및 소정의 함수를 상기 펌웨어 적어도 일부에 적용한 소정의 결과에 대한 테스트 중 하나 이상을 포함하는, 무선 통신 디바이스.

청구항 7

삭제

청구항 8

제 1 항에 있어서,

상기 검증 컨피규레이션은 무선 네트워크를 가로질러 다른 컴퓨터 디바이스로부터 수신되고,

상기 검증 컨피규레이션은 보고 파라미터를 더 포함하는, 무선 통신 디바이스.

청구항 9

제 8 항에 있어서,

상기 하나 이상의 검증 방식은 상기 무선 디바이스의 타입, 상기 무선 디바이스와 연관된 네트워크 서비스 제공자의 ID, 및 상기 펌웨어의 타입 중 하나 이상에 기초하여 복수의 검증 방식에서 선택되는, 무선 통신 디바이스.

청구항 10

제 8 항에 있어서,

상기 검증 컨피규레이션은 복수의 추적 파라미터에서 선택된 추적 파라미터, 복수의 보고 파라미터에서 선택된 상기 보고 파라미터, 및 복수의 제어 명령 파라미터에서 선택된 제어 명령 파라미터 중 하나 이상을 포함하는, 무선 통신 디바이스.

청구항 11

제 8 항에 있어서,

상기 검증 컨피규레이션은 부가 펌웨어 정보를 식별하여 수집하는 추적 파라미터를 더 포함하는, 무선 통신 디바이스.

청구항 12

제 1 항에 있어서,

상기 펌웨어 검증 모듈은 또한 무선 네트워크를 가로질러 제한된 액세스 (limited-access) 통신 채널을 확립하도록 동작 가능하고,

상기 제한된 액세스 통신 채널은 소정의 제한된 서비스 컨피규레이션에 기초하는, 무선 통신 디바이스.

청구항 13

제 12 항에 있어서,

상기 제한된 액세스 통신 채널은 상기 디바이스의 최종 사용자에게 이용 가능하지 않은, 무선 통신 디바이스.

청구항 14

제 1 항에 있어서,

상기 디바이스의 동작 특성을 변경하라는 제어 명령을 수신 및 실행하도록 동작 가능한 디바이스 제어 모듈을 더 포함하고, 상기 제어 명령은 상기 펌웨어 무결성에 기초하는, 무선 통신 디바이스.

청구항 15

제 14 항에 있어서,

상기 제어 명령은 디세이블 명령, 이네이블 명령, 및 리컨피규어 (reconfigure) 명령 중 하나 이상을 포함하고, 상기 디세이블 명령은 상기 무선 디바이스를 비긴급 통신 동안 동작 불가 상태로 만들고, 상기 이네이블 명령은 상기 무선 디바이스를 통신 동안 동작 가능 상태로 만들며, 상기 리컨피규어 명령은 상기 무선 디바이스의 펌웨어에 관련된 하나 이상의 데이터 값을 설정하는, 무선 통신 디바이스.

청구항 16

제 14 항에 있어서,

상기 디바이스 제어 모듈은 또한 상기 제어 명령의 발행자 (issuer) 와 연관된 인가 및 상기 제어 명령의 검증

중 하나 이상을 검사하도록 동작 가능한, 무선 통신 디바이스.

청구항 17

무선 디바이스로서,

상기 무선 디바이스의 동작을 제어하는 수단; 및

상기 무선 디바이스의 동작을 제어하는 수단의 무결성을 나타내는 정보를 수집하기 위해 상기 무선 디바이스의 동작을 제어하는 수단에 검증 컨피규레이션을 적용하는 수단을 포함하고,

상기 검증 컨피규레이션은 하나 이상의 검증 방식을 포함하며,

상기 적용하는 수단은 펌웨어를 조각 (segment) 내고 상기 제어하는 수단과 연관된 상기 펌웨어의 하나 이상의 소정의 세그먼트에 상기 하나 이상의 검증 방식을 적용하도록 동작 가능한, 무선 디바이스.

청구항 18

무선 디바이스 상의 펌웨어 무결성을 관리하는 장치로서,

펌웨어에 적용되어 상기 펌웨어 무결성을 테스트하는 하나 이상의 검증 방식을 포함한 검증 컨피규레이션을 생성하고 상기 무선 디바이스에 송신하도록 동작 가능한 펌웨어 관리 모듈;

상기 무선 디바이스에 의한 상기 검증 컨피규레이션의 실행에 기초하여 생성된 검증 테스트 결과를 수신 및 저장하도록 동작 가능한 정보 리포지터리; 및

상기 생성된 검증 테스트 결과에 기초하여, 상기 펌웨어 무결성을 나타내는 무결성 결정을 생성하도록 동작 가능한 분석기를 포함하고,

상기 하나 이상의 검증 방식은 상기 펌웨어를 조각 (segment) 내는 것을 포함하고,

상기 무결성 결정은 상기 펌웨어의 각각의 세그먼트의 무결성 결정을 포함하는, 펌웨어 무결성 관리 장치.

청구항 19

제 18 항에 있어서,

상기 검증 컨피규레이션은 상기 무선 디바이스에 대해 선택된 소정의 검증 결과를 더 포함하는, 펌웨어 무결성 관리 장치.

청구항 20

제 18 항에 있어서,

상기 분석기는 소정의 검증 결과를 더 포함하고, 상기 분석기는 상기 생성된 검증 테스트 결과를 상기 소정의 검증 결과와 비교하여 상기 무결성 결정을 생성하도록 동작 가능한, 펌웨어 무결성 관리 장치.

청구항 21

제 18 항에 있어서,

상기 무선 디바이스의 동작 특성을 변경하라는 제어 명령을 송신하도록 동작 가능한 디바이스 제어 모듈을 더 포함하고, 상기 제어 명령은 상기 무결성 결정에 기초하는, 펌웨어 무결성 관리 장치.

청구항 22

제 21 항에 있어서,

상기 디바이스 제어 모듈은 상기 제어 명령을 상기 무선 디바이스에 송신하기 전에 상기 제어 명령을 검증하도록 동작 가능한, 펌웨어 무결성 관리 장치.

청구항 23

제 22 항에 있어서,

상기 디바이스 제어 모듈은 복수의 제어 허가 및 복수의 사용자 ID 를 포함하는 상관된 데이터를 포함하고, 상기 제어 명령은 사용자 ID 와 제어 액티비티 중 하나 이상을 포함하며, 상기 디바이스 제어 모듈은 상기 사용자 ID 와 상기 제어 액티비티를 상기 상관된 데이터와 비교하여 상기 제어 명령을 실행할지 여부에 관한 허가 결정을 생성하는 허가 로직을 포함하는, 펌웨어 무결성 관리 장치.

청구항 24

제 22 항에 있어서,

상기 디바이스 제어 모듈은 무선 네트워크를 가로질러 위치한 다른 컴퓨터 디바이스로부터 상기 제어 명령을 수신하도록 동작 가능한, 펌웨어 무결성 관리 장치.

청구항 25

제 18 항에 있어서,

상기 검증 컨피규레이션은 복수의 추적 파라미터에서 선택된 추적 파라미터, 복수의 보고 파라미터에서 선택된 보고 파라미터, 및 복수의 제어 명령 파라미터에서 선택된 제어 명령 파라미터 중 하나 이상을 더 포함하는, 펌웨어 무결성 관리 장치.

청구항 26

제 18 항에 있어서,

상기 펌웨어 관리 모듈은 복수의 검증 방식에서 상기 하나 이상의 검증 방식을 선택하도록 동작 가능하고, 무선 네트워크를 가로질러 상기 검증 컨피규레이션을 송신하도록 동작 가능한, 펌웨어 무결성 관리 장치.

청구항 27

제 18 항에 있어서,

상기 분석기는 또한 상기 무결성 결정, 상기 검증 컨피규레이션, 및 상기 검증 컨피규레이션에 기초하여 수집된 부가 펌웨어 정보를 포함한 보고서를 생성하도록 동작 가능한, 펌웨어 무결성 관리 장치.

청구항 28

제 18 항에 있어서,

상기 무선 디바이스의 타입, 상기 무선 디바이스와 연관된 네트워크 서비스 제공자의 ID, 및 상기 펌웨어의 타입 중 하나 이상에 기초하여 복수의 검증 방식에서 상기 하나 이상의 검증 방식을 선택하도록 동작 가능한 컨피규레이터 모듈을 더 포함하는, 펌웨어 무결성 관리 장치.

청구항 29

삭제

청구항 30

무선 디바이스 상의 펌웨어 무결성을 관리하는 장치로서,

검증 컨피규레이션을 생성하고, 무선 네트워크를 가로질러 상기 무선 디바이스에 송신하는 생성 수단으로서, 상기 검증 컨피규레이션은 펌웨어에 적용되어 상기 펌웨어 무결성을 테스트하는 하나 이상의 검증 방식을 포함하는, 상기 생성 수단;

상기 무선 디바이스에 의한 상기 검증 컨피규레이션의 실행에 기초하여 검증 테스트 결과를 수신 및 저장하는 저장 수단; 및

상기 검증 테스트 결과를 분석하고, 분석에 기초하여 상기 펌웨어 무결성을 나타내는 무결성 결정을 포함한 보고서를 생성하는 분석 수단을 포함하고,

상기 하나 이상의 검증 방식은 상기 펌웨어를 조각 (segment) 내는 것을 포함하고,

상기 무결성 결정은 상기 펌웨어의 각각의 세그먼트의 무결성 결정을 포함하는, 펌웨어 무결성 관리 장치.

청구항 31

무선 디바이스 상의 펌웨어 무결성을 검증하는 방법으로서,

상기 무선 디바이스 상의 펌웨어 무결성을 테스트하는 하나 이상의 검증 방식을 포함한 검증 컨피규레이션을 생성하는 단계;

상기 검증 컨피규레이션을 상기 무선 디바이스에 전송하는 단계;

상기 무선 디바이스에 의한 펌웨어 상의 상기 하나 이상의 검증 방식의 적용에 기초하여 생성된 검증 테스트 결과를 수신하는 단계; 및

상기 생성된 검증 테스트 결과에 기초하여 상기 펌웨어 무결성을 나타내는 무결성 결정을 생성하는 단계를 포함하고,

상기 하나 이상의 검증 방식은 상기 펌웨어를 조각 (segment) 내는 것을 포함하고,

상기 무결성 결정은 상기 펌웨어의 각각의 세그먼트의 무결성 결정을 포함하는, 펌웨어 무결성 검증 방법.

청구항 32

제 31 항에 있어서,

상기 무결성 결정을 생성하는 단계는 상기 생성된 검증 테스트 결과를 소정의 검증 결과와 비교하는 단계를 더 포함하는, 펌웨어 무결성 검증 방법.

청구항 33

제 31 항에 있어서,

상기 무선 디바이스의 동작 특성을 변경하라는 제어 명령을 상기 무선 디바이스에 송신하는 단계를 더 포함하고, 상기 제어 명령은 상기 무결성 결정에 기초하는, 펌웨어 무결성 검증 방법.

청구항 34

제 33 항에 있어서,

상기 제어 명령을 상기 무선 디바이스에 송신하기 전에 상기 제어 명령을 검증하는 단계를 더 포함하는, 펌웨어 무결성 검증 방법.

청구항 35

제 34 항에 있어서,

상기 제어 명령은 사용자 ID 및 제어 액티비티를 포함하고, 상기 제어 명령을 검증하는 단계는 상기 사용자 ID 및 상기 제어 액티비티를 복수의 사용자 ID 와 상관된 복수의 제어 허가와 비교하는 단계를 더 포함하는, 펌웨어 무결성 검증 방법.

청구항 36

제 31 항에 있어서,

상기 무선 디바이스의 타입, 상기 무선 디바이스와 연관된 네트워크 서비스 제공자의 ID, 및 상기 펌웨어의 타입 중 하나 이상에 기초하여 복수의 검증 방식에서 상기 하나 이상의 검증 방식을 선택하는 단계를 더 포함하는, 펌웨어 무결성 검증 방법.

청구항 37

삭제

청구항 38

무선 디바이스 상의 펌웨어 무결성 검증 방법으로서,

상기 무선 디바이스 상의 펌웨어 무결성을 테스트하는 하나 이상의 검증 방식을 수신하는 단계;

상기 하나 이상의 검증 방식을 펌웨어에 적용한 것에 기초하여 검증 테스트 결과를 생성하는 단계; 및

분석을 위해 상기 검증 테스트 결과를 전송하여 상기 펌웨어 무결성을 결정하는 단계를 포함하고,

상기 하나 이상의 검증 방식은 상기 펌웨어를 조각 (segment) 내는 것을 포함하고,

상기 무결성을 결정하는 단계는 상기 펌웨어의 각각의 세그먼트의 무결성 결정을 포함하는, 펌웨어 무결성 검증 방법.

청구항 39

제 38 항에 있어서,

상기 하나 이상의 검증 방식은 중복 검사, 상기 펌웨어 내의 소정 위치에 있는 소정의 값에 대한 테스트, 펌웨어 서명 정보의 검사, 및 소정의 함수를 상기 펌웨어의 적어도 일부에 적용한 소정의 결과에 대한 테스트 중 하나 이상을 포함하는, 펌웨어 무결성 검증 방법.

청구항 40

제 38 항에 있어서,

상기 하나 이상의 검증 방식을 상기 펌웨어의 하나 이상의 소정의 세그먼트에 적용하는 단계를 더 포함하는, 펌웨어 무결성 검증 방법.

청구항 41

제 38 항에 있어서,

상기 하나 이상의 검증 방식은 상기 무선 디바이스의 타입, 상기 무선 디바이스와 연관된 네트워크 서비스 제공자의 ID, 및 상기 펌웨어의 타입 중 하나 이상에 기초하여 복수의 검증 방식에서 선택되는, 펌웨어 무결성 검증 방법.

청구항 42

제 38 항에 있어서,

검증 컨피규레이션을 수신하는 단계를 더 포함하고, 상기 검증 컨피규레이션은 복수의 추적 파라미터에서 선택된 추적 파라미터, 복수의 보고 파라미터에서 선택된 보고 파라미터, 및 복수의 제어 명령 파라미터에서 선택된 제어 명령 파라미터 중 하나 이상을 포함하는, 펌웨어 무결성 검증 방법.

청구항 43

제 38 항에 있어서,

소정의 제한된 서비스 컨피규레이션에 기초하여 무선 네트워크를 가로질러 제한된 액세스 통신 채널을 확립하는 단계를 더 포함하는, 펌웨어 무결성 검증 방법.

청구항 44

제 38 항에 있어서,

상기 무선 디바이스의 동작 특성을 변경하라는 제어 명령을 수신하는 단계를 더 포함하고, 상기 제어 명령은 상기 검증 테스트 결과에 기초하는, 펌웨어 무결성 검증 방법.

청구항 45

기계에 의한 실행 시, 상기 기계로 하여금,

무선 디바이스 상의 펌웨어 무결성을 테스트하는 하나 이상의 검증 방식을 포함한 검증 컨피규레이션을 생성하

는 단계;

상기 검증 컨피규레이션을 상기 무선 디바이스에 전송하는 단계;

상기 무선 디바이스에 의한 펌웨어 상의 상기 하나 이상의 검증 방식의 적용에 기초하여 생성된 검증 테스트 결과를 수신하는 단계; 및

상기 생성된 검증 테스트 결과에 기초하여 상기 펌웨어 무결성을 나타내는 무결성 결정을 생성하는 단계를 포함하는 동작을 수행하도록 하는 명령어를 포함하고,

상기 하나 이상의 검증 방식은 상기 펌웨어를 조각 (segment) 내는 것을 포함하고,

상기 무결성 결정은 상기 펌웨어의 각각의 세그먼트의 무결성 결정을 포함하는, 기계 판독가능 매체.

청구항 46

무선 디바이스 상의 펌웨어 무결성을 테스트하는 하나 이상의 검증 방식을 포함한 검증 컨피규레이션을 생성하는 수단;

상기 검증 컨피규레이션을 상기 무선 디바이스에 전송하는 수단;

상기 무선 디바이스에 의한 펌웨어 상의 상기 하나 이상의 검증 방식의 적용에 기초하여 생성된 검증 테스트 결과를 수신하는 수단; 및

상기 생성된 검증 테스트 결과에 기초하여 상기 펌웨어 무결성을 나타내는 무결성 결정을 생성하는 수단을 포함하고,

상기 하나 이상의 검증 방식은 상기 펌웨어를 조각 (segment) 내는 것을 포함하고,

상기 무결성 결정은 상기 펌웨어의 각각의 세그먼트의 무결성 결정을 포함하는, 하나 이상의 프로세서.

청구항 47

기계에 의한 실행 시, 상기 기계로 하여금,

무선 디바이스 상의 펌웨어 무결성을 테스트하는 하나 이상의 검증 방식을 수신하는 단계;

상기 하나 이상의 검증 방식을 펌웨어에 적용한 것에 기초하여 검증 테스트 결과를 생성하는 단계; 및

분석을 위해 상기 검증 테스트 결과를 전송하여 상기 펌웨어 무결성을 결정하는 단계를 포함하는 동작을 수행하도록 하는 명령어를 포함하고,

상기 하나 이상의 검증 방식은 상기 펌웨어를 조각 (segment) 내는 것을 포함하고,

상기 무결성 결정은 상기 펌웨어의 각각의 세그먼트의 무결성 결정을 포함하는, 기계 판독가능 매체.

청구항 48

무선 디바이스 상의 펌웨어 무결성을 테스트하는 하나 이상의 검증 방식을 수신하는 수단;

상기 하나 이상의 검증 방식을 펌웨어에 적용한 것에 기초하여 검증 테스트 결과를 생성하는 수단; 및

분석을 위해 상기 검증 테스트 결과를 전송하여 상기 펌웨어 무결성을 결정하는 수단을 포함하고,

상기 하나 이상의 검증 방식은 상기 펌웨어를 조각 (segment) 내는 것을 포함하고,

상기 무결성 결정은 상기 펌웨어의 각각의 세그먼트의 무결성 결정을 포함하는, 하나 이상의 프로세서.

명 세 서

[0001] **35 U.S.C. §119 에 따른 우선권 주장**

[0002] 본 특허 출원은 본원의 양수인에게 양도되어 본원에서 명확히 참조로서 병합하고 있는 2005 년 6 월 13 일 출원된 발명의 명칭이 "무선 디바이스 상의 펌웨어 검증을 위한 방법 및 장치 (METHOD AND APPARATUS FOR FIRMWARE VERIFICATION ON A WIRELESS DEVICE)" 인 가출원 제 60/690,209 호를 우선권 주장한다.

[0003] **배경기술**

[0004] 본원에서 설명되는 양태는 일반적으로 무선 통신 디바이스 및 컴퓨터 네트워크에 관한 것이다. 더욱 상세하게는, 본원에서 설명되는 양태는 무선 디바이스로부터 수집된 펌웨어 관련 정보의 수집 (collection), 보고 및 분석과 함께 무선 디바이스의 펌웨어 무결성 (integrity) 을 검증하는 것에 관한 것이다.

[0005] 무선 네트워킹은 구리선이나 광케이블과 같은 직접적인 전기 접속 없이 하나 이상의 무선 디바이스를 다른 컴퓨터 디바이스에 접속한다. 무선 디바이스는, 데이터 패킷을 송수신할 수 있도록, 무선 컴퓨터 네트워크 또는 부분적으로 무선인 컴퓨터 네트워크를 가로질러 보통 패킷 형태로 데이터를 통신하고, 네트워크 상의 "데이터" 또는 "통신" 채널을 개방한다. 무선 디바이스는 종종 프로그램 및 하드웨어 컴포넌트와 같은 무선 디바이스 자원을 갖는데, 무선 디바이스 자원은 예를 들어, 네트워크를 통해 데이터를 송수신하기 위해 개방형 통신 접속을 이용하는 것과 같이, 자신의 설계 및 전용 프로토콜이나 컨피규레이션 (configuration) 에 따라 데이터를 사용 및 생성하도록 개별적·협동적으로 동작한다.

[0006] 또한, 이들 무선 디바이스는 무선 디바이스가 작동하는 것을 가능하게 하는 데이터 및 프로그램 코드를 갖는 펌웨어를 포함한다. 이 데이터 및 프로그램 코드는 무선 디바이스의 동작에 있어서 중요하다. 예를 들어, 데이터 및 프로그램 코드는 무선 디바이스가 네트워크와 통신하는데 사용하는 프로토콜을 지정하거나, 무선 디바이스가 동작할 수도 있는 무선 네트워크(들)를 지정할 수도 있다.

[0007] 일 양태에서, 무선 디바이스의 펌웨어 무결성은 무선 디바이스의 펌웨어 내의 값들이 그 버전의 펌웨어에 대한 정확한 값들인지 여부에 관련된다. 예를 들어, 펌웨어 무결성의 측정은 예를 들어, 프로그램 내의 버그에 의해 무심코, 또는 예를 들어, 컴퓨터 바이러스나 고의적인 조작에 의해 고의로 펌웨어가 손상되었는지 여부를 결정할 수도 있다. 다른 양태에서, 무선 디바이스의 펌웨어 무결성은 펌웨어의 버전이 무선 디바이스에 대한 현재 버전인지 여부에 관련된다. 소정의 무선 디바이스에 대한 펌웨어 버전은 주기적으로 갱신되거나 대체될 필요가 있을 수도 있다. 또한, 심지어, 무선 디바이스에 잘못된 펌웨어가 설치되거나, 설치된 펌웨어가 특정 무선 네트워크 제공자에게 허용 가능하지 않을 수도 있다.

[0008] 무선 디바이스의 펌웨어 무결성이 손상되면 많은 문제가 일어날 수도 있다. 예를 들어, 무선 디바이스가 기능을 하지 않거나, 무선 네트워크 상의 잘못된 통신 프로토콜을 사용함으로써 네트워크의 동작과 간섭할 수도 있다. 다른 예에서는, 펌웨어의 변경으로 인해, 무선 디바이스의 구입이 이루어진 무선 네트워크 서비스 제공자와 다른 무선 네트워크 서비스 제공자를 위해 그 무선 디바이스가 사용될 수도 있다. 이 경우에, 원래 네트워크 서비스 제공자의 네트워크 상에서만 무선 디바이스를 사용할 것이라는 협정에 기초하여 원래 무선 네트워크 서비스 제공자가 무선 디바이스의 가격에 보조금을 지급하면, 원래 무선 네트워크 서비스 제공자는 손해를 입을 수도 있다. 따라서, 무선 디바이스가 다른 무선 네트워크 서비스 제공자와 함께 동작할 수 있도록 펌웨어를 변경하는 것은 무선 디바이스의 소유자가 서명한 협정을 위반할 수도 있다.

[0009] 따라서, 무선 디바이스의 펌웨어 무결성의 검증을 고려하는 장치 및 방법을 제공하는 것이 유익할 것이다.

[0010] **간략한 요약**

[0011] 본원에서 설명되는 양태는 무선 디바이스 상에서 펌웨어 검증을 위해 동작 가능한 장치, 방법, 컴퓨터 판독가능 매체 및 프로세서를 포함한다.

[0012] 몇몇 양태에서, 무선 통신 디바이스는 펌웨어를 갖는 컴퓨터 플랫폼, 및 검증 컨피규레이션을 실행하여 펌웨어 정보를 수집하도록 동작 가능한 펌웨어 검증 모듈을 포함하고, 펌웨어 정보는 펌웨어 무결성을 나타낸다.

[0013] 다른 양태에서, 무선 디바이스는 무선 디바이스의 동작을 제어하는 수단, 및 무선 디바이스의 동작을 제어하는 수단에 검증 컨피규레이션을 적용하여 무선 디바이스의 동작을 제어하는 수단의 무결성을 나타내는 정보를 수집하는 수단을 포함한다.

[0014] 또 다른 양태에서, 무선 디바이스 상의 펌웨어 무결성을 관리하는 장치는 검증 컨피규레이션을 생성하고 무선 디바이스에 송신하도록 동작 가능한 펌웨어 관리 모듈을 포함한다. 검증 컨피규레이션은 펌웨어에 적용되어 펌웨어 무결성을 테스트하는 검증 방식을 포함한다. 이 장치는 무선 디바이스에 의한 검증 컨피규레이션의 실행에 기초하여 생성된 검증 테스트 결과를 수신 및 저장하도록 동작 가능한 정보 리포지터리를 더 포함한다. 또한, 이 장치는 생성된 검증 테스트 결과에 기초하여 무결성 결정을 생성하도록 동작 가능한 분석기를 포함하고, 무결성 결정은 펌웨어 무결성을 나타낸다.

[0015] 또 다른 양태에서, 무선 디바이스 상의 펌웨어 무결성을 관리하는 장치는 검증 컨피규레이션을 생성하고 무선

네트워크를 가로질러 무선 디바이스에 송신하는 생성 수단을 포함한다. 검증 컨피규레이션은 펌웨어에 적용되어 펌웨어 무결성을 테스트하는 검증 방식을 포함한다. 이 장치는 무선 디바이스에 의한 검증 컨피규레이션의 실행에 기초한 검증 테스트 결과를 수신 및 저장하는 저장 수단을 더 포함한다. 또한, 이 장치는 검증 테스트 결과를 분석하고 분석에 기초하여 보고서를 생성하는 분석 수단을 더 포함하고, 보고서는 펌웨어 무결성을 나타내는 무결성 결정을 포함한다.

[0016] 다른 양태에서, 무선 디바이스 상에서 펌웨어 무결성을 검증하는 방법은 무선 디바이스 상의 펌웨어 무결성을 테스트하는 검증 방식을 포함한 검증 컨피규레이션을 생성하는 단계, 검증 컨피규레이션을 무선 디바이스에 전송하는 단계, 무선 디바이스에 의한 펌웨어 상의 검증 방식의 적용에 기초하여 생성된 검증 테스트 결과를 수신하는 단계, 및 생성된 검증 테스트 결과에 기초하여 무결성 결정을 생성하는 단계를 포함하고, 무결성 결정은 펌웨어 무결성을 나타낸다.

[0017] 다른 양태에서, 무선 디바이스 상의 펌웨어 무결성을 검증하는 방법은 무선 디바이스 상의 펌웨어 무결성을 테스트하는 검증 방식을 수신하는 단계, 검증 방식을 펌웨어에 적용한 것에 기초하여 검증 테스트 결과를 생성하는 단계, 및 검증 테스트 결과를 전송하고 분석하여 펌웨어 무결성을 결정하는 단계를 포함한다.

[0018] 몇몇 양태에서, 기계 판독가능 매체는, 기계에 의한 실행 시 기계로 하여금 무선 디바이스 상의 펌웨어 무결성을 테스트하는 검증 방식을 포함한 검증 컨피규레이션을 생성하는 단계, 검증 컨피규레이션을 무선 디바이스에 전송하는 단계, 무선 디바이스에 의한 펌웨어 상의 검증 방식의 적용에 기초하여 생성된 검증 테스트 결과를 수신하는 단계, 및 생성된 검증 테스트 결과에 기초하여 무결성 결정을 생성하는 단계를 포함한 동작들을 수행하도록 하는 명령어를 포함하고, 무결성 결정은 펌웨어 무결성을 나타낸다. 몇몇 관련 양태에서, 상술한 동작들을 수행하도록 하나 이상의 프로세서가 구성될 수도 있다.

[0019] 다른 양태에서, 기계 판독가능 매체는, 기계에 의한 실행 시 기계로 하여금 무선 디바이스 상의 펌웨어 무결성을 테스트하는 검증 방식을 수신하는 단계, 펌웨어에 검증 방식을 적용한 것에 기초하여 검증 테스트 결과를 생성하는 단계, 및 검증 테스트 결과를 전송하고 분석하여 펌웨어 무결성을 결정하는 단계를 포함한 동작들을 수행하도록 하는 명령어를 포함한다. 관련 양태에서, 상술한 동작들을 수행하도록 하나 이상의 프로세서가 구성될 수도 있다.

[0020] **도면의 간단한 설명**

[0021] 이하, 개시된 양태를 한정하기 위한 것이 아니라 예시하기 위해 제공되며, 동일 참조부호가 동일 구성요소를 지시하는, 첨부된 도면을 참조하여 개시된 양태를 설명할 것이다.

[0022] 도 1 은 무선 디바이스의 펌웨어 무결성을 검증하는 시스템의 일 양태의 개략도이다.

[0023] 도 2 는 도 1 의 시스템의 동작의 일 양태와 연관된 메시지 흐름도이다.

[0024] 도 3 은 도 1 의 무선 디바이스의 일 양태의 개략도이다.

[0025] 도 4 는 도 3 의 무선 디바이스의 펌웨어의 조각내기 (segmentation) 의 일 양태의 개략도이다.

[0026] 도 5 는 도 1 의 사용자 관리자와 연관된 컨피규레이터 (configurator) 모듈의 일 양태의 개략도이다.

[0027] 도 6 은 도 1 의 사용자 관리자 및/또는 무선 디바이스와 연관된 디바이스 제어 모듈의 일 양태의 개략도이다.

[0028] 도 7 은 도 1 과 연관된 셀룰러 전화 네트워크의 일 양태의 개략도이다.

[0029] 도 8 은 무선 디바이스 상에서 동작 가능하며, 무선 디바이스 상의 펌웨어 무결성을 결정하는 방법의 일 양태의 흐름도이다.

[0030] 도 9 는 소정의 장치 상에서 동작 가능하며, 무선 디바이스 상에서 펌웨어 무결성을 결정하는 방법의 일 양태의 흐름도이다.

[0031] **상세한 설명**

[0032] 도 1 및 도 2 를 참조하면, 펌웨어 무결성 결정 (11) 을 행하기 위한 무선 디바이스 펌웨어 검증 시스템 (10) 의 일 양태는 검증 컨피규레이션 (65) 에 기초하여 상주 펌웨어 (14) 의 무결성을 검사하는 상주 펌웨어 검증 모듈 (20) 을 갖는 무선 디바이스 (12) 를 포함한다. 본 양태에서, 검증 컨피규레이션 (65) 은 사용자 관리자 서버 (40) 와 연관된 원격 펌웨어 관리 모듈 (21) 에 의해 생성되고, 원격 펌웨어 관리 모듈 (21) 로부터 수신된다 (이벤트 (200 및 201)). 예를 들어, 사용자 관리자 서버 (40) 는 무선 디바이스 (12) 로부터 무선

네트워크 (42) 를 가로질러 위치한, 서버와 같은 컴퓨터 디바이스 (18) 상에 상주할 수도 있다. 또한, 예를 들어, 검증 컨피규레이션 (65) 은 펌웨어 관리 모듈 (21) 과 연관된 컨피규레이터 모듈 (44) 을 실행함으로써 생성될 수도 있다. 일 양태에서, 검증 컨피규레이션 (65) 은 무선 디바이스 (12) 에 의해 실행 가능한 검증 방식 (89) 을 포함하는데, 이 검증 방식 (89) 은 펌웨어 (14) 에 적용되어 검증 테스트 결과 (47) 를 생성한다 (이벤트 (202)). 예를 들어, 일 양태에서, 검증 방식 (89) 은 펌웨어 (14) 의 적어도 일부에 적용되어 검증 테스트 결과 (47) 로서 체크섬 값을 생성하는 소정의 중복 검사를 포함하지만, 이에 한정되는 것은 아니다. 그러나, 아래에서 더 상세히 설명되는 바와 같이, 기타 검증 방식 (89) 을 사용하여, 검증 테스트 결과 (47) 를 얻을 수도 있다는 것에 주목해야 한다. 어느 경우이든, 상주 펌웨어 검증 모듈 (20) 은 예를 들어, 정보 로그 (46) 에 검증 테스트 결과 (47) 를 저장한다. 또한, 일 양태에서, 펌웨어 검증 모듈 (20) 은 무선 네트워크 (42) 를 가로질러 정보 로그 (46) 를 사용자 관리자 서버 (40) 에 전송한다 (이벤트 (204)). 사용자 관리자 서버 (40) 는 정보 리포지터리 (73) 에 정보 로그 (46) 를 저장하도록 동작할 수도 있다.

[0033] 사용자 관리자 서버 (40) 와 연관된 펌웨어 관리 모듈 (21) 은 정보 로그 (46) 에 액세스하고 분석기 (45) 를 실행하여, 무선 디바이스 (12) 상의 펌웨어 (14) 의 무결성을 나타내는 무결성 보고서 (61) 를 생성한다 (이벤트 (206)). 예를 들어, 일 양태에서, 분석기 (45) 는 소정의 검증 결과 (37) 를 포함하는데, 이 검증 결과 (37) 를 정보 로그 (46) 에 생성된 검증 테스트 결과 (47) 와 비교하여 무결성 결정 (11) 을 생성한다. 소정의 검증 결과 (37) 는, 소정의 검증 방식 (89) 을 변경되지 않은 버전의 펌웨어 (14) 에 적용한 결과에 대응하는, 임의 포맷의 알려진 데이터 또는 정보를 포함한다. 상술한 양태에서, 예를 들어, 소정의 검증 결과 (37) 는 위에서 설명한 생성된 체크섬 값과 비교되는 소정의 체크섬 값을 포함할 수도 있다. 이 경우에, 소정의 검증 결과 (37) 와 생성된 검증 테스트 결과 (47) 가 일치하면, 무결성 결정 (11) 은 펌웨어 (14) 가 변경되지 않음, 또는 적절한 상태임을 나타내는 출력일 수도 있다. 다른 방법으로는, 예를 들어, 일치하지 않으면, 무결성 결정 (11) 은 펌웨어 (14) 가 변경되었음을 나타내는 출력일 수도 있다. 또한, 아래에서 더 상세히 설명되는 바와 같이, 분석기 (45) 는 무결성 결정 (11) 을 포함한 무결성 보고서 (61) 를 생성하고, 검증 컨피규레이션 (65) 에 따라, 보고서 (61) 는 펌웨어 (14) 와 연관된 부가 펌웨어 정보 (15) 를 더 포함할 수도 있다.

[0034] 그 다음에, 펌웨어 관리 모듈 (21) 은 분석을 위해 운영자 컴퓨터 (22) 에 무결성 보고서 (61) 를 송신하는 것을 실행할 수도 있다 (이벤트 (208)). 일 양태에서, 예를 들어, 그 다음에, 운영자 컴퓨터 (22) 에서 운영자 (23) 는 무결성 보고서 (61) 를 검토하고, 보고서 (61) 내용에 기초하여, 사용자 관리자 서버 (40) 를 통해 무선 디바이스 (12) 에 제어 명령 (78) 을 송신하라는 결정을 내릴 수도 있다 (이벤트 (210, 212 및 216)). 일 양태에서, 운영자 (23) 는 펌웨어 관리 모듈 (21) 을 실행하여 무선 네트워크 (42) 를 가로질러 무선 디바이스 (12) 에 제어 명령 (78) 을 송신한다. 예를 들어, 제어 명령 (78) 은 다음과 같은 명령을 포함하지만, 이에 한정되는 것은 아니다: 무선 디바이스 (12) 의 사용자가 무선 네트워크 (42) 와 통신할 수 있는 능력을 셧다운하는 "디세이블" 명령; 펌웨어 컨피규레이션을 리로딩하거나 리셋하는 "리컨피규어 (reconfigure)" 명령; 및 무선 디바이스 (12) 의 사용자가 무선 네트워크 (42) 와 통신할 수 있는 능력을 재확립하는 "이네이블" 명령. 일 예로서, 운영자 (23) 는 무선 네트워크 (42) 에 적당한 프로토콜을 따르지 않는 메시지를 무선 디바이스 (12) 가 전송하는 것으로부터 무선 네트워크 (42) 를 보호하기 위해 무선 디바이스 (12) 를 디세이블하기로 결정할 수도 있다. 이와 유사하게, "리컨피규어" 명령을 전송하여 변경된 펌웨어 (14) 를 교정함으로써, 펌웨어를 복구하고, 펌웨어를 그 소정의 변경되지 않은 상태로 리턴시킬 수도 있고, 일단 변경된 펌웨어 (14) 가 교정되면 "디세이블" 명령 다음에 "이네이블" 명령을 전송하여 통신을 허락할 수도 있다.

[0035] 또한, 일 양태에서, 펌웨어 관리 모듈 (21) 은, 제어 명령 (78) 을 검토하고 무선 디바이스 (12) 에 제어 명령 (78) 을 송신할지 여부에 관한 허가 결정 (95) 을 내리는 (이벤트 (214)) 디바이스 제어 모듈 (94) 을 포함할 수도 있다. 예를 들어, 아래에서 더 상세히 설명되는 바와 같이, 허가 결정 (95) 은 제어 명령 (78) 의 소스 또는 생성기, 제어 명령 (78) 과 연관된 액션 타입, 및 무선 디바이스 (12) 및 이와 연관된 무선 네트워크 (42) 와 연관된 기타 인자에 기초할 수도 있다. 또한, 아래에서 더 상세히 설명되는 바와 같이, 몇몇 양태에서, 디바이스 제어 모듈 (94) 은 제어 명령 (78) 의 소스를 쿼리하여 무선 디바이스 (12) 에 전송하기 전에 제어 명령을 확인 및/또는 검증할 수도 있다.

[0036] 이와 관련하여, 일 양태에서, 펌웨어 검증 모듈 (20) 은 제어 명령 (78) 을 수신 및 실행하는 (이벤트 (218)) 디바이스 제어 모듈 (94) 을 포함할 수도 있다. 다른 양태에서, 로컬 디바이스 제어 모듈 (94) 은 제어 명령 (78) 의 소스 또는 생성기를 쿼리하여, 실행 전에 제어 명령을 확인할 수도 있다. 또한, 추가적으로 또는 다른 방법으로서, 디바이스 제어 모듈 (94) 은 사용자 관리자 서버 (40) 를 쿼리하여, 제어 명령 (78) 이 유

효한지 및/또는 제어 명령 (78) 의 발신자가 명령을 발할 권한이 있는지를 검증할 수도 있다.

[0037] 이와 같이, 본 발명의 장치, 방법, 컴퓨터 판독가능 매체 및 프로세서는 검증 테스트 결과 (47) 를 얻어서 무결성 결정 (11) 을 행하는데 사용하기 위해 검증 방식 (89) 을 생성하고 무선 디바이스 (12) 의 펌웨어 (14) 에 적용하는 것을 제공한다. 또한, 설명된 양태는 검증 컨피규레이션 (65) 에 기초한 부가 펌웨어 정보 (15) 의 수집, 분석, 및 보고를 제공할 수도 있고, 또한, 제어 명령 (78) 이 무결성 결정 (11) 에 응답하여 무선 디바이스 (12) 상에서 실행되는 것을 허용할 수도 있다.

[0038] 도 3 을 참조하면, 무선 디바이스 (12) 는, 셀룰러 전화기 (12), PDA (personal digital assistant), 양방향 문자 호출기 (text pager), 휴대용 컴퓨터와 같은 임의 타입의 컴퓨터화된 무선 디바이스를 포함할 수 있고, 무선 통신 포털을 가지며, 또한 네트워크나 인터넷에 유선 접속될 수도 있는 개별 컴퓨터 플랫폼까지도 포함할 수 있다. 무선 디바이스는 리모트-슬레이브 (remote-slave), 또는 최종 사용자 (end-user) 를 갖는 것이 아니라 단순히 리모트 센서, 진단 도구, 데이터 릴레이 등과 같은 무선 네트워크 (42) 를 가로질러 데이터를 통신하는 기타 디바이스일 수 있다. 따라서, 무선 디바이스 상에서 펌웨어를 검증, 수집, 및 보고하는 장치 및 방법은 무선 모뎀, PCMCIA 카드, 액세스 단말기, 개인용 컴퓨터, 전화기, 또는 그 임의의 컴비네이션이나 서브컴비네이션을 비롯한 유선 또는 무선 통신 포털을 포함하는 임의 형태의 무선 디바이스 또는 컴퓨터 모듈 상에서 수행될 수 있지만, 이에 한정되는 것은 아니다.

[0039] 또한, 무선 디바이스 (12) 는 무선 디바이스 내에 입력을 생성하는 입력 메커니즘 (96), 및 무선 디바이스의 사용자에 의해 소비되는 정보를 생성하는 출력 메커니즘 (97) 을 갖는다. 예를 들어, 입력 메커니즘 (96) 은 키 또는 키보드, 마우스, 터치스크린 디스플레이, 음성 인식 모듈 등과 같은 메커니즘을 포함할 수도 있다. 또한, 예를 들어, 출력 메커니즘 (97) 은 디스플레이, 오디오 스피커, 햅틱 (haptic) 피드백 메커니즘 등을 포함할 수도 있다.

[0040] 또한, 무선 디바이스 (12) 는, 무선 네트워크 (42) 를 가로질러 데이터를 송신할 수 있고, 소프트웨어 애플리케이션을 수신 및 실행할 수 있으며, 무선 네트워크 (42) 에 접속된 사용자 관리자 서버 (40) 또는 다른 컴퓨터 디바이스로부터 송신된 데이터를 표시할 수 있는 컴퓨터 플랫폼 (13) 을 갖는다. 컴퓨터 플랫폼 (13) 은 컴퓨터 플랫폼에 공통인 ROM (read-only memory) 및/또는 RAM (random-access memory), EPROM, EEPROM, 플래시 카드, 또는 임의의 메모리와 같은 휘발성 및 비휘발성 메모리를 포함할 수도 있는 데이터 리포지터리 (31) 를 포함한다. 또한, 데이터 리포지터리 (31) 는 하나 이상의 플래시 메모리 셀을 포함할 수도 있고, 또는 자기 매체, 광 매체, 테이프, 또는 소프트 디스크나 하드 디스크와 같은 임의의 제 2 또는 제 3 저장 디바이스일 수도 있다.

[0041] 또한, 컴퓨터 플랫폼 (13) 은 ASIC (application-specific integrated circuit), 또는 기타 칩셋, 프로세서, 로직 회로, 또는 기타 데이터 처리 장치일 수도 있는 처리 엔진 (87) 을 포함한다. 처리 엔진 (87) 또는 ASIC 과 같은 기타 프로세서는 무선 디바이스 (12) 의 데이터 리포지터리 (31) 에서 펌웨어 검증 모듈 (20) 과 같은 임의의 상주 프로그램과 인터페이싱하는 API (application programming interface) 계층 (34) 을 실행할 수도 있다. API (34) 는 각각의 무선 디바이스 상에서 실행되는 런타임 환경이다. 그러한 런타임 환경의 일 예로는 캘리포니아주 샌디에이고에 위치한 퀄컴사에 의해 개발된 BREW® (Binary Runtime Environment for Wireless®) 소프트웨어가 있다. 예를 들어, 무선 컴퓨팅 디바이스 상에서 애플리케이션 실행을 제어하도록 동작하는 기타 런타임 환경이 사용될 수도 있다.

[0042] 처리 엔진 (87) 은 무선 네트워크 (42) 상에서 무선 디바이스 (12) 의 기능성 및 무선 디바이스의 운용성을 이네이블하는 하드웨어, 펌웨어, 소프트웨어, 및 그 조합으로 구현된 다양한 처리 서브시스템 (88) 을 포함한다. 예를 들어, 처리 서브시스템 (88) 은 다른 네트워크화된 디바이스와의 통신의 개시 및 유지, 및 데이터 교환을 허용한다. 셀룰러 전화기와 같은 일 양태에서, 통신 처리 엔진 (87) 은 다음과 같은 처리 서브시스템들 (88) 중 하나 또는 조합을 포함할 수도 있다: 사운드, 비휘발성 메모리, 파일 시스템, 송신, 수신, 검색기, 계층 1, 계층 2, 계층 3, 메인 컨트롤, 원격 절차 (remote procedure), 핸드셋, 전력 관리, 진단, 디지털 신호 처리기, 보코더, 메시징, 호 관리자, Bluetooth® 시스템, Bluetooth® LPOS, 위치 결정, 위치 엔진, 사용자 인터페이스, 슬립, 데이터 서비스, 보안, 인증, USIM/SIM, 음성 서비스, 그래픽, USB, MPEG 나 GPRS 등과 같은 멀티미디어. 개시된 양태에서, 처리 엔진 (87) 의 처리 서브시스템 (88) 은 컴퓨터 플랫폼 (13) 상에서 실행되는 애플리케이션과 상호 작용하는 임의의 서브시스템 컴포넌트를 포함할 수도 있다. 예를 들어, 처리 서브시스템 (88) 은 상주 펌웨어 검증 모듈 (20) 대신에 API (34) 로부터의 데이터 판독 및 데이터 기입을 수신하

는 임의의 서브시스템 컴포넌트를 포함할 수도 있다. 또한, 수집된 다음에 정보 로그 (46) 에 기록되는 부가 펌웨어 정보 (15) 의 모두 또는 일부는 이들 서브시스템 (88) 으로부터 입수 가능하다.

[0043] 컴퓨터 플랫폼 (13) 은 무선 디바이스 (12) 와 무선 네트워크 (42) 사이뿐만 아니라, 무선 디바이스 (12) 의 여러 컴포넌트 사이에서 통신을 가능하게 하는, 하드웨어, 펌웨어, 소프트웨어, 및 그 조합으로 구현된 통신 모듈 (85) 을 더 포함할 수도 있다.

[0044] 또한, 컴퓨터 플랫폼 (13) 은 펌웨어 (14) 를 포함할 수도 있는데, 이 펌웨어 (14) 는 무선 디바이스 (12) 의 동작에 영향을 주는 펌웨어 코드 (84) 와 같은 실행 가능 명령어 세트 및/또는 펌웨어 데이터 (83) 와 같은 데이터를 포함한 임의의 비휘발성 메모리를 포함할 수도 있다. 예를 들어, 펌웨어 (14) 는 하드웨어 디바이스에 임베디드되는 소프트웨어를 포함할 수도 있다. 비휘발성 메모리의 몇몇 예로는 ROM, EPROM, EEPROM, 및 플래시 카드가 있다. 또한, 펌웨어 (14) 는 펌웨어 (14) 의 무결성을 결정하는데 사용되는 검증 정보 (19) 를 포함한다. 예를 들어, 검증 정보 (19) 는 펌웨어 (14) 를 구성하는 데이터 및/또는 실행 가능 명령어의 모두 또는 어떤 일부를 포함하지만, 이에 한정되는 것은 아니고, 펌웨어 (14) 를 구성하는 데이터 및/또는 실행 가능 명령어의 모두 또는 일부의 함수인 데이터를 더 포함할 수도 있다. 일 양태에서, 예를 들어, 검증 정보 (19) 는 주어진 펌웨어를 식별 및/또는 인증하는 정보인 펌웨어 서명 (80) 을 포함한다. 예를 들어, 펌웨어 서명 (80) 은 펌웨어 이름, 펌웨어 버전, 펌웨어 크기나 펌웨어 제조자 중 하나 이상을 나타내는 데이터를 포함하지만, 이에 한정되는 것은 아니다. 다른 예에서, 검증 정보 (19) 는 펌웨어 (14) 내의 소정의 위치 (82) 에 저장된 소정의 값 (81) 을 포함할 수도 있는데, 펌웨어 (14) 를 변경하려는 어떤 시도가 있으면 그 값 및/또는 위치가 변할 것이다. 또 다른 양태에서, 검증 정보 (19) 는 펌웨어 데이터 (83) 의 모두 또는 일부, 및/또는 펌웨어 코드 (84) 의 모두 또는 일부를 포함한다. 이 경우, 펌웨어 데이터 (83) 및/또는 펌웨어 코드 (84) 는 검증 방식 (89) 에 의해 조작되어 검증 테스트 결과 (47) 를 생성할 수도 있다.

[0045] 컴퓨터 플랫폼 (13) 은 무선 디바이스 (12) 상에서 펌웨어 검증 액티비티를 관리하는 펌웨어 검증 모듈 (20) 을 더 포함한다. 펌웨어 검증 모듈 (20) 은 무선 디바이스 (12) 의 펌웨어 (14) 의 무결성에 관련된 임의의 정보의, 무선 디바이스 (12) 상에서의 수집, 및 무선 네트워크 (42) 를 가로지르는 전송을 관리하도록 동작 가능한 임의의 하드웨어, 소프트웨어, 펌웨어 및/또는 기타 실행 가능 명령어 세트를 포함할 수도 있다. 일 양태에서, 펌웨어 검증 모듈 (20) 은 검증 컨피규레이션 (65) 에 기초하여 정보를 수집, 저장 및 정보에의 액세스를 제공하고, 또는 정보를 전송할 수 있는 능력을 제공하는 검증 로직 (24) 을 포함한다. 또한, 몇몇 양태에서, 검증 로직 (24) 은 검증 테스트 결과 (47) 를 생성하고, 이 결과를 소정의 검증 결과 (37) 와 비교하여 무결성 결정 (11) 을 생성할 수 있는 능력을 제공할 수도 있다. 펌웨어 검증 모듈 (20) 은 어느 때라도 개시될 수도 있고, 정보 로그 (46) 에 기록된 검증 테스트 결과 (47) 및/또는 부가 펌웨어 정보 (15) 를 무선 디바이스 (12) 상에 저장하여 무선 디바이스 (12) 와의 유선 또는 무선 접속을 통해 어느 때라도 얻을 수도 있다.

[0046] 펌웨어 검증 모듈 (20) 은 펌웨어 사용 및/또는 검증에 관련된 임의의 펌웨어 검증 정보를 수집할 수 있다. 검증 컨피규레이션 (65) 에 기초하여, 펌웨어 검증 모듈 (20) 은 펌웨어 검증 방식 (89) 을 펌웨어 (14) 에 적용하고, 검증 테스트 결과 (47) 를 생성할 수도 있다. 또한, 펌웨어 검증 모듈 (20) 은, 상주 데이터 리포지터리 (31) 내에 또는 무선 네트워크 (42) 를 통해 무선 디바이스에 접속 가능하거나 무선 디바이스 (12) 에 액세스 가능한 다른 메모리 디바이스 내에, 정보 로그 (46) 내의 이러한 정보를 저장할 수도 있다. 또한, 정보 로그 (46) 는 수집된 펌웨어 검증 정보와 관련하여 검증 컨피규레이션 (65) 의 상세를 포함할 수도 있다.

[0047] 소정의 검증 결과 (37) 가 무선 디바이스 (12) 에 알려져 있는 일 양태에서, 예를 들어, 소정의 검증 결과가 검증 컨피규레이션 (65) 에 포함되어 있으면, 펌웨어 검증 모듈 (20) 은 검증 로직 (24) 을 실행하여 테스트 결과 (47) 를 소정의 결과 (37) 와 로컬 비교함으로써 펌웨어 (14) 의 무결성 결정 (11) 을 얻을 수도 있다. 이와 같이, 일 양태에서, 펌웨어 검증 모듈 (20) 은 무선 디바이스 (12) 상의 펌웨어 정보를 검색 및 기록하는 상주 또는 자급식 (self-contained) 능력뿐만 아니라 그러한 펌웨어 정보의 전송 및 원격 분석을 허용하는 상주 또는 자급식 능력을 무선 디바이스 (12) 에 제공한다.

[0048] 다른 방법으로는, 펌웨어 검증 모듈 (20) 은 테스트 결과 (47) 및/또는 정보 로그 (46) 를 다른 컴퓨터 디바이스에 송신하여 무선 디바이스 (12) 의 펌웨어 (14) 의 무결성을 얻을 수도 있다. 예를 들어, 펌웨어 검증 모듈 (20) 은 무선 디바이스 (12) 로 하여금 정보 로그 (46) 를 무선 네트워크 (42) 를 가로질러 사용자 관리자 서버 (40) 에 선택적으로 송신하게 할 수도 있다. 일 양태에서, 정보 로그 (46) 는 무선 디바이스 (12) 로부터 무선 네트워크 (42) 에 개방형 통신 접속을 통해 송신되어, 무선 디바이스 (12) 에서 음성 또는 데이터 호와 같이 개방형 접속을 가로질러 "피기백 (piggyback)" 된다. 셀룰러 네트워크 구성에 있어서, 정보 로그

(46) 는 단문 메시지 서비스를 통해 사용자 관리자 서버 (40) 에 송신될 수 있다.

[0049] 다른 양태에서, 원격 사용자 관리자 서버 (40) 는 무선 디바이스 (12) 로부터 상주 펌웨어 검증 모듈 (20) 을 통해 정보 로그 (46) 를 판독하고, 몇몇 경우에는, 제어 명령 (78) 을 컴퓨터 플랫폼 (13) 에 기입하며 펌웨어 (14) 를 리셋하는 것과 같이 무선 디바이스 (12) 의 동작을 변경한다. 따라서, 펌웨어 검증 모듈 (20) 에의 액세스를 통해, 사용자 관리자 서버 (40) 는 펌웨어 검증 정보 수집, 분석 및 보고를 위한 파라미터를 원격으로 제어할 수 있게 된다.

[0050] 펌웨어 검증 모듈 (20) 은 검증 컨피규레이션 (65) 에 기초하여 동작한다. 검증 컨피규레이션 (65) 은 무선 네트워크 (42) 에 접속된 임의의 컴퓨터 디바이스에 의해 생성될 수도 있고, 또는 예를 들어, 사용자로부터의 수동 입력에 의해, 및/또는 로컬 접속된 미디어 리더로부터의 전송을 통해 무선 디바이스 (12) 에 로컬 송신될 수도 있고, 또는 심지어 제조 시 무선 디바이스 (12) 상에 로딩되었을 수도 있다. 아래에 설명하는 바와 같이, 일 양태에서, 예를 들어, 검증 컨피규레이션 (65) 은 사용자 관리자 서버 (40) 에 의해 생성된다.

[0051] 검증 컨피규레이션 (65) 은 펌웨어 검증 모듈 (20) 에 의해 수행될 동작을 명령하는 명령어 및 데이터를 포함한다. 예를 들어, 상술한 바와 같이, 검증 컨피규레이션 (65) 은 검증 방식 (89) 을 포함할 수도 있는데, 이 검증 방식 (89) 은 펌웨어 (14) 의 무결성을 테스트하는 명령어를 포함한다. 검증 방식 (89) 은 다음과 같은 테스트에 관련된 명령어를 포함할 수도 있지만, 이에 한정되는 것은 아니다: 체크섬, 패리티 비트, 체크 디지트, 세로 중복 검사 (longitudinal redundancy check), 순환 중복 검사 (cyclic redundancy check; CRC), 수평 중복 검사 (horizontal redundancy check), 수직 중복 검사 (vertical redundancy check), 암호 메시지 다이제스트 (cryptographic message digest), 플레처 체크섬 (Fletcher's checksum), 및 애들러-32 (Adler-32) 를 비롯한 중복 검사; 펌웨어 (14) 내의 소정의 위치에서 소정의 값에 대한 테스팅; 및 펌웨어 (14) 내에 포함된 데이터 및/또는 코드의 모두 또는 일부에 소정의 함수를 적용한 소정의 결과에 대한 테스팅. 다른 방법으로는, 검증 방식 (89) 은 예를 들어, 무선 네트워크 (42) 를 가로질러 다른 컴퓨터 디바이스와 같은 소정의 소스로부터 소정의 검증 방식을 검색하는 명령어를 포함할 수도 있다. 또한, 예를 들어, 펌웨어 (14) 의 일정 부분의 변화를 추적하거나 보안을 강화하기 위해서는, 펌웨어 (14) 를 조각낼 수도 있고, 하나 이상의 검증 방식 (89) 을 펌웨어 (14) 의 세그먼트 중 하나 이상에 적용할 수도 있다. 그 자체로서, 검증 방식 (89) 은 펌웨어 (14) 의 각각의 세그먼트에 적용되는 방식을 식별할 수도 있다.

[0052] 예를 들어, 도 4 를 참조하면, 펌웨어 검증 방식 (89) 의 일 양태는 CRC 알고리즘을 포함하는데, 펌웨어 검증 모듈 (20) 은 이 CRC 알고리즘을 펌웨어 (14) 의 상이한 세그먼트에 적용한다. 일 양태에서, 펌웨어 (14) 는 코드 세그먼트 (306, 308, 310) 와 같은 소정 개수의 코드 세그먼트, 및 데이터 세그먼트 (312, 314, 316) 와 같은 소정 개수의 데이터 세그먼트로 분할된다. 검증 로직 (24) 은 검증 컨피규레이션 (65) 을 실행하여, CRC 알고리즘을 각각의 세그먼트 (306, 308, 310, 312, 314, 316) 에 적용하고, 검증 테스트 결과 값 (322, 324, 326, 328, 330, 332) 을 생성한다. 또한, 검증 컨피규레이션 (65) 이 소정의 검증 결과 (37) 를 포함하는 본 양태에서는, 검증 로직 (24) 을 실행하여 테스트 결과 값 (322, 324, 326, 328, 330, 332) 을 소정의 검증 값 (334, 336, 338, 340, 342, 344) 과 비교함으로써, 펌웨어 (14) 의 각각의 세그먼트에 대한 무결성 결정 (11) 을 생성한다. 그러나, 다른 경우에는, 소정의 검증 값 (334, 336, 338, 340, 342, 344) 이 예를 들어, 사용자 관리자 서버 (40) 와 같은 다른 컴퓨터 디바이스에 저장될 수도 있고, 생성된 검증 테스트 결과 값 (322, 324, 326, 328, 330, 332) 이 비교를 위해 무선 디바이스 (12) 로부터 기타 디바이스에 송신된다. 어느 경우이든, 펌웨어를 세그먼트로 분할하는 본 방법은 몇몇 이유 때문에 유익하다. 우선, 단지 세그먼트 중 하나 이상이 무결성 문제가 있는 것으로 발견되면, 그 세그먼트만을 복원하면 될 것이다. 또한, 무선 디바이스의 동작에 중요하지 않은 세그먼트가 무결성 문제가 있는 것으로 발견된 유일한 세그먼트이면, 무선 디바이스 (12) 를 디세이블하지 않아도 된다. 또한, 다수의 펌웨어 검증 방식 (89) 은 펌웨어 (14) 의 보다 소수의 데이터 항목에 적용될 때 더 신뢰성 있게 동작할 수도 있다. 예를 들어, 펌웨어 (14) 의 데이터 항목이 보다 소수인 경우에, 패리티에 기초한 펌웨어 검증 방식 (89) 을 더 신뢰할 수도 있다.

[0053] 계속 도 4 를 참조하면, 다른 펌웨어 검증 방식 (89) 은 단순히 펌웨어 서명 (80) 을 기록할 수도 있다. 예를 들어, 이 경우에, 펌웨어 서명 (80) 은 펌웨어 버전 (81), 펌웨어 크기 (82), 및 현재 날짜 (83) 와 관련된 값 또는 데이터를 포함할 수도 있다. 그러면, 이러한 정보는 이 경우에 소정의 펌웨어 버전, 소정의 펌웨어 크기, 및 소정의 날짜인 소정의 검증 테스트 결과 값 (37) 과 비교되어, 펌웨어 (14) 의 무결성을 결정한다.

[0054] 또한, 다시 도 3 을 참조하면, 검증 컨피규레이션 (65) 은 정보 로그 (46) 내에 어느 정보를 수집해야 하는지, 또한 이 정보를 얼마나 자주 수집해야 하는지를 명령하는 추적 파라미터 (90) 를 더 포함할 수도 있다. 예

를 들어, 추적 파라미터 (90) 는 검증 방식 (89) 을 얼마나 자주 개시해야 하는지에 관한 명령어, 및 생성된 검증 테스트 결과 (47) 를 기록하라는 명령어를 포함할 수도 있다. 또한, 예를 들어, 추적 파라미터 (90) 는 어느 부가 펌웨어 정보 (15) 를 수집해야 하는지, 또한 그 부가 펌웨어 정보 (15) 를 언제 수집해야 하는지를 규정하는 명령어를 포함할 수도 있다. 예를 들어, 추적 파라미터 (90) 는 소정의 상태 또는 상태 정보를 식별하여, 소정의 애플리케이션 및/또는 소정의 서브시스템 (88) 으로부터 소정 시간에 부가 펌웨어 정보 (15) 로서 수집할 수도 있다. 부가 펌웨어 정보 (15) 는 성공한 및/또는 성공하지 못한 펌웨어 액세스 시도, 펌웨어에 행해진 변경, 무선 디바이스 (12) 및/또는 서브시스템 (88) 에 의해 수행 중인 동작에 관련된 임의의 정보, 무선 디바이스 진단 정보, 무선 디바이스 (12) 상의 임의의 상주 애플리케이션의 상태 및/또는 동작에 관련된 정보 등을 포함할 수도 있지만, 이에 한정되는 것은 아니다. 또한, 예를 들어, 추적 파라미터 (90) 는 제어 명령 (78) 의 실행과 같은 디바이스 상에서 일어나고 있는 어떤 액티비티나 액션의 추적을 명령하고, 액션 레코드 (49) 와 같은 정보 로그 (46) 내에 이들 액티비티/액션에 관련된 정보 저장을 요청한다.

[0055] 또한, 검증 컨피규레이션 (65) 은 펌웨어 검증 모듈 (20) 이 언제 정보 로그 (46) 를 보고하거나 송신해야 하는지, 또는 정보 로그 (46) 에의 액세스를 누구에게 허용할지를 규정하는 보고 파라미터 (91) 를 포함할 수도 있다. 예를 들어, 보고 파라미터 (91) 는 펌웨어 검증 방식 (89) 을 펌웨어 (14) 에 적용한 후에 즉시 정보 로그 (46) 를 송신하라는 명령어를 포함할 수도 있다. 기타 보고 파라미터 (91) 는 소정 시간 또는 소정 구간으로, 또는 무선 네트워크 (42) 와의 통신 채널 확립과 같은 소정 이벤트의 발생 시에 정보 로그 (46) 를 송신하라는 명령어를 포함할 수도 있다.

[0056] 또한, 일 양태에서, 검증 컨피규레이션 (65) 은 제어 명령 파라미터 (92) 를 포함할 수도 있는데, 이 제어 명령 파라미터 (92) 는 무선 디바이스 (12) 상의 동작을 제어하기 위해 소정의 컨디션 (93) 과 연관된 제어 명령 (78) 을 포함할 수도 있다. 예를 들어, 무선 디바이스 (12) 가 생성된 검증 테스트 결과 (47) 를 소정의 검증 테스트 결과 (37) 와 비교함으로써 무결성 결정 (11) 을 로컬 생성하는 경우에, 제어 명령 파라미터 (92) 는 틀리거나 변경된 펌웨어 (14) 가 발견된 경우에 펌웨어 검증 모듈 (20) 이 무선 디바이스 (12) 를 로컬 제어하는 것을 허용할 수도 있다. 예를 들어, 컨디션 (93) 은 다음과 같은 어떤 무결성 결정 (11) 일 수도 있다: (1) 적절한 펌웨어가 존재함을 나타내는 결정, 및 (2) 펌웨어 (14) 가 변경되었음을 나타내는 결정. 컨디션 (1) 의 경우에, 제어 명령 (78) 은 무선 디바이스 (12) 의 동작을 실행하라는 "동작 계속 (continue operation)" 명령일 수도 있다. 컨디션 (2) 의 경우에, 제어 명령 (78) 은 무선 네트워크 (42) 와 통신하는 무선 디바이스 (12) 의 능력을 셧다운하라는 "디세이블 (disable)" 명령일 수도 있다. 주어진 애플리케이션에 따라, 제어 명령 파라미터 (92) 에 포함될 수도 있는 다양한 컨디션 (93) 및 대응하는 제어 명령 (78) 이 존재할 수도 있다. 예를 들어, 몇몇 실시예에서, 다양한 파라미터, 비교 및 결과는 정보 로그 (46) 에 기록될 수도 있다. 또한, 제어 명령 (78) 과 연관된 이들 액션과 같은, 검증 컨피규레이션 (65) 에 기초하여 수행되는 액션은 액션 레코드 (49) 에 기록될 수도 있다 (도 3).

[0057] 이와 같이, 검증 컨피규레이션 (65) 은 펌웨어 검증 모듈 (20) 의 동작을 제어하는 플렉서블 (flexible) 수단을 제공한다.

[0058] 또한, 몇몇 양태에서, 펌웨어 검증 모듈 (20) 은 로컬 생성되거나 원격 생성된 제어 명령 (78) 을 수신하도록 동작 가능한 디바이스 제어 모듈 (94) 을 포함한다. 또한, 디바이스 제어 모듈 (94) 은 무선 디바이스 (12) 상에서 제어 명령 (78) 을 실행하도록 동작 가능한 제어 로직을 포함할 수도 있다. 아래에서 더 상세히 설명되는 바와 같이, 디바이스 제어 모듈 (94) 은 무선 디바이스 (12) 상에서 제어 명령 (78) 을 실행하기 전에 제어 명령 (78) 을 검증할 수도 있다.

[0059] 예를 들어, 제어 명령 (78) 은 각각의 무선 디바이스 (12) 상에서 실행될 수 있는 임의의 동작일 수도 있고, 디세이블 명령, 이네이블 명령, 및 리컨피규어 명령과 같은 명령을 포함하지만, 이에 한정되는 것은 아니며, 여기서, 디세이블 명령은 무선 디바이스 (12) 를 비긴급 통신 동안 동작 불가 상태로 만들거나 완전히 동작 불가 상태로 만들고, 이네이블 명령은 무선 디바이스 (12) 를 통신 동안 동작 가능 상태로 만들며, 리컨피규어 명령은 무선 디바이스의 동작 특성에 관련된 펌웨어 값 중 하나 이상을 설정한다. 몇몇 실시예에서, 예를 들어, 리컨피규어 명령은 예를 들어, 펌웨어 (14) 상에 소프트웨어를 겹쳐 쓰도록 (over-write) 동작 가능한 소프트웨어 패치를 포함함으로써 OTA (over-the-air) 로 펌웨어 데이터 및/또는 값을 변경하는 것을 포함할 수도 있다. 일반적으로, 제어 명령 (78) 은 펌웨어 검증 모듈 (20) 의 결과에 응답하여 로컬 또는 원격으로 발행되고, 보통은 펌웨어 (14) 의 무결성을 얻는 것에 응답하여 발행될 것이다.

[0060] 또한, 펌웨어 검증 모듈 (20) 은 무선 네트워크 (42) 를 가로질러 제한된 액세스 통신 채널을 확립하도록 동작

가능한 제한된 서비스 컨피규레이션 (38) 을 포함할 수도 있는데, 일 양태에서, 제한된 액세스 통신 채널은 통상 무선 디바이스 (12) 의 최종 사용자에게 이용 가능하지 않다. 예를 들어, 제한된 액세스 통신 채널은 정보 로그 (46) 를 송신하거나 제어 명령 (78) 을 수신하는데 사용될 수도 있다. 또한, 달리 무선 디바이스 (12) 로부터의 통신이 디세이블된 경우에, 제한된 액세스 통신 채널은 "911" 호출과 같은 긴급 호출을 허용하거나, 무선 네트워크 제공자와 연관된 운영자나 기타 지정된 당사자에 대한 호출을 허용할 수도 있다. 제한된 액세스 통신 채널의 ID (identification) 및 설정은 제한된 서비스 설정 (39) 에 기초한다. 제한된 서비스 설정 (39) 은 허용되는 통신 타입을 식별할 수도 있으며, 사용 가능한 연관된 통신 채널을 식별할 수도 있다.

제한된 서비스 컨피규레이션 (38) 은 무선 네트워크 (42) 를 통해 수신될 수도 있고, 예를 들어, 직렬 접속을 통해 무선 디바이스 (12) 에 로컬 전송될 수도 있고, 또는 무선 디바이스 (12) 상에 미리 로딩될 수도 있다.

[0061] 다시 도 1 을 참조하면, 무선 네트워크 (42) 는 적어도 부분적으로, 무선 네트워크 (42) 에 접속된 무선 디바이스 (12) 와 임의의 기타 디바이스 간의 무선 통신을 가능하게 하도록 동작 가능한 임의의 통신 네트워크를 포함한다. 또한, 무선 네트워크 (42) 는 모든 네트워크 컴포넌트, 및 네트워크를 구성하는 모든 접속된 디바이스를 포함할 수도 있다. 예를 들어, 무선 네트워크 (42) 는 다음 네트워크 중 하나 이상, 또는 임의의 조합을 포함할 수도 있다: 셀룰러 전화 네트워크, 지상 전화 네트워크, 위성 전화 네트워크; IrDA (Infrared Data Association) 기반 네트워크와 같은 적외선 네트워크; 단거리 무선 네트워크; Bluetooth® 기술 네트워크; ZigBee® 프로토콜 네트워크; UWB (ultra wide band) 프로토콜 네트워크; HomeRF (home radio frequency) 네트워크; SWAP (shared wireless access protocol) 네트워크; WECA (wireless Ethernet compatibility alliance) 네트워크, Wi-Fi Alliance (wireless fidelity alliance) 네트워크, 및 802.11 네트워크와 같은 광대역 네트워크; 공중 전화 교환 네트워크; 인터넷과 같은 공중 이종 통신 네트워크; 사설 통신 네트워크; 및 육상 이동 무선 네트워크. 전화 네트워크의 적절한 예는 다음과 같은 아날로그 및 디지털 네트워크/기술 중 하나 이상, 또는 임의의 조합을 포함한다: CDMA (code division multiple access), WCDMA (wideband code division multiple access), UMTS (universal mobile telecommunications system), AMPS (advanced mobile phone service), TDMA (time division multiple access), FDMA (frequency division multiple access), OFDMA (orthogonal frequency division multiple access), GSM (global system for mobile communications), 1X (single carrier) RTT (radio tranmission technology), EV-DO (evolution data only) 기술, GPRS (general packet radio service), EDGE (enhanced data GSM environment), HSPDA (high speed downlink data packet access), 아날로그 및 디지털 위성 시스템, 및 무선 통신 네트워크 및 데이터 통신 네트워크 중 하나 이상에서 사용될 수도 있는 임의의 기타 기술/프로토콜.

[0062] 사용자 관리자 서버 (40) 는 임의 타입의 하드웨어, 소프트웨어, 펌웨어, 서버, 개인용 컴퓨터, 미니 컴퓨터, 메인프레임 컴퓨터, 또는 전용 또는 범용 컴퓨팅 디바이스와 같은 임의의 컴퓨팅 디바이스 중 하나 이상을 포함할 수도 있다. 또한, 사용자 관리자 서버 (40) 는 전적으로 무선 디바이스 (12) 상에 상주할 수도 있다.

또한, 사용자 관리자 서버 (40) 와 연관된 별개 서버 또는 컴퓨터 디바이스가 함께 동작하여, 당사자에게 사용 가능한 포맷으로 데이터를 제공하고/하거나 무선 디바이스 (12) 와 사용자 관리자 서버 (40) 간의 데이터 흐름 제어를 위해 별개 계층을 제공할 수 있다. 사용자 관리자 서버 (40; 또는 복수의 모듈) 는 무선 네트워크 (42) 를 가로질러 상주 펌웨어 검증 모듈 (20) 과 같은 소프트웨어 에이전트 또는 애플리케이션을 무선 디바이스 (12) 에 송신하여, 무선 디바이스 (12) 가 그 상주 애플리케이션 및 서브시스템으로부터의 정보를 리턴하도록 할 수 있다. 예를 들어, 무선 디바이스 (12) 는 펌웨어 검증 방식 (89) 을 펌웨어 (14) 에 적용한 결과를 정보 로그 (46) 의 형태로 송신할 수 있는데, 그러면, 사용자 관리자 서버 (40) 는 이 결과를 소정의 검증 결과 (37) 와 비교하여 무선 디바이스 (12) 의 펌웨어 무결성을 나타내는 무결성 결정 (11) 을 생성할 수도 있다.

[0063] 사용자 관리자 서버 (40) 는 펌웨어 검증 동작을 관리하는 원격 펌웨어 관리 모듈 (21) 을 포함한다. 원격 펌웨어 관리 모듈 (21) 은 사용자 관리자 서버 (40) 에 의해 동작 가능한 소프트웨어, 하드웨어, 펌웨어, 및 일반적인 임의의 실행 가능 명령어를 포함할 수도 있다. 원격 펌웨어 관리 모듈 (21) 은 펌웨어 검증 모듈 (20) 의 상주 버전의 모두 또는 일부를 무선 디바이스 (12) 에 다운로딩할 수도 있다. 다른 방법으로는, 원격 펌웨어 관리 모듈 (21) 의 상주 버전은 초기 조립 프로세스 동안에 무선 디바이스 (12) 상에 로딩되거나 컨피규레이션 프로세스 동안에 직접 접속을 통해 로딩될 수도 있다. 또한, 원격 펌웨어 관리 모듈 (21) 은, 무선 디바이스 (12) 로부터 검증 컨피규레이션 (65) 을 생성하고 정보 로그 (46) 의 수집 및 분석을 관리하도록 사용자 관리자 서버 (40) 에 의해 실행 가능한 검증 로직 (59) 을 포함한다. 소정의 메모리/데이터 저장 레벨에 도달할 때, 또는 무선 디바이스 (12) 가 무선 디바이스 (12) 와 무선 네트워크 (42) 간에 부적절한 프로토

콜을 제공하는 것과 같은 소정의 컨디션에 도달할 때, 소정 시간에서 원격 펌웨어 관리 모듈 (21) 은 사용자로부터의 명령에 기초하여 로그 (46) 를 "풀링 (pull)" 하거나, 무선 디바이스 (12) 로부터 로그를 "푸싱 (push)" 할 수도 있다.

[0064] 도 1 및 도 5 를 참조하면, 일 양태에서, 원격 펌웨어 관리 모듈 (21) 은, 하드웨어, 펌웨어, 소프트웨어 및/또는 컨피규레이터 모듈 (44) 이 검증 컨피규레이션 (65) 을 생성할 수 있도록 해주는 임의의 기타 연관된 로직을 포함하는 컨피규레이터 모듈 (44) 을 포함한다. 일 양태에서, 컨피규레이터 모듈 (44) 은 다수의 가변 파라미터 중에서 행해진 선택에 기초하여 주어진 검증 컨피규레이션 (65) 의 다양한 컴포넌트를 어셈블링하는 컨피규레이션 로직 (56) 을 실행한다. 예를 들어, 검증 컨피규레이션 (65) 을 구성하는 그 파라미터는 무선 디바이스 및/또는 네트워크 서비스 제공자의 타입/메이크/모델에 따라 변할 수도 있다. 그 자체로서, 컨피규레이션 로직 (56) 은 복수의 무선 디바이스 타입 (16) 및 복수의 네트워크 서비스 제공자 (17) 의 메뉴에서 선택할 수 있는 능력을 사용자에게 제공하여, 검증 컨피규레이션 (65) 의 파라미터가 선택될 적절한 메뉴를 생성할 수도 있다. 이와 유사하게, 각 타입의 파라미터 중 하나 이상을 선택하여 검증 컨피규레이션 (65) 을 구성할 수도 있다. 예를 들어, 컨피규레이션 로직 (56) 은 복수의 펌웨어 검증 방식 (50), 복수의 추적 파라미터 (51), 복수의 보고 파라미터 (52), 복수의 제어 명령 파라미터 (53) 및 복수의 소정의 검증 결과 값 (54) 중 하나 이상의 메뉴에서 선택할 수 있는 능력을 사용자에게 제공할 수도 있다. 다른 방법으로는, 여러 파라미터를 개별적으로 선택하기보다는, 컨피규레이션 로직 (56) 은 검증 컨피규레이션 (65) 을 구성하는 상술한 파라미터의 소정 그룹화를 포함하는 복수의 소정의 검증 컨피규레이션 (55) 의 메뉴에서 선택할 수 있는 능력을 사용자에게 제공할 수도 있다. 또한, 일 양태에서, 복수의 무선 디바이스 타입 (16) 중 선택된 무선 디바이스 타입과 복수의 네트워크 서비스 제공자 (17) 중 선택된 네트워크 서비스 제공자는 특정 무선 디바이스 (12) 에 적절한 소정의 검증 파라미터 세트 및/또는 복수 타입의 펌웨어 (63) 중 소정의 하나와 상관될 수도 있다. 예를 들어, ABC 무선 서비스 제공자 상에서 동작하는 XYZ 브랜드의 무선 디바이스의 경우에, 컨피규레이션 로직 (56) 은 무선 디바이스 (12) 에 어떤 펌웨어 (14) 가 설치되어야 하는지를 결정할 수도 있으므로, 적절한 대응 파라미터 세트를 포함하는 검증 컨피규레이션 (65) 을 생성할 수도 있다.

[0065] 일단 검증 컨피규레이션 (65) 이 결정되면, 컨피규레이터 모듈 (44) 및/또는 원격 펌웨어 관리 모듈 (21) 은 하나 이상의 무선 디바이스 (12) 에 검증 컨피규레이션 (65) 을 송신하여 그 디바이스 상에서 펌웨어 검증의 추적 및 관리를 개시하도록 동작 가능하다.

[0066] 원격 펌웨어 관리 모듈 (21) 은 검증 컨피규레이션 (65) 실행에 기초하여 무선 디바이스 (12) 로부터 수신된, 검증 테스트 결과 (47) 및/또는 부가 펌웨어 정보 (15) 를 비롯한, 정보 로그 (46) 를 저장하는 정보 리포지터리 (73) 를 포함할 수도 있다. 정보 리포지터리 (73) 는 임의 타입의 메모리 또는 저장 디바이스를 포함할 수도 있다. 원격 펌웨어 관리 모듈 (21) 과 연관된 것으로서 도시되어 있지만, 정보 리포지터리 (73) 는 예를 들어, 무선 네트워크 (42) 에 접속된 다른 서버 또는 컴퓨터 디바이스 상에, 무선 디바이스 (12) 상에 또는 무선 네트워크 보조 컴퓨터 (22) 상에 사용자 관리자 서버 (40) 와 통신하여 어디든지 위치할 수도 있다.

[0067] 또한, 상술한 바와 같이, 원격 펌웨어 관리 모듈 (21) 은 분석기 (45) 를 포함할 수도 있는데, 이 분석기 (45) 는 보고서 (61) 및 무결성 결정 (11) 을 생성하기 위해 정보 리포지터리 (73) 에 기록된 펌웨어 검증 정보를 분석 및 처리하는 하드웨어, 소프트웨어, 펌웨어 및 그 조합을 포함할 수도 있다. 또한, 분석기 (45) 는 정보 리포지터리 모듈 (73) 에 포함된 정보 로그 (46) 를 분석 및 해석하는 알고리즘, 의사 결정 루틴, 통계 프로그램 등을 포함한 분석 로직 (41) 을 더 포함할 수도 있다. 원격 펌웨어 관리 모듈 (21) 과 연관된 것으로서 도시되어 있지만, 분석기 (45) 는 무선 네트워크 (42) 에 접속된 다른 서버 상에, 무선 디바이스 (12) 상에 또는 무선 네트워크 보조 컴퓨터 (22) 상에 사용자 관리자 서버 (40) 와 통신하여 어디든지 위치할 수도 있다.

[0068] 또한, 다수의 펌웨어 검증 방식 (89) 이 발견적 방법 (heuristic) 이기 때문에, 얻어진 펌웨어 (14) 의 무결성 결정 (11) 은 주관적인 값 또는 확률일 수도 있다. 또한, 상술한 바와 같이, 얻어진 펌웨어 (14) 의 무결성 결정 (11) 은 또한 특정 시간에 무선 디바이스 (12) 의 특정 메이크 및/또는 모델에 펌웨어 (14) 의 어떤 버전 (81) 이 설치되는지에 따라 다를 수도 있다. 따라서, 예를 들어, 기존 펌웨어 (14) 가 손상되지 않았거나, 제조 시 무선 디바이스 (12) 에는 적당한 펌웨어 (14) 이었지만, 더 이상 펌웨어 (14) 의 현재 유효 버전 (81) 이 아닐 수도 있으므로, 이 경우에, 분석기 (45) 는 펌웨어 (14) 의 무결성이 손상된 것으로 결정할 수도 있다.

[0069] 또한, 일 양태에서, 펌웨어 무결성 결정 (11) 은 무선 디바이스 (12) 가 적당한 펌웨어 (14) 를 가지고 있는지 여부, 및 무선 디바이스 (12) 상의 펌웨어가 손상되었는지, 또는 손상될 수도 있는지 여부 양자의 측정 또는 펌웨어 (14) 가 손상되지 않았다는 확실성의 측정이다. 따라서, 예를 들어, 무선 디바이스 (12) 가 더 이상

네트워크 서비스 제공자에 의해 지원되지 않는 펌웨어 (14) 의 버전을 갖는 경우, 또는 검증 테스트 결과 (47) 를 소정의 검증 결과 (37) 와 비교하여 측정된 바와 같이 무선 디바이스 (12) 상의 펌웨어 (14) 의 버전이 손상되었을 수도 있는 경우, 무선 디바이스 (12) 상의 펌웨어 (14) 의 무결성 결정 (11) 은 낮은 무결성을 나타낼 수도 있다. 몇몇 양태에서, 이러한 검증 테스트 결과 (47) 와 소정의 검증 결과 (37) 의 비교는 단지 펌웨어 (14) 가 손상되었는지 여부의 일 지시일 수도 있으므로, 무결성 결정 (11) 은 예를 들어, "십중팔구 (most likely)", "10% 가능성 (10% chance)" 등과 같은 확률이나 주관적인 카테고리일 수도 있다.

[0070] 일 양태에서, 보고서 (61) 및/또는 정보 로그 (46) 는 특정 무선 디바이스 (12) 와 연관된 펌웨어 검증 관련 정보의 평가를 위해, 예를 들어, 무선 디바이스 (12) 의 기술자, 필드 엔지니어, 운송업자, 운영자 (23) 또는 사용자에 의해 수동으로 검토될 수도 있다. 무선 디바이스 (12) 의 운영자 (23) 또는 사용자는 정보 로그 (46) 및/또는 보고서 (61) 에 기초하여 각각의 무선 디바이스 (12) 에 대한 "무선 디바이스 디세이블" 명령과 같은 새로운 검증 컨피규레이션 (65) 또는 제어 명령 (78) 을 생성할 수도 있다. 통상, 보고서 (61) 는 정보 로그 (46) 의 분석을 통해 펌웨어 검증에 관련된 문제를 검출 및 교정하는데 있어서 유용할 수도 있다. 그 자체로서, 보고서 (61) 는 바이러스 보고서, 무선 디바이스 (12) 에 적절한 펌웨어 버전, 부적절한 펌웨어 버전에 대한 셧다운 시간 등과 같은 소정의 표준 (37) 에 통합될 수도 있는 임의의 기타 관련 정보뿐만 아니라, 정보 리포지터리 (73) 에 포함된 정보 로그 (46) 및 기타 정보의 분석을 표현한 임의 형태의 출력을 포함한다.

[0071] 보고서 (61) 를 생성하는 것으로서 도시되어 있지만, 펌웨어 관리 모듈 (21) 및 그 대응하는 컴포넌트는 테이블, 맵, 그래픽 뷰, 플레인 텍스트, 인터랙티브 프로그램 또는 웹 페이지, 또는 임의의 기타 데이터 디스플레이 또는 프레젠테이션과 같은 임의 형태로 무선 디바이스 (12) 로부터 수집된 펌웨어 검증 관련 정보의 신속한 뷰를 제공할 수 있다. 예를 들어, 펌웨어 관리 모듈 (21) 은 펌웨어 검증 관련 정보를 모니터 또는 디스플레이 디바이스 상에 나타낼 수 있고/있거나, 추후 분석 또는 검토를 위해 이러한 정보를 예를 들어 전자 메일을 통해 다른 컴퓨터 디바이스에 송신할 수도 있다. 또한, 펌웨어 관리 모듈 (21) 은 정보 로그 (46) 에 기초하여 및/또는 분석기 (45) 에 의해 생성된 보고서 (61) 에 기초하여 각각의 무선 디바이스 (12) 상에서 실행될 제어 명령 (78) 을 송신하고/하거나 검증 컨피규레이션 (65) 을 변경하도록 실행 가능할 수도 있다.

[0072] 도 6 을 참조하면, 원격 펌웨어 관리 모듈 (21) 과 펌웨어 검증 모듈 (20) 모두는 로컬 또는 원격으로 제어 명령 (78) 을 수신/생성하고, 무선 디바이스 (12) 상에서 제어 명령 (78) 을 실행하거나 무선 디바이스 (12) 에 제어 명령 (78) 을 송신하도록 동작 가능한 디바이스 제어 모듈 (94) 을 가질 수도 있다. 일 양태에서, 예를 들어, 제어 명령 (78) 은 사용자 ID (28; identification) 및 제어 액티비티 (29) 모두를 포함할 수도 있다. 사용자 ID (28) 는 제어 명령 (78) 의 발신자를 식별하는 어떤 방법일 수도 있다. 예를 들어, 사용자 ID (28) 는 이름, 번호, 디지털 서명, 해시, 디지털 인증서, 또는 당사자와 연관될 수도 있는 임의의 다른 타입의 데이터 또는 값일 수도 있다. 또한, 사용자 ID (28) 는 제어 명령 (78) 에 명시적으로 포함되기보다는, 제어 명령 (78) 의 발신자로부터 얻어질 수도 있다. 또한, 제어 액티비티 (29) 는 제어 명령 (78) 의 실행을 통해 펌웨어 검증 모듈 (20) 에 의해 수행될 동작이다. 상술한 바와 같이, 이들 동작은 통신을 디세이블하는 것, 통신을 이네이블하는 것, 펌웨어 및/또는 통신 파라미터를 리컨피규어하는 것 등을 포함한다.

[0073] 제어 명령 (78) 을 실행하거나 전송하기 전에, 디바이스 제어 모듈 (94) 는 허가 로직 (25) 을 실행하여 제어 명령 (78) 을 발행한 사용자의 진정성이나 권한을 검사하고/하거나 사용자가 명령을 정말로 개시하기를 원하는지를 검증 및 확인할 수도 있다. 제어 명령 (78) 의 검증은 예를 들어, 운영자 (23) 가 실제로 무선 디바이스 (12) 상에서 제어 액티비티 (29) 를 실행하기를 원하는지를 확인하기 위해 운영자 (23) (또는 기타 사용자) 에 대한 프롬프트를 포함할 수도 있다. 제어 명령의 확인 또는 취소는 명령 검증 (43) 으로서 수신될 수도 있다. 또한, 예를 들어, 제어 명령을 인증하기 위해, 허가 로직 (25) 은 제어 명령 (78) 으로부터의 사용자 ID (28) 및 제어 액티비티 (29) 를 구문 분석할 수도 있고, 복수의 제어 허가 (27) 와 상관되며 또한 복수의 무선 디바이스 ID (33; identification) 와 상관되는 복수의 사용자 ID (26) 의 데이터베이스를 사용하여 제어 명령 (78) 을 발행하기 위한 인가를 검사할 수도 있다. 제어 허가 (27) 는 주어진 사용자 ID (28) 및/또는 특정 무선 디바이스의 ID 인 무선 디바이스 ID 에 대한 하나 이상의 인가된 제어 액티비티 (29) 를 식별할 수도 있다. 예를 들어, 어떤 사용자는 일정한 제어 액티비티에 제한되거나, 일정한 무선 디바이스를 제어할 수도 있다. 그러나, 복수의 사용자 ID (26), 복수의 제어 허가 (27) 및 복수의 무선 디바이스 ID (33) 는 임의의 방법으로 상관될 수도 있다는 것에 주목해야 한다. 예를 들어, 제어 명령 (78) 은 운영자 (23) 의 사용자 ID (28), 및 복수의 무선 디바이스 ID (33) 중 특정 ID 에 대한 "통신 디세이블 (disable communications)" 의 제어 액티비티 (29) 를 포함할 수도 있다. 허가 로직 (25) 은 제어 허가 (27) 및 사용자 ID (26) 의 데이터베이스를 검색하여, 운영자 (23) 가 주어진 무선 디바이스 (12) 를 디세이블하는 것이 허가되었는지를

결정한다. 허가 로직 (25) 은 이러한 인가 검사에 기초하여, 및/또는 명령 검증 (43) 의 값에 기초하여 허가 결정 (30) 을 생성한다.

[0074] 도 1 을 참조하여 상술한 바와 같이, 본 양태에서 운영자 (23) 는 사람으로서 도시되어 있지만, 다른 양태에서 운영자 (23) 는 예를 들어, 무선 디바이스 (12) 의 사용자로부터의 외부 통신 또는 보고서 (61) 를 분석하고, 이에 응답하는 하드웨어, 소프트웨어, 펌웨어 및 그 조합일 수도 있는 컴퓨팅 디바이스일 수도 있다. 또한, 운영자 (23) 는 무선 디바이스 (12) 일 수 있는 사용자 관리자 서버 (40) 와 동일한 컴퓨팅 디바이스 상에 상주할 수도 있다. 일 양태에서, 운영자 (23) 는 보고서 (61) 에 응답할 수도 있는 사람이다. 또한, 운영자 (23) 는 보고서 (61) 를 분석 및 해석하는 알고리즘, 의사 결정 루틴, 통계 프로그램 등을 더 포함할 수도 있다. 무선 네트워크 보조 컴퓨터 (22) 와 연관되어 있는 것으로 도시되었지만, 운영자 (23) 는 예를 들어, 사용자 관리자 서버 (40) 상에, 네트워크에 접속된 다른 서버 상에, 또는 심지어 무선 디바이스 (12) 상에 무선 네트워크 (42) 와 통신하여 어디든지 위치할 수도 있다.

[0075] 도 7 을 참조하면, 일 양태에서, 무선 디바이스 (12) 는 셀룰러 전화기를 포함한다. 셀룰러 전화기 시스템 (71) 은 캐리어 네트워크 (64) 를 통해 유선 네트워크 (58) 에 접속된 무선 네트워크 (42) 를 포함할 수도 있다. 무선 디바이스 (12) 는 증가된 컴퓨팅 능력을 갖도록 제조되고 있고, 종종 무선 네트워크 (42) 를 통해 음성 및 데이터를 포함한 패킷을 통신할 수 있다. 상술한 바와 같이, 이들 "스마트" 무선 디바이스 (12) 는, 셀룰러 전화기 (12) 상에서 동작하며 그 디바이스의 일정한 기능성을 제어하는 소프트웨어 애플리케이션을 소프트웨어 개발자가 생성할 수 있도록 하는 API (34) 를 자신의 로컬 컴퓨터 플랫폼 (13) 상에 갖는다. 도 7 은 본 시스템의 일 양태에 따른 요소의 상호 관계 및 셀룰러 무선 네트워크의 컴포넌트를 더 상세히 도시한 대표적인 도면이다. 셀룰러 무선 네트워크 (71) 는 단지 예시적인 것으로서, 무선 디바이스 (12) 와 같은 원격 모듈이 서로 간에 및/또는 무선 네트워크 캐리어 및/또는 서버를 비롯한 무선 네트워크 (42) 의 컴포넌트 간에 OTA (over-the-air) 로 통신하는 임의의 시스템을 포함할 수 있지만, 이에 한정되는 것은 아니다.

[0076] 시스템 (71) 에서, 사용자 관리자 서버 (40) 는 무선 디바이스 (12) 로부터 수집된 데이터 로그 (46) 와 같은 펌웨어 검증 정보를 저장하는 별개의 데이터 리포지터리 (60) 와 유선 네트워크 (58) (예를 들어, LAN (local area network)) 를 통해 통신할 수 있다. 또한, 데이터 관리 서버 (62) 는 후처리 (post-processing) 능력, 데이터 흐름 제어 등을 제공하기 위해 사용자 관리자 서버 (40) 와 통신할 수도 있다. 또한, 사용자 관리자 서버 (40), 데이터 리포지터리 (60) 및 데이터 관리 서버 (62) 는 셀룰러 통신 서비스를 제공하는 것이 필요한 임의의 기타 네트워크 컴포넌트를 갖는 셀룰러 전화기 시스템 (91) 상에 존재할 수도 있다. 사용자 관리자 서버 (40), 및/또는 데이터 관리 서버 (62) 는, 인터넷, 보안 LAN, WAN, 또는 기타 네트워크와 같은 데이터 링크일 수도 있는 데이터 링크 (70 및 66) 를 통해 캐리어 네트워크 (64) 와 통신한다. 캐리어 네트워크 (64) 는 MSC (68; mobile switching center) 에 송신되는 메시지 (일반적으로 데이터 패킷임) 를 제어한다. 또한, 캐리어 네트워크 (64) 는 인터넷과 같은 네트워크 (70) 및/또는 POTS (plain old telephone service) 에 의해 MSC (68) 와 통신한다. 통상, 네트워크 (70) 에서, 네트워크 또는 인터넷 부분은 데이터를 전송하고, POTS 부분은 음성 정보를 전송한다. MSC (68) 는 데이터 전송을 위한 인터넷 부분과 음성 전송을 위한 POTS 부분 및/또는 데이터 네트워크와 같은 다른 네트워크 (74) 에 의해 다수의 기지국 (72; BTS) 에 접속될 수도 있다. 결국, BTS (72) 는 SMS (short message service) 또는 기타 OTA (over-the-air) 방법에 의해 무선 디바이스 (12) 와 같은 무선 디바이스에 무선으로 메시지를 방송한다.

[0077] 도 8 을 참조하면, 무선 디바이스 상의 펌웨어 무결성 검증을 위한 방법의 일 양태는 펌웨어 검증 모듈 (20) 의 적어도 일부를 무선 디바이스 (12) 의 컴퓨터 플랫폼 (13) 상에 로딩하는 단계를 포함한다 (블록 (120)). 예를 들어, 펌웨어 검증 모듈 (20) 은 디바이스의 제조 동안에 무선 디바이스의 하드웨어 및/또는 펌웨어 내에 구현될 수도 있다. 다른 방법으로는, 펌웨어 검증은 사용자 관리자 서버 (40) 에 의해 무선 디바이스 (12) 에 "푸싱" 되거나 무선 네트워크 (42) 를 가로질러 무선 디바이스 (12) 에 의해 사용자 관리자 서버 (40) 로부터 "풀링" 될 수도 있다. 다른 방법으로는, 펌웨어 검증 모듈 (20) 은 무선 디바이스 (12) 가 각각의 무선 디바이스 (12) 에 대한 펌웨어 검증 모듈 (20) 의 최신 버전을 갖는지 여부에 따라 "풀링" 또는 "푸싱" 될 수도 있다. 다른 방법으로는, 펌웨어 검증 모듈 (20) 의 로딩은, 예를 들어, 무선 디바이스 (12) 가 무선 네트워크 (42) 와 통신하는데 있어서 어려움을 겪는다거나, 무선 디바이스 (12) 가 상이한 네트워크 서비스 제공자와 통신한다는 것과 같은, 소정의 이벤트에 의해 개시되는 임의의 방법으로 구성 가능할 수도 있다. 다른 방법으로는, 펌웨어 검증 모듈 (20) 의 무선 디바이스 (12) 로의 푸싱 또는 풀링은 예를 들어, 소정의 이벤트에 의해 개시되는 임의의 방법으로 구성 가능할 수도 있다.

[0078] 또한, 본 방법의 양태는 무선 디바이스 (12) 의 컴퓨터 플랫폼 (13) 상의 펌웨어 무결성을 테스트하는 검증 컨

피규레이션 (65) 의 적어도 일부를 로딩하는 단계를 포함한다 (블록 (122)). 예를 들어, 검증 컨피규레이션 (65) 은 디바이스의 제조 동안에 무선 디바이스의 하드웨어 및/또는 펌웨어 내에 구현될 수도 있다. 다른 방법으로는, 검증 컨피규레이션 (65) 은 무선 네트워크 (42) 를 가로질러 무선 디바이스 (12) 에 의해 사용자 관리자 서버 (40) 로부터 "풀링" 되거나, 사용자 관리자 서버 (40) 에 의해 무선 디바이스 (12) 로 "푸싱" 될 수도 있다. 다른 대안으로는, 검증 컨피규레이션 (65) 의 로딩은, 예를 들어, 무선 디바이스 (12) 가 무선 네트워크 (42) 와 통신하는데 있어서 어려움을 겪는다거나, 무선 디바이스 (12) 가 상이한 네트워크 서비스 제공자와 통신한다는 것과 같은 소정의 이벤트에 의해 개시되는 임의의 방법으로 개시될 수도 있다. 다른 대안으로는, 검증 컨피규레이션 (65) 을 무선 디바이스 (12) 에 푸싱하거나 풀링하는 것은 예를 들어, 소정의 이벤트에 의해 개시되는 임의의 방법으로 구성 가능할 수도 있다.

[0079] 또한, 본 방법의 양태는 검증 컨피규레이션 (65) 에 따라 검증 테스트 결과를 비롯한 펌웨어 검증 정보를 수집하는 단계를 포함한다 (블록 (124)). 예를 들어, 검증 테스트 결과 (47) 는 소정의 검증 방식 (89) 을 펌웨어 (14) 에 적용함으로써 생성될 수도 있다. 또한, 부가 펌웨어 정보 (15) 는 그 동작 동안에 무선 디바이스의 처리 엔진 (87) 으로부터 검색될 수도 있다. 검증 테스트 결과 (47) 와 부가 펌웨어 정보 (15) 모두는 정보 로그 (46) 에 저장될 수도 있다.

[0080] 선택적으로, 본 방법의 양태는 소정의 검증 결과를 생성된 검증 테스트 결과와 비교함으로써 펌웨어 무결성을 결정하는 단계를 포함한다 (블록 (126)). 일 양태에서, 예를 들어, 이러한 무결성 결정 (11) 은 정보 로그 (46) 에 기록될 수도 있다.

[0081] 또한, 본 방법의 양태는 분석을 위해 수집된 펌웨어 검증 정보를 다른 컴퓨터 디바이스에 전송하는 단계를 포함한다 (블록 (128)). 일 양태에서, 예를 들어, 정보 로그 (46) 는 예를 들어, 표준 HTTP, FTP, 또는 어떤 다른 데이터 전송 프로토콜을 통해 검증 컨피규레이션 (65) 의 보고 파라미터 (91) 에 따라 무선 디바이스 (12) 로부터 사용자 관리자 서버 (40) 에 업로딩된다. 다른 양태에서, 수집된 펌웨어 검증 정보는 무선 디바이스 (12) 가 액세스할 수도 있는 임의의 통신 수단을 사용하여 무선 디바이스로부터 업로딩된다.

[0082] 또한, 본 방법의 양태는 펌웨어 무결성 관련 정보의 분석에 기초하여 제어 명령을 수신, 선택적으로 검증, 및 실행하는 단계를 포함할 수도 있다 (블록 (130)). 상술한 바와 같이, 원격 펌웨어 관리 모듈 (21) 은 분석기 (45) 를 실행하여 무결성 결정 (11) 을 포함한 보고서 (61) 를 생성할 수도 있다. 무결성 결정 (11) 및/또는 정보 로그 (46) 의 검토에 기초하여, 운영자 (23) 또는 다른 사용자는 원격 펌웨어 관리 모듈 (21) 을 사용하여 제어 명령 (78) 을 생성함으로써 무선 디바이스 (12) 의 액티비티를 제어할 수도 있다. 디바이스 제어 모듈 (94) 은 제어 명령 (78) 의 진정성 및 권한을 검증할 수도 있고, 그 다음에 제어 로직 (35) 을 실행하여 제어 액티비티 (29) 를 개시할 수도 있다.

[0083] 도 9 를 참조하면, 무선 디바이스 (12) 상의 펌웨어 (14) 의 무결성을 검증하는 장치 상에서 동작 가능한 방법의 일 양태는 검증 컨피규레이션을 생성하여 무선 디바이스 상의 펌웨어 무결성을 테스트하는 단계를 포함한다 (블록 (140)). 일 양태에서, 기술자 또는 운영자 (23) 와 같은 사용자는 펌웨어 관리 모듈 (21) 에 액세스하고, 컨피규레이터 모듈 (44) 을 실행하여 주어진 무선 디바이스 (12) 에 대한 검증 컨피규레이션 (65) 을 생성한다. 컨피규레이터 모듈 (44) 은 컨피규레이션 로직 (56) 을 사용하여 검증 컨피규레이션 (65) 을 구성하는 여러 파라미터를 결정 및/또는 개별화 (customize) 할 수도 있고, 이들 파라미터는 무선 디바이스의 타입/메이크/모델, 실제 네트워크 서비스 제공자, 및 펌웨어 타입에 따라 다를 수도 있다.

[0084] 또한, 본 방법의 양태는 검증 컨피규레이션을 무선 디바이스에 전송하는 단계를 포함한다 (블록 (142)). 예를 들어, 사용자 관리자 서버 (40) 는 무선 네트워크 (42) 를 가로질러 무선 디바이스 (12) 에 검증 컨피규레이션 (65) 을 송신할 수도 있다. 다른 방법으로는, 다른 양태에서, 검증 컨피규레이션 (65) 은 정적 또는 직렬 접속을 통해 무선 디바이스 (12) 에 전송될 수도 있다. 다른 대안으로는, 검증 컨피규레이션 (65) 은 제조 동안에 무선 디바이스 (12) 상에 미리 로딩될 수도 있다.

[0085] 또한, 본 방법의 양태는 검증 컨피규레이션에 기초하여 무선 디바이스로부터 펌웨어 검증 관련 정보를 수신하는 단계를 포함한다 (블록 (144)). 예를 들어, 사용자 관리자 서버 (40) 는 무선 디바이스 (12) 로부터 검증 테스트 결과 (47) 및/또는 부가 펌웨어 정보 (15) 를 포함한 정보 로그 (46) 를 수신할 수도 있다. 정보 로그 (46) 내의 데이터는 각각의 무선 디바이스 (12) 에 의한 검증 컨피규레이션 (65) 의 처리에 대응한다. 또한, 일 양태에서, 사용자 관리자 서버 (40) 는 무선 네트워크 (42) 를 통해 정보 로그 (46) 를 수신한다. 또한, 정보 로그 (46) 는 사용자 관리자 서버 (40) 및/또는 펌웨어 관리 모듈 (21) 에 의해 어셈블링되어 전체로서 또는 조각으로 수신될 수도 있다. 다른 양태에서, 사용자 관리자 서버 (40) 는 무선 디바이스 (12) 와

의 정적 또는 직렬 접속에 의해, 또는 사용자 관리자 서버 (40) 와 통신하는 어떤 다른 컴퓨터 디바이스나 저장 매체로부터 정보 로그 (46) 를 수신한다.

[0086] 또한, 본 방법의 양태는 무선 디바이스 상의 펌웨어 무결성을 나타내는 정보 로그 내의 데이터에 기초하여 보고서를 생성하는 단계를 포함한다 (블록 (146)). 예를 들어, 분석기 (45) 는 생성된 검증 테스트 결과 (47) 를 소정의 검증 결과 (37) 와 비교한 것에 기초하여 보고서 (61) 를 생성한다. 보고서 (61) 는, 그 비교에 기초하여 펌웨어 (14) 의 예상 무결성을 나타내는 무결성 결정 (11) 을 포함할 수도 있다.

[0087] 선택적으로, 일 양태에서, 펌웨어 무결성 보고서는 분석을 위해 전송된다 (블록 (148)). 예를 들어, 펌웨어 관리 모듈 (21) 은 검토를 위해 다른 컴퓨터 디바이스, 무선 디바이스의 사용자, 또는 제 3 자에게 보고서 (61) 를 송신하도록 검증 로직 (59) 을 실행할 수도 있다. 일 양태에서, 펌웨어 관리 모듈 (21) 은 운영자 (23) 에 의한 검토를 위해 컴퓨터 디바이스 (22) 에 보고서 (61) 를 송신한다. 운영자 (23) 는 보고서 (61) 에 기초하여 무선 디바이스 (12) 의 펌웨어 (14) 를 대체하라는 요청을 각각의 무선 디바이스 (12) 의 사용자에게 송신하는 것과 같은 액션을 취할 수도 있다. 다른 양태에서는, 보고서 (61) 의 분석을 통해, 제어 명령 (78) 을 발행하여 무선 디바이스의 동작을 제어한다. 예를 들어, 결함 펌웨어가 검출되면, 운영자 (23) 또는 다른 당사자는 예를 들어, 디바이스를 디세이블하라는 명령을 발행하여, 무선 네트워크에 손상을 주는 것을 방지하거나 비인가된 동작을 방지할 수도 있다.

[0088] 선택적으로, 일 양태에서, 본 발명의 방법은 보고서 내의 펌웨어 검증 관련 정보에 기초하여 제어 명령을 수신하는 단계 (및, 선택적으로, 검증하는 단계) 를 포함한다 (블록 (150)). 예를 들어, 펌웨어 관리 모듈 (21) 은 보고서 (61) 에 응답하여 운영자 (23) 로부터 제어 명령 (78) 을 수신할 수도 있다. 선택적으로, 디바이스 제어 모듈 (94) 은 허가 로직 (25) 을 실행하여 각각의 무선 디바이스 (12) 에 제어 명령 (78) 을 발행할지에 관한 허가 결정 (30) 을 내릴 수도 있다.

[0089] 선택적으로, 일 양태에서, 본 발명의 방법은 무선 디바이스에 제어 명령을 송신하는 단계를 포함한다 (블록 (152)). 예를 들어, 디바이스 제어 모듈 (94) 은 제어 로직 (35) 을 실행하여 무선 디바이스 (12) 에 제어 명령 (78) 을 전송할 수도 있다. 일 양태에서, 디바이스 제어 모듈 (94) 은 무선 네트워크 (42) 를 가로질러 무선 디바이스 (12) 에 제어 명령 (78) 을 송신한다.

[0090] 이와 같이, 상술한 양태는 무선 네트워크 서비스 제공자, 무선 디바이스 제조자, 펌웨어 제조자 등과 같은 당사자가 무선 디바이스 상의 펌웨어 무결성을 유지할 수 있도록 해준다. 예를 들어, 네트워크 서비스 제공자는 자신의 고객에게 좋은 서비스를 제공하고 수익을 창출할 수 있도록 손상된 펌웨어를 검출할 필요가 있을 수도 있다. 또한, 예를 들어, 손상된 펌웨어를 갖는 무선 디바이스가 무선 네트워크 상의 다른 무선 디바이스와 간섭하는 통신 프로토콜을 사용할 수도 있기 때문에, 네트워크 서비스 제공자는 자신의 무선 네트워크를 보호하기 위해, 손상된 펌웨어를 갖는 무선 디바이스를 셧다운할 필요가 있을 수도 있다. 또한, 무선 디바이스를 위한 펌웨어가 쓸모없게 되었을 때, 또는 무선 디바이스가 협정을 위반하여 상이한 서비스 제공자의 네트워크 상에서 사용 중일 때, 네트워크 서비스 제공자는 무선 디바이스를 디세이블할 수 있는 것이 필요할 수도 있다.

[0091] 또한, 상술한 양태는 무선 디바이스의 제조자가 상이한 무선 디바이스 및 상이한 펌웨어 버전에 대해 펌웨어 검증 애플리케이션을 구성할 수 있도록 해주므로, 각각의 펌웨어 버전 또는 각각의 무선 디바이스 타입에 대해 애플리케이션을 기입할 필요가 없어진다.

[0092] 또한, 상술한 양태는 펌웨어의 어느 부분이 손상되었는지에 기초하여 무선 디바이스를 디세이블할지 여부를 결정할 수 있는 펌웨어 검증 메커니즘을 제공한다. 예를 들어, 버기 프로그램은 단지 무선 디바이스의 출력 디바이스 상에서 재미있는 그림을 그리는 펌웨어의 코드 세그먼트에 대한 펌웨어 무결성을 손상시킬 수도 있다.
이러한 상황에서, 상술한 양태는 그 결정을 고려하므로, 무선 디바이스를 디세이블하기보다는, 단지 펌웨어를 복구할 필요가 있다는 것을 무선 디바이스의 사용자에게 통지하는 것을 고려한다. 이 경우에, 무선 디바이스를 디세이블하면, 무선 디바이스의 사용자가 불편을 느낄 수도 있고, 네트워크 서비스 제공자가 수익을 잃을 수도 있다. 또한, 디바이스를 디세이블하거나 무선 디바이스의 사용자가 무선 디바이스의 수리를 요청하기보다는, 상술한 양태는 무선 디바이스의 무결성을 복구하기 위해 펌웨어를 재구성하는 것을 제공한다.

[0093] 본원에 개시된 양태와 관련하여 설명된 예시적인 로직, 로직 블록, 모듈, 및 회로는 범용 프로세서, DSP (digital signal processor), ASIC (application specific integrated circuit), FPGA (field programmable gate array) 또는 기타 프로그램 가능 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트, 또는 본원에 설명된 기능을 수행하도록 설계된 그 임의의 조합을 이용하여 구현되거나 수행될 수도 있다.

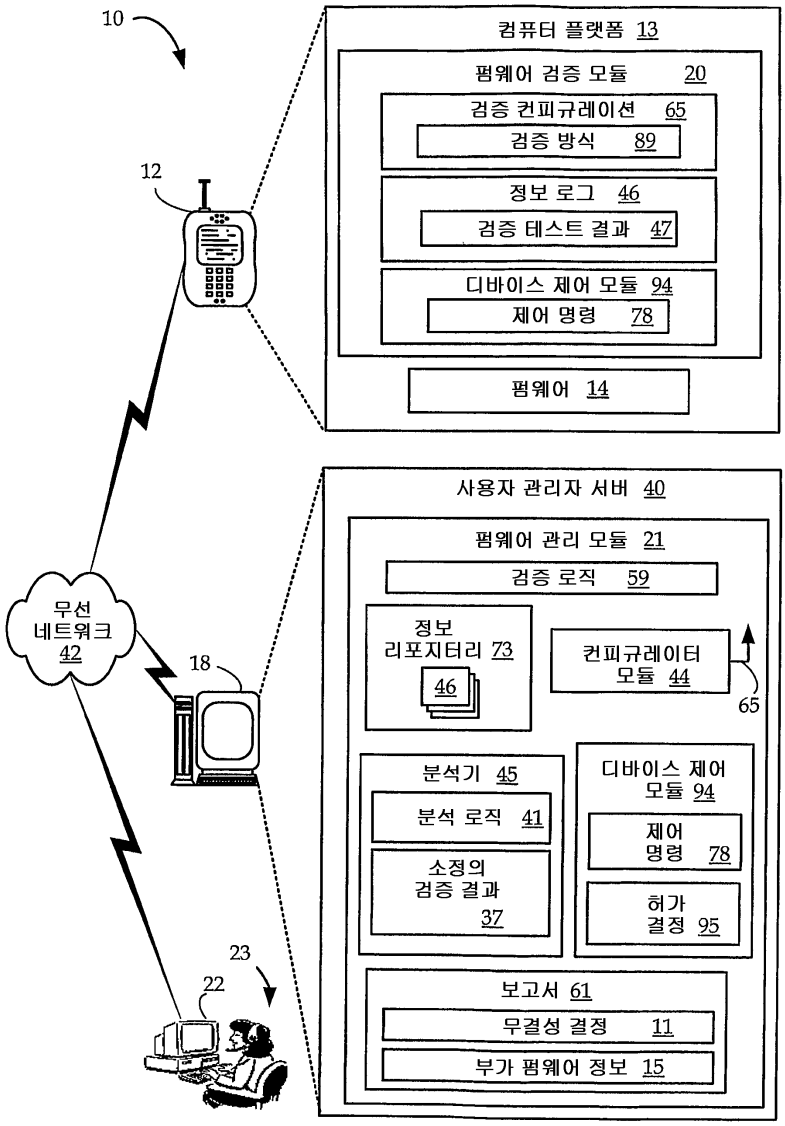
범용 프로세서는 마이크로프로세서일 수도 있지만, 다른 방법으로는, 범용 프로세서가 임의의 통상 프로세서, 컨트롤러, 마이크로컨트롤러, 또는 상태 기계일 수도 있다. 또한, 프로세서는 예를 들어, DSP 와 마이크로프로세서의 조합, 복수의 마이크로프로세서, DSP 코어와 결합한 하나 이상의 마이크로프로세서, 또는 임의의 기타 그러한 구성과 같은, 컴퓨팅 디바이스의 조합으로서 구현될 수도 있다.

[0094] 또한, 본원에 개시된 양태들과 관련하여 설명된 방법 또는 알고리즘의 액션 및/또는 단계는 하드웨어, 프로세서에 의해 실행되는 소프트웨어 모듈, 또는 양자의 조합으로 직접 구현될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드 디스크, 탈착식 디스크, CD-ROM, 또는 당해 기술분야에서 공지되어 있는 임의의 기타 형태의 저장 매체에 상주할 수도 있다. 예시적인 저장 매체는 프로세서에 접속되어, 프로세서가 저장 매체로부터 정보를 판독하고, 저장 매체에 정보를 기록할 수 있도록 해준다. 다른 방법으로는, 저장 매체는 프로세서에 통합될 수도 있다. 프로세서 및 저장 매체는 ASIC 에 상주할 수도 있다. ASIC 은 사용자 단말기에 상주할 수도 있다. 다른 방법으로는, 프로세서와 저장 매체는 사용자 단말기에 이산 컴포넌트로서 상주할 수도 있다.

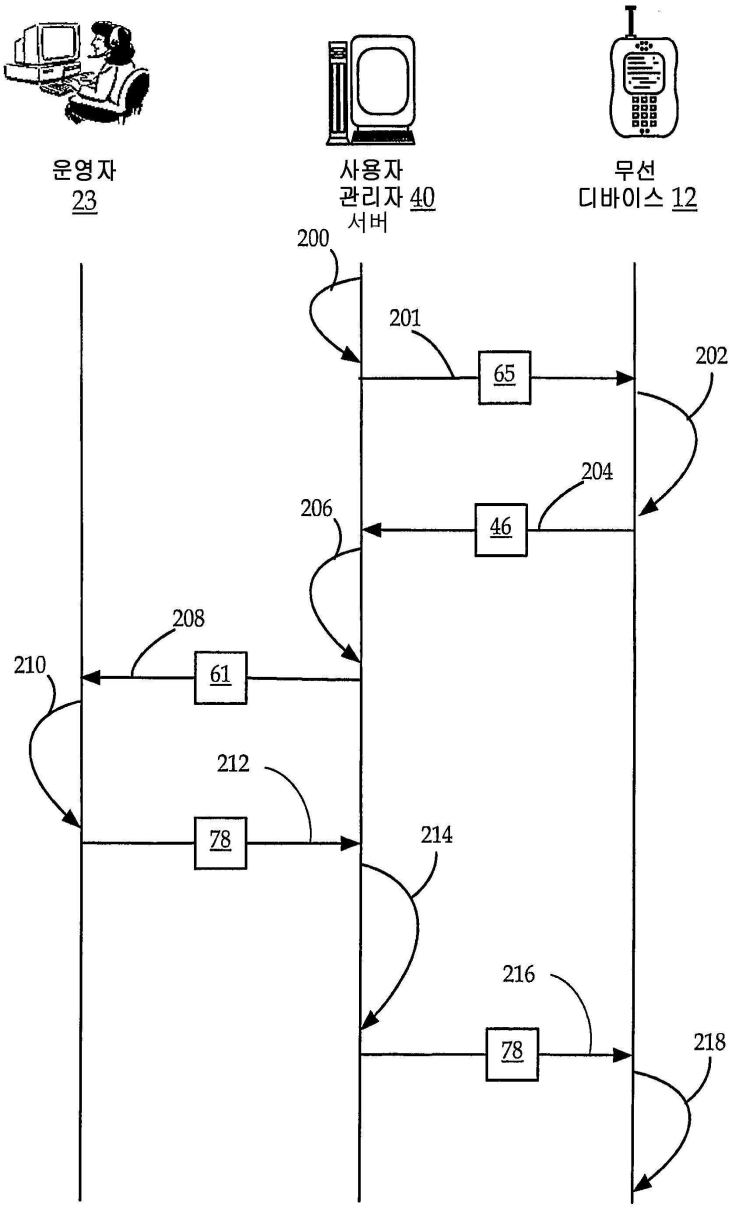
[0095] 이상, 상기 개시내용은 예시적인 양태를 나타내지만, 첨부된 청구항에서 규정되는 것과 같은 상술한 양태의 범위로부터 일탈함이 없이 본원에서 다양한 변화 및 수정을 행할 수 있다는 것에 주목해야 한다. 또한, 상술한 양태의 요소는 단수로 설명되거나 청구되지만, 단수에 한정된다고 명시적으로 제시되지 않는 한 복수로 생각된다.

도면

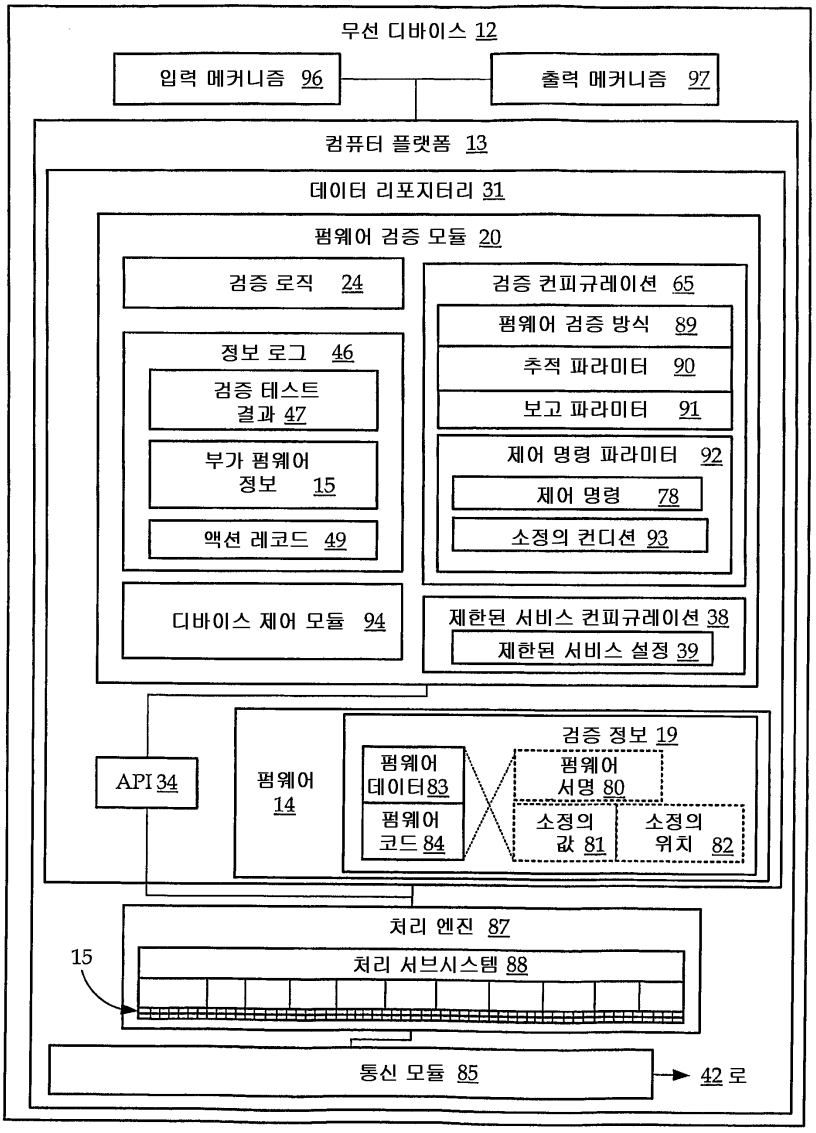
도면1


10
12
컴퓨터 플랫폼 13
펌웨어 검증 모듈 20
검증 컨피규레이션 65
검증 방식 89
정보 로그 46
검증 테스트 결과 47
디바이스 제어 모듈 94
제어 명령 78
펌웨어 14
사용자 관리자 서버 40
펌웨어 관리 모듈 21
검증 로직 59
정보 리포지터리 73
46
컨피규레이터 모듈 44
65
분석기 45
분석 로직 41
소정의 검증 결과 37
디바이스 제어 모듈 94
제어 명령 78
허가 결정 95
보고서 61
무결성 결정 11
부가 펌웨어 정보 15
무선 네트워크 42
18
23
22

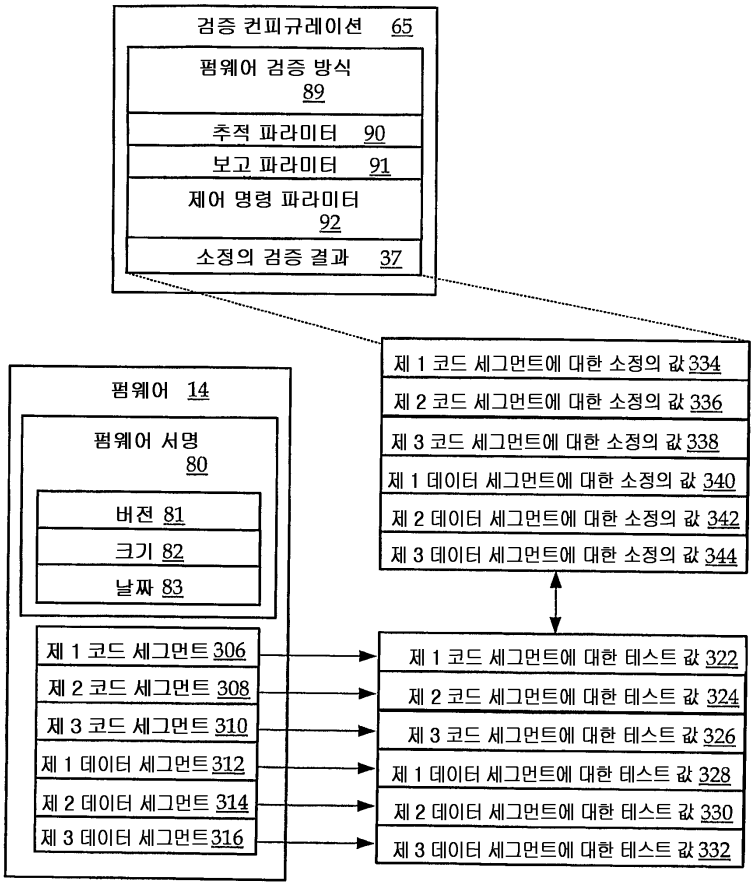
도면2


운영자
23
사용자
관리자 40
서버
무선
디바이스 12
200
201
65
202
204
206
46
208
210
61
212
78
214
216
78
218

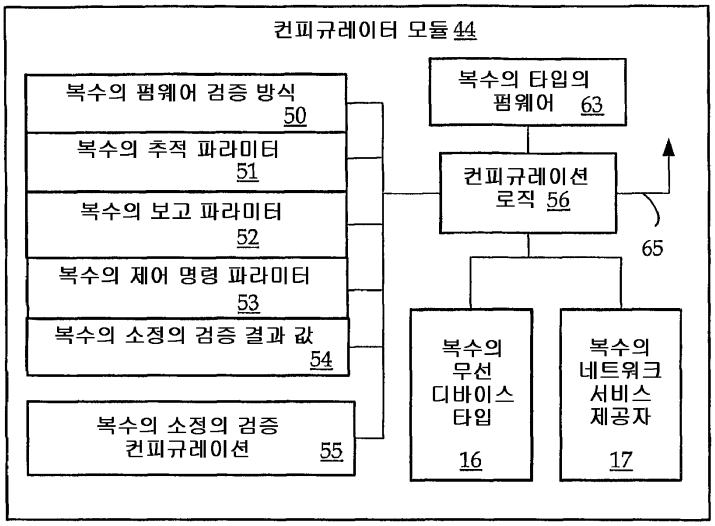
도면3


무선 디바이스 12
입력 메커니즘 96
출력 메커니즘 97
컴퓨터 플랫폼 13
데이터 리포지터리 31
펌웨어 검증 모듈 20
검증 로직 24
검증 컨피규레이션 65
펌웨어 검증 방식 89
추적 파라미터 90
보고 파라미터 91
제어 명령 파라미터 92
제어 명령 78
소정의 컨디션 93
정보 로그 46
검증 테스트 결과 47
부가 펌웨어 정보 15
액션 레코드 49
디바이스 제어 모듈 94
제한된 서비스 컨피규레이션 38
제한된 서비스 설정 39
API 34
펌웨어 14
검증 정보 19
펌웨어 데이터 83
펌웨어 서명 80
펌웨어 코드 84
소정의 값 81
소정의 위치 82
처리 엔진 87
15
처리 서브시스템 88
통신 모듈 85
42 로

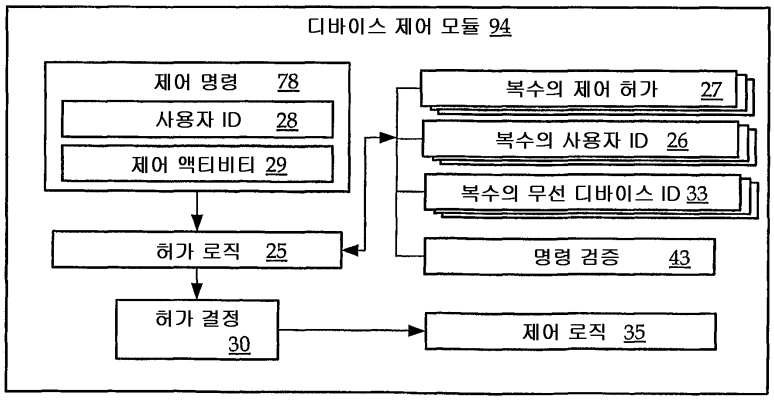
도면4


검증 컨피규레이션 65
펌웨어 검증 방식 89
추적 파라미터 90
보고 파라미터 91
제어 명령 파라미터 92
소정의 검증 결과 37
펌웨어 14
펌웨어 서명 80
버전 81
크기 82
날짜 83
제 1 코드 세그먼트 306
제 2 코드 세그먼트 308
제 3 코드 세그먼트 310
제 1 데이터 세그먼트 312
제 2 데이터 세그먼트 314
제 3 데이터 세그먼트 316
제 1 코드 세그먼트에 대한 소정의 값 334
제 2 코드 세그먼트에 대한 소정의 값 336
제 3 코드 세그먼트에 대한 소정의 값 338
제 1 데이터 세그먼트에 대한 소정의 값 340
제 2 데이터 세그먼트에 대한 소정의 값 342
제 3 데이터 세그먼트에 대한 소정의 값 344
제 1 코드 세그먼트에 대한 테스트 값 322
제 2 코드 세그먼트에 대한 테스트 값 324
제 3 코드 세그먼트에 대한 테스트 값 326
제 1 데이터 세그먼트에 대한 테스트 값 328
제 2 데이터 세그먼트에 대한 테스트 값 330
제 3 데이터 세그먼트에 대한 테스트 값 332

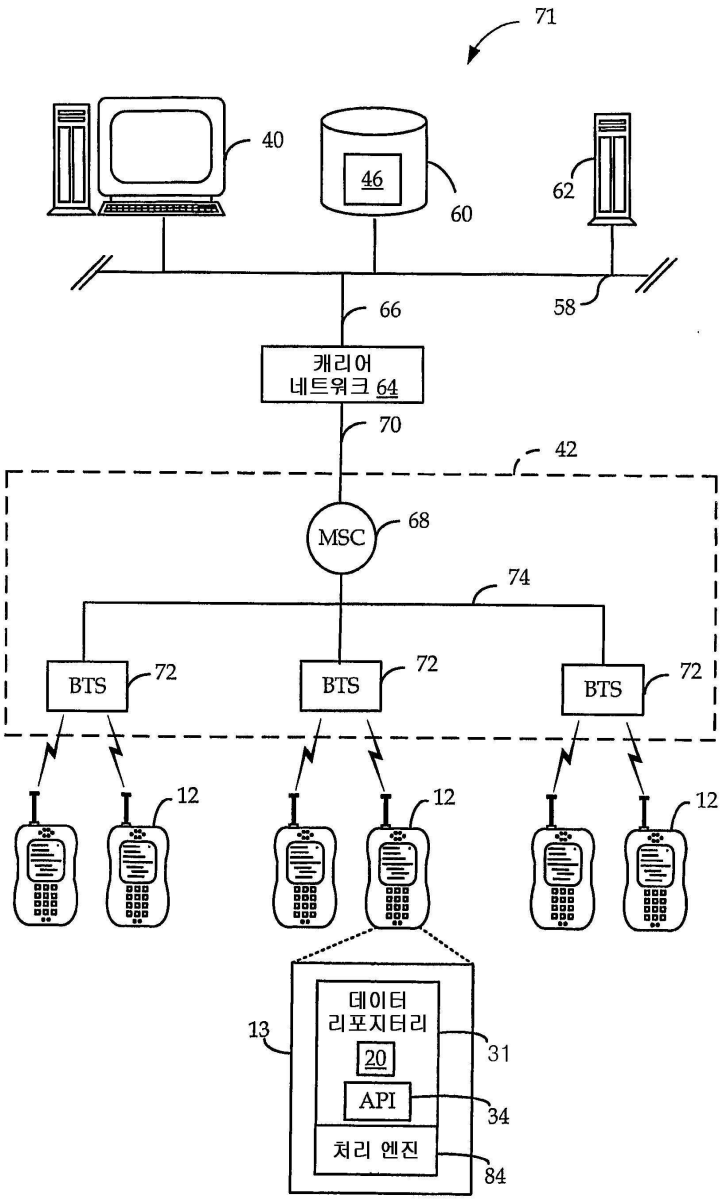
도면5


컨피규레이터 모듈 44
복수의 펌웨어 검증 방식 50
복수의 추적 파라미터 51
복수의 보고 파라미터 52
복수의 제어 명령 파라미터 53
복수의 소정의 검증 결과 값 54
복수의 소정의 검증 컨피규레이션 55
복수의 타입의 펌웨어 63
컨피규레이션 로직 56
65
복수의 무선 디바이스 타입 16
복수의 네트워크 서비스 제공자 17

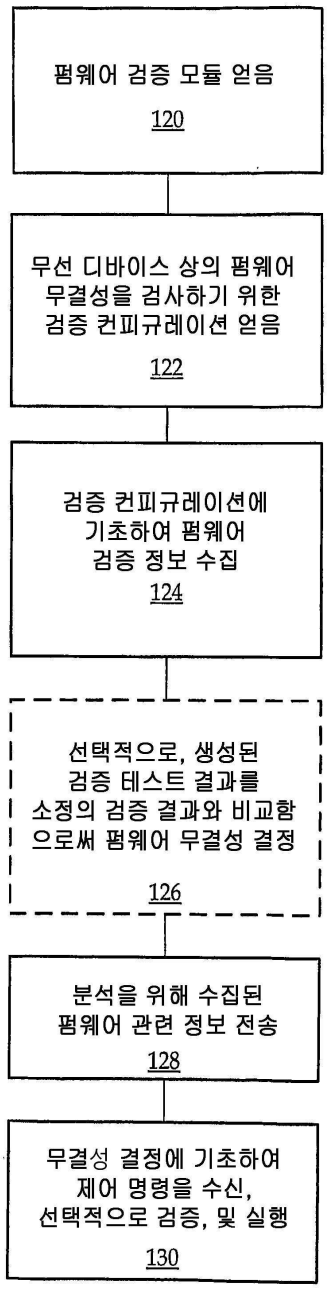
도면6


디바이스 제어 모듈 94
제어 명령 78
사용자 ID 28
제어 액티비티 29
허가 로직 25
허가 결정 30
복수의 제어 허가 27
복수의 사용자 ID 26
복수의 무선 디바이스 ID 33
명령 검증 43
제어 로직 35

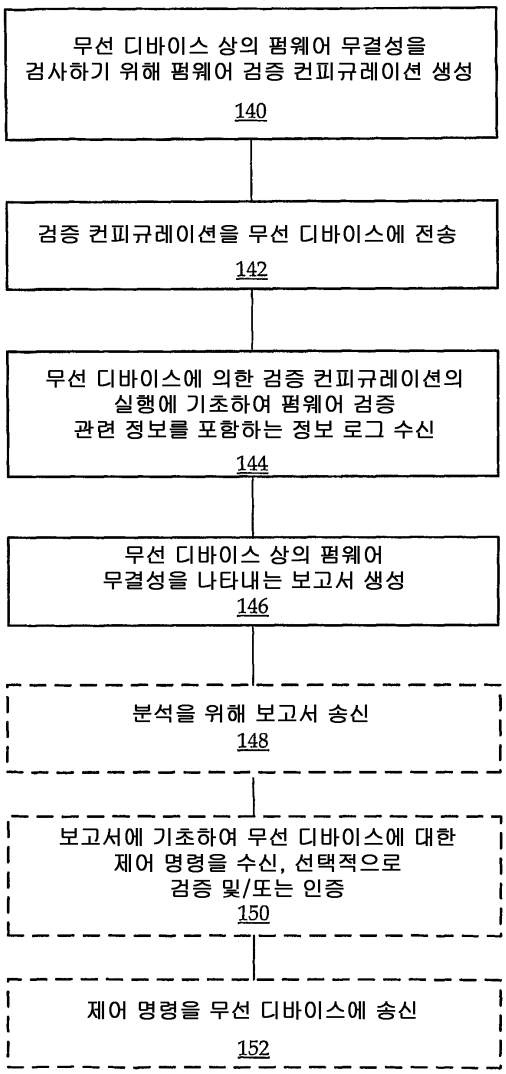
도면7


71
40
46
60
62
58
66
캐리어 네트워크 64
70
42
MSC
68
74
BTS
72
12
13
데이터 리포지터리
20
31
API
34
처리 엔진
84

도면8


펌웨어 검증 모듈 얻음
120
무선 디바이스 상의 펌웨어 무결성을 검사하기 위한 검증 컨피규레이션 얻음
122
검증 컨피규레이션에 기초하여 펌웨어 검증 정보 수집
124
선택적으로, 생성된 검증 테스트 결과를 소정의 검증 결과와 비교함으로써 펌웨어 무결성 결정
126
분석을 위해 수집된 펌웨어 관련 정보 전송
128
무결성 결정에 기초하여 제어 명령을 수신, 선택적으로 검증, 및 실행
130

도면9


무선 디바이스 상의 펌웨어 무결성을
검사하기 위해 펌웨어 검증 컨피규레이션 생성
140
검증 컨피규레이션을 무선 디바이스에 전송
142
무선 디바이스에 의한 검증 컨피규레이션의
실행에 기초하여 펌웨어 검증
관련 정보를 포함하는 정보 로그 수신
144
무선 디바이스 상의 펌웨어
무결성을 나타내는 보고서 생성
146
분석을 위해 보고서 송신
148
보고서에 기초하여 무선 디바이스에 대한
제어 명령을 수신, 선택적으로
검증 및/또는 인증
150
제어 명령을 무선 디바이스에 송신
152