(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 9/445 (2006.01)

(45) 공고일자 2006년10월16일
(11) 등록번호 10-0634773
(24) 등록일자 2006년10월10일

(21) 출원번호 10-2003-7002109
(22) 출원일자 2003년02월13일
번역문 제출일자 2003년02월13일
(86) 국제출원번호 PCT/US2002/016485
국제출원일자 2002년05월23일

(65) 공개번호 10-2004-0004361
(43) 공개일자 2004년01월13일
(87) 국제공개번호 WO 2002/97620
국제공개일자 2002년12월05일

(81) 지정국 국내특허 : 아랍에미리트, 안티구와바부다, 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아 헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 벨리제, 캐나다, 스위스, 중국, 콜롬비아, 코스타리카, 쿠바, 체코, 독일, 덴마크, 도미니카, 알제리, 에쿠아도르, 에스토니아, 스페인, 핀란드, 영국, 그라나다, 그루지야, 가나, 감비아, 크로아티아, 헝가리, 인도네시아, 이스라엘, 인도, 아이슬랜드, 일본, 케냐, 키르키즈스탐, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 모로코, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 모잠비크, 노르웨이, 뉴질랜드, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 슬로베니아, 슬로바키아, 시에라리온, 타지키스탄, 투르크맨, 터어키, 트리니아드토바고, 탄자니아, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 세르비아 앤 몬테네그로, 남아프리카, 짐바브웨, 오만, 필리핀, 튀니지, 잠비아,

AP ARIPO특허 : 가나, 감비아, 케냐, 레소토, 말라위, 모잠비크, 수단, 시에라리온, 스와질랜드, 탄자니아, 우간다, 잠비아, 짐바브웨,

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르키즈스탐, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크맨,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 사이프러스, 독일, 덴마크, 스페인, 핀란드, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 터어키,

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기니, 말리, 모리타니, 니제르, 세네갈, 차드, 토고, 기니 비사우, 적도 기니,

(30) 우선권주장 09/872,418 2001년05월31일 미국(US)

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

(72) 발명자
런드블레이드로렌스
미국92117캘리포니아주샌디에고나브가턱3062

필립스마크에스
미국92117캘리포니아주샌디에고그로스벤트리애비뉴4008

미니어브라이언

미국92128캘리포니아주샌디에고폰타넬플레이스13704

좡옌
미국92126캘리포니아주샌디에고제이드코스트로드8223넘버120

크리쉬난아난드
미국92128캘리포니아주샌디에고소르본코트13775

스프리그스티븐에이
미국92064캘리포니아주포웨이트레블틴코트12124

치메이텔리마젠
미국92110캘리포니아주샌디에고린우드스트리트1752넘버쥐

올리버미첼
미국92131캘리포니아주샌디에고카미니토수엘토9737

호렐제랄드
캐나다브이8엠2에이치5브리티쉬콜럼비아브렌트우드베이토린로드
6500

크로스랜드카렌
미국92122캘리포니아주샌디에고메이나드스트리트5044

(74) 대리인 특허법인코리아나

심사관 : 이상헌

(54) 무선 환경에서의 안전한 애플리케이션 분배 및 실행

요약

본 발명은, 애플리케이션을 테스트하여 애플리케이션이 실행될 환경과 관련된 소정의 표준을 만족하는 것을 인증하는 시스템 및 방법을 제공함으로써 안전하고 보장된 애플리케이션 분배 및 실행을 제공한다. 또한, 규칙 및 허가 리스트, 애플리케이션 제거, 및 디지털 서명 등의 변경 검출 기술을 이용하여, 본 발명은 애플리케이션이 변경되었는지를 결정하고, 주어진 무선 장치 환경에서 실행되는 것이 허가되는지를 결정하고, 애플리케이션을 제거함으로써 테스트되거나 테스트되지 않은 애플리케이션을 안전하게 분배하고 실행하는 메카니즘을 제공한다.

대표도

도 1

명세서

기술분야

본 발명은 무선 장치에 이용되는 애플리케이션의 처리에 관한 것으로, 특히, 무선 장치상에서 실행되는 애플리케이션의 보호, 안전, 및 보전을 증가시키기 위한 것이다.

배경기술

무선 통신은 최근에 급속하게 성장해왔다. 소비자 또는 기업이 이동 전화 및 퍼스널 디지털 어시스턴트 (PDA) 등의 무선 장치상에 더 의존함에 따라, 무선 서비스 제공자, 즉, 캐리어는 이들 무선 장치에 추가적인 기능을 제공하기 위하여 노력하고 있다. 이 추가적인 기능은 무선 장치의 수요를 증가시킬 뿐만 아니라 현재 사용자들간의 사용을 증가시킬 수 있다. 그러나, 기능을 증가시키는 것은, 특히, 무선 장치에 의해 액세스될 수 있는 애플리케이션을 증가시키는 것은 비용이 증가하고 복잡해져, 캐리어가 이 기능을 제공하는 것을 방해한다.

또한, 일단 무선 장치에 배치된 애플리케이션이 적절하게 실행될지에 대한 보증이 거의 없다. 현재, 무선 장치상에서 실행되는 애플리케이션의 능력에 대한 신뢰는 개발자, 무선 장치 제조자 및/또는 캐리어에 의존한다. 더 많은 애플리케이션이 개발되고 무선 장치상의 애플리케이션의 수가 증가함에 따라, 무선 장치 환경은 더 동적으로 된다. 예를 들어, 무선 장치는 임의의 주어진 시간에 이용가능한 애플리케이션의 큰 풀(pool)로부터 상이한 많은 애플리케이션을 검색 또는 실행하도록 선택할 수 있다. 그러므로, 주어진 애플리케이션이 무선 장치에 분배되어 안전하게 실행되는 것을 보장하는 것은 제어를 더욱 더 어렵게 한다.

이것은, 애플리케이션의 부적절한 실행이 무선 장치에 불리하게 영향을 미칠 뿐만 아니라 다른 무선 장치를 포함하는 다른 네트워크 구성요소 및 캐리어 네트워크에 해로울 수 있기 때문에 특히 관심의 대상이 된다. 예를 들어, 제한되지 않는다면, 하나의 애플리케이션이 무선 장치의 파워를 제어할 수 있고 다른 무선 장치들간에 간섭을 일으킬 수 있으며 무선 장치를 제공하는 셀의 모든 용량을 감소시킬 수 있다.

현재, 무선 장치 제조자 또는 캐리어 모두 동적 애플리케이션 분배 및 실행 환경에서 애플리케이션 테스팅 및 안전한 분배를 지지하도록 갖추어져 있지 않다. 그러므로, 무선 장치, 캐리어 네트워크, 다른 네트워크 구성요소에 해로울 수 있는 애플리케이션이 무선 장치상에 분배되고 실행되는지에 관심이 있다.

또한, 많은 애플리케이션이 개발됨에 따라 다른 안전성 문제가 야기되고 애플리케이션이 무선 장치에 전송되는 환경이 더 동적으로 된다. 애플리케이션의 수와 이들 애플리케이션을 생성하는 개발자의 수가 증가함에 따라, 임의의 주어진 애플리케이션의 소오스, 즉, 개발자를 알고자 하는 소망이 또한 증가한다. 캐리어 또는 핸드셋 제조자는 어느 정도의 신뢰성으로 애플리케이션의 소오스가 해를 끼칠 것인지를 판정할 수 있는지를 알기를 원할 것이다.

결과적으로, 이 기술에서는, 무선 장치상에 애플리케이션을 분배하고 실행하는데 있어서 좀더 안전한 환경을 제공하는 시스템 및 방법이 필요하다.

발명의 개요

본 발명에 따른 시스템 및 방법은, 소정의 표준 (criteria) 으로 애플리케이션을 테스트하고, 부인방지(nonrepudiation)를 위하여 개발자에게 추적 기능을 제공하고, 애플리케이션에 의도되지 않은 변경이 있는지를 체크하고, 애플리케이션이 무선 장치로부터 제거되도록 하고, 및/또는 애플리케이션이 실행될 수 있는 환경을 정의하는 규칙(rule) 및 허가(permission)를 사용하는 애플리케이션 분배 및 실행에 대하여 더 안전한 환경을 생성함으로써 현존하는 시스템의 단점을 극복한다.

애플리케이션이 소정의 표준을 충족하는 것을 인증하는 것은 시간적으로 빨리 실행동안 발생될 수 있는 가능한 에러를 발견하는 이점을 제공한다. 이것은 애플리케이션의 실행에 해로운 영향을 미치는 것을 방지하는데 도움이 된다.

추적 기능은 부인방지의 이점을 제공한다. 애플리케이션에 임의의 문제가 있다면, 애플리케이션의 소오스, 즉, 개발자로 되돌아가서 문제점을 보정하기에 이롭다. 또한, 추적 기능은 개발자가 의도적이든 의도적이지 않든간에 해로운 결과를 갖는 애플리케이션을 생성하는 것을 방지한다.

또한, 무선 장치에서 애플리케이션을 수신하기전에, 애플리케이션이 변경되는지를 판정하는 능력은 수신된 애플리케이션이 전송된 것과 동일하다고 보장함으로써 안전성이 증가하는 이점을 제공한다. 애플리케이션이 무선 환경에서 좀더 자유롭게 분배됨에 따라, 애플리케이션이 변경되었는지를 판정하는 능력은 무선 장치에 의해 수신된 애플리케이션이 사고로 또는 의도적으로 변경되지 않았다는 확실성을 증가시킨다.

애플리케이션이 실행될 수 있을때를 정의한 규칙 및 허가의 세트를 제공하는 것은, 플랫폼, 예를 들어, 권한이 부여되지 않은 시스템 또는 환경상에서 애플리케이션의 권한부여되지 않은 실행을 방지함으로써 애플리케이션 분배 및 실행 시스템의 안전성을 또한 증가시킨다.

무선 장치로부터 애플리케이션을 제거하는 능력은 애플리케이션 분배 시스템의 안전성을 또한 증가시킨다. 제조자에 의해 또는 다운로드된 애플리케이션을 통해 애플리케이션이 인스톨된 경우, 애플리케이션이 예측되지 않은 부정적인 결과 때문에 애플리케이션을 제거하는 메카니즘을 갖는 것은, 손상될 수 있는 해롭고 원하지 않는 코드를 제거함으로써 애플리케이션 분배 및 실행 시스템의 안전성을 증가시킨다.

본 발명에 따른 시스템 및 방법은 여기 개시된 기술 또는 그 이상을 실시할 수 있다. 여기 개시되고 참조된 모든 기술을 실시함으로써, 본 발명에 관련된 시스템 및 방법이 품질높고 안전한 애플리케이션의 분배 및 실행을 제공한다.

본 발명의 일실시예에 따르면, 애플리케이션을 분배 및 처리하는 방법은, 애플리케이션과 식별 정보를 수신하는 단계, 상기 애플리케이션이 소정의 표준을 만족하는 것을 인증하는 단계, 상기 애플리케이션에 허가를 할당하는 단계, 변경 검출 기술을 사용하여 애플리케이션, 허가, 및 식별 정보를 장치로 전송하는 단계, 전송하는 동안 애플리케이션이 변경되었는지를 판정하는 단계, 장치상에 규칙을 저장하는 단계, 허가 및 규칙을 사용하여, 애플리케이션이 처리될 수 있는지를 판정하는 단계, 및 장치로부터 상기 애플리케이션을 제거하는 단계를 구비한다.

본 발명의 다른 실시예에 따르면, 무선 장치상에서 애플리케이션을 실행하는 방법은, 허가를 평가하는 규칙을 저장하는 단계, 변경 검출 기술을 사용하여 애플리케이션, 허가, 및 식별을 구비하는 정보를 수신하는 단계, 무선 장치상에서 애플리케이션을 실행하는 요구를 수신하는 단계, 수신된 정보를 평가하여 수신된 정보가 변경되었는지를 판정하는 단계, 수신된 정보가 변경되지 않았을때는 애플리케이션과 관련된 허가를 평가하는 단계, 및 허가가 부여되면, 애플리케이션을 실행하는 단계를 구비한다.

본 발명의 또다른 실시예에 따르면, 무선 장치상에 애플리케이션을 실행하는 방법은, 허가를 평가하는 규칙을 저장하는 단계, 변경 검출 기술을 이용하여 애플리케이션, 허가, 및 식별을 구비하는 정보를 수신하는 단계, 무선 장치상에서 애플리케이션을 실행하는 요구를 수신하는 단계, 수신된 정보를 평가하여 수신된 정보가 변경되었는지를 판정하는 단계, 수신된 정보가 변경되지 않았을때, 애플리케이션과 관련된 허가를 평가하는 단계, 및 허가가 부여되면, 애플리케이션을 실행하는 단계를 구비한다.

도면의 간단한 설명

명세서에 병합되어 일부를 구성하는 첨부된 도면은 본 발명의 바람직한 실시예를 나타내는 것이며, 이는 위에서 주어진 일반적인 기술과 이하에 주어진 바람직한 실시예와 함께, 본 발명의 원리를 설명하기 위하여 제공된다.

도 1 은 본 발명의 예시적인 실시예의 안전한 애플리케이션 분배 및 실행의 고레벨 프로세스를 나타내는 플로우챠트.

도 2 는 본 발명의 예시적인 실시예가 실행될 수 있는 시스템 구성을 나타내는 블록도.

도 3 은 본 발명의 예시적인 실시예에서 안전한 애플리케이션 분배 처리 시스템이 실행될 수 있는 무선 네트워크 구성을 나타내는 블록도.

도 4 는 본 발명의 예시적인 실시예에서의 무선 장치 및 몇개의 내부 구성요소를 나타내는 블록도.

도 5 는 본 발명의 예시적인 실시예에서 디지털 서명을 생성하는데 사용되고 무선 장치에 전송된 정보를 나타내는 블록도.

도 6 은 본 발명의 예시적인 실시예에서 애플리케이션을 분배하는데 있어서 서버 또는 서버들에 의해 이용되는 단계를 나타내는 플로우챠트.

도 7 은 본 발명의 예시적인 실시예에서 애플리케이션을 실행할때 무선 장치에 의해 사용되는 단계를 나타내는 플로우챠트.

실시예

참조 번호는 첨부된 도면에 기재된 바와 같이 본 발명의 예시적이고 바람직한 실시예를 상세하게 하기 위한 것이며, 동일 참조 번호는 몇개의 도면에서 동일 또는 대응하는 부분을 나타낸다. 본 발명의 특질, 목적, 이점은 첨부된 도면과 결합하여 다음의 상세한 설명에 의해 당업자에게는 명백해질 것이다.

본 발명은 애플리케이션이 실행될 환경과 관련된 소정의 표준을 만족하는 것을 인증하기 위하여 애플리케이션을 테스트하는 시스템 및 방법을 제공함으로써 안전하고 보장된 애플리케이션 분배 및 실행을 제공한다. 또한, 규칙 및 허가 리스트, 애플리케이션 제거 및 디지털 서명 등의 변경 검출 기술을 사용하여, 본 발명은 애플리케이션이 변경되었는지, 주어진 무선 장치 환경에서 실행되도록 허가되었는지, 및 애플리케이션이 제거되는 것이 바람직한지를 판정함으로써 테스트되거나 테스트되지 않은 애플리케이션을 안전하게 분배하고 실행하는 메카니즘을 제공한다.

당업자는 앞서 설명한 것이 설명의 간략화를 위하여 분배되고 실행되는 애플리케이션 파일 형태임을 인식할 것이다. "애플리케이션"은 또한 오브젝트 코드, 스크립트, 자바 파일, 북마크 파일 (또는 PQA 파일), WML 스크립트, 바이트 코드, 및 펄 (perl) 스크립트 등의 실행가능한 내용을 갖는 파일을 포함할 수 있다. 또한, 여기서 언급된 "애플리케이션"은 개방될 필요가 있는 서류 또는 액세스될 필요가 있는 다른 데이터 등 특질에 있어서 실행될 수 없는 파일을 포함할 수 있다.

도 1 은 본 발명의 예시적인 실시예에 따른 방법의 안전한 애플리케이션 분배 및 실행의 고레벨 프로세스를 나타내는 플로우챠트이다. 본 발명의 실시예는 개발자 식별이 애플리케이션과 관련될 수 있도록 하고, 애플리케이션이 실행되는 환경에 대하여 애플리케이션을 테스트하고, 장치 또는 시스템이 애플리케이션을 실행할 수 있는다는 것을 지시하는데 사용될 수 있는 허가를 할당하고, 애플리케이션이 비합법적이거나 바람직하지 않은 동작을 수행하면 애플리케이션을 제거한다.

시스템 및 방법은 애플리케이션의 안전한 분배 및 실행을 증가시키기 위하여 이 모든 이들 기술을 채용하는 것이 바람직하다. 그러나, 이들 하나이상의 기술을 채용하는 것은 애플리케이션의 안전한 분배 및 실행을 증가시킨다는 것이 인식될 것이다.

고레벨 프로세스는 개발자 식별과 애플리케이션을 관련시킴으로써 시작된다 (단계 100). 이 프로세스는 분배된대로 애플리케이션과 개발자 식별을 관련시킴으로써 수행될 수 있다. 다른 방법으로, 관련된 개발자 식별이 시스템내의 서버상에 대응하는 애플리케이션에 따라 저장될 수 있다. 또한, 개발자 식별 정보는 쉽게 변경될 수 없도록 저장되어 애플리케이션 정보와 관련되는 것이 바람직하다.

그후, 애플리케이션은 부적절한 동작에 대하여 테스트된다 (단계 105). 부적절한 동작이 애플리케이션이 실행되는 장치에 영향을 줄 수 있을 뿐만 아니라 그 장치와 접속되거나 네트워크된 다른 장치들에 영향을 줄 수 있는 환경에서 애플리케이션이 사용될 수 있다. 그 동작 동안, 장치 또는 접속된 다른 장치에 부정적인 영향을 주거나 부적절한 시스템 호출을 발생시키지 않도록 애플리케이션을 테스트하는 것이 바람직하다. 일실시예에 있어서, 이 테스트는, 애플리케이션이 소정의 표준을 충족하는지를 판정하도록 테스트되는 인증(certification) 프로세스에 의해 수행된다. 또한, 애플리케이션을 테스트하기 위하여 개발자와 독립적인 인증 프로세스를 갖는 것이 바람직하다. 이 인증 프로세스의 독립성은 정확하고 신뢰성있는 테스트를 조장한다.

애플리케이션을 실행하기 전에, 애플리케이션이 장치상에서 실행되도록 허가되었는지를 판정하도록 체크된다 (단계 110). 이 체크는 이하 설명된 허가 및 규칙을 이용하여 또는 당업자에게 알려진 다른 허가 메카니즘을 사용하여 수행될 수 있다. 또한, 애플리케이션을 실행하기 전에 매번 애플리케이션을 체크하는 것이 바람직하다. 이 계속적인 체크 프로세스는 애플리케이션 실행의 안전성을 증가시킨다. 예를 들어, 다른 애플리케이션을 통해 실행 장치상에 그 애플리케이션을 삽입했었던 트로이 목마를 갖는 애플리케이션에 대하여 보호한다.

그후, 부적절하거나 바람직하지 않은 동작을 수행하는 애플리케이션은 장치로부터 제거된다 (단계 115). 이것은 애플리케이션이 임의의 또다른 손상을 주는 것을 방지하고 또한 다른 용도를 위해 장치내의 메모리를 비운다. 다른 방법으로, 애플리케이션은 애플리케이션으로부터 반드시 제거될 필요는 없다. 애플리케이션을 제거하는 것은 장치상의 애플리케이션을 방치되거나 애플리케이션을 사용불가능하게 하는 것을 의미할 수 있다.

도 2 는 본 발명의 예시적인 실시예가 실행될 수 있는 시스템 구성을 나타낸다. 개발자 (200) 는 무선 장치 (230) 상에 사용되는 애플리케이션을 생성한다. 상술한 바와 같이, 상술한 설명이 애플리케이션 파일 형태를 포함하는 것으로 설명하였지만, 다른 파일 형태가 사용될 수 있음을 당업자는 인식할 것이다. 또한, 당업자는 본 발명이 다른 무선 또는 비무선(non-wireless) 장치와 사용될 수 있고 무선 네트워크, 비무선 네트워크, 또는 그 결합을 채용할 수 있음을 인식할 것이다.

일반적으로, 개발자 (200) 는 무선 장치 (230) 상에서 실행하는 애플리케이션을 개발하는 한 셋트의 개발 설계서를 가질 것이다. 일실시예에서, 무선 장치는 미국 캘리포니아 샌디에고에 위치한 퀄컴 코오포레이션에 의해 개발된 BREW™ 소프트웨어 등의 무선 장치와의 애플리케이션 인터페이스를 보조하는 소프트 플랫폼을 포함한다. 개발자는 소프트웨어 플랫폼 또는 BREW™ 소프트웨어를 만족하는 애플리케이션, 설계서 표준, 및 규정(convention)을 생성할 수 있다.

일실시예에서, 개발자 (200) 는 중앙 서버 (205)에 접속되어 애플리케이션을 중앙 서버 (205) 로 전자적으로 전송하도록 한다. 일실시예에서, 중앙 서버는 무선 장치로의 애플리케이션 분배에 사용되는 애플리케이션 제어 센터 헤드쿼터 (Application Control Center Headquarter) 서버이다. 개발자 (200) 는 애플리케이션을 디지털적으로 서명하여 (후술함) 애플리케이션이 변경되었는지를 판정한다. 중앙 서버로의 물리적인 접속은 필수적인 것이 아님을 인식할 것이다. 예를 들어, 개발자 (200) 는 1급 메일 등을 통해 CD-ROM 상에 저장된 중앙 서버 (205) 로 애플리케이션을 전송할 수 있다.

또한, 개발자는 다양한 소오스 식별 정보를 중앙 서버 (205) 로 전송한다. 이 소오스 식별 정보는 회사 이름, 회사의 택스 (tax) 식별, 또는 다른 식별 정보 등 개발자를 식별하는 애플리케이션과 관련될 수 있는 임의의 형태의 정보를 포함할 수 있다.

중앙 서버 (205) 는 그 자체에 의해 또는 인증 서버 (210) 를 사용하여 애플리케이션의 분석 및 인증에 사용된다. 일실시예에서, 애플리케이션 제어 센터 (ACC) 는 인증 서버로서 이용될 수 있다. 인증 서버 (210) 는 애플리케이션이 소정의 인증 표준을 만족하는지를 판정하기 위하여 애플리케이션을 분석하는데 사용될 수 있다. 이 표준은 애플리케이션이 무선 장치 또는 플랫폼상에서 실행하기 위한 개발 설계서를 만족했는지를 판정하는 것을 포함할 수 있다. 그러나, 인증 표준은 무선 장치 또는 플랫폼상에서 실행하기 전에 애플리케이션이 만족해야만 하는 임의의 표준일 수 있다. 이러한 표준은 (a) 애플리케이션이 무선 장치의 동작에 해롭지 않도록 (예를 들어, 전화가 고장나지 않도록), 애플리케이션이 개발자에 의해 요구된 대로 기능하고, (b) 애플리케이션이 액세스해서는 안되는 데이터 또는 메모리를 액세스하지 않고 (예를 들어, 다른 애플리케이션, 오퍼레이팅 시스템, 또는 플랫폼 소프트웨어에 의해 소유된 데이터 또는 파일을 액세스하지 않음) , 및 (c) 무선 장치의 입출력을 불리하게 독점하는 등 무선 장치 리소스에 부정적으로 영향을 주지 않는 것을 입증하는 것을 포함할 수 있다.

중앙 서버 (205) 는 또한 애플리케이션과 관련된 리스트에 한셋트의 허가를 할당할 수 있다. 이 허가 리스트는 애플리케이션이 인증 프로세스를 통과했는지, 어떤 네트워크 (220) 가 애플리케이션이 실행되는 것을 승인했는지, 및 무선 장치가 애플리케이션을 지지하는지를 포함하는 다양한 팩터에 의해 결정된다. 이 허가 리스트를 결정하는데 사용되는 많은 팩터가 있으며 본 발명을 구현할때 당업자에게 맡겨진다.

중앙 서버 (205) 는 개발자 식별 정보를 수신하고 개발자 (200) 에 의해 생성된 애플리케이션과 그 개발자 식별 정보를 상관한다. 애플리케이션에 임의의 문제점이 있으면, 중앙 서버는 애플리케이션의 소오스를 식별할 수 있다. 일실시예에서, 개발자 정보는 무선 장치 (230) 를 통과하여 무선 장치 또는 무선 장치에 접속된 다른 시스템에 의해 상관 (correlation) 이 수행될 수 있다.

일실시예에서, 중앙 서버는 또한 애플리케이션 다운로드 서버 (ADS; 215) 에 접속된다. 애플리케이션 다운로드 서버 (215) 는 애플리케이션을 다운로드하기 위하여 무선 네트워크 (220) 를 통해 무선 장치와 인터페이스하는데 사용된다. 중앙 서버는 또한 애플리케이션과 관련된 허가 리스트 및 개발자 식별을 무선 장치에 전송될때까지 저장될 수 있는 ADS 에 전송할 수 있다. 애플리케이션, 허가 리스트, 및 개발자 식별은 중앙 서버에 의해 디지털적으로 서명되어 변경으로부터의 안전을 증가시키는 것이 바람직하다.

당업자는, ADS 가 다양한 무선 장치 (230) 로 애플리케이션, 파일 및 다른 정보를 분배하기 위한 다중 네트워크 (220) 에 접속되는데 사용될 수 있음을 인식할 것이다. 또한, 무선 및 비무선 네트워크는 무선 장치에 애플리케이션의 허가 리스트 및 개발자 식별을 전송하는데 채용될 수 있다.

애플리케이션에 대한 요구에 응답하여, ADS (215) 는 네트워크 (220) 를 통해 무선 장치 (230) 에 애플리케이션, 허가 리스트, 개발자 식별, 및 디지털 서명(들)을 전송할 것이다. 일실시예에서, 무선 장치 (230) 는 애플리케이션, 허가 리스트 및/또는 개발자 정보가 변경되는지를 판정하기 위하여 디지털 서명을 체크하는 키를 포함할 것이다.

디지털 서명이 본 발명에서 채용되면, 중앙 서버는 안전 키를 사용하여 디지털 서명을 생성하고 무선 장치에 키를 인스톨하여 디지털 서명을 평가하는 것이 바람직하다. 안전 키를 사용함으로써, 무선 장치는 디지털 서명이 사기꾼에 의해 생성되지 않고 중앙 서버에 의해 생성되었다는는 고도의 신뢰성을 가질 것이다.

애플리케이션이 무선상에 임의의 에러를 발생시키거나 임의의 다른 이유로, 무선 장치는 애플리케이션의 제거를 개시할 수 있다. 또한, 애플리케이션은 ADS 또는 중앙 서버로부터의 요구에 기초하여 무선 장치로부터 제거될 수 있다. 서버로부터의 이 요구는 임의의 이유때문에 발생될 수 있다. 예를 들어, 서버는, 애플리케이션이 또다른 장치상에서 부적절하게 수행되거나 새로운 버전의 애플리케이션이 분배되거나 애플리케이션이 제거되어야 하는 사업상의 이유등으로 무선 장치로부터 애플리케이션의 제거를 개시할 수 있다. 이 애플리케이션 제거 프로세스는 또한 무선 장치 환경을 오류가 있는 및/또는 파괴적인 애플리케이션의 반복적인 실행으로부터 보호할 수 있다.

도 3 은 본 발명의 예시적인 실시예에서 애플리케이션 분배 시스템이 실행될 수 있는 무선 네트워크 구성을 나타낸다. 중앙 서버 (302) 는, 그 자체 또는 인증 서버와의 결합에 의해 정의된 프로그래밍 표준 또는 규정 셋트와 양립할 수 있는 애플리케이션 프로그램을 인증하는 엔티티(entity)이다. 위에서 설명한 바와 같이, 이들 프로그램 표준은 애플리케이션이 BREW^{TM} 플랫폼 등의 소프트웨어 플랫폼상에서 실행될 수 있도록 확립될 수 있다.

일실시예에서, 중앙 서버 데이터베이스 (304) 는, 네트워크 (300) 의 무선 장치 (330) 각각에 언제든지 다운로드되는 애플리케이션 프로그램을 위한 식별의 레코드, 애플리케이션 프로그램이 다운로드된 개체에 대한 전자 서비스 번호 (Electronic Service Number: ESN), 및 애플리케이션 프로그램을 갖는 무선 장치 (330) 에 유일한 이동 식별 번호 (Mobil Identification Number: MIN) 으로 구성된다. 다른 방법으로, 중앙 서버 데이터베이스 (304) 는 무선 장치 모델의 네트워크 (300) 의 각각의 무선 장치 (330) 에 대한 레코드, 무선 네트워크 캐리어, 무선 장치 (330) 가 사용되는 영역, 및 애플리케이션 프로그램을 갖는 무선 장치 (330) 를 식별하는데 이용될 수 있는 임의의 다른 정보를 포함한다. 또한, 중앙 서버 데이터베이스는 또한 애플리케이션과 관련된 이 개발자 식별 정보를 저장할 수 있다.

일실시예에서, 중앙 서버 (302) 는 제거 코맨드 소오스 (322) 를 포함할 수 있다. 제거 코맨드 소오스 (322) 는 하나 이상의 타겟 애플리케이션 프로그램을 제거할 것인지를 판정하는 사람(들) 또는 엔티티(들)이다. 제거 코맨드 소오스 (322) 는 또한 타겟 애플리케이션 프로그램(들)을 갖는 식별된 무선 장치 (330) 에 제공되는 제거 코맨드 (316; 후술함) 을 구성하는 엔티티이다. 다른 방법으로, 제한없이, 제거 코맨드 소오스 (322) 는 타겟 애플리케이션 프로그램의 개발 및 발행과 관련된 하나이상의 사람 또는 엔티티, 무선 장치 (330) 의 제조와 관련된 사람 또는 엔티티, 및/또는 네트워크 (300) 의 어느 부분의 기능과 관련된 사람 또는 엔티티이다.

중앙 서버 (302) 는, 바람직하게 안전한 인터넷 등 네트워크 (308) 를 통해 하나이상의 컴퓨터 서버 (306), 예를 들어, ADS 와 통신한다. 서버 (306) 는 또한 네트워크 (308) 를 통해 캐리어 네트워크 (310) 와 통신한다. 캐리어 네트워크 (310) 는 인터넷 및 POTS (Plain Ordinary Telephone System; 일괄하여 도 3 에서 311로 표기됨)에 의해 MSC (312) 와 통신한다. 캐리어 네트워크 (310) 와 MSC (312) 간의 인터넷 접속 (311) 은 데이터를 전송하고, POTS (311) 은 보이스(voice) 정보를 전송한다. MSC (312) 는 다중 기지국 (BTS; 314) 에 접속된다. MSC (312) 는 (데이터 전송을 위한) 인터넷 (311) 과 (보이스 전송을 위한) POTS (311) 에 의해 BTS 에 접속된다. BTS (314) 는 쇼트 메시징 서비스 (short message service: SMS) 또는 다른 임의의 방송 방법에 의해 무선 장치 (330) 에 메시지를 무선으로 전송한다.

본 발명의 BTS (314) 에 의해 전송된 메시지의 일예는 제거 코맨드 (316) 이다. 여기에서 더 설명한 바와 같이, 무선 장치는 제거 코맨드 (316) 을 수신하는 것에 응답하여 무선 장치 (330) 에 저장된 타겟 애플리케이션 프로그램을 인스톨하지 않음 (uninstall) 으로써 응답한다. 일실시예에서, 제거 프로그램은 타겟 애플리케이션 프로그램을 사용불가능하게 하거나 재프로그램(reprogram)하여 다르게 수행하도록 추가적으로 또는 선택적으로 프로그램될 수 있다. 무선 장치는 또한 애플리케이션 및 허가 리스트 등의 임의의 관련된 정보를 삭제할 수 있다.

제거 코맨드 (316) 는 (타겟 애플리케이션 프로그램의 제거를 초기화하는 것을 판정하는 사람(들) 또는 엔티티(들) 과 동일할 수도 있으며 동일하지 않을 수도 있는) 제거 코맨드 소오스 (322) 에 의해 구성된다. 제거 코맨드 (316) 는 무선 장치 (330) 에 동시 통신하는 네트워크 (300) 를 통해 제거 코맨드 소오스 (322) 에 의해 전송된다.

상술한 실시예에 기재된 제거 코맨드를 사용하여, 애플리케이션 분배 및 실행의 안전성은 오류가 있거나 또는 바람직하지 않은 애플리케이션을 인스톨하지 않는 메카니즘을 제공함으로써 증가된다. 당업자는 앞서 설명한 제거 코맨드가 중앙 서버에 의해 개시되었지만 무선 장치는 또한 애플리케이션 및 그 관련된 정보의 제거 또는 인스톨하지 않는 것을 개시할 수 있음을 인식할 것이다.

마찬가지로, 상기의 네트워크는 중앙 서버에서부터 다양한 서버 (306) (예를 들어, ADS) 까지의 애플리케이션, 허가 리스트 및 관련된 디지털 서명을 MSC 및 BTS 를 통해 무선 장치 (330) 로 전송하는데 사용될 수 있다.

도 4 는 본 발명의 예시적인 실시예에서의 무선 장치와 몇개의 내부 구성요소를 나타낸다. 이 실시예가 무선 장치 (400) 에 관한 것이지만, 이 실시예는 임의의 의도된 제한없이 일예로 사용된다. 본 발명은, 제한없이, 퍼스널 디지털 어시스턴트 (PDA), 무선 모뎀, PCMCIA 카드, 액세스 터미널, 퍼스널 컴퓨터, 디스플레이 또는 키패드 없는 장치, 또는 그들의 임의의 조합 또는 그들의 하위 조합 등의 무선 및 비무선 장치를 포함하는 네트워크를 통해 통신할 수 있는 임의의 형태의 원격 모듈상에서 선택적으로 수행될 수 있다. 이들 원격 모듈의 예는 또한 키패드, 비쥬얼 디스플레이 또는 사운드 디스플레이 등의 사용자 인터페이스를 가질 수 있다.

도 4 에 도시된 무선 장치 (400) 는 무선 장치 (400) 가 제조될때 인스톨된 애플리케이션 주문형 집적 회로 (ASIC; 415) 를 갖는다. ASIC 는 ASIC 내에 포함된 소프트웨어에 의해 구동되는 하드웨어 구성요소이다. 애플리케이션 프로그래밍 인터페이스 (API; 410) 는 또한 제조시에 무선 장치 (400) 에 인스톨된다. 일실시예에서, API 는 BREW API 또는 소프트웨어 플랫폼을 나타낸다. API (410) 는 ASIC 와 상호 동작하도록 구성된 소프트웨어 프로그램이다. API (410) 는 ASIC (415) 하드웨어와 무선 장치 (400) 상에 인스톨된 애플리케이션 프로그램 (후술함) 간의 인터페이스로서 제공된다. 다른 방법으로, 무선 장치 (400) 는 프로그램이 무선 장치 (400) 의 하드웨어 구성과 양립하는 방식으로 동작되도록 하는 임의의 다른 형태의 회로를 포함할 수 있다. 무선 장치 (400) 는 또한 기억 영역 (405) 를 갖는다. 기억영역 (405) 는 RAM 및 ROM 으로 구성되지만, 다른 방법으로, EPROM, EEPROM 또는 플래쉬 카드 삽입물 등의 임의의 형태의 메모리일 수 있다.

무선 장치의 기억 영역 (405) 는 수신된 애플리케이션 및 허가 리스트 (425) 를 저장하는데 사용될 수 있다. 또한, 기억 영역 (405) 은 하나 이상의 키 (405)를 저장하는데 사용될 수 있다. 이들 키는 서명된 정보가 변경되었는지를 판정하는 서명 알고리즘을 사용하는 디지털 서명에 적용될 수 있다.

규칙 (435) 은 또한 무선 장치 (400) 상에 인스톨될 수 있다. 이들 규칙은 허가 리스트와 결합하여 사용되어 애플리케이션이 실행되도록 허용되는지를 판정한다. 예를 들어, 규칙은 인증 플래그가 허가 리스트에 설정되면 (즉, 애플리케이션 통과 인증을 가리키면) 애플리케이션이 실행되는 것을 허용한다는 것을 나타낸다. 허가 리스트는 애플리케이션이 인증을 통과했는지에 의존하여 설정되거나 설정되지 않은 인증 플래그를 가질 것이다. 규칙을 허가 리스트에 포함된 정보에 적용함으로써, 애플리케이션을 실행하는 허가가 부여되거나 부정된다.

무선 장치 (400) 의 제조자 (도시생략) 은 무선 장치 (400) 가 제조될때 무선 장치 (400) 의 기억 영역 (405) 에 애플리케이션 프로그램을 다운로드할 수 있다. 이들 애플리케이션 프로그램은 게임, 책, 또는 임의의 다른 형태의 데이터 또는 소프트웨어 프로그램 등의 무선 장치의 사용자에게 잠재적으로 유용하거나 사용자를 즐겁게 하는 임의의 프로그램일 수 있다. 애플리케이션 프로그램은 또한 무선 장치가 제조된 후에 방송을 통해 무선 장치 (400) 에 다운로드될 수 있다.

무선 장치 (400) 에 의해 실행될 때, 제거 프로그램은 무선 장치 (400) 상에 저장된 애플리케이션중의 하나로부터 하나이상의 타겟 애플리케이션 프로그램들을 인스톨하지 않는다. 타겟 애플리케이션 프로그램은 이하 설명하는 다양한 이유로 무선 장치 (400) 로부터 인스톨하지 않아야할 필요가 있는 애플리케이션 프로그램이다.

무선 장치 (400) 는 제조자에 의해 인스톨된 로컬 데이터베이스 (420) 를 갖는다. 무선 장치의 API 는 무선 장치 (400) 상에 저장된 애플리케이션 프로그램의 각각에 대한 정보를 식별하는 레코드로 로컬 데이터베이스 (420) 를 자동적으로 업데이트하도록 프로그램된다. 로컬 데이터베이스 (420) 는 무선 장치 (402) 상에 저장된 각각의 애플리케이션 프로그램에 유일한 서명 식별의 레코드를 포함한다. 또한, 로컬 데이터베이스 (420) 는 무선 장치 (400) 상의 기억 영역 (405) 내의 애플리케이션 프로그램의 위치의 레코드 및 애플리케이션 프로그램이 무선 장치 (400) 상에 다운로드되어 위치하는 트랙을 유지하는데 유용한 임의의 다른 정보를 포함할 수 있다.

도 5 는 본 발명의 예시적인 실시예에서 디지털 서명을 생성하는 사용되며 무선 장치에 전송되는 정보를 나타내는 블록도이다. 당업자에게 알려진 바와 같이, 디지털 서명은 디지털 파일이 변경되었는지를 트래킹하는데 사용될 수 있다. 서술한 바와 같이, 디지털 서명은 서류, 애플리케이션, 데이터베이스 등을 포함하는 임의의 디지털 파일에 적용될 수 있다. 일반적

으로, 디지털 서명은 서명 알고리즘을 사용하여 파일에 키를 적용함으로써 생성된다. 이 디지털 서명은 파일내에 포함된 정보를 사용하여 생성된다. 일반적으로 디지털 서명은 파일과 함께 수령자에게 전송된다. 파일 및 디지털 서명의 수령자는 키를 수신된 파일과 디지털 서명에 적용하여 수령자에게 전송하는 동안 파일이 변경되었는지를 판정한다.

디지털 서명을 생성하고 평가하는데 사용되는 키는 서명자의 식별을 판정하는데 사용될 수 있다. 예를 들어, 키는 엔티티가 디지털 서명을 생성시키도록 발생되어 안전하게 유지될 수 있다. 이 엔티티는 디지털 서명을 평가하기 위하여 사용될 수 있는 대응 키를 분배할 수 있다. 키가 안전하게 유지되고 손상되지 않으면, 디지털 서명을 평가하는 수령자는 정보가 변경되었는지를 판정할 뿐만 아니라 서명자의 식별을 판정할 수 있다.

다른 방법으로, 제 3 엔티티는 안전한 방법으로 특정 엔티티를 위한 키를 생성할 수 있다. 그러므로, 특정 식별과 관련된 키를 갖는 수령자는 엔티티가 서명자였는지를 판정할 수 있을 것이다.

본 발명의 일실시예에서, 디지털 서명 (515) 은 디지털 서명 알고리즘 (530) 에 입력된 서명자의 키 (525), 예를 들어, 중앙 서버 (도 2 참조) 의 키, 애플리케이션 (500), 허가 리스트 (505), 및 개발자 식별 정보 (510) 를 사용하여 발생된다. 그 결과는 입력에 포함된 정보에 의존한 디지털 서명 (515) 이다.

디지털 서명 (515) 를 생성한 후, 애플리케이션 (500), 허가 리스트 (505), 개발자 식별 정보 (510), 및 디지털 서명 (515) 은 무선 장치 (520) 로 전송된다. 그후, 무선 장치는 애플리케이션 또는 관련된 정보 (즉, 허가 리스트 및 개발자 식별 정보) 중의 어느 것이 변경되었는지를 판정하기 위하여 디지털 서명을 사용할 수 있다. 또한, 안전 키 등의 상술한 기술중의 하나를 사용하여, 무선 장치는 또한 무선 장치로 이 정보를 전송한 서명자의 식별의 확실성을 가질 수 있다.

도 6 은 본 발명의 예시적인 실시예와 관련된 방법으로 애플리케이션을 분배하는데 있어서 서버 또는 서버들에 의해 사용될 수 있는 단계를 나타내는 플로우챠트이다. 이 예시적인 실시예에서, 프로세스는 애플리케이션 및 디지털 서명을 수신함으로써 개시된다 (단계 600). 디지털 서명은 그 수신전에 애플리케이션이 변경되었는지를 판정할 수 있도록 애플리케이션에 관련된 정보이다. 또한, 디지털 서명을 서명하는데 사용되는 키는 제 3 자에 의해 할당되어 애플리케이션을 서명한 엔티티 또는 개발자가 할당된 키를 수신하는 개발자임을 확인하는 것이 바람직하다.

애플리케이션 및 디지털 서명을 수신한 후, 디지털 서명은 애플리케이션을 전송한 개발자가 애플리케이션을 서명한 사람과 동일한지를 판정하기 위하여 평가된다 (단계 605). 제 3 자가 개발자에게 키를 할당하여 디지털 서명을 생성하면, 제 3 자는 또한 키를 할당하여 도 2 와 관련하여 설명한 중앙 서버 등의 수신자에 대한 디지털 서명을 평가할 수 있다.

그후, 개발자의 식별 또는 엔티티가 애플리케이션을 서명 및/또는 생성했는지가 저장되고 애플리케이션과 관련된다 (단계 610). 저장은 개발자의 식별이 나중에 판정될 필요가 있을때 검색될 수 있도록 테이블, 데이터베이스, 또는 몇가지 다른 방법으로 수행될 수 있다. 일실시예에서, 개발자의 식별은 서버내에 저장되지 않고 무선 장치내에 저장된다.

그후, 수신된 애플리케이션은 특정한 표준을 만족하는지를 판정하기 위하여 인증된다 (단계 615). 일실시예에서, 애플리케이션은, 무선 장치에 사용된 미국 캘리포니아 샌디에고에 위치한 퀄컴 코오포레이션에 의해 개발된 BREW^{TM} 플랫폼 등의 특정 플랫폼상에서 실행하도록 기록될 수 있다. 특정 플랫폼 또는 장치는 애플리케이션이 장치상에서 실행되기 전에 애플리케이션이 만족해야 하는 특정 요구사항을 가질 수 있다. 예를 들어, 플랫폼 또는 장치는, 장치 또는 메모리에 위치한 다른 애플리케이션들의 보전이 손상되지 않도록 애플리케이션이 장치내의 특정 메모리 위치를 액세스하지 않는 것을 요구할 수 있다. 이들 표준은 특정될 수 있으며 애플리케이션은 이들 표준이 만족되는지를 판정하기 위하여 테스트될 수 있다. 바람직하게, 이들 표준은 미리 결정된 것이며 개발자에게 제공되어 애플리케이션의 개발에 결합될 수 있다.

인증후에, 주어진 환경에 대한 애플리케이션과 관련된 허가가 할당된다 (단계 620). 허가는 본 발명이 실시되는 환경에 의존하여 많은 팩터에 기초하여 할당될 수 있다. 일실시예에서, 애플리케이션은 무선 장치를 위한 것이다. 이 실시예에서, 허가의 할당은 예를 들어 캐리어 네트워크, 무선 장치의 요구사항, 인증 테스트 결과, 및 개발자, 캐리어 또는 다른 테스트 환경에 의존할 수 있다. 그러므로, 허가 리스트의 예는 애플리케이션이 인증 테스트를 통과하고 특정 캐리어의 네트워크상에서 실행될 수 있는 것을 가리키는 것이다.

그후, 서버는 애플리케이션, 허가 리스트, 및 개발자 식별을 디지털적으로 서명한다 (단계 625). 일실시예에서, 이 서명은 안전 키를 이용하여 수행되어 서버의 식별이 이 디지털적으로 서명된 정보를 수신한 사람에 의해 판정될 수 있다. 서버에 의해 수신된 개발자의 서명은, 또한 서명되거나 개발자의 서명이 무선 장치에 송신될 필요는 없다.

그후, 단계 (625) 에서 생성된 애플리케이션, 허가 리스트, 개발자 식별, 및 서명은 무선 장치로 전송된다 (단계 630).

도 7 은 본 발명의 예시적인 실시예에 따른 방법으로 애플리케이션을 실행할때 무선 장치에 의해 사용되는 단계를 나타내는 플로우챠트이다. 이 실시예에서, 무선 장치는 애플리케이션과 관련된 허가를 평가하기 위한 규칙을 저장한다 (단계 700). 당업자는, 본 발명이 규칙/허가 패터다임을 설명하지만 특정 장치 또는 플랫폼에 대한 애플리케이션에 허가를 부여하는데 사용될 수 있는 많은 패러다임이 있으며, 이들은 본 발명의 범위내에 있음을 인식할 것이다.

그후, 무선 장치는 애플리케이션, 허가 리스트, 개발자 식별 및 디지털 서명을 수신한다 (단계 705). 일실시예에서, 무선 장치는 수신된 디지털 서명을 평가하여 서명자의 식별을 판정할 수 있다. 디지털 서명은 또한 애플리케이션, 허가 리스트 또는 개발자 식별이 서명된 후에 변경되었는지를 판정하는데 사용될 수 있다.

그후, 무선 장치는 애플리케이션을 실행하는 요구를 수신한다 (단계 710). 이 요구는 프로그램을 실행하기를 원하는 무선 장치의 사용자로부터 기인될 수 있다. 다른 방법으로, 요구는 무선 장치로의 네트워크 접속 또는 직접 접속을 통해 무선 장치에 전송된 몇가지 요구로부터 또는 무선 장치 자체에 의해 생성될 수 있다.

요구를 수신한 후, 무선 장치는 그 실행전에 애플리케이션과 관련된 디지털 서명과 허가 리스트를 평가한다 (단계 720). 서술한 바와 같이, 일실시예에서, 무선 장치는 허가 리스트를 평가하는 규칙을 사용할 수 있다. 디지털 서명을 평가함으로써 애플리케이션, 허가 리스트 또는 개발자의 식별이 변경되지 않았다는 것을 판정하면, 무선 장치는 저장된 규칙을 사용하여 허가 리스트를 평가한다. 변경이 없고 허가 리스트에 대한 규칙의 평가가 애플리케이션이 무선 장치에서 실행하도록 허가를 부여한 것을 가리키면, 프로세싱은 장치상의 애플리케이션을 실행하도록 진행한다 (단계 730).

단계 (720) 에서의 평가가 서명후에 애플리케이션, 허가 리스트, 또는 개발자 식별이 변경되었다는 것을 가리키거나, 또는 애플리케이션이 무선 장치상에서 실행되는 허가가 부정되는 것을 가리키면, 애플리케이션은 실행되지 않는다 (단계 725). 프로세싱은 무선 장치로부터 애플리케이션을 제거하도록 진행된다 (단계 750). 또한, 허가 리스트 및 개발자 식별이 또한 무선 장치로부터 제거되는 것이 바람직하다.

단계 (730) 후에, 애플리케이션 실행은 비합법적이거나 부적절한 동작을 수행하는지를 판정하도록 모니터된다 (단계 735). 무선 장치 또는 무선 장치가 사용되는 플랫폼은 비합법적이거나 부적절한 임의의 동작을 정의할 수 있다. 이들 동작은 메모리의 제한된 영역 또는 다른 프로그램 또는 파일에 의해 사용되는 메모리의 위치를 액세스하는 것을 포함할 수 있다. 또한, 이들 동작은 무선 장치 뿐만 아니라 무선 장치가 부착된 네트워크상의 다른 장치에 영향을 주지 않도록 무선 장치의 리소스의 해로운 사용을 포함할 수 있다.

그러한 비합법적이거나 부적절한 동작이 시도되면, 애플리케이션의 실행이 정지되고 (단계 745), 바람직하게 개발자 식별 및 허가 리스트와 함께 무선 장치로부터 제거된다 (단계 750). 상술한 바와 같이, 다른 방법으로, 제거 프로세스는 애플리케이션을 사용불가하게 하여 그 실행을 방지하고 무선 장치상에 애플리케이션을 유지하는 것을 포함할 수 있다.

단계 (735) 에서 비합법적이거나, 부적절하거나 바람직하지 않은 동작이 수행되지 않으면, 애플리케이션은 실행을 유지하도록 허가된다 (단계 740).

결론

인증, 변경 검출, 소오스 식별 결정, 허가 할당, 및 애플리케이션을 제거하는 능력을 병합하는 메카니즘을 사용하여, 본 발명에 따른 시스템 및 방법은 안전한 애플리케이션 분배 및 실행을 증가시킨다. 시스템 및 방법은 이들 메카니즘의 몇개 또는 모두를 실시할 수 있다. 더 많은 메카니즘이 실시될수록, 성취되는 안정성의 정도는 높아진다.

일실시예에서, 개발자는 애플리케이션을 서버로 전송한다. 개발자는 애플리케이션을 서명하여 권한부여되지 않은 변경에 대하여 보호할 수 있다. 서버는 개발자의 식별을 체크하고 애플리케이션에 대한 인증 테스트를 수행한다. 서버는 또한 허가 리스트를 생성하면서 애플리케이션에 대한 허가를 할당한다. 애플리케이션, 허가 리스트, 개발자 식별은 서버에 의해 디지털적으로 서명되어 디지털 서명과 함께 무선 장치로 전송된다. 무선 장치는 애플리케이션을 실행하기 전에 저장된 규칙에 대하여 변경 및 허가 리스트에 대한 디지털 서명을 체크한다. 일실시예에서, 이들 체크는 무선 장치상에서 애플리케이션을 실행하기 전에 수행된다. 체크가 애플리케이션이 변경되었거나 실행 허가가 부정되는 것을 지시하면, 애플리케이션은 실행되지 않고 무선 장치로부터 제거된다. 또한, 실행하는 동안, 애플리케이션이 비합법적이거나 부적절한 동작을 시도하면, 애플리케이션은 종료되고 무선 장치로부터 제거된다.

본 발명의 구현에 대한 상술한 설명은 설명을 목적으로 하는 것이다. 본 발명은 개시된 정밀한 형태로 제한되는 것은 아니다. 변경 및 변형은 상술한 설명의 견지에서 가능하며 본 발명의 실행으로부터 얻어질 수 있다. 예를 들어, 상술한 구현은 소프트웨어를 포함하지만, 본 발명의 일실시예는 하드웨어와 소프트웨어의 조합 또는 하드웨어 단독으로 수행될 수 있다. 본 발명은 객체지향 및 비객체지향 프로그래밍 시스템으로 실행될 수 있다. 또한, 본 발명의 형태는 메모리에 저장된 것으로서 기술되었지만, 당업자는 이들 형태가 하드디스크, 플로피 디스크, 또는 CD-ROM 과 같은 2차 기억장치; 인터넷 또는 다른 전파 미디어로부터의 캐리어 웨이브; 또는 다른 형태의 RAM 또는 ROM 등의 다른 형태의 컴퓨터 판독 가능 미디어에 저장될 수 있음을 인식할 것이다. 본 발명의 범위는 청구항과 그 동등물에 의해 정의된다.

(57) 청구의 범위

청구항 1.

무선 네트워크를 통해 통신하는 무선 장치상에서의 이용을 위해 애플리케이션을 서버 프로세싱하고 분배하는 방법으로서,

상기 애플리케이션 및 상기 애플리케이션과 관련된 제 1 식별 정보를 수신하는 단계로서, 상기 제 1 식별 정보는 상기 애플리케이션의 소스의 식별을 확인하는데 이용가능한, 단계; 및

상기 애플리케이션이 소정의 표준 세트에서의 각 표준을 만족하는 것을 인증하는 단계로서, 상기 각 표준은 무선 환경과 개별적으로 관련되는, 단계를 포함하고,

상기 인증 단계 후에,

상기 애플리케이션에 허가 세트를 할당하는 단계로서, 상기 허가 세트는 상기 소정의 표준 세트에서의 각 표준과 각각 관련되는 복수의 허가를 구비하는, 단계; 및

상기 애플리케이션, 상기 허가 세트, 및 제 2 식별 정보를 상기 무선 장치로 전송하는 단계로서, 상기 제 2 식별 정보는 상기 서버의 식별을 확인하는데 이용가능한, 단계를 포함하고,

상기 애플리케이션은 상기 무선 장치와 상기 무선 네트워크 사이의 무선 통신을 수행하는 임의의 동작과도 독립적인, 애플리케이션을 서버 프로세싱하고 분배하는 방법.

청구항 2.

제 1 항에 있어서,

상기 소정의 표준 세트는 일반 (generic) 무선 네트워크와 관련된 제 1 표준 및 특정 (specific) 무선 네트워크와 관련된 제 2 표준을 포함하는, 애플리케이션을 서버 프로세싱하고 분배하는 방법.

청구항 3.

제 1 항에 있어서,

상기 전송 단계에서, 적어도 상기 애플리케이션은 변경 검출 기술을 이용하여 전송되는, 애플리케이션을 서버 프로세싱하고 분배하는 방법.

청구항 4.

제 3 항에 있어서,

상기 변경 검출 기술은 디지털 서명을 이용하는, 애플리케이션을 서버 프로세싱하고 분배하는 방법.

청구항 5.
삭제

청구항 6.
삭제

청구항 7.
삭제

청구항 8.
삭제

청구항 9.
삭제

청구항 10.
삭제

청구항 11.
삭제

청구항 12.
삭제

청구항 13.
삭제

청구항 14.
삭제

청구항 15.
삭제

청구항 16.
삭제

청구항 17.
삭제

청구항 18.
삭제

청구항 19.
삭제

청구항 20.
삭제

청구항 21.
삭제

청구항 22.
삭제

청구항 23.
삭제

청구항 24.

무선 네트워크를 통해 통신하는 무선 장치상에서의 이용을 위해 애플리케이션을 프로세싱하고 분배하는 시스템으로서,

캐리어 네트워크;

상기 캐리어 네트워크에 접속되는 상기 무선 네트워크를 지원하는 인프라스트럭처; 및

상기 캐리어 네트워크에 접속되는 서버를 포함하고,

상기 서버는,

상기 애플리케이션 및 상기 애플리케이션과 관련된 제 1 식별 정보를 수신하되, 상기 제 1 식별 정보는 상기 애플리케이션의 소스의 식별을 확인하는데 이용가능하도록 수신하고,

상기 애플리케이션이 소정의 표준 세트에서의 각 표준을 만족하는 것을 인증하되, 상기 각 표준은 무선 환경과 개별적으로 관련되도록 인증하고,

상기 인증 후에,

상기 애플리케이션에 허가 세트를 할당하되, 상기 허가 세트는 상기 소정의 표준 세트에서의 각 표준과 각각 관련되는 복수의 허가를 구비하도록 할당하고,

상기 애플리케이션, 상기 허가 세트, 및 제 2 식별 정보를 상기 캐리어 네트워크 및 상기 인프라스트럭처를 통해 상기 무선 장치로 전송하되, 상기 제 2 식별 정보는 상기 서버의 식별을 확인하는데 이용가능하게 전송하도록 구성되며,

상기 애플리케이션은 상기 무선 장치와 상기 무선 네트워크 사이의 무선 통신을 수행하는 임의의 동작과도 독립적인, 애플리케이션을 프로세싱하고 분배하는 시스템.

청구항 25.

제 24 항에 있어서,

상기 애플리케이션, 상기 허가 세트, 및 상기 제 2 식별 정보를 상기 무선 장치로 전송하도록 하는 단계에서, 변경 검출 기술이 이용되는, 애플리케이션을 프로세싱하고 분배하는 시스템.

청구항 26.

제 24 항에 있어서,

상기 서버는,

인터-서버 네트워크;

상기 애플리케이션을 수신하도록 구성되는 제 1 서버;

상기 애플리케이션을 인증하도록 구성되는 제 2 서버; 및

상기 허가 세트를 할당하고 상기 애플리케이션을 전송하도록 구성되는 제 3 서버를 포함하고,

상기 제 1, 제 2, 및 제 3 서버는 각각 상기 인터-서버 네트워크에 접속되고, 상기 제 3 서버는 상기 캐리어 네트워크에 접속되는, 애플리케이션을 프로세싱하고 분배하는 시스템.

청구항 27.

삭제

청구항 28.

삭제

청구항 29.

무선 네트워크를 통해 통신하는 무선 장치상에서의 이용을 위해 애플리케이션을 프로세싱하고 분배하는 시스템으로서,

캐리어 네트워크 수단;

상기 캐리어 네트워크 수단에 접속되는 상기 무선 네트워크를 지원하는 인프라스트럭처 수단; 및

상기 캐리어 네트워크 수단에 접속되는 서버 수단을 포함하고,

상기 서버 수단은,

상기 애플리케이션 및 상기 애플리케이션과 관련된 제 1 식별 정보를 수신하는 수단으로서, 상기 제 1 식별 정보는 상기 애플리케이션의 소스의 식별을 확인하는데 이용가능한, 수단;

상기 애플리케이션이 소정의 표준 세트에서의 각 표준을 만족하는 것을 인증하는 수단으로서, 상기 각 표준은 무선 환경과 개별적으로 관련되는, 수단;

상기 인증 수단에 의해 인증이 된 후에, 상기 애플리케이션에 허가 세트를 할당하는 수단으로서, 상기 허가 세트는 상기 소정의 표준 세트에서의 각 표준과 각각 관련되는 복수의 허가를 구비하는, 수단; 및

상기 애플리케이션, 상기 허가 세트, 및 제 2 식별 정보를 상기 무선 장치로 전송하는 수단으로서, 상기 제 2 식별 정보는 상기 서버의 식별을 확인하는데 이용가능하도록 전송하는, 수단을 포함하고,

상기 애플리케이션은 상기 무선 장치와 상기 무선 네트워크 사이의 무선 통신을 수행하는 임의의 동작과도 독립적인, 애플리케이션을 프로세싱하고 분배하는 시스템.

청구항 30.

삭제

청구항 31.

삭제

청구항 32.
삭제

청구항 33.

무선 네트워크를 통해 통신하는 무선 장치상에서의 실행을 위해 애플리케이션을 프로세싱하는 방법으로서,

상기 무선 네트워크를 통해 서버로부터, 상기 애플리케이션, 허가 세트, 및 식별 정보를 포함하는 전송 메시지를 수신하는 단계;

상기 허가에 대하여, 상기 무선 장치에 미리 저장되는 규칙을 평가하는 것에 기초하여, 상기 애플리케이션 실행 가능 여부를 결정하는 단계;

상기 애플리케이션 실행이 가능하다면, 상기 애플리케이션을 실행하는 단계; 및

상기 애플리케이션 실행이 가능하지 않다면, 상기 무선 장치로부터 상기 애플리케이션을 제거하는 단계를 포함하는, 애플리케이션 프로세싱 방법.

청구항 34.

제 33 항에 있어서,

상기 애플리케이션이 상기 전송 과정에서 변형되었는지 여부를 결정하는 단계를 더 포함하고,

상기 애플리케이션이 상기 전송 과정에서 변형된 것으로 결정되면, 상기 애플리케이션을 상기 무선 장치로부터 제거하는, 애플리케이션 프로세싱 방법.

청구항 35.
삭제

청구항 36.
삭제

청구항 37.
삭제

청구항 38.
삭제

청구항 39.
삭제

청구항 40.
삭제

청구항 41.
삭제

청구항 42.
삭제

청구항 43.
삭제

청구항 44.
삭제

청구항 45.
삭제

청구항 46.
삭제

청구항 47.
삭제

청구항 48.
삭제

청구항 49.
삭제

청구항 50.
삭제

청구항 51.

무선 네트워크를 통해 통신하고 애플리케이션을 실행할 수 있는 무선 장치로서,

상기 애플리케이션, 허가 세트, 및 식별 정보를 수신하는 무선 인터페이스; 및

상기 무선 인터페이스에 접속되는 컴퓨터 플랫폼으로서, 미리 규정된 규칙을 저장하는 제 1 저장 장치와 상기 애플리케이션, 상기 허가 세트, 및 상기 식별 정보를 저장하는 제 2 저장 장치를 포함하는, 컴퓨터 플랫폼을 포함하고,

상기 컴퓨터 플랫폼은,

상기 허가 세트에 대하여, 상기 규칙을 평가하는 것에 기초하여, 상기 애플리케이션 실행 가능 여부를 결정하고,

상기 애플리케이션 실행이 가능하다면, 상기 애플리케이션을 실행하고,

상기 애플리케이션 실행이 가능하지 않다면, 상기 무선 장치로부터 상기 애플리케이션을 제거하도록 구성되며,

상기 애플리케이션은 상기 무선 장치와 상기 무선 네트워크 사이의 무선 통신을 수행하는 임의의 동작과도 독립적인, 무선 장치.

청구항 52.

무선 네트워크를 통해 통신하고 애플리케이션을 실행할 수 있는 무선 장치로서,

상기 애플리케이션, 허가 세트, 및 식별 정보를 수신하는 무선 인터페이스 수단; 및

상기 무선 인터페이스 수단에 접속되는 컴퓨터 플랫폼 수단을 포함하고,

상기 컴퓨터 플랫폼 수단은,

미리 규정된 규칙을 저장하는 제 1 저장 장치 수단;

상기 애플리케이션, 상기 허가 세트, 및 상기 식별 정보를 저장하는 제 2 저장 장치 수단; 및

상기 허가 세트에 대하여, 상기 규칙을 평가하는 것에 기초하여, 상기 애플리케이션 실행 가능 여부를 결정하는 수단으로서, 상기 애플리케이션 실행이 가능하다면, 상기 애플리케이션을 실행하고, 상기 애플리케이션 실행이 가능하지 않다면, 상기 무선 장치로부터 상기 애플리케이션을 제거하는, 수단을 포함하고,

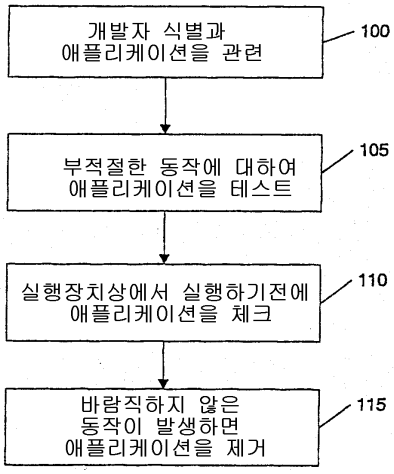
상기 애플리케이션은 상기 무선 장치와 상기 무선 네트워크 사이의 무선 통신을 수행하는 임의의 동작과도 독립적인, 무선 장치.

청구항 53.

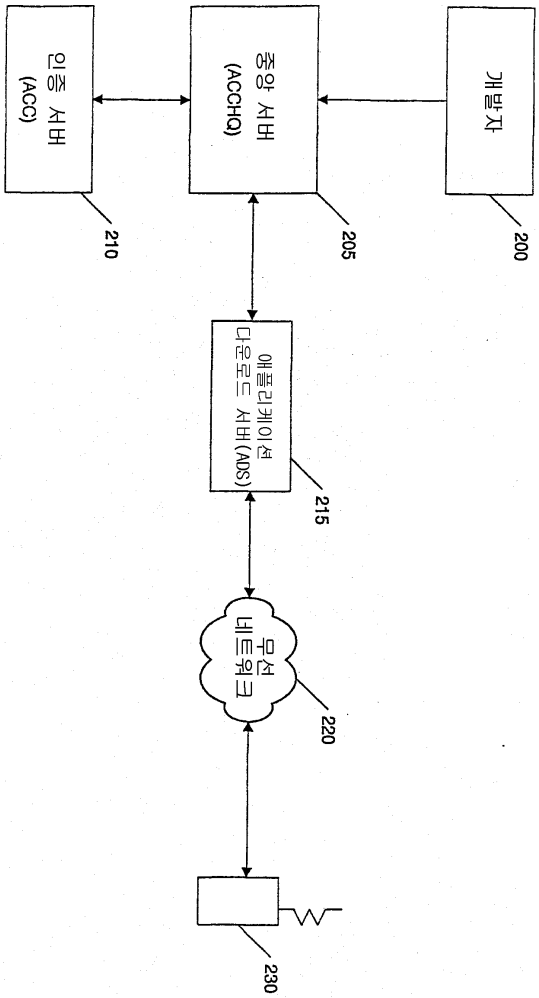
삭제

도면

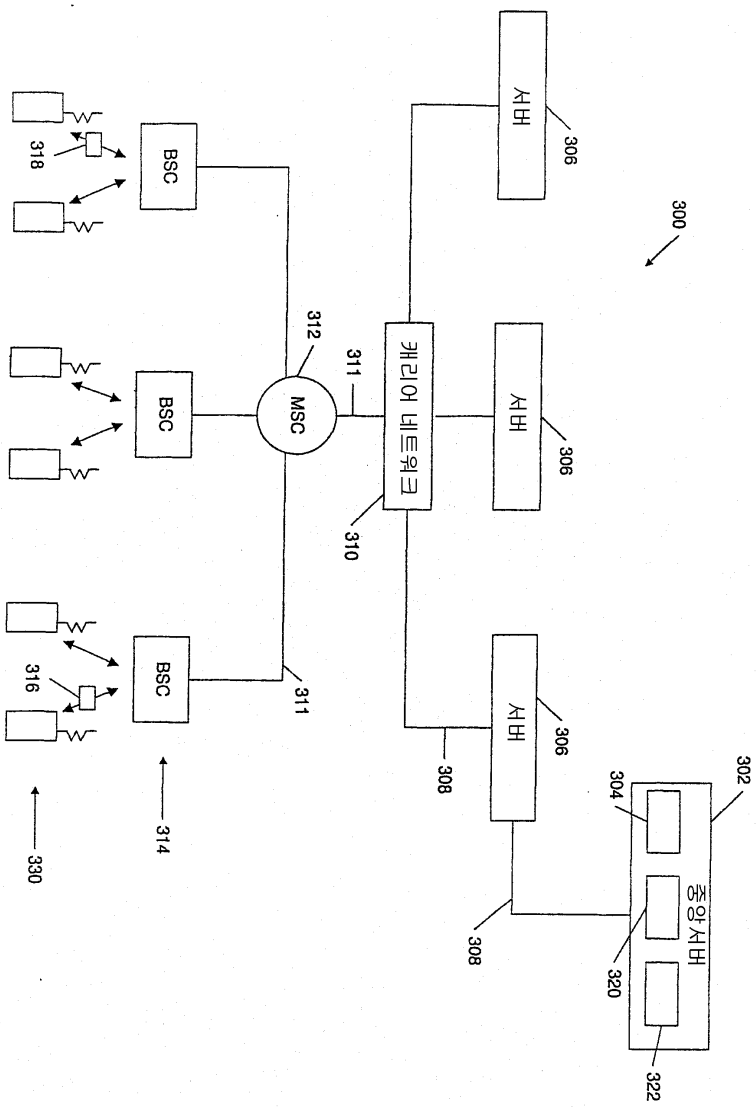
도면1



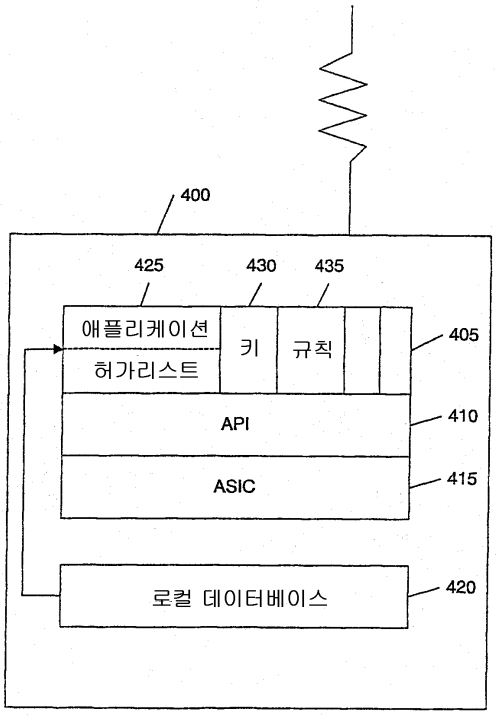
도면2


인증 서버
(ACC)
210
중앙 서버
(ACCHQ)
205
개발자
200
애플리케이션
다운로드 서버 (ADS)
215
무선
네트워크
220
230

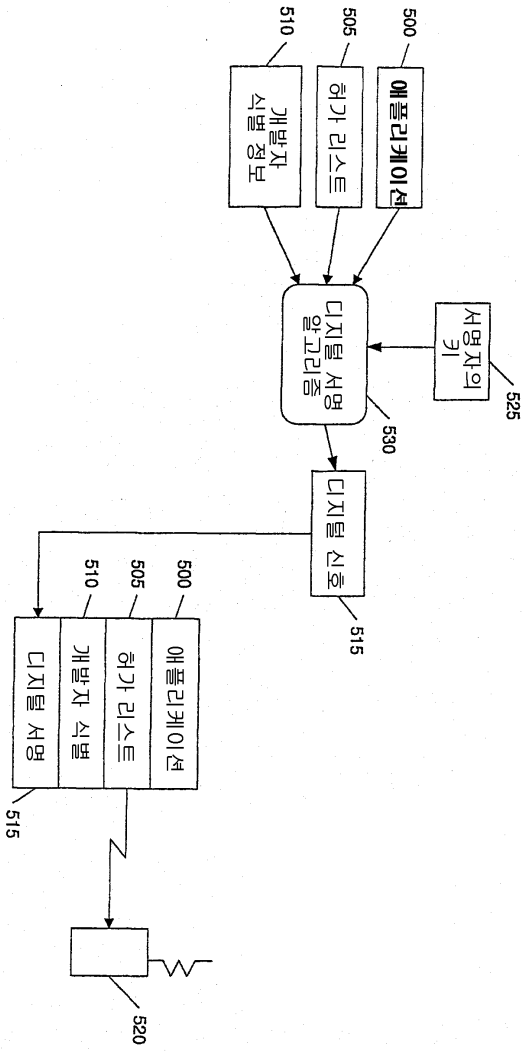
도면3


서버
306
300
BSC
318
312
311
MSC
캐리어 네트워크
310
BSC
316
311
308
304
302
중앙서버
320
322
314
330

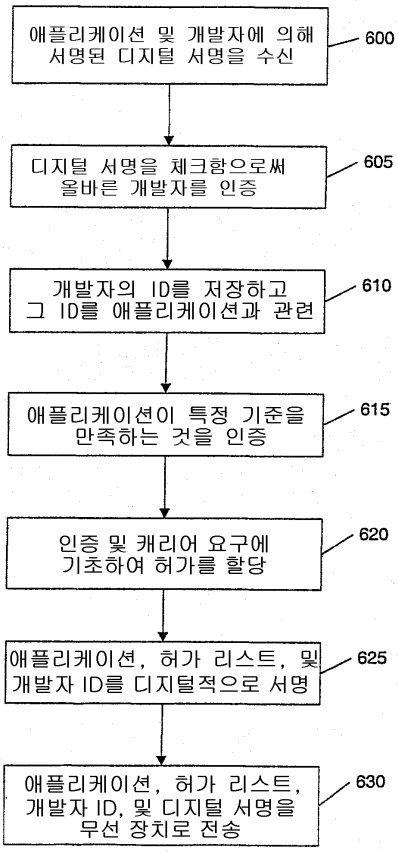
도면4


400
425
430
435
애플리케이션
허가리스트
키
규칙
405
API
410
ASIC
415
로컬 데이터베이스
420

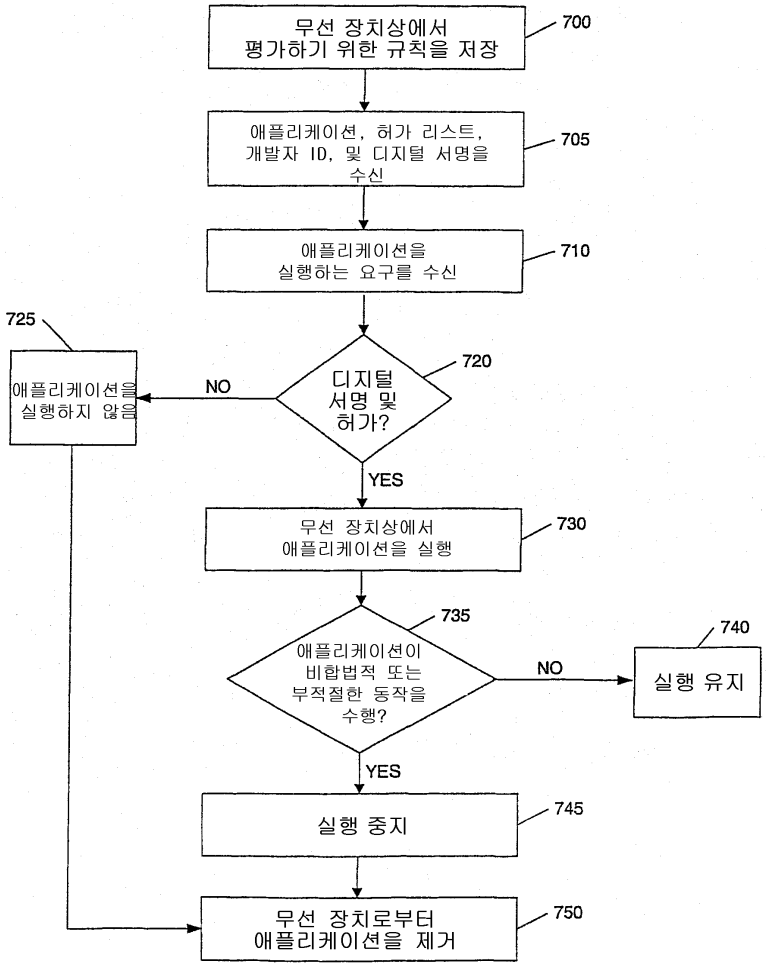
도면5


500
505
510
애플리케이션
허가 리스트
개발자 식별 정보
디지털 서명 알고리즘
서명자의 키
525
530
디지털 신호
515
500
505
510
애플리케이션
허가 리스트
개발자 식별
디지털 서명
515
520

도면6


애플리케이션 및 개발자에 의해 서명된 디지털 서명을 수신
600
디지털 서명을 체크함으로써 올바른 개발자를 인증
605
개발자의 ID를 저장하고 그 ID를 애플리케이션과 관련
610
애플리케이션이 특정 기준을 만족하는 것을 인증
615
인증 및 캐리어 요구에 기초하여 허가를 할당
620
애플리케이션, 허가 리스트, 및 개발자 ID를 디지털적으로 서명
625
애플리케이션, 허가 리스트, 개발자 ID, 및 디지털 서명을 무선 장치로 전송
630

도면7


무선 장치상에서 평가하기 위한 규칙을 저장
700
애플리케이션, 허가 리스트, 개발자 ID, 및 디지털 서명을 수신
705
애플리케이션을 실행하는 요구를 수신
710
디지털 서명 및 허가?
720
NO
725
애플리케이션을 실행하지 않음
YES
무선 장치상에서 애플리케이션을 실행
730
애플리케이션이 비합법적 또는 부적절한 동작을 수행?
735
NO
740
실행 유지
YES
실행 중지
745
무선 장치로부터 애플리케이션을 제거
750