(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0123091
(43) 공개일자 2018년11월14일

(51) 국제특허분류(Int. Cl.)
H04W 12/02 (2009.01) *H04W 12/04* (2009.01)
H04W 64/00 (2009.01)
(52) CPC특허분류
H04W 12/02 (2013.01)
H04W 12/04 (2013.01)
(21) 출원번호 10-2018-7029207
(22) 출원일자(국제) 2017년04월14일
심사청구일자 2018년10월10일
(85) 번역문제출일자 2018년10월10일
(86) 국제출원번호 PCT/US2017/027792
(87) 국제공개번호 WO 2017/181132
국제공개일자 2017년10월19일
(30) 우선권주장
62/322,780 2016년04월14일 미국(US)
62/420,360 2016년11월10일 미국(US)

(71) 출원인
애플 인크.
미국 캘리포니아 (우편번호 95014) 쿠퍼티노 원 애플 파크 웨이
(72) 발명자
호크, 제롤드 브이.
미국 95014 캘리포니아주 쿠퍼티노 메일 스탑 111-에이치오엠 애플 파크 웨이 1
마르퀘즈, 알레잔드로 제이.
미국 95014 캘리포니아주 쿠퍼티노 메일 스탑 35-3엠피 애플 파크 웨이 1
(뒷면에 계속)
(74) 대리인
장덕순, 백만기

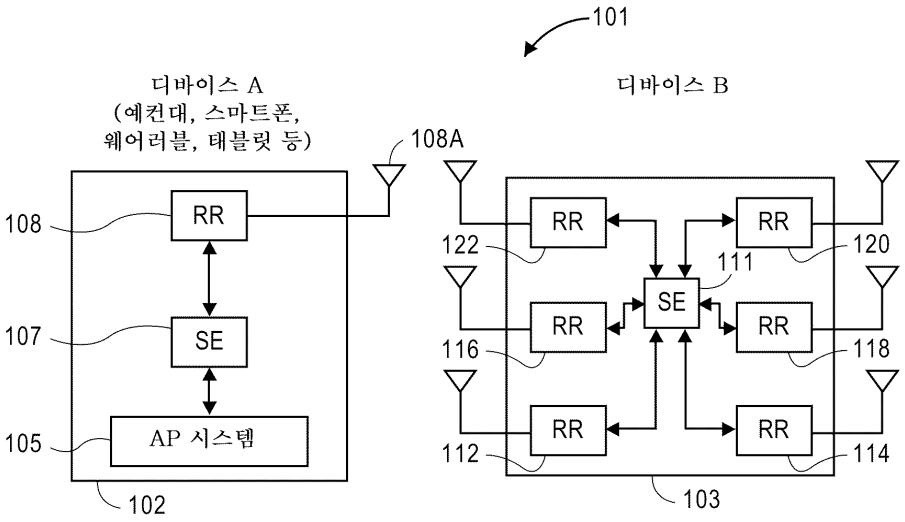
전체 청구항 수 : 총 30 항

(54) 발명의 명칭 **보안 레인징을 위한 방법 및 아키텍처**

(57) 요 약

보안 레인징 시스템은 보안 프로세싱 시스템을 사용하여, 하나 이상의 레인징 키들을 디바이스 상의 레인징 무선통신장치로 전달할 수 있고, 레인징 무선통신장치는 시스템에서 국부적으로 레인징 키들에 기초하여 레인징 코드들을 유도할 수 있다. 결정론적 난수 생성기는 레인징 키 및 하나 이상의 세션 파라미터들을 사용하여 레인징 코드들을 유도할 수 있고, 각각의 디바이스(예컨대, 셀룰러 전화기 및 다른 디바이스)는 독립적으로 레인징 코드들을 유도하고 그들을 레인징 동작들에서의 그들의 사용과 동시에 유도할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04W 64/00 (2013.01)
(72) 발명자
파아스케, 티모시 알.
미국 95014 캘리포니아주 쿠퍼티노 메일 스탑 23-3에스오씨 애플 파크 웨이 1
센, 인드란일 에스.
미국 95014 캘리포니아주 쿠퍼티노 메일 스탑 35-1엠피 애플 파크 웨이 1
시버트, 에르브
미국 95014 캘리포니아주 쿠퍼티노 메일 스탑 76-6아이오에스 애플 파크 웨이 1
시에라, 얀니크 엘.
미국 95014 캘리포니아주 쿠퍼티노 메일 스탑 302-2에스큐 애플 파크 웨이 1
티아라, 라만 에스.
미국 95014 캘리포니아주 쿠퍼티노 메일 스탑 35-4알에프디 애플 파크 웨이 1

명 세 서

청구범위

청구항 1

데이터 프로세싱 시스템으로서,

국부적으로 생성된 유사랜덤 레인징 코드(ranging code)를 송신하고 수신된 레인징 코드와의 상관을 위해 국부적으로 생성된 코드 시퀀스를 사용하여 상기 데이터 프로세싱 시스템과 다른 시스템 사이의 레인지(range)를 결정하도록 구성된 제1 무선 송수신기;

하나 이상의 사용자 애플리케이션들을 프로세싱하도록 구성된 애플리케이션 프로세싱 시스템; 및

하나 이상의 하드웨어 버스들을 통해 상기 제1 무선 송수신기에 커플링되고 상기 애플리케이션 프로세싱 시스템에 커플링된 보안 프로세싱 시스템 - 상기 보안 프로세싱 시스템은, 상기 제1 무선 송수신기와 상기 보안 프로세싱 시스템 사이의 암호화된 통신 채널을 확립하여, 상기 암호화된 통신 채널을 통해 상기 제1 무선 송수신기에 레인징 키(ranging key)들을 제공하여 상기 제1 무선 송수신기가 상기 국부적으로 생성된 유사랜덤 레인징 코드를 생성하게 하도록 구성됨 -을 포함하는, 시스템.

청구항 2

제1항에 있어서, 상기 제1 무선 송수신기는 넓은 대역폭의 무선 주파수 송수신기이고, 상기 데이터 프로세싱 시스템은 셀룰러 송수신기를 포함하는, 시스템.

청구항 3

제2항에 있어서,

상기 애플리케이션 프로세싱 시스템 및 상기 보안 프로세싱 시스템에 커플링되고, 상기 다른 시스템과 상기 데이터 프로세싱 시스템 사이의 네트워크 통신들을 제공하도록 구성된 제2 무선 송수신기를 추가로 포함하고,

상기 데이터 프로세싱 시스템은 셀룰러 전화기 또는 웨어러블 디바이스인데, 이는 상기 셀룰러 전화기 또는 웨어러블 디바이스와 상기 다른 시스템 사이의 보안 레인징 동작 이후에 암호 동작들을 수행하고, 상기 암호 동작들은 상기 다른 시스템을 잠금해제하거나 또는 상기 셀룰러 전화기 또는 웨어러블 디바이스와 상기 다른 시스템 사이의 데이터 교환을 야기하고, 상기 데이터 교환은 아이덴티티(identity), 선호도들, 목적지, 또는 상기 데이터 프로세싱 시스템의 사용자와 연관된 연락처 정보(contact information) 중 하나 이상을 포함하는, 시스템.

청구항 4

데이터 프로세싱 시스템으로서,

보안 프로세서 및 보안 프로세서 펌웨어, 보안 부트(secure boot) 판독 전용 메모리(ROM) 및 암호 가속기 및 암호 시스템에서 사용하기 위한 하나 이상의 개인 키들을 저장하기 위한 보안 저장소를 포함하는 보안 프로세싱 시스템;

부트 ROM 및 하나 이상의 시스템 버스들을 포함하고, 하나 이상의 사용자 애플리케이션들 및 운영 체제를 실행하도록 구성된 애플리케이션 프로세싱 시스템;

하나 이상의 시스템 버스들에 커플링되어 상기 운영 체제 및 상기 하나 이상의 사용자 애플리케이션들을 저장하는 시스템 메모리;

상기 보안 프로세싱 시스템과 상기 애플리케이션 프로세싱 시스템을 커플링시켜서 상기 보안 프로세싱 시스템과 상기 애플리케이션 프로세싱 시스템 사이의 통신을 허용하는 하드웨어 인터페이스; 및

유사랜덤 레인징 코드들을 송신 및 수신하도록 구성되고, 상기 하드웨어 인터페이스를 통해 상기 보안 프로세싱 시스템에 커플링되어 적어도 하나의 암호화된 레인징 키를 수신하는 제1 무선 송수신기 - 상기 제1 무선 송수신기는 상기 암호화된 레인징 키를 복호화하고 상기 레인징 키를 사용하여 레인징 상관 동작들에서 사용하기 위한

유사랜덤 레인징 코드들을 생성하도록 구성됨 -를 포함하는, 시스템.

청구항 5

제4항에 있어서, 상기 암호화된 레인징 키는 상기 제1 무선 송수신기의 공개 키를 이용하여 암호화되고, 상기 제1 무선 송수신기는 상기 제1 무선 송수신기의 대응하는 개인 키를 이용하여 상기 암호화된 레인징 키를 복호화하는, 시스템.

청구항 6

제5항에 있어서, 상기 시스템은,

상기 애플리케이션 프로세싱 시스템에 커플링된 셀룰러 전화기 송수신기 - 상기 애플리케이션 프로세싱 시스템은 상기 셀룰러 전화기 송수신기와 함께 사용하기 위한 전화 및 텍스트 메시지 사용자 인터페이스를 제공함 -를 추가로 포함하는, 시스템.

청구항 7

제6항에 있어서, 상기 시스템은,

네트워크를 통해 데이터 통신을 제공하여, 상기 보안 프로세싱 시스템이 모바일 시스템 내의 다른 보안 프로세싱 시스템과 상호 인증하게 하도록 구성된 제2 무선 송수신기 - 상기 모바일 시스템은 상기 제1 무선 송수신기와 함께 보안 레인징 동작들을 수행하도록 구성된 하나 이상의 레인징 송수신기들을 포함함 -를 추가로 포함하고, 상기 데이터 프로세싱 시스템은 성공적인 보안 레인징 동작 이후에 상기 모바일 시스템을 잠금해제하는, 시스템.

청구항 8

제7항에 있어서, 상기 제2 무선 송수신기는 블루투스 호환(Bluetooth compliant) 통신 또는 WiFi 호환 통신 중 적어도 하나를 제공하고, 상기 보안 부트 ROM은 상기 보안 프로세서 펌웨어가 실행되도록 허용되기 전에 상기 펌웨어의 코드 시그니처(code signature)를 검증하고, 상기 펌웨어는 상기 보안 프로세서 상에서 실행되어 하나 이상의 암호 기능들을 제공하는, 시스템.

청구항 9

제8항에 있어서, 상기 보안 프로세서는 상기 보안 저장소의 적어도 일부분에 액세스하지 못하는, 시스템.

청구항 10

시스템에 의해 실행될 때, 상기 시스템으로 하여금 방법을 수행하게 하는 실행가능한 명령어들을 저장하는 비일시적 기계 판독가능 매체로서, 상기 방법은,

제1 무선 통신 채널을 통해 제1 디바이스 내의 제1 무선 송수신기로부터 제2 디바이스 내의 제2 무선 송수신기로 데이터를 송신하여 상기 제1 무선 송수신기와 상기 제2 무선 송수신기 사이의 보안 접속을 확립하는 단계;

제1 보안 프로세싱 시스템으로부터 제2 보안 프로세싱 시스템으로 데이터를 송신하는 단계, 및 상기 보안 접속을 통해 상기 제2 보안 프로세싱 시스템으로부터 데이터를 수신하여, 상기 제1 보안 프로세싱 시스템을 상기 제2 보안 프로세싱 시스템에 인증하고 상기 제2 보안 프로세싱 시스템을 상기 제1 프로세싱 시스템에 인증하는 단계;

상기 제1 및 제2 보안 프로세싱 시스템들이 상호 인증된 후에 상기 보안 접속을 통해, 상기 제1 보안 프로세싱 시스템으로부터 상기 제2 보안 프로세싱 시스템으로 데이터를 송신하는 단계, 및 상호 인증 이후에 상기 보안 접속을 통해, 상기 제2 보안 프로세싱 시스템으로부터 데이터를 수신하여, 보안 키 교환을 수행하여 하나 이상의 레인징 키들의 세트를 제공하는 단계; 및

상기 제1 디바이스 내의 제3 무선 송수신기에 상기 하나 이상의 레인징 키들을 제공하는 단계 - 상기 제3 무선 송수신기는 상기 제2 디바이스 내의 적어도 하나의 제4 무선 송수신기와 함께 유사랜덤 코드들을 사용하여 비행시간(time of flight) 레인징 동작들을 수행하도록 구성됨 -를 포함하는, 매체.

청구항 11

제10항에 있어서, 상기 제1 무선 통신 채널은, 상기 제3 무선 송수신기와 상기 제4 무선 송수신기 사이의 레인징 동작들에 대한 무선 통신 채널과는 상이한 블루투스 또는 WiFi 무선 통신 채널인, 매체.

청구항 12

제11항에 있어서, 상기 보안 키 교환은 하나 이상의 키 유도 함수들을 통해 상기 하나 이상의 레인징 키들을 유도하는데, 상기 하나 이상의 키 유도 함수들은, 상기 보안 접속으로부터의 하나 이상의 키들을, 상기 하나 이상의 키 유도 함수들에 대한 입력으로서 사용하는, 매체.

청구항 13

제12항에 있어서, 상기 보안 접속으로부터의 상기 하나 이상의 키들은 블루투스 키인, 매체.

청구항 14

제11항에 있어서, 상기 하나 이상의 레인징 키들은 암호화된 형태로 상기 제3 무선 송수신기에 제공되고, 상기 제3 무선 송수신기는 상기 암호화된 형태를 복호화하여 상기 하나 이상의 레인징 키들을 유도하는, 매체.

청구항 15

제14항에 있어서, 상기 방법은,

상기 제3 무선 송수신기에 하나 이상의 데이터 암호화 키들을 제공하는 단계를 추가로 포함하고, 상기 데이터 암호화 키들은 상기 제4 무선 송수신기로 전송되거나 또는 그로부터 수신된 시간 스탬프들을 암호화하는 데 사용되는, 매체.

청구항 16

제15항에 있어서, 상기 제1 무선 송수신기 및 상기 제1 보안 프로세싱 시스템은 셀룰러 전화기 또는 스마트 워치의 일부이고, 상기 제2 디바이스는 시스템의 일부이고, 상기 제1 디바이스는, 상기 제1 디바이스와 상기 제2 디바이스 사이의 성공적인 레인징 동작 이후에 상기 시스템을 잠금해제하는 셀룰러 전화기인, 매체.

청구항 17

시스템에 의해 실행될 때, 상기 시스템으로 하여금 방법을 수행하게 하는 실행가능한 명령어들을 저장하는 비일시적 기계 판독가능 매체로서, 상기 방법은,

제1 디바이스 내의 프로세싱 시스템으로부터 암호화된 레인징 키를 수신하는 단계;

상기 암호화된 레인징 키를 복호화하는 단계;

하나 이상의 세션 파라미터들을 결정하는 단계;

상기 제1 디바이스에서 국부적으로, 상기 레인징 키 및 상기 하나 이상의 세션 파라미터들로부터 코드 시퀀스를 유도하는 단계;

제2 디바이스로부터 코드 시퀀스를 수신하는 단계;

상기 유도된 코드 시퀀스와 상기 수신된 코드 시퀀스에 대한 상관 동작을 수행하여, 상기 수신된 코드 시퀀스가 상기 유도된 코드 시퀀스에 매칭되는지 여부를 결정하는 단계; 및

상기 수신된 코드 시퀀스와 상기 유도된 코드 시퀀스 사이의 상기 상관에 기초하여 상기 제1 디바이스와 상기 제2 디바이스 사이의 레인지를 결정하는 단계를 포함하는, 매체.

청구항 18

제17항에 있어서, 상기 제1 디바이스 및 상기 제2 디바이스 각각은 독립적으로 그리고 별개로, 상기 상관 동작들과 동시에 상기 유도된 코드 시퀀스를 유도하고, 상기 제1 디바이스는 셀룰러 전화기이고, 상기 제2 디바이스는 복수의 레인징 무선통신장치(ranging radio)들을 포함하는 시스템인데, 상기 레인징 무선통신장치들은 별개로 그리고 독립적으로 상관 동작들을 수행하는, 매체.

청구항 19

제18항에 있어서, 상기 유도된 코드 시퀀스는, 상기 유도된 코드 시퀀스를 사용하는 상기 상관 동작들 동안 적시에 유도되는, 매체.

청구항 20

제18항에 있어서, 성공적인 레인징 동작은 상기 셀룰러 전화기로 하여금 상기 시스템을 잠금해제하고 상기 시스템에 사용자 데이터를 제공하게 하는데, 상기 사용자 데이터는 상기 시스템에 대한 사용자 설정들 또는 연락처 정보 또는 목적지 정보 중 하나 이상을 포함하는, 매체.

청구항 21

제17항에 있어서, 상기 세션 파라미터들은, 하나 이상의 시퀀스 식별자들; 또는 하나 이상의 세션 식별자들; 또는 하나 이상의 송신기 식별자들 중 적어도 하나를 포함하는, 매체.

청구항 22

제17항에 있어서, 상기 유도된 코드 시퀀스는 결정론적 난수 생성기에 의해 유도되는데, 상기 결정론적 난수 생성기는 상기 레인징 키와 상기 하나 이상의 세션 파라미터들의 조합에 의해 생성된 시드(seed)를 입력으로서 수신하는, 매체.

청구항 23

제22항에 있어서, 상기 결정론적 난수 생성기로부터의 출력은, 프리앰블 코드 선택, 상기 출력의 사이클릭 시프트(cyclic shift), 또는 상기 출력의 극성 반전 중 적어도 하나를 수행하기 위한 하나 이상의 파라미터들을 포함하는, 매체.

청구항 24

제17항에 있어서, 상기 방법은,

상기 제1 디바이스 내의 상기 프로세싱 시스템으로부터 암호화된 데이터 키를 수신하는 단계; 및

상기 암호화된 데이터 키를 복호화하여 데이터 키를 생성하는 단계 - 상기 데이터 키는 상기 제1 디바이스와 상기 제2 디바이스 사이의 상기 레인지가 결정될 때의 레인징 동작들에서 사용되는 시간 스탬프들을 암호화 또는 복호화하는 데 사용됨 -를 추가로 포함하고, 상기 레인징 동작들은 상기 제1 디바이스와 상기 제2 디바이스 사이의 양방향 비행 시간 레인징을 포함하는, 매체.

청구항 25

제24항에 있어서, 상기 방법은,

제2 수신된 코드 시퀀스를, 알려진 국부적으로 저장된 코드 시퀀스와 상관시켜 상기 상관에 기초하여 레인지를 제공하는 단계를 추가로 포함하고, 상기 양방향 비행시간 레인징은 세션에서의 랜덤 응답 시간을 포함하는, 매체.

청구항 26

제17항에 있어서, 상기 제1 디바이스 및 상기 제2 디바이스 각각은 그의 추정된 레인지를 다른 하나의 디바이스로부터의 추정 레인지와 비교하는, 매체.

청구항 27

시스템에 의해 실행될 때, 상기 시스템으로 하여금 방법을 수행하게 하는 실행가능한 명령어들을 저장하는 비일시적 기계 판독가능 매체로서, 상기 방법은,

제1 무선 통신 채널을 통해 제1 디바이스 내의 제1 무선 송수신기로부터 제2 디바이스 내의 제2 무선 송수신기로 데이터를 송신하여 상기 제1 무선 송수신기와 상기 제2 무선 송수신기 사이의 보안 접속을 확립하는 단계;

제1 보안 프로세싱 시스템으로부터 제2 보안 프로세싱 시스템으로 데이터를 송신하는 단계, 및 상기 보안 접속

을 통해 상기 제2 보안 프로세싱 시스템으로부터 데이터를 수신하여, 상기 제1 보안 프로세싱 시스템을 상기 제2 보안 프로세싱 시스템에 인증하고 상기 제2 보안 프로세싱 시스템을 상기 제1 프로세싱 시스템에 인증하는 단계;

상기 제1 및 제2 보안 프로세싱 시스템들이 상호 인증된 후에 상기 보안 접속을 통해, 상기 제1 보안 프로세싱 시스템으로부터 상기 제2 보안 프로세싱 시스템으로 데이터를 송신하는 단계, 및 상호 인증 이후에 상기 보안 접속을 통해, 상기 제2 보안 프로세싱 시스템으로부터 데이터를 수신하여, 보안 키 교환을 수행하여 근거리 통신(near field communication) 채널에서 사용하기 위한 하나 이상의 키들의 세트를 제공하는 단계; 및

상기 제1 디바이스 내의 제3 무선 송수신기에 상기 하나 이상의 키들을 제공하는 단계 - 상기 제3 무선 송수신기는 상기 제2 디바이스 내의 적어도 하나의 제4 무선 송수신기와 함께 근거리 통신을 수행하도록 구성됨 -를 포함하는, 매체.

청구항 28

제27항에 있어서, 상기 제1 무선 통신 채널은, 상기 제3 무선 송수신기와 상기 제4 무선 송수신기 사이의 근거리 통신에 대한 무선 통신 채널과는 상이한 블루투스 또는 WiFi 무선 통신 채널인, 매체.

청구항 29

제28항에 있어서, 상기 보안 키 교환은 하나 이상의 키 유도 함수들을 통해 상기 하나 이상의 키들을 유도하는데, 상기 하나 이상의 키 유도 함수들은, 상기 보안 접속으로부터의 하나 이상의 키들을, 상기 하나 이상의 키 유도 함수들에 대한 입력으로서 사용하는, 매체.

청구항 30

제29항에 있어서, 상기 보안 접속으로부터의 상기 하나 이상의 키들은 블루투스 키인, 매체.

발명의 설명

기 술 분 야

배 경 기 술

[0001] 본 출원은 2016년 11월 10일자로 출원된 미국 가특허 출원 제62/420,360호 및 2016년 4월 14일자로 출원된 미국 가특허 출원 제62/322,780호에 관련되고 그의 이익을 주장한다.

[0002] IEEE 802.15.4a로서 알려진 IEEE 표준에 기초하는 초광대역 무선통신장치(radio)들은, 이러한 무선통신장치들 중 하나를 각각 포함하는 2개의 객체들 사이의 거리를 측정 또는 결정하는 데 사용될 수 있는 정밀한 레인징(ranging)을 제공할 수 있다. 그 표준에 따른 레인징에 관한 추가 정보는, 문헌[the article "Ranging in the IEEE 802.15.4a standard" by Zafer Sahinoglu and Sinan Gezici from Mitsubishi Electric Research Laboratories, 2006]에서 발견될 수 있다.

발명의 내용

[0003] 보안 레인징은, 독립적으로 하나 이상의 레인징 키(ranging key)들에 의해 생성되거나 또는 그로부터 유도되는 레인징 코드(ranging code)들의 사용을 통해, 디바이스들 사이, 예컨대 (1) 2개의 스마트폰들 사이 또는 (2) 스마트폰 또는 웨어러블 디바이스와 다른 디바이스 사이의 무선 통신에서 사용되어, 양쪽 디바이스들이 수신된 신호들의 비행 시간(time of flight)에 기초하여 디바이스들 사이의 거리 또는 레인지(range)를 별개로 결정하게 할 수 있다. 보안 레인징은 2개의 디바이스들의 근접성의 보증을 제공하는 것을 목표로 한다. 상호 인증과 조합되어, 그것은 무선 상호작용에 대한 중계 공격들에 대한 증가된 레벨의 보안을 제공하는 데 사용될 수 있다. 일단 상호 인증되면, 디바이스들은 그들이 서로 가까이 있다는 보장을 획득할 수 있고, 그들은 이러한 보장을 요구할 수 있는 추가 상호작용들에 참여할 수 있다. 근접성 보장은, 패스코드 또는 지문의 입력 등에 의해 통상 나타내는 사용자 동의에 더하여, 또는 그에 대한 대체물로서 사용될 수 있다. 근접성 검증에 의해 가능해지는 상호작용들의 예들은, 디바이스들의 상태와 같은 데이터를 교환하는 것 또는 정책 정보를 전송하는 것 또는

정책 정보를 수용하는 것 또는 다른 디바이스의 잠금해제 또는 커맨트들을 전송하는 것을 포함할 수 있다.

[0004] 일 실시예에서, 데이터 프로세싱 시스템은, 국부적으로 생성된 유사랜덤 레인징 코드를 송신하고 수신된 레인징 코드와의 상관을 위해 국부적으로 생성된 코드 시퀀스를 사용하여 데이터 프로세싱 시스템과 다른 시스템, 예컨대 다른 디바이스 사이의 레인지를 결정하도록 구성된 제1 무선 송수신기; 하나 이상의 사용자 애플리케이션들, 예컨대 셀룰러 전화 사용자 애플리케이션을 프로세싱하도록 구성된 애플리케이션 프로세싱 시스템; 및 하나 이상의 하드웨어 버스들을 통해 제1 무선 송수신기에 커플링되고 애플리케이션 프로세싱 시스템에 커플링된 보안 프로세싱 시스템 및/또는 보안 요소 - 보안 프로세싱 시스템은, 제1 무선 송수신기와 보안 프로세싱 시스템 사이의 암호화된 통신 채널을 확립하도록 구성되고, 제1 무선 송수신기에 하나 이상의 레인징 키들을 제공하여 제1 무선 송수신기가 국부적으로 생성된 유사랜덤 레인징 코드들을 생성하게 하도록 구성됨 -를 포함할 수 있다. 일 실시예에서, 제1 무선 송수신기는 초광대역 무선 주파수 송수신기이고, 데이터 프로세싱 시스템은 셀룰러 전화기 송수신기를 포함한다. 일 실시예에서, 시스템은, 애플리케이션 프로세싱 시스템 및 보안 프로세싱 시스템에 커플링된 제2 무선 송수신기, 예컨대 블루투스 송수신기 또는 WiFi 송수신기 또는 근거리 통신(near field communication, NFC) 송수신기 또는 다른 유형의 무선통신장치들을 추가로 포함할 수 있고, 제2 무선 송수신기는 다른 디바이스와 데이터 프로세싱 시스템 사이의 네트워크 통신들(또는 다른 유형의 통신)을 제공하도록 구성될 수 있고, 데이터 프로세싱 시스템은 셀룰러 전화기 또는 워치일 수 있는데, 이는 셀룰러 전화기와 다른 디바이스 사이의 보안 레인징 동작 이후에 다른 디바이스를 잠금해제할 수 있다.

[0005] 일 실시예에서, 각각의 디바이스 내의 보안 요소 프로세싱 시스템의 일부일 수 있는 보안 요소들은, 예를 들어, 각각의 디바이스 상의 블루투스 송수신기를 사용하여, 셋업 동작을 수행하여 보안 통신 채널을 확립하고 이어서 각각의 보안 프로세싱 요소를 상호 인증하고 이어서 보안 키 교환을 수행하여 하나 이상의 데이터 키들 및 하나 이상의 레인징 키들의 세트를 제공할 수 있는데, 하나 이상의 데이터 키들은 레인징 프로세스에서 사용되는 시간스탬핑된 정보를 암호화하는 데 사용될 수 있다. 일 실시예에서, 보안 키 교환을 통해 생성된 하나 이상의 레인징 키들은 암호화된 형태로 초광대역 무선 송수신기에 제공될 수 있는데, 초광대역 무선 송수신기는 다른 디바이스 상의 다른 초광대역 무선통신장치와 함께 유사랜덤 코드들을 사용하여 비행 시간 레인징 동작들을 수행하도록 구성된다.

[0006] 다른 실시예에서, 하나 이상의 디바이스들은 방법을 수행할 수 있는데, 본 방법은, 제1 디바이스 내의 프로세싱 시스템으로부터 암호화된 레인징 키를 수신하는 단계; 암호화된 레인징 키를 복호화하는 단계; 하나 이상의 세션 파라미터들을 결정하는 단계; 제1 디바이스에서 국부적으로, 레인징 키 및 하나 이상의 세션 파라미터들로부터 코드 시퀀스를 유도하는 단계; 제2 디바이스로부터 코드 시퀀스를 수신하는 단계; 유도된 코드 시퀀스와 수신된 코드 시퀀스에 대한 상관 동작을 수행하여, 수신된 코드 시퀀스가 유도된 코드 시퀀스에 매칭되는지 여부를 결정하는 단계; 및 수신된 코드 시퀀스와 유도된 코드 시퀀스 사이의 상관에 기초하여 제1 디바이스와 제2 디바이스 사이의 레인지를 결정하는 단계를 포함할 수 있다. 일 실시예에서, 제1 디바이스 및 제2 디바이스 각각은 독립적으로 그리고 별개로, 상관 동작들과 동시에 유도된 코드 시퀀스를 유도하고, 제1 디바이스는 셀룰러 전화기 또는 스마트폰 또는 워치일 수 있고, 제2 디바이스는 복수의 레인징 무선통신장치(ranging radio)들을 포함하는 모바일 시스템일 수 있는데, 레인징 무선통신장치들 각각은 별개로 그리고 독립적으로 상관 동작들을 수행하고 또한 유도된 코드 시퀀스를 유도한다. 일 실시예에서, 유도된 코드 시퀀스는, 유도된 코드 시퀀스를 사용하는 상관 동작들 동안 적시에 유도된다. 일 실시예에서, 성공적인 레인징 동작은 셀룰러 전화기 또는 스마트폰 또는 워치로 하여금 다른 디바이스를 잠금해제하게 하고, 다른 디바이스에 사용자 데이터를 제공할 수 있는데, 여기서 사용자 데이터는 다른 디바이스에 대한 사용자 설정들(예컨대, 사용자의 집 또는 아파트에서 어떤 조명을 켤지) 또는 연락처 또는 식별 정보 또는 목적지 정보 등 중 하나 이상을 포함할 수 있다. 일 실시예에서, 세션 파라미터들은, 하나 이상의 시퀀스 식별자들; 또는 하나 이상의 세션 식별자들; 또는 하나 이상의 송신기 식별자들 중 적어도 하나를 포함할 수 있다. 일 실시예에서, 유도된 코드 시퀀스는 결정론적 난수 생성기에 의해 유도되는데, 결정론적 난수 생성기는 레인징 키와 하나 이상의 세션 파라미터들의 조합에 의해 생성된 시드(seed)를 입력으로서 수신한다.

[0007] 본 명세서에서 기술된 방법들 및 시스템들은 데이터 프로세싱 시스템, 예컨대 하나 이상의 스마트폰들, 태블릿 컴퓨터들, 랩톱 컴퓨터들, 스마트 워치들, 웨어러블 디바이스들, 오디오 액세서리들, 다른 디바이스 내의 온보드 컴퓨터들, 및 다른 데이터 프로세싱 시스템들 및 다른 소비자 전자 디바이스들에 의해 구현될 수 있다. 본 명세서에서 기술된 방법들 및 시스템들은 또한, 하나 이상의 비일시적 기계 판독가능 매체에 저장된 실행가능한 컴퓨터 프로그램 명령어들을 실행하는 하나 이상의 데이터 프로세싱 시스템들에 의해 구현될 수 있는데, 실행가능한 컴퓨터 프로그램 명령어들은 프로그래밍 명령어들이 실행될 때 하나 이상의 데이터 프로세싱 시스템들로

하여금 본 명세서에서 기술된 하나 이상의 방법들을 수행하게 한다. 따라서, 본 명세서에서 기술된 실시예들은 방법들, 데이터 프로세싱 시스템들, 및 비일시적 기계 판독가능 매체를 포함할 수 있다.

[0008] 상기 발명의 내용은 본 발명에서의 모든 실시예들의 총망라한 목록을 포함하는 것은 아니다. 모든 시스템들 및 방법들은 위에서 요약된 다양한 태양들 및 실시예들의 모든 적합한 조합들, 및 또한 하기의 발명을 실시하기 위한 구체적인 내용에 개시된 것들로부터 실시될 수 있다.

도면의 간단한 설명

[0009] 본 발명은 첨부 도면의 도면들에서 제한이 아닌 예로서 예시되며 첨부 도면에서 유사한 도면 부호는 유사한 요소들을 나타낸다.

도 1은 2개의 디바이스들 사이의 보안 레인징을 수행하기 위한 시스템의 일례를 도시한다.

도 2는 레인징 무선통신장치 및 블루투스 무선통신장치를 각각 포함하는 2개의 디바이스들 사이의 보안 레인징을 수행하기 위한 시스템의 일례를 도시한다.

도 3은 본 명세서에서 기술된 일 실시예에 따른 방법을 예시하는 흐름도이다.

도 4는 보안 레인징을 수행하는 데 사용되는 상관 동작들과 동시에 각각의 디바이스 상에서 레인징 코드들이 독립적으로 그리고 국부적으로 생성되는 보안 레인징을 수행하기 위한 시스템의 일례를 도시한다.

도 5a는 연장된 기간에 걸쳐 레인징 키들을 생성하기 위한 일 실시예에 따른 방법을 예시하는 흐름도이다.

도 5b는 결정론적 난수 생성기와 함께 사용하기 위한 시드를 생성하기 위한 일 실시예에 따른 일례를 도시한다.

도 6a, 도 6b, 및 도 6c는 2개의 디바이스들, 예컨대 스마트폰 및 스마트폰에 의해 잠금해제되는 다른 디바이스 사이의 양방향 레인징 동작들의 3가지 예들을 도시한다.

도 7은 본 명세서에서 기술된 바와 같이 레인징 키 및 하나 이상의 세션 파라미터들에 기초하여 유도되는 국부적으로 유도된 코드 시퀀스일 수 있는 추가적인 코드 시퀀스를 포함하는 일 실시예에 따른 데이터 패킷의 일례를 도시한다.

도 8은 본 명세서에서 기술된 하나 이상의 실시예들에서 사용될 수 있는 양방향 레인징 동작을 예시하는 도면을 도시한다.

도 9는, 보안 인터페이스를 통해 함께 커플링된 보안 요소 시스템 및 애플리케이션 프로세서 시스템을 포함하는 데이터 프로세싱 시스템의 일례를 도시하는 블록도이다.

도 10은 레인징 무선통신장치와 안전하게 동작하기 위한 별개의 보안 요소 및 보안 엔클레이브 프로세싱(secure enclave processing, SEP) 시스템을 포함하는 데이터 프로세싱 시스템의 다른 예의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0010] 아래에서 논의되는 상세사항들을 참조하여 다양한 실시예들 및 태양들이 설명될 것이고, 첨부된 도면들은 다양한 실시예들을 예시할 것이다. 하기의 설명 및 도면들은 예시적이며, 제한적인 것으로 해석되어서는 안 된다. 많은 구체적인 상세사항들이 다양한 실시예들의 철저한 이해를 제공하기 위해 기술된다. 그러나, 특정 예들에서, 주지된 또는 종래의 상세사항들은 실시예들의 간결한 논의를 제공하기 위해 설명되지 않는다.

[0011] 본 명세서에서의 "하나의 실시예" 또는 "일 실시예"에 대한 언급은 그 실시예와 관련하여 기술된 특정한 특징, 구조, 또는 특성이 적어도 하나의 실시예에 포함될 수 있음을 의미한다. 본 명세서 내의 여러 곳에 나오는 문구 "일 실시예에서"는 반드시 모두 동일한 실시예를 언급하는 것은 아니다. 다음의 도면들에 도시된 프로세스들은 하드웨어(예컨대, 회로부, 전용 로직 등), 소프트웨어, 또는 이 둘의 조합을 포함하는 프로세싱 로직에 의해 수행된다. 프로세스들이 일부 순차적 동작들의 관점에서 하기에 기술되지만, 기술된 동작들 중 일부는 상이한 순서로 수행될 수 있음이 이해되어야 한다. 또한, 일부 동작들은 순차적인 대신에 동시에 수행될 수 있다.

[0012] 도 1에 도시된 시스템(101)은, 디바이스 A 및 디바이스 B로 지칭될 수 있는 2개의 디바이스들 사이의 일 실시예에서의 보안 레인징을 수행하는 데 사용될 수 있다. 디바이스 A는, 예를 들어 스마트폰, 웨어러블 디바이스(예컨대, 워치), 또는 태블릿 컴퓨터 또는 다른 데이터 프로세싱 시스템일 수 있고, 디바이스 B는 또 다른 데이터 프로세싱 시스템 또는 다른 디바이스, 예컨대 일 실시예에서 보안 프로세싱 요소를 포함하는 모바일 시스템일

수 있다. 일 실시예에서, 디바이스 B 또는 다른 디바이스는, 예를 들어 문, 집, 아파트, 작업장(shed), 게이트 또는 전동식 디바이스 또는 차량, 모바일 시스템, 자전거, 금고(safe), 안전 금고(safety deposit box), 벽장, 랩톱 컴퓨터, 데스크톱 컴퓨터, 태블릿 컴퓨터, 서버 컴퓨터 시스템, 스마트폰, 웨어러블 디바이스(예컨대, 스마트 워치), 자물쇠(padlock), 상자(chest), RFID 판독기, RFID 태그 등일 수 있다. 도 1에서 디바이스 A로서 도시된 디바이스(102)는, 보안 엔클레이브 또는 보안 요소 프로세싱 시스템(107) 및 애플리케이션 프로세싱 시스템(105) - 이들은 함께 커플링됨 -을 포함할 수 있다. 애플리케이션 프로세싱 시스템(105)은, 예를 들어 전화 또는 텍스트 메시징 애플리케이션들 또는 웹 브라우저 애플리케이션들 등과 같은 사용자 프로그램들을 실행할 수 있다. 보안 요소 프로세서(107)는, 디바이스(102) 상의 파일들을 암호화하거나 또는 복호화하는 것 또는 사용자 패스코드들 또는 사용자의 지문들 등을 수신 및 보호하는 것과 같은 다른 보안 동작들을 수행하는 것과 같은 암호 동작들을 수행할 수 있다. 디바이스(102)는 또한, 안테나(108A)에 커플링되는 레인징 무선통신장치(108)와 같은 하나 이상의 레인징 무선통신장치들을 포함할 수 있다. 레인징 무선통신장치(RR)(108)는, IEEE 802.15.4a로서 알려진 IEEE 표준을 구현하는 무선통신장치들과 유사한 초광대역 무선통신장치로서 구현될 수 있다. 레인징 무선통신장치(108)는 유사랜덤 레인징 코드들을 디바이스(103) 상의 레인징 무선통신장치들로 송신할 수 있고, 그러한 코드들의 송신들을 수신할 수 있다. 일 실시예에서, 레인징 무선통신장치(108)가 제1 코드 시퀀스를 디바이스(103) 상의 레인징 무선통신장치들 중 하나 이상의 레인징 무선통신장치들로 송신하는 양방향 레인징이 채용될 수 있고, 그러한 레인징 무선통신장치들 각각은, 다시 레인징 무선통신장치(108)로 송신되는 코드 시퀀스로 응답하는데, 레인징 무선통신장치(108)는 이어서 디바이스(103) 상의 레인징 무선통신장치들 중 하나의 레인징 무선통신장치로부터의 코드 시퀀스에 응답할 수 있다. 도 8은 2개의 레인징 무선통신장치들 사이의 양방향 레인징 동작의 일례를 도시한다. 도 1에 도시된 예에서, 디바이스(103)는 하나 이상의 레인징 무선통신장치들을 포함하는 다른 디바이스일 수 있다. 도 1에 도시된 예에서, 디바이스 A(디바이스(102)) 및 디바이스 B(디바이스(103))가, 스마트폰일 수 있는 디바이스(102)에 대해 다른 디바이스를 위치시키도록 삼각측량을 수행하게 하기 위해 다른 디바이스의 주연부 둘레에 분포된 6개의 레인징 무선통신장치들이 있다. 6개 미만의 레인징 무선통신장치들이 대안적인 실시예들에서 채용될 수 있다는 것이 이해될 것이다. 또한, 디바이스(103)가 단일 레인징 무선통신장치를 사용하지만 다른 디바이스를 가로질러 분산된 안테나들을 가질 수 있다는 것이 이해될 것인데, 여기서 레인징 무선통신장치는 6개의 레인징 무선통신장치들이 다른 디바이스 둘레에 분산된 것과 동일한 결과를 제공하기 위해 상이한 안테나들로 시분할 다중화를 수행할 수 있다. 디바이스(103) 내의 레인징 무선통신장치들 각각은 그 무선통신장치에 커플링되는 대응하는 안테나를 포함한다. 레인징 무선통신장치들(112, 114, 116, 118, 120, 122)은 하나 이상의 버스들을 통해 디바이스(103) 내의 보안 프로세싱 요소(111)(예컨대, 보안 엔클레이브 또는 보안 요소 프로세서)에 커플링된다. 보안 요소 프로세싱 시스템(111) 및 보안 요소 프로세싱(107)은 도 3에 도시된 방법 또는 도 5에 도시된 방법을 수행할 수 있다. 또한, 레인징 무선통신장치들(108, 112, 114, 116, 118, 120, 122) 각각은, 보안 요소 프로세싱 시스템(107) 및 보안 요소 프로세싱 시스템(111)에 의해 확립되는 하나 이상의 레인징 키들로부터의 레인징 코드들의 국부적 그리고 독립적인 생성을 허용하기 위하여 도 4에 도시된 형태로 구현될 수 있다.

[0013] 일 실시예에서, 제1 통신 채널은 레인징 통신 채널과는 상이한 무선 프로토콜 또는 통신 채널을 사용하여 확립될 수 있다. 예를 들어, 블루투스 무선통신장치 또는 WiFi 무선통신장치 또는 NFC 무선통신장치가 각각의 디바이스 상에서 사용되어 디바이스들 사이의 보안 접속을 확립하며 이어서 각각의 디바이스 상의 보안 요소들이 보안 키 교환을 수행하게 할 수 있는데, 보안 키 교환으로부터 레인징 키들이 유도되거나 생성될 수 있다.

[0014] 블루투스(BT) 또는 WiFi 또는 NFC 무선통신장치 또는 다른 무선 채널과 같은 무선 통신 채널은 그의 더 높은 효율을 위해 그리고 또한 그것이 이미 잘 정의된 보안 전송 프로토콜을 지원하는 바와 같이 사용될 수 있다. 이러한 채널의 확립은 이미 근접성의 힌트를 제공하지만, 중계 공격들에 취약한데, 여기서 공격자는 2개의 디바이스들 사이에서 단순한 리피터(repeater)로서 작용하고 그에 따라 디바이스들이 서로의 레인지 내에 있다고 그들이 믿게 할 수 있지만, 이것은 거짓이다. 중계 공격들에 대한 기존의 무선 프로토콜들의 이러한 취약성은 보안 레인징을 수행하기 위한 핵심 이유일 수 있다.

[0015] 보안 레인징을 준비하기 위하여, 키 재료는 보안 레인징에 의해 사용되는 것과는 상이한 무선 통신 채널을 사용하여 교환될 수 있다(그리고 그에 따라 아마도 중계 공격들에 취약함).

[0016] 디바이스들이 이러한 초기 무선 통신 채널(BT/WiFi, NFC 무선통신장치들, 다른 무선통신장치들)에 대한 서로의 레인지 내에 있을 때, 채널은 통신을 개시하는 데 사용되는데, 이는 완전 순방향 비밀성을 가능하게 하기 위해 제1 레벨의 암호화를 제공할 수 있다.

[0017] BT 또는 WiFi 또는 NFC 무선통신장치들과 같은 근본적인 기술은 사전확립된 페어링을 통해 상호 인증을 제공할

수 있다. 프라이버시의 관점에서, (버전 4.2로부터의) 저전력 블루투스(Bluetooth Low Energy)는 이미 페어링된 디바이스들 사이의 프라이버시-보존 채널 확립을 지원하여, 디바이스들이 외견상 랜덤 식별자들을 사용하게 한다.

[0018] 이러한 제1 채널을 사용하면, 양쪽 종점 디바이스(end-point device)들 상의 보안 프로세서들(예컨대, 보안 요소 프로세싱 시스템(107, 111))은, 애플리케이션 레벨에서, 각 측의 보안 프로세서에 의해 알려진 이미 교환된 정보(공유된 대칭 키 또는 각각의 공개 키)를 사용하여 상호 인증된 키 교환을 확립할 수 있다. 그러한 방식의 일례는 글로벌플랫폼(GlobalPlatform)에 의해 정의되는 보안 채널 프로토콜 11이다. 생성된 교환된 키는 K_AB에 의해 나타낸다. 교환의 결과로서, 예를 들어 공통 비밀(common secret)이 생성되고 이어서 다수의 키들을 유도하기 위해 사용되는 경우, 하나 또는 다수의 키들이 공유될 수 있다는 것에 유의한다. 이 경우에, K_AB는 모든 이러한 키들의 세트를 나타내고, 일반적으로 "키 재료"로 지칭된다.

[0019] 프라이버시 목표를 달성하고 사용자의 추적을 방지하기 위하여, 보안 프로세서들은 상대방의 인증이 성공될 때까지 어떠한 식별자 또는 링크가능한 항목도 해제하지 않을 수 있고, 이러한 식별자는 그것이 도청자에게 보이지 않도록 암호화되어야 할 것이다. 예를 들어, 보안 블루투스 채널에 의해 제공된 보안은, 인증 및 암호화 둘 모두를 제공하여, 보안 프로세서 채널이 그의 인증된 키 교환 프로토콜에 대한 추가적인 미조정(tweak)들을 부가할 필요가 없도록 할 수 있다.

[0020] 이러한 아키텍처의 중요한 특징은, 일 실시예에서, 보안을 증가시키기 위하여 통신 채널/애플리케이션 프로세서 및 보안 프로세서 채널의 키 재료를 조합하는 능력이다. 이러한 특징은 프라이버시 이점들을 제공할 수 있는데, 이는 통신 층으로부터의 완전 순방향 비밀성을 보안 프로세서들로부터의 개선된 성능 및 강한 상호 인증과 조합한다.

[0021] 따라서, 일 실시예에서, 보안 프로세서들에 의해 애플리케이션 레벨에서 교환된 키 재료 K_AB는, 추가로 사용되기 전에, 예를 들어 BT/WiFi 또는 NFC 접속 및/또는 프로토콜들의 기록(transcript)들의 다른 일부들로부터의 다른 키 재료와 조합된다. 다른 키 재료의 그러한 일례는, 2개의 디바이스들의 성공적인 블루투스 페어링의 결과로서 2개의 디바이스들에 의해 공유되는 128-비트 비밀 키인 블루투스 링크 키인데, 이는 2개의 이미 페어링된 디바이스들 사이의 추가 접속들을 위해 나중에 재사용된다. 따라서, K_AB 및 링크 키는, K_AB를 대신하는 새로운 재료를 획득하기 위하여 표준 키 유도 함수에 삽입(inject)될 수 있다. 링크 키 자체 대신에, 링크 키로부터 유도된 키, 또는 심지어, SW에 이용가능한 경우, 블루투스 세션 키 또는 이러한 후자로부터 유도된 값을 사용할 수 있다.

[0022] 이어서, 키 재료 K_AB는 하기의 사용 사례들에 대해 사용될 수 있다:

[0023] 1) 키 확인: 양쪽 당사자들은 이에 의해 그들이 동일한 키를 생성하였음을 확인하고 BT/WiFi 접속 및 상호 인증 세션들을 결부시키는데, 즉, 그들은 WiFi/BT 상에서 그들이 통신하고 있는 엔티티가 보안 프로세서가 인증되었던 동일한 엔티티라는 보증을 얻는다.

[0024] 2) 보안 레인징: 공유된 키(K_AB로 나타냄)는, 레인징 무선통신장치에서 사용하기 위한 프리앰블들 또는 레인징 코드들과 같은 예측 불가능한 신호들을 생성하거나, 또는 레인징 무선통신장치에서 교환된 데이터를 보호하는 데 사용될 수 있다.

[0025] 3) 데이터 전송: 보안 레인징이 수행되기 전/후에, 이러한 키 재료는 양쪽 당사자들 사이에서 전송되고 있는 데이터의 무결성 및 기밀성을 보호하는 데 사용될 수 있다.

[0026] 4) 장기 사전공유된 비밀 확립: 일 실시예에서, 보안 프로세서들 사이의 상호 인증된 키 교환을 통해 생성된 공유된 키 K_AB는 장기 비밀 MK_AB로서 유지되고 보안 프로세서들 경계 내에(예컨대, 도 9에 도시된 보안 요소 시스템(903) 내에) 보유된다. 이어서, 그것은 보안 프로세서들 사이의 다른 유형의 상호 인증된 키 교환 프로토콜에서 추가 반복 동안 사용된다. 목표는, 일 실시예에서, 예를 들어 보안 채널 프로토콜 11(SCP11)과 같은 완전한(full-fledged) 비대칭 키 기반 프로토콜을 한 번만 사용하거나, 또는 수천 시간마다 한 번 사용하고, 이어서 SCP11을, 보안 채널 프로토콜 3(SCP03)과 같은 사전공유된 대칭 키들에 기초하는 더 단순한 프로토콜로 대체하는 것인데, 여기서 각각의 당사자는 랜덤 챌린지(random challenge)를 내보내고 공유된 세션 키는 사전공유된 키 및 양쪽 챌린지들의 연접(concatenation)으로부터 유도된다. 도 5는 이러한 2개의 상이한 프로토콜들을 사용하는 방법의 일례를 도시한다.

[0027] 일 실시예에서, 키 재료 K_AB는 사용 사례들 1, 2 및 3에 대해 있는 그대로 사용되지 않지만, 대신에, 사용 사례 각각에 대해, K_AB는 이러한 사용 사례 및 이러한 세션에 대해서만 전용되는 특정 세션 키 재료로 유도된다.

예를 들어, 보안 레인징에 대해 K_AB를 사용하는 대신에, K_AB는 2개의 디바이스들에 의해 교환되는 파라미터들을 사용하여 K_AB_R에 의해 나타낸 키 재료로 유도되어 보안 레인징에 대해서만 사용된다. 유도 함수는, 예를 들어 X9.63 키 유도 함수일 수 있다.

[0028] 일 실시예에서, 사용 사례 3에 대해 사용되는 키 재료는 일단 보안 레인징 동작이 완료되었다면 근접성의 보증 이전 및 이후의 데이터 교환 사이의 명백한 분리를 이루기 위해 수정될 수 있다.

[0029] 도 2는, 디바이스(201) 상의 레인징 무선통신장치(211) 및 디바이스(202) 상의 레인징 무선통신장치들(221, 223)과 같은 양쪽 레인징 무선통신장치들을 통해 통신할 수 있는 디바이스(201) 및 디바이스(202)를 포함하는 레인징 시스템(200)의 일례를 도시한다. 추가로, 도 2에 도시된 시스템(200) 내의 각각의 디바이스는, 예를 들어 디바이스(201) 내의 블루투스 무선통신장치(205) 및 디바이스(202) 내의 블루투스 무선통신장치(217)와 같은, 블루투스 무선통신장치를 포함한다. 각각의 블루투스 무선통신장치는 안테나를 포함하는데, 안테나는 블루투스 무선통신장치에 커플링되어 무선통신장치들이 2개의 블루투스 무선통신장치들 사이에서 신호들을 송신 및 수신하게 한다. 일 실시예에서, 블루투스 무선통신장치는, 보안 요소 프로세서들(207, 219)에 의해 사용하기 위한 보안 접속을 확립하여 본 명세서에서 기술된 바와 같은 하나 이상의 레인징 키들을 확립하는 데 사용될 수 있다. 대안적인 실시예에서, WiFi 또는 NFC 무선통신장치와 같은 다른 무선통신장치가 블루투스 무선통신장치에 대한 대안으로서 사용될 수 있다. 각각의 디바이스 상의 애플리케이션 프로세싱 시스템(203) 및 애플리케이션 프로세싱 시스템(215)은 사용자 프로그램들, 예컨대 셀룰러 전화 프로그램들 또는 내비게이션 프로그램들 또는 텍스트 메시징 프로그램들 등의 실행을 위해 제공될 수 있다. 또한, 이러한 사용자 애플리케이션 프로그램들은, 사용자가 하나의 디바이스, 예컨대 스마트폰을 셋업하여, 사용자의 포켓 또는 지갑 등 내에 스마트폰을 갖고서 다른 디바이스(예컨대, 디바이스 B)에 단지 걸어서 다가감으로써 또는 사용자가 다른 디바이스를 잠금해제하도록 구성된 웨어러블 디바이스를 착용하고 있는 동안 다른 디바이스를 잠금해제하도록 하기 위한 사용자 인터페이스들을 제공할 수 있다. 도 2에 도시된 시스템 내의 각각의 디바이스는 메모리(예컨대, 메모리들(209, 225))를 포함할 수 있는데, 메모리는 디바이스 내의 그리고 디바이스들 사이의 통신들을 인증하거나 또는 암호화하거나 또는 달리 보안하기 위해 암호 동작들에서 사용될 수 있는 암호 값들 또는 파라미터들, 예컨대 인증서들을 저장한다. 특히, 메모리(209)는 각각의 디바이스 내의 레인징 무선통신장치에 대한 인증서뿐만 아니라 디바이스(202)에 대한 인증서(인증서 B로서 도시됨)를 포함할 수 있다. 일 실시예에서, 메모리들(209, 225)은 보안 요소들(107, 111)에 의해서만 액세스가능하다. 일 실시예에서, 보안 요소 프로세싱 시스템은 보안 인터페이스를 통해 블루투스 무선통신장치 및 레인징 무선통신장치들 양쪽 모두에 커플링된다. 그러한 보안 인터페이스는 아래의 도 4에 예시되어 있다. 이러한 보안 인터페이스는 미국 캘리포니아주 쿠퍼티노 소재의 Apple Inc.에 의해 제공되는 iPhone 디바이스 내의 보안 엔클레이브 프로세서와 애플리케이션 프로세싱 시스템 사이의 보안 인터페이스와 유사할 수 있다.

[0030] 도 3은 도 2에 도시된 레인징 시스템을 사용하여 수행될 수 있는 방법을 도시한다. 추가로, 이 방법은 각각의 디바이스에서 레인징 동작들을 수행하는 데 사용되는 암호화된 코드 시퀀스(ciphered code sequence)를 국부적으로 그리고 별개로 생성하기 위하여 도 4에 도시된 각각의 디바이스 내의 아키텍처를 사용할 수 있다. 동작(301)에서, 각각의 디바이스, 예컨대 도 2에 도시된 디바이스 A 및 디바이스 B는 제1 통신 채널, 예컨대 하나 이상의 알려진 블루투스 프로토콜들을 사용하여 또는 대안적인 무선 채널(예컨대, WiFi 또는 NFC)을 사용하여 페어링되었던 2개의 디바이스들 사이의 블루투스 통신 채널을 통해 보안 접속을 확립할 수 있다. 이어서, 동작(303)에서, 각각의 디바이스 내의 보안 요소들은 동작(301)에서 확립된 보안 접속을 통해 이어서 서로를 상호 인증할 수 있다. 인증은 공유된 비밀 또는 인증서들의 사용을 통해 이루어질 수 있는데, 공유된 비밀 또는 인증서들은, 예컨대 최종 사용자들이 주어진 공유된 비밀 또는 인증서를 신뢰하는지 여부를 결정하기 위한 질의에 응답하여 최종 사용자로부터의 확인 시에 현장에서 보안 요소 내로 프로비저닝되거나 또는 제조 시에 프로비저닝된다. 그러한 확인은 "당신은 디바이스 식별 번호 XYZ…를 갖는 디바이스에 대해, 제조사 X에 의해 서명된, 인증서 B를 신뢰하는가?"와 같은 질의에 응답하여 일어날 수 있다. 2개의 요소들 또는 디바이스들 사이의 상호 인증을 수행하기 위한 본 기술 분야에 알려진 많은 프로토콜들이 있고, 이 경우에, 보안 요소들(207, 219) 또는 도 4의 보안 요소들(401, 403)은 동작(301)에서 확립된 보안 접속을 이용하여, 보안 키 교환 동작, 예컨대 도 3에 도시된 동작(305)으로 진행하기 전에 서로를 상호 인증할 수 있다는 것이 이해될 것이다. 일 실시예에서, 도 3에 도시된 동작(305)은 동작(303)과 조합하여 수행될 수 있다. 상호 인증 이후에, 보안 요소들, 예컨대 보안 요소들(207, 219) 또는 도 4에 도시된 보안 요소들(401, 403)은, 보안 접속을 통해 보안 키 교환을 수행하여, 하나 이상의 초기 형태들의 레인징 키 및 하나 이상의 연관된 데이터 키들, 예컨대 도 8에 도시된 양방향 레인징 동작과 같은 레인징 동작들에서 사용되는 시간 스탬프 정보를 암호화 및 복호화하는 데 사용될 수 있는 데이터 키들을 유도하는데, 도 8에 도시된 양방향 레인징 동작은 그러한 시간 스탬프들의 사용을

포함한다. 또한, 추가적인 보안이 선택적인 동작(307)에 의해 제공될 수 있다. 일 실시예에서, 동작(307)은 블루투스 링크 키 또는 보안 접속으로부터 유도된 다른 키를 레인징 키에 삽입하여 최종 레인징 키 및 최종 연관된 데이터 키를 생성하는 것을 포함할 수 있다. 일 실시예에서, 키 유도 함수는 동작(305)에서 유도된 초기 레인징 키 및 블루투스 링크 키를 입력들로서 취하여, 키 유도 함수에 따른 레인징 키들의 세트 또는 최종 레인징 키를 생성할 수 있다. 추가로, 연관된 데이터 키도 또한 블루투스 링크 키와 함께 삽입될 수 있다. 이어서, 동작(309)에서, 보안 요소는, 예를 들어 보안 요소 프로세싱 시스템 경계, 예컨대 도 9에 도시된 메모리(905) 내에 저장될 수 있는 레인징 무선통신장치의 공개 키를 사용하여, 최종 레인징 키 및 연관된 데이터 키를 암호화할 수 있다. 이어서, 암호화된 레인징 키 및 연관된 데이터 키는 보안 인터페이스를 통해 보안 요소로부터 하드웨어 인터페이스를 통해 하나 이상의 레인징 무선통신장치들로 송신될 수 있다. 이것은 동작(309)으로서 나타나 있고, 도 4는 각각의 디바이스 상의 각각의 레인징 무선통신장치와 보안 요소 사이의 보안 인터페이스의 일례를 도시한다. 도 9는 또한 보안 요소 시스템(903)과 레인징 무선통신장치(917) 사이의 보안 인터페이스의 사용을 도시하는데, 레인징 무선통신장치(917)는 보안 인터페이스(919)를 통해 보안 요소 시스템(903)에 커플링된다.

[0031] 도 3을 다시 참조하면, 동작(311)에서, 레인징 무선통신장치는 암호화된 레인징 키 및 암호화된 연관된 데이터 키를 수신하고, 양쪽 키들을 복호화하고, 이어서 세션 파라미터들, 예컨대 하나 이상의 세션 식별자들, 하나 이상의 시퀀스 식별자들, 및 하나 이상의 송신기 식별자들을 결정할 수 있고, 이어서 복호화된 레인징 키 및 하나 이상의 세션 파라미터들에 기초하여 레인징 무선통신장치에서 국부적으로 암호화된 코드 시퀀스를 유도할 수 있다. 이어서, 동작(313)에서, 각각의 디바이스는 암호화된 코드 시퀀스를 사용하여 그리고 또한 IEEE 표준 802.15.4a(이는 동작(311)에서 국부적으로 생성된 암호화된 코드 시퀀스를 사용하여 수행되는 레인징에 더하여 레인징을 수행하는 데 사용될 수 있음)의 일부인 레인징 프리앰블들을 사용하여 보안 레인징을 수행할 수 있다. 동작(315)에서, 각각의 디바이스 상의 각각의 보안 요소는 상관들로부터 획득된 레인지들을 비교하여, 그들이 예상한 대로이고 매칭되는 것을 검증할 수 있다. 예를 들어, 도 4에 도시된 보안 요소(401)는 제어기(423)로부터 레인지 데이터를 수신할 수 있고, 또한 보안 요소(403)(이는 제어기(455)로부터 레인지 데이터를 획득하였음)로부터 레인지 데이터를 수신할 수 있다. 이러한 레인지들이 미리결정된 허용범위 내에서 매칭되고 암호화된 코드 시퀀스들이 예상한 대로였고 매칭되는 경우, 각각의 보안 요소는, 그것이 인증되었던 다른 디바이스와 함께 레인지 동작을 안전하게 수행하였음을 결정할 수 있고, 그에 따라서 보안 접속 및 보안 레인징이 수행되었음을 검증한 후에 추가 암호 동작들 또는 데이터 교환 동작들 또는 다른 동작들(도 3에서의 동작(317) 참조)을 수행할 수 있다. 예를 들어, (동작(315) 이후의) 보안 레인징은 디바이스 B로 하여금 디바이스 B가 스스로 잠금해제하게 하는 암호 동작들을 수행하게 할 수 있고, 이어서 디바이스 B 및 스마트폰 또는 웨어러블 디바이스 양쪽 모두는 디바이스들 사이에서 데이터, 예컨대 사용자의 아이덴티티(identity), 사용자의 선호도들(예컨대, 조명을 켤지), 목적지, 새로운 또는 수정된 연락처 정보(contact information) 등을 교환할 수 있다. 다른 실시예들에서, 보안 레인징은, 컴퓨터 또는 다른 데이터 프로세싱 시스템의 잠금해제, 또는 2개의 디바이스들 사이의 성공적인 레인징 이후에 수행되는 동작으로 지정되었던 다른 동작을 수행하는 것을 초래할 수 있다.

[0032] 동작(315)에 대한 변형예들이 일부 실시예들에서 수행될 수 있다. 일 실시예에서, 레인징 무선통신장치들 중 하나 이상 내에서 상관들이 수행되고, 레인지 값만이 보안 요소들로 통신된다. 일 실시예에서, 레인징 동작들은 디바이스들 중 하나에 의해 완성될 수 있는데, 이때 결과들은 다른 디바이스로 안전하게 통신된다. 다른 실시예들은 이러한 실시예들의 다양한 조합들을 수행할 수 있다.

[0033] 실제로, 도 3에 도시된 방법은, 스마트폰 또는 다른 데이터 프로세싱 시스템(예컨대, 스마트 워치 또는 다른 웨어러블 디바이스)(디바이스 A)의 사용자가, 다른 디바이스(디바이스 B)에 걸어서 다가가고, 본 명세서에서 기술된 바와 같이 스마트폰을 인증하고 스마트폰으로 보안 레인징 동작을 수행하는 것에 응답하여 다른 디바이스가 스스로 잠금해제하게 할 수 있다. 일 실시예에서, 사용자는 다른 디바이스(디바이스 B)를 터치하지 않고서 다른 디바이스(디바이스 B)에 걸어서 다가갈 수 있고, 다른 디바이스(디바이스 B)가 스스로 잠금해제하게 할 수 있고; 다른 실시예에서, 사용자는 다른 디바이스(디바이스 B)가 잠금해제하게 하기 위하여 다른 디바이스(디바이스 B), 예컨대 집의 문 손잡이를 터치하도록 요구될 수 있다. 다른 디바이스(디바이스 B)를 잠금해제하는 것에 더하여 또는 다른 디바이스(디바이스 B)를 잠금해제하는 것에 대한 대안으로서, 전화기 또는 워치는 또한 사용자가 다른 디바이스 내의 일정 기능 또는 시스템을 턴온하거나, 다른 디바이스에서의 설정들, 또는 다른 디바이스로 수행될 수 있는 임의의 다른 동작들에 변화를 만들게 하기 위해 사용될 수 있다.

[0034] 일 실시예에서, 보안 레인징 동작(313)은, 시퀀스의 송신 측에서, 암호화된 코드 시퀀스 및 하나 이상의 암호화

된 시간 스탬프들의 송신을 포함할 수 있다. 시퀀스의 수신 측에서, 디바이스는 상관 동작과 동시에, 암호화된 코드 시퀀스를 국부적으로 유도할 것이고, 국부적으로 유도되는 암호화된 코드 시퀀스를 수신된 코드 시퀀스와 상관시켜 보안 레인징을 수행할 것이다. 이것은, 각각의 디바이스가 암호화된 코드 시퀀스의 수신과 동시에 암호화된 코드 시퀀스를 국부적으로 그리고 독립적으로 생성하는 바와 같이 도 4에서 알 수 있다. 코드 시퀀스들이 매칭되지 않는 경우, 레인징 무선통신장치는, 공격자가 시스템을 좌절시키고자 시도하고 있고, 예를 들어 다른 디바이스에 액세스하고자 시도하고 있음을 보안 요소에 알려줄 수 있다. 도 4에 도시된 시스템에서, 디바이스 A는 보안 요소(401) - 이는 보안 요소 시스템(903) 또는 보안 요소 시스템(1005)일 수 있음 -를 포함하고, 또한 보안 인터페이스(405)를 통해 보안 요소(401)에 커플링되는 레인징 무선통신장치(415)를 포함한다. 유사하게, 디바이스 B는 보안 요소(403) - 이는 보안 요소(903) 또는 보안 요소 시스템(1005)과 유사할 수 있음 -, 및 보안 인터페이스(407)를 통해 보안 요소(403)에 커플링되는 레인징 무선통신장치(417)를 포함한다. 일 실시예에서, 보안 인터페이스들(405, 407)은, 레인징 무선통신장치들과 보안 요소들 사이의 데이터 접속에 대한 향상된 보안을 제공하는 보안 인터페이스 회로들이다.

[0035] 도 4에 도시된 예에서, 보안 요소는, 셋업 프로세스(402)를 통해, 하나 이상의 레인징 키들 및 하나 이상의 연관된 데이터 키들, 예컨대 키들(409, 411)을 생성한다(여기서, 레인징 키는 K_AB_R로서 나타내고 연관된 데이터 키는 K_AB_D로서 나타낸다). 일 실시예에서, 셋업 프로세스(402)는 동작들(301 내지 309)을 사용하여 레인징 키 및 연관된 데이터 키를 암호화된 형태로 생성하고, 이어서 보안 인터페이스를 통해 암호화된 키들을 디바이스 상의 대응하는 레인징 무선통신장치로 송신할 수 있다. 예를 들어, 보안 요소(401)는 레인징 무선통신장치(415)의 공개 키를 이용하여 레인징 키 및 연관된 데이터 키를 암호화하고 그러한 암호화된 키들의 세트를 레인징 무선통신장치로 송신할 수 있으며, 이 레인징 무선통신장치는 이어서 (레인징 무선통신장치의 개인 키를 사용하여) 양쪽 키들을 복호화하고 이어서 본 명세서에서 기술된 방식으로 키들을 사용하여 암호화된 코드 시퀀스를 생성할 수 있는데, 이는 일 실시예에서 동작(311)과 동일할 수 있다.

[0036] 도 4에 도시된 예에서, 암호화된 코드 시퀀스의 생성은 각 측에서 별개로 그리고 독립적으로(즉, 디바이스 B와는 별개로 그리고 독립적으로 디바이스 A에서) 수행된다. 예를 들어, 레인징 무선통신장치 A는 암호화된 레인징 키 및 연관된 데이터 키를 수신할 것이고, 키들을 복호화할 것이다. 이어서, 레인징 키는 세션 파라미터들, 예컨대 세션 식별자 또는 시퀀스 식별자 또는 송신기 식별자 또는 그러한 세션 파라미터들의 조합으로 조합되어 시드(419)를 생성할 수 있고, 이러한 시드는 이어서 난수 생성기(421)에 대한 입력으로서 사용될 수 있다. 시드(419)는 레인징 키 및 하나 이상의 세션 파라미터들의 연접(또는 다른 조합)일 수 있다.

[0037] 다양한 실시예들에서, 난수 생성기(421)는 유사 난수 생성기(PRNG), 예컨대 결정론적 랜덤 비트 생성기(DRBG)일 수 있거나, 또는 유사 랜덤 함수(PRF) 군을 사용하여 구현될 수 있다. 그러한 실시예들에서, 난수 생성기(421)는 결정론적 방식으로 동작하여, 주어진 시드에 대해 난수들의 동일한 시퀀스를 생성하도록 구성된다. 난수들의 시퀀스는 카운터 또는 다른 증분기를 사용함으로써 생성되어, 난수 생성기(421)로 하여금 특정 시드에 기초하여, 난수들의 시퀀스를 출력들(431)로서 출력하게 할 수 있다. 그러한 출력들(431)은, 이어서, 일 실시예에서 프리앰블 코드 선택자, 사이클릭 시프터 및 극성 변경기(429)에 의해 추가로 프로세싱될 수 있는데, 이는 프리앰블 코드, 출력의 사이클릭 시프트를 선택하고, 또한 일 실시예에서 하나 이상의 비트들의 극성을 반전시킬 수 있다.

[0038] 이어서, 사이클릭 시프터(429)로부터의 출력의 결과는 상관기(425) 또는 RF 송수신기(427)에 제공될 수 있다. 레인징 무선통신장치 A가 다른 레인징 무선통신장치들로 송신하고 있을 때, 사이클릭 시프터(429)로부터의 출력은 출력(434)을 통해 RF 송수신기(427)의 송신기에 제공되어, 다른 레인징 무선통신장치들, 예컨대 레인징 무선통신장치(417)에 의한 수신을 위해 암호화된 코드 시퀀스의 송신을 허용한다. 레인징 무선통신장치(415)가 암호화된 코드 시퀀스들을 수신하고 있을 때, RF 송수신기(427) 내의 수신기는 수신된 코드 시퀀스인 출력(433)을 상관기(425)에 제공하는데, 상관기(425)는 또한 사이클릭 시프터(429)로부터의 출력(435)을 수신하여 상관기(425)에서의 종래의 상관 동작을 수행하여, 암호화된 코드 시퀀스가 출력(435) 상의 국부적으로 생성된 암호화된 코드 시퀀스에 매칭되는지 여부를 결정하고 또한 본 기술 분야에 알려져 있는 기법들을 사용하여 레인징 동작을 수행한다. 상관기(425)에 의한 상관 동작의 출력은 제어기(423)에 제공될 수 있는데, 이는 레인지 및 또한 암호화된 코드 시퀀스들이 매칭되는지(이 경우에 2개의 디바이스들은 공격받고 있지 않음) 여부 양쪽 모두를 나타낼 수 있다. 제어기(423)는 본 명세서에서 기술된 바와 같이 시드(419) 내로 조합되는 세션 파라미터들을 제공할 수 있고, 또한 보안 요소(401)와 통신하여 보안 레인징 동작이 성공적이었는지 여부를 나타낼 수 있다. 레인징 무선통신장치(417)는 레인징 무선통신장치(415)와 유사한 방식으로 작동하고, 출력들(463)을 생성하는 난수 생성기(453)와 같은 유사한 요소들을 포함하는데, 출력들(463)은 이어서 사이클릭 시프터(461)를 사용하여

시프트되고 반전되어 2개의 출력들을 제공 - 하나는 상관기(457)에 제공하고 다른 하나는 RF 송수신기(459)에 제공함 -할 수 있다. 제어기(455)는 시드(451)를 생성하기 위해 레인징 키와 함께 입력으로서 제공될 수 있는 세션 파라미터들을 제공하고 이들을 계속해서 추적할 수 있는데, 시드는 결정론적 난수 생성기(453)에 대한 입력이 된다.

[0039] 일 실시예에서, 결정론적 난수 생성기(DRNG)로부터의 특정 출력에 대한 특정 프리앰블 코드, 사이클릭 시프트 및 극성 변화를 특정하는 파라미터들이, DRNG(예컨대, 난수 생성기들(421, 453))로부터의 특정 출력의 하나 이상의 부분들 내에 포함될 수 있고, 이러한 파라미터들은 사이클릭 시프터(예컨대, 프리앰블 코드 선택자, 사이클릭 시프터 및 극성 인버터들(429, 461))에 의해 사용되어, DRNG로부터의 특정 출력의 이러한 부분들에 의해 특정되는 특정 시프트 및 반전을 수행할 수 있다.

[0040] 예를 들어, 특정 출력 내의 하나의 필드는 특정 프리앰블 코드(이는 96개 중 랜덤 하나임) 및 특정 사이클릭 시프트(이는 랜덤임)를 특정할 수 있고, 다른 필드는 특정 극성 반전(이는 랜덤임)을 특정할 수 있고, 그에 따라서 사이클릭 시프트들 및 극성 반전들은 DRNG로부터의 랜덤 출력들이 변함에 따라 변한다. 이러한 방식으로, 추가적인 가변성이 국부적으로 유도된 코드 시퀀스들 내에 삽입된다. 이것은 또한, 레인징 시스템의 각 측(즉, 디바이스 A 및 디바이스 B)이 DRNG로부터의 각각의 특정 출력에 대해 동일한 프리앰블 코드, 사이클릭 시프트 및 극성 반전을 생성할 것임을 보장한다. 레인징 시스템 내의 각 측이 일 실시예에서, 주어진 레인징 키 및 세션 파라미터들의 세트에 대해 DRNG로부터 동일한 출력들을 생성할 것임이 이해될 것이다.

[0041] 일 실시예에서, DRNG 및 시프터/인버터들(429, 461)로부터의 다수의 출력들이 조합되어 길고 비반복적인 시퀀스를 생성할 수 있는데; 다시 말해서, DRNG 및 프리앰블 코드 선택자, 사이클릭 시프터 및 극성 인버터들(429, 461)로부터의 일부 많은 수(예컨대, 512개)의 출력들은 연접되어 암호화된 코드 시퀀스를 생성할 수 있고, 그러한 암호화된 코드 시퀀스는 세션에서 시퀀스 식별자들 중 단지 하나에 대해 사용된다. 세션에서 다음 시퀀스 식별자에 대해, 512개의 출력들의 다른 세트가 생성될 수 있다. 이러한 동작들은 시퀀스를 복제하거나 예측하는 것을 매우 어렵게 한다.

[0042] 일 실시예에서, 시스템에 대한 부채널 공격(side-channel attack)들에 단련시키기 위해 다양한 기법들이 구현될 수 있다. 부채널 공격은 시스템의 물리적 구현으로부터의 정보 누설들(예컨대, 전력 소비, 전자기 누설들 등)에 기초하여 시스템의 보안을 손상시키려는 시도이고, 정보 누설을 감소시키거나 또는 누설된 정보와 비밀 정보 사이의 상관들을 제거함으로써 저항할 수 있다. 부채널 공격들에 대한 저항은 암호 프로세스들 내의 다양한 포인트들에서 구현될 수 있다. 일 실시예에서, 시스템의 전체적인 성능은, DRNG의 초기 상태의 구성에 대한 부채널 공격들에 대한 보호에 집중함으로써 개선될 수 있다. 일단 초기 상태를 생성하기 위한 프로세스가 부채널 공격들에 대해 단련되면, 암호로 보안된 DRNG가 사용될 수 있으며, 이는 DRNG 생성 페이즈 동안 부채널 대책들을 구현할 필요성을 감소 또는 제거하고, 암호 동작들의 개선된 성능을 가능하게 한다. 일 실시예에서, 부채널 저항은 파라미터들을 이용한 키 유도를 단일 단계로 집중시켜, 이러한 스테이지의 부채널 보호만을 허용함으로써 가능해질 수 있다. 일 실시예에서, 부채널 저항은 각각의 파라미터에 대한 유도를 캐스케이딩(cascading)함으로써 가능해질 수 있는데, 이는 각각의 중개 결과가 변하는 횟수를 제한한다. 예를 들어, 키 유도 함수(KDF)는 레인징 키(key) 및 파라미터들의 세트(param1, param2, param3)에 기초하여 캐스케이딩 방식으로 시드를 계산하여, 시드 = KDF(KDF(KDF(key, param1),param2),param3)로 되도록 할 수 있다. 그러한 캐스케이딩은 키 유도 함수의 부채널 보호에 대한 필요성을 감소시킬 수 있는데, 이는 공격자가 함수에 대한 더 작은 양의 입력 또는 출력을 캡처할 수 있기 때문이다.

[0043] 도 3에 도시된 방법 및 도 4에 도시된 아키텍처는, 보안 레인징 동작을 위조하려고 시도하는 공격자들을 방해하기 위하여 추가적인 랜덤 파라미터를 동작들 내로 도입하는 세션 파라미터들을 이용하여 수행될 수 있다. 각각의 디바이스 내의 제어기 또는 각각의 디바이스 내의 보안 요소는 2개의 디바이스들 사이의 보안 키 교환 또는 다른 통신들에 기초하여 세션 파라미터들을 유지 및 제어할 수 있다. 도 6a에 도시된 예에서, 별개의 세션 식별자들을 각각 갖는 2개의 별개의 세션들이 2개의 별개의 양방향 레인징 동작들로서 나타나 있다. 디바이스(600)와 디바이스(602) 사이의 제1 세션에서, 디바이스(600)로부터의 송신(601)이 디바이스(602)로 진행하고, 디바이스(602)는 다시 디바이스(600)로 송신(603)으로 응답하는데, 디바이스(600)는 이어서 시퀀스 식별자 3(송신(605)으로서 나타냄)을 통해 디바이스(602)에 응답한다. 실패 송신 또는 실패 세션의 경우에, 세션은 제2(및 상이한) 세션 식별자를 갖는 제2 세션으로서 반복될 수 있고 특정 시퀀스 식별자 번호를 각각 갖는 3개의 송신들(607, 609, 611)을 포함할 수 있다. 예를 들어, 디바이스(602)로부터 디바이스(600)로의 송신(609)은 시퀀스 식별자 2를 갖는 것으로 나타나 있으며, 이 시퀀스 식별자는 레인징 키와 함께 입력으로서 사용되어 두 값들로부터 시드를 생성할 수 있는데, 이는 이어서 결정론적 난수 생성기로부터의 출력을 생성할 수 있고, 이어서

출력 키는, 예를 들어 프리앰블 코드 선택자, 사이클릭 시프터 및 극성 변경기에 의해 추가로 프로세싱되어 암호화된 코드 시퀀스를 유도한다. 도 6b 및 도 6c는 스마트폰과 같은 단일 레인징 무선통신장치를 갖는 단일 디바이스가 모바일 시스템과 같은 다른 디바이스 상의 하나 이상의 레인징 무선통신장치들로 브로드캐스팅하는 일례를 도시한다. 도 6b에 도시된 예에서, 디바이스 A는 송신(625)에서 모바일 시스템 상의 6개의 센서들(레인징 무선통신장치들) 모두에 대한 브로캐스트들을 송신한다. 이에 응답하여, 레인징 무선통신장치들은 (RF 충돌들을 피하기 위하여) 미리결정된 순서의 시퀀스로 응답하도록 그리고 또한 각 측이 송신과 연관된 시퀀스 식별자를 아는 것을 보장하도록 구성된다. 따라서, 송신(627, 629, 631, 633, 635, 637)은 모바일 시스템 상의 상이한 레인징 무선통신장치들로부터 오고, 각각은 레인징 키와 함께 시드를 생성하기 위한 입력으로서 사용될 수 있는 연관된 상이한 시퀀스 식별자를 갖는다. 예를 들어, 레인징 키 및 시퀀스 식별자는 연접되거나 또는 달리 조합되어 시드를 생성하여서, 암호화된 코드 시퀀스가 시리즈(627 내지 637) 내의 각각의 시퀀스 또는 송신에 대해 상이하도록 할 수 있다. 송신(637) 이후에, 디바이스(621)는 시퀀스 식별자 8을 갖는 것으로 나타나 있는 송신(639)으로 응답하는데, 이 시퀀스 식별자는 다시 레인징 키와 함께 입력으로서 사용되어 시드를 생성하며, 시드는 이어서 도 4에 도시된 아키텍처에서 결정론적 난수 생성기에 대한 입력으로서 사용된다.

[0044] 도 6c는 디바이스(651)로부터의 6개의 레인징 무선통신장치들에 대한 브로드캐스트의 다른 예를 도시한다. 도 6c에 도시된 예는, 송신기 식별자가 사용되는 것 이외에는, 도 6b에 도시된 예와 유사하다. 따라서, 디바이스(652) 상의 각각의 레인징 무선통신장치는 송신기 식별자를 갖는데, 이 송신기 식별자는 레인징 키와 함께 사용되어 시드를 생성하며, 시드는 이어서 전술된 바와 같이 결정론적 난수 생성기에 대한 입력으로서 사용된다. 따라서, 송신(655 내지 665)은 동일한 시퀀스 식별자 번호를 공유하지만 상이한 송신기 식별자 번호들을 가지며, 이는 상이한 시드의 생성을 야기할 것이다. 도 5b는 레인징 키, 예컨대 키들(409)의 일부로서의 레인징 키 및 세션 파라미터들이 시드를 생성하는 시드 생성기(525)에 대한 입력으로서 제공되는 방식의 일례를 도시하는데, 시드는 이어서 결정론적 난수 생성기에 대한 입력으로서 사용된다.

[0045] 도 7은 IEEE 802.15.4a 표준에 기초하는 패킷의 일례를 도시한다. 패킷(701)은 종래의 레인징 동작들을 수행하는 데 사용될 수 있는 종래의 UWB 프리앰블(703)을 포함할 수 있다. 추가로, 패킷은, 종래의 방식으로 사용될 수 있는 프레임 시작 식별자(start of frame delimiter)(705)를 포함할 수 있다. 추가로, 패킷(701)은 또한 데이터(709) 및 물리 계층 헤더(707)를 포함할 수 있다. 일 실시예에서의 암호화된 코드 시퀀스(711)는 사이클릭 시프터(429) 및 사이클릭 시프터(461)에 의해 출력되거나 또는 도 3의 동작(311)에서 생성되는 국부적으로 생성된 암호화된 코드 시퀀스일 수 있고, 본 명세서에서 기술된 상관 동작들에서 사용되어, 암호화된 코드 시퀀스를 사용한 보안 레인징, 예컨대 동작(313)에서 수행되는 보안 레인징을 수행한다. 일 실시예에서, 도 7에 도시된 패킷(701)을 사용하여 2개의 별개의 상관 동작들이 수행될 수 있다. 특히, 레인징 동작들을 수행하기 위한 상관 동작은 UWB 프리앰블(703)을 사용하여 수행될 수 있고, 보안 레인징을 수행하기 위한 제2 상관 동작은 암호화된 코드 시퀀스(711)를 사용하여 수행될 수 있다. 일 실시예에서, 2개의 별개의 상관 동작들은 시스템의 보안을 검증하기 위해 비교될 수 있다. 일반적으로, 시스템이 안전하고 공격받고 있지 않은 경우의 레인징 동작들은 미리결정된 허용범위와 매칭해야 한다.

[0046] 도 5a는 상이한 암호 프로토콜들이 시간 경과에 따라 수행될 수 있는 방식의 일례를 도시한다. 특히, 동작(501)에서, 예를 들어 블루투스 접속을 통해 보안 접속이 확립될 수 있고, 이는 동작(301)과 유사하다. 이어서, 동작(503)에서 보안 키 교환이 수행되어, 레인징 키들을 유도하기 위한 장기 대칭 키 쌍(예컨대, MK_AB)을 유도할 수 있다. 이어서, 동작(505)에서, 초기 사용 이후에, 레인징 키들로서 사용하기 위한 세션 키들은 장기 키 - 장기 키는 미리결정된 수의 세션들 이후에 폐기될 수 있음 -를 사용하여 유도될 수 있어서, 동작(503)이 다시 수행되어 레인징 키들을 유도하기 위한 다른 장기 대칭 키 쌍을 유도하고, 이어서 동작(505)이 반복되게 한다.

[0047] 일 실시예에서, 다른 디바이스(예컨대, 디바이스 B) 내의 보안 요소가 동일한 장기 대칭 키를 사용하여 모바일 전화 디바이스 내의 보안 요소와 페어링될 수 있는 동작들이 수행될 수 있다. 이어서, 세션 키들은 장기 키들에 기초하여 확립될 수 있다. 이어서, 레인징 키는 블루투스 세션 키 또는 제1 통신 채널에 의해 확립되는 다른 키들로부터의 기여를 통해 또는 그의 기여 없이 세션 키로부터 유도될 수 있다. 장기 대칭 키를 사용하여 인증하는 것은 신속하게 수행될 수 있지만, 장기 대칭 키가 너무 많이 사용되는 경우 그 키를 노출시킬 수 있다.

[0048] 일 실시예에서, 다른 디바이스(예컨대, 디바이스 B) 및 모바일 전화 디바이스 또는 위치 내의 보안 요소는 각각 장기 비대칭 키 쌍들을 갖는다. 보안 요소들은 공개 키들을 교환함으로써 페어링될 수 있다. 세션 키는, 예를 들어, 비대칭 장기 키들과 함께 사용하기 위한 SCP11 또는 다른 보안 채널 프로토콜을 사용하여, 비대칭 장기

키들에 기초하여 직접 확립될 수 있다. 레인징 키는 BT 세션 키로부터의 기여를 통해 또는 그의 기여 없이 세션 키로부터 유도될 수 있다. 장기 비대칭 키의 사용은 장기 대칭 키의 사용에 비해 성능 결점들을 가질 수 있지만, 더 안전할 수 있다.

[0049] 일 실시예에서, 보안 요소들 사이에서 중기(mid-term) 대칭 키가 주기적으로 확립된다. 세션 키들은, 예를 들어, 대칭 키들을 이용하는 SCP03 또는 다른 보안 채널 프로토콜을 사용하여, 중기 키들에 기초하여 확립될 수 있다. 이어서, 레인징 키는 BT 세션 키로부터의 기여를 통해 또는 그의 기여 없이 세션 키로부터 유도될 수 있다. 일 실시예에서, 보안 요소들은 때때로 비대칭 키를 사용하여 동작을 수행하여 새로운 장기 대칭 키(MK_AB)를 생성할 수 있다.

[0050] 도 9는 보안 요소 및 애플리케이션 프로세서 및 하나 이상의 레인징 무선통신장치들 및 하나 이상의 다른 무선통신장치들, 예컨대 블루투스 무선통신장치를 포함하는 시스템의 일례를 도시한다. 도 9에 도시된 시스템은 일 실시예에서의 디바이스(201) 또는 도 4에 도시된 디바이스 A로서 사용될 수 있다. 게다가, 도 9에 도시된 시스템은 또한 디바이스 B에서 사용될 수 있는데, 디바이스 B는 하나 이상의 레인징 무선통신장치들을 갖는 보안 요소 시스템을 포함하고, 내비게이션 및 무선통신장치 또는 엔터테인먼트 제어기들 및 다른 기능을 디바이스 B의 사용자들에게 제공하기 위해 하나 이상의 애플리케이션 프로세서들을 포함할 수 있다. 일 실시예에서, 보안 요소 시스템(903)은 시스템 온 칩(system on chip)으로서 구현될 수 있다. 다른 실시예에서, 애플리케이션 프로세서(921) 및 보안 요소 시스템(903)은 시스템 온 칩 상에서 구현될 수 있고, 단일 집적회로 상에 하나 이상의 프로세서들 및 메모리 제어기들 및 다른 컴포넌트들을 포함한다. 도 9에 도시된 예에서, 보안 요소 시스템(903)은, 보안 요소 시스템(903) 내의 펌웨어(911)로서 저장된 소프트웨어를 실행함으로써, 사용자 파일들을 암호화하는 것 또는 코드 시그니처들을 검증하는 것 또는 사용자 패스코드들을 프로세싱하는 것 또는 다른 보안 동작들을 수행하는 것과 같은 암호 동작들을 수행할 수 있다. 펌웨어(911)는 암호 동작들 또는 기능들을 제공하기 위해 보안 요소 프로세서(915) 상에서 실행되는 실행가능한 프로그램 명령어들을 저장할 수 있다. 보안 요소 프로세서(915)는 또한 신뢰하는 소프트웨어일 수 있는 보안 요소 ROM(913)에 커플링될 수 있는데, 이 신뢰하는 소프트웨어는, 펌웨어의 코드 시그니처를 검사하고, 펌웨어가 보안 요소 프로세서(915)에 의해 실행되게 하기 전에 펌웨어가 유효하고 손상되지 않았음을 시그니처 코드가 나타내는 것을 검증함으로써, 그 펌웨어가 실행되도록 허용하기 전에 펌웨어(911) 내의 소프트웨어의 유효성을 확인할 수 있다. 보안 요소 시스템(903)은 또한, 하드웨어 가속기를 사용하는 대칭 암호 방식뿐만 아니라 비대칭 암호 방식을 수행할 수 있는 암호 가속기, 예컨대 암호 가속기(907)를 포함할 수 있다. 가속기(907)는 비휘발성인 변경불가능한 메모리(905)에 커플링될 수 있는데, 이 메모리는 디바이스 식별자 또는 디바이스 식별자들의 세트 및 하나 이상의 인증서들의 세트 및 개인 키들을 보안 방식으로 저장할 수 있으며, 이들은 일 실시예에서 시스템의 나머지로부터 숨겨져 있고 시스템의 나머지에 의해 판독가능하지 않다. 암호 가속기(907)는 개인 키들 및 메모리(905) 내의 다른 데이터에 액세스하고, 메모리(905)에 대한 액세스는 보안 요소 시스템(903) 외부의 컴포넌트들에 대해 허용되지 않는다. 메모리(905)에 대한 액세스 불가는, 보안 요소 시스템(903)이 "안전하다"고 간주될 수 있는 하나의 이유이다. 일 실시예에서, 가속기(907)는 가속기 메모리(909)에 커플링될 수 있는데, 이 메모리는 암호 가속기(907)에 의해 수행되는 암호 동작들을 수행하기 위해 사용되는 스크래치 패드 메모리일 수 있다. 시스템(901)은, 도 9에 도시된 실시예에서, 보안 인터페이스(919)를 포함하는데, 보안 인터페이스는 애플리케이션 프로세서(921)와 보안 요소 프로세서(915) 사이의 통신을 허용하는 인박스(in-box) 및 아웃박스(out-box)일 수 있다. 일 실시예에서, 하나 이상의 레인징 무선통신장치들(917)은 또한 보안 인터페이스(919)에 커플링되어 보안 프로세서(915)가 하나 이상의 레인징 무선통신장치들(917)과 통신하게 할 수 있다. 애플리케이션 프로세서(921)는 하나 이상의 버스들(923)에 커플링될 수 있는데, 버스들은 하나 이상의 입력 및 출력 디바이스들(927), 예컨대 터치스크린 디스플레이 및 블루투스 무선통신장치, 다른 무선통신장치들, 예컨대 WiFi 및 NFC 무선통신장치들 등에 커플링된다. 입력 및 출력 디바이스들(927)의 예들은 디바이스에 의존하고, 다른 입력 또는 다른 출력 디바이스들을 포함할 수 있다. 애플리케이션 프로세서(921)는 또한, 애플리케이션 프로세서를 부팅시키기 위한 소프트웨어를 제공하는 애플리케이션 프로세서 ROM 또는 판독 전용 메모리(925)에 커플링된다. 유사하게, 보안 요소 ROM(913)은 보안 요소 프로세서(915)를 부팅시키기 위한 코드를 제공한다.

[0051] 대안적인 실시예에서, 제1 디바이스(예컨대, 스마트폰 또는 워치와 같은 디바이스 A) 및 제2 디바이스(예컨대, 디바이스 B) 내의 블루투스 또는 WiFi 송수신기들 사이의 제1 무선 통신 채널이 2개의 송수신기들 사이의 보안 접속을 확립하기 위해 사용된다. 제1 무선 통신 채널이 확립되고 보안된 후에, 제1 디바이스 내의 제1 보안 프로세싱 시스템(보안 요소 프로세서) 및 제2 디바이스 내의 제2 보안 프로세싱 시스템(다른 보안 요소 프로세서)이 데이터를 교환하여 서로를 인증한다(각각의 보안 요소 프로세서가 다른 보안 요소 프로세서를 인증하는 양방향 인증). 이어서, 제1 및 제2 보안 프로세싱 시스템은 보안 키 교환을 수행하여, 제1 및 제2 디바이스들

내의 NFC 무선통신장치들 사이의 근거리 통신에서 사용하기 위한 하나 이상의 키들을 유도한다. 이 실시예에서의 NFC 무선통신장치들은 유도된 키들을 사용하여, 각각의 디바이스 내의 각각의 NFC 무선통신장치가, 다른 디바이스 내의 다른 NFC 무선통신장치가 안전하게 인증되는 것을 검증하게 하고, 그에 따라서 제1 디바이스가 제2 디바이스 상의 문을 열거나 또는 제2 디바이스에 대한 다른 동작들을 수행하게 한다. 따라서, 제1 및 제2 디바이스들 내의 NFC 무선통신장치들은, 예를 들어 도 2에서의 레인징 무선통신장치들을 대신하고, NFC 무선통신장치들은 10 또는 50 또는 100 센티미터 미만의 동작 거리를 가질 수 있어서 더 긴 레인지 사용이 불가능하도록 (그리고 그에 따라서 이러한 거리들 중 하나를 초과한 원격 공격들이 불가능하도록) 한다.

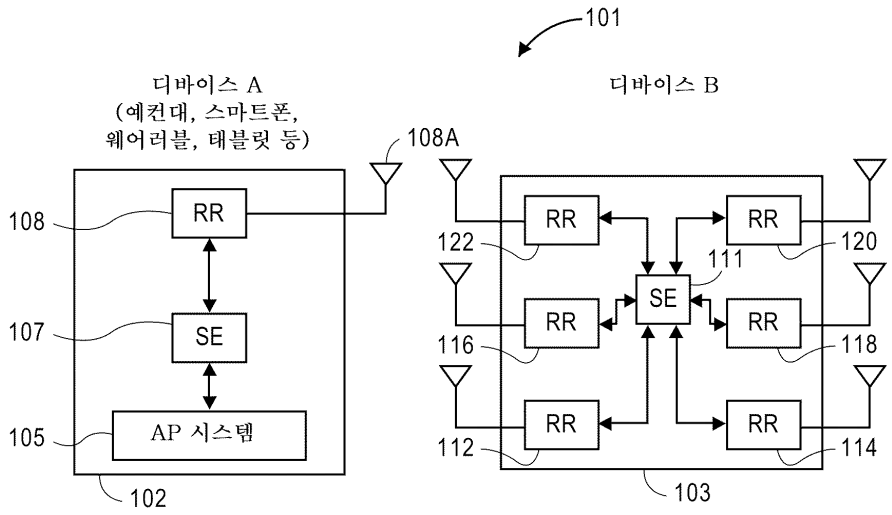
[0052] 도 10은 도 9에 도시된 시스템에 대한 대안예의 일례를 도시한다. 도 10에 도시된 시스템에서, 2개의 보안 요소들(1001, 1005), 애플리케이션 프로세서(들)(1009), 하나 이상의 레인징 무선통신장치들(1007) 및 하나 이상의 다른 무선통신장치들(예컨대, 블루투스 무선통신장치, WiFi 무선통신장치, 근거리 통신 무선통신장치, 셀룰러 전화기 무선통신장치 등)이 있다. 하나 이상의 다른 무선통신장치들은 I/O(입력/출력) 디바이스들(1012)의 일부일 수 있다. 도 10에서의 시스템은 일 실시예에서 디바이스(201) 또는 도 4에서의 디바이스 A로서 사용될 수 있다. 애플리케이션 프로세서(들)(1009)는 애플리케이션 프로세서(921)와 구조 및 기능에 있어서 유사할 수 있고, AP ROM(1014) 및 버스들(1011)은 각각 AP ROM(925) 및 버스들(923)과 구조 및 기능에 있어서 유사할 수 있다. 보안 요소 시스템(1001)은 보안 요소 시스템(903)과 구조 및 기능에 있어서 유사할 수 있고, 보안 인터페이스(1003)를 통해 애플리케이션 프로세서(들)(1009)에 커플링될 수 있는데, 보안 인터페이스는, 일 실시예에서, 인박스 및 아웃박스를 통해 암호화된 통신을 허용한다. 보안 인터페이스(1003)는 또한 보안 요소 시스템(1005)에 커플링되는데, 보안 요소 시스템은, 보안 요소 시스템(1001)이 레인징 무선통신장치(들)(1007)에 대한 보안 요소 프로세싱의 전부를 제공할 것을 요구하는 대신에, 레인징 무선통신장치(들)(1007)에 대한 보안 요소 프로세싱의 적어도 일부를 제공할 수 있다. 예를 들어, 보안 요소 시스템(1001)은 도 10에서의 시스템의 부팅 시에 코드 시그니처들을 인증할 수 있고 보안 요소 시스템(1005)을 인증할 수 있으며, 이어서 보안 요소 시스템(1001)에 의해 인증된 후에, 보안 요소 시스템(1005)은, 예를 들어 도 3에서의 동작들(303 내지 315)을 수행함으로써 레인징 무선통신장치(들)(1007)에 대한 보안 요소 프로세싱을 수행할 수 있다. 다른 실시예에서, 보안 요소 시스템(1005)은 이러한 동작들의 더 작은 서브세트를 수행할 수 있다. 이러한 동작들의 대부분에 대해 보안 요소 시스템(101) 대신에 보안 요소 시스템(1005)을 사용하는 것은, 일 실시예에서 보안 요소 시스템(1005)이 보안 요소 시스템(1001)에 의해 인증된 후에 보안 요소 시스템(1001)(및 또한 애플리케이션 프로세서(들)(1009))이 슬립 또는 저전력 상태로 유지되게 할 수 있다. 일 실시예에서, 보안 요소 시스템(1005)과 레인징 무선통신장치(들)(1007) 사이의 접속은, 보안 요소 시스템(1005)과 레인징 무선통신장치(들)(1007) 사이의 인증되고 암호화된 통신들을 사용하는 하드웨어 접속일 수 있다. 도 10에 도시된 실시예에서, 보안 요소 시스템(1001) 및 애플리케이션 프로세서(들)(1009)는 보안 인터페이스(1003)를 통해 보안 요소 시스템(1005)과 통신하고, 시스템(1001) 및 프로세서(들)(1009)는 보안 요소 시스템(1005)을 통해 레인징 무선통신장치(들)(1007)와 간접적으로 통신하고; 추가로 또는 대안으로서, 레인징 무선통신장치(들)(1007)는 접속들(1006, 1008)로서 나타낸 직접 접속들을 통해 보안 요소 시스템(1001) 및 애플리케이션 프로세서(들)(1009)와 암호화된 메시지들을 통신할 수 있다.

[0053] 보안 요소 시스템은 다른 데이터 프로세싱 시스템 내의 프로세싱 시스템일 수 있다. 예를 들어, 보안 요소 시스템은 미국 캘리포니아주 쿠퍼티노 소재의 Apple Inc.로부터의 소정의 iPhone들 내의 보안 엔클레이브 코프로세서일 수 있고; 이러한 코프로세서는 (메인 애플리케이션 프로세서의 보안 부팅과는 별개로) 그 자신의 보안 부팅 프로세스를 실행하고, 사용자 패스코드들, 지문들 등의 프로세싱에 관련된 보안 프로토콜들을 실행한다. 보안 요소 시스템들의 실시예들에 관한 추가 정보는 2016년 1월 10일자로 출원된 미국 가특허 출원 제62/276,913호 및 2015년 6월 5일자로 출원된 미국 가특허 출원 제62/171,705호에서 발견될 수 있고, 이러한 미국 가특허 출원들 둘 모두는 본 명세서에 참고로 포함된다. 보안 요소 시스템들의 실시예들은 또한 미국 특허 출원 공개 US 2014/0089682 A1호에 기술되어 있는데, 이는 또한 본 명세서에 참고로 포함된다.

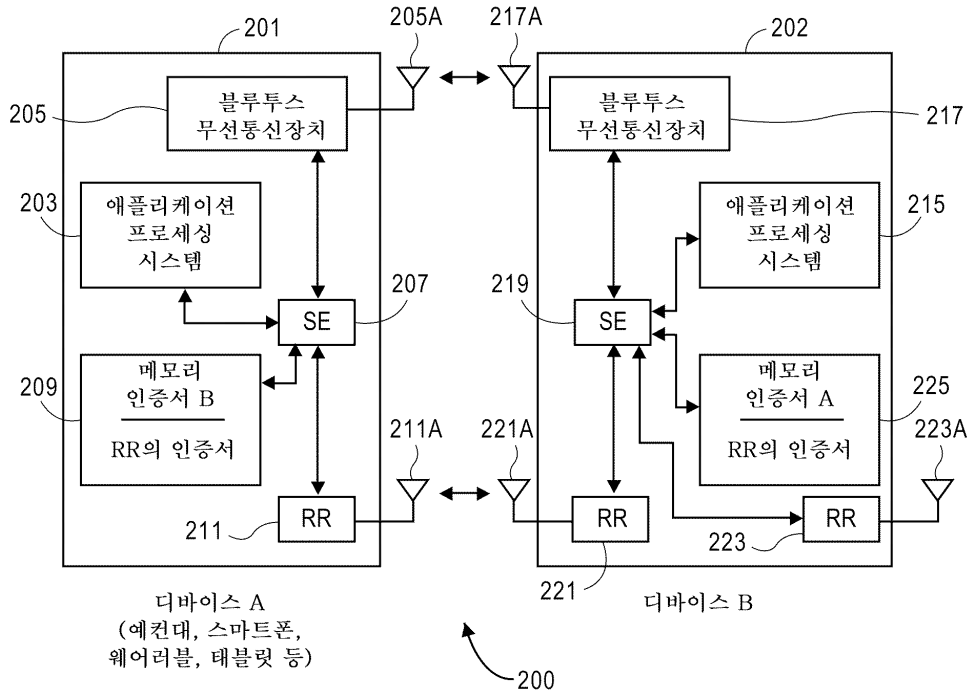
[0054] 전술한 명세서에서, 특정 예시적인 실시예들이 기술되었다. 다음의 청구범위에 기재된 바와 같은 보다 넓은 사상 및 범주로부터 벗어남이 없이 이 실시예들에 대하여 다양한 수정들이 이루어질 수 있음이 명백할 것이다. 이에 따라서, 명세서 및 도면들은 한정적 의미보다는 오히려 예시적 의미에서 고려되어야 한다.

도면

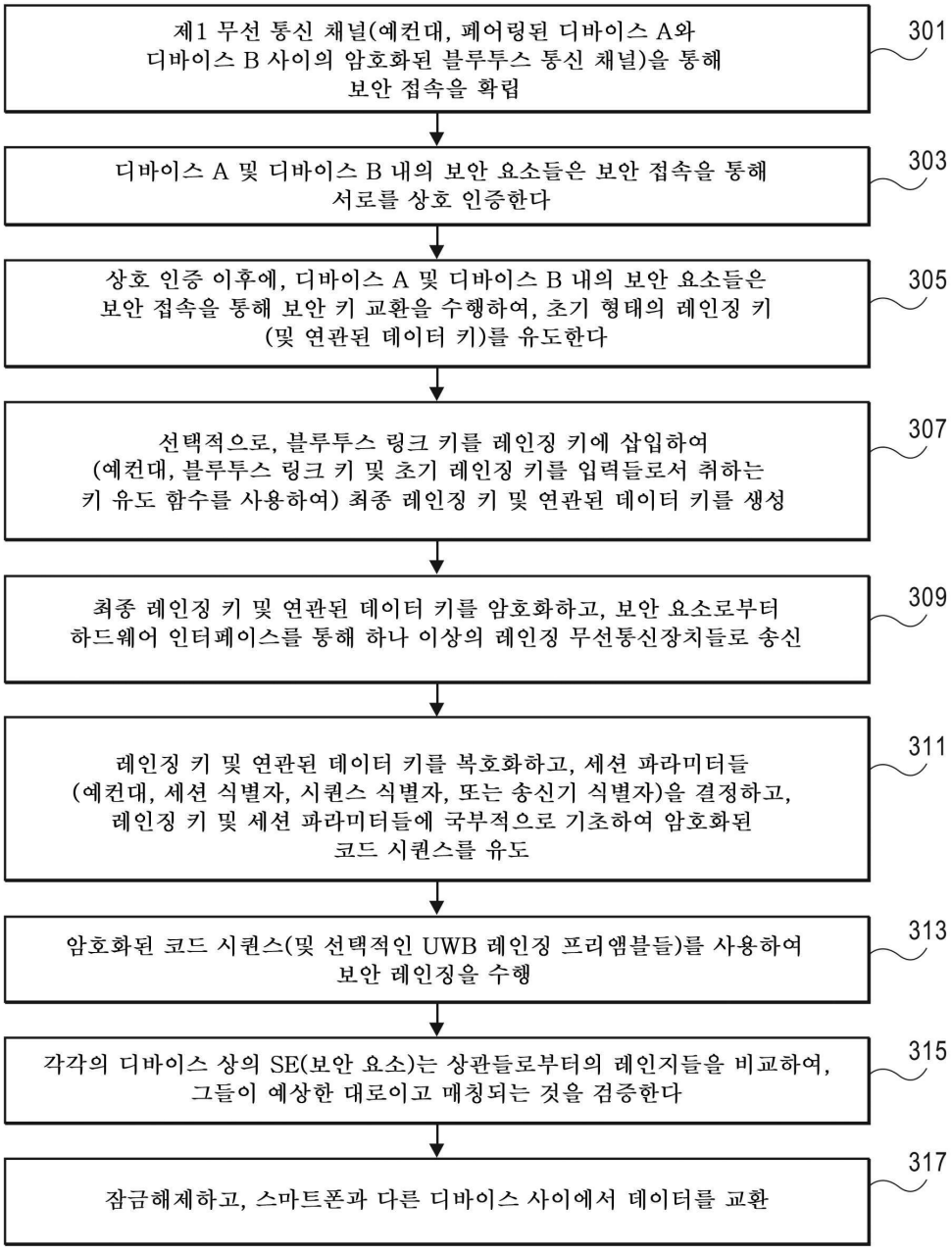
도면1


101
디바이스 A
(예컨대, 스마트폰,
웨어러블, 태블릿 등)
디바이스 B
108A
108
RR
107
SE
105
AP 시스템
102
122
120
111
116
118
112
114
103

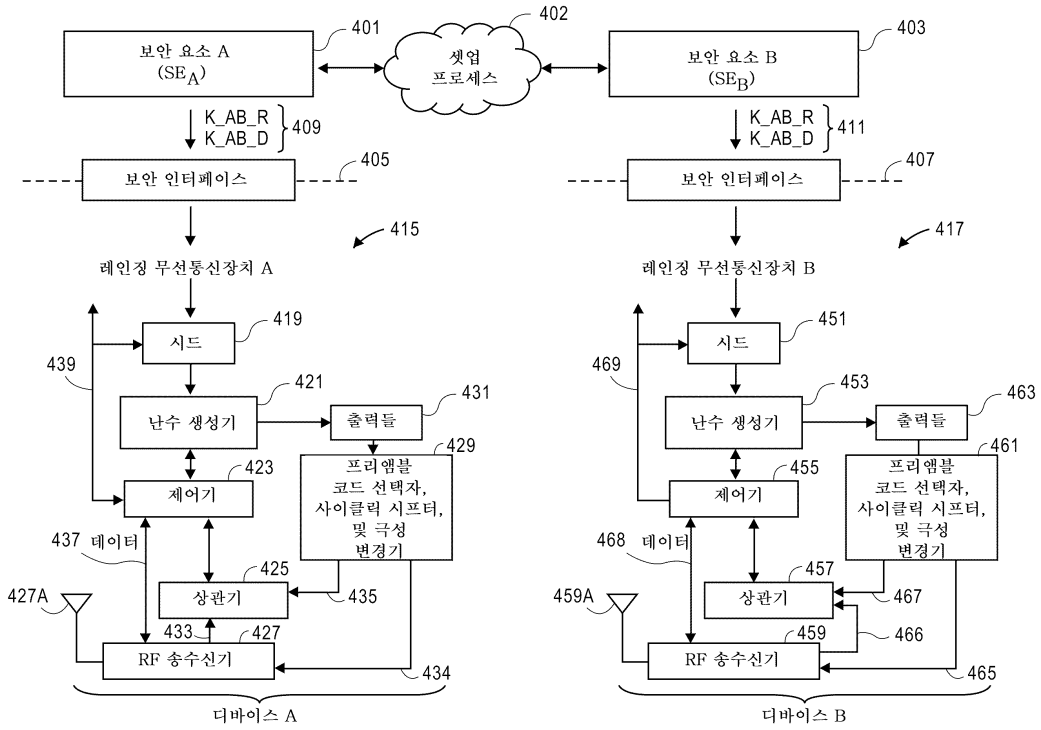
도면2


201
205A
217A
202
205
블루투스
무선통신장치
217
203
애플리케이션
프로세싱
시스템
215
207
219
SE
209
메모리
인증서 B
RR의 인증서
225
211A
221A
223A
211
RR
223
221
디바이스 A
(예컨대, 스마트폰,
웨어러블, 태블릿 등)
디바이스 B
200

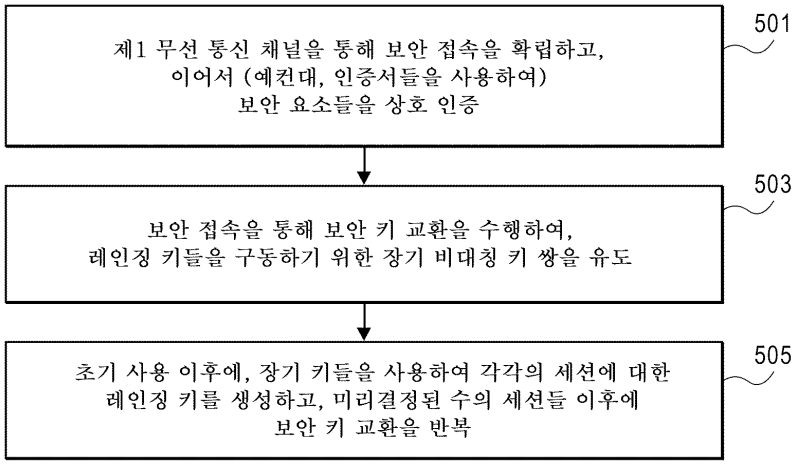
도면3


제1 무선 통신 채널(예컨대, 페어링된 디바이스 A와 디바이스 B 사이의 암호화된 블루투스 통신 채널)을 통해 보안 접속을 확립
301
디바이스 A 및 디바이스 B 내의 보안 요소들은 보안 접속을 통해 서로를 상호 인증한다
303
상호 인증 이후에, 디바이스 A 및 디바이스 B 내의 보안 요소들은 보안 접속을 통해 보안 키 교환을 수행하여, 초기 형태의 레인징 키 (및 연관된 데이터 키)를 유도한다
305
선택적으로, 블루투스 링크 키를 레인징 키에 삽입하여 (예컨대, 블루투스 링크 키 및 초기 레인징 키를 입력들로서 취하는 키 유도 함수를 사용하여) 최종 레인징 키 및 연관된 데이터 키를 생성
307
최종 레인징 키 및 연관된 데이터 키를 암호화하고, 보안 요소로부터 하드웨어 인터페이스를 통해 하나 이상의 레인징 무선통신장치들로 송신
309
레인징 키 및 연관된 데이터 키를 복호화하고, 세션 파라미터들 (예컨대, 세션 식별자, 시퀀스 식별자, 또는 송신기 식별자)을 결정하고, 레인징 키 및 세션 파라미터들에 국부적으로 기초하여 암호화된 코드 시퀀스를 유도
311
암호화된 코드 시퀀스(및 선택적인 UWB 레인징 프리앰블들)를 사용하여 보안 레인징을 수행
313
각각의 디바이스 상의 SE(보안 요소)는 상관들로부터의 레인지들을 비교하여, 그들이 예상한 대로이고 매칭되는 것을 검증한다
315
잠금해제하고, 스마트폰과 다른 디바이스 사이에서 데이터를 교환
317

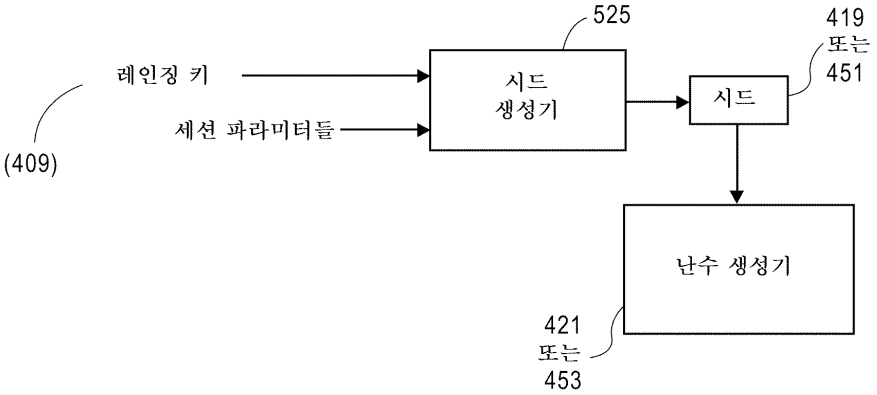
도면4



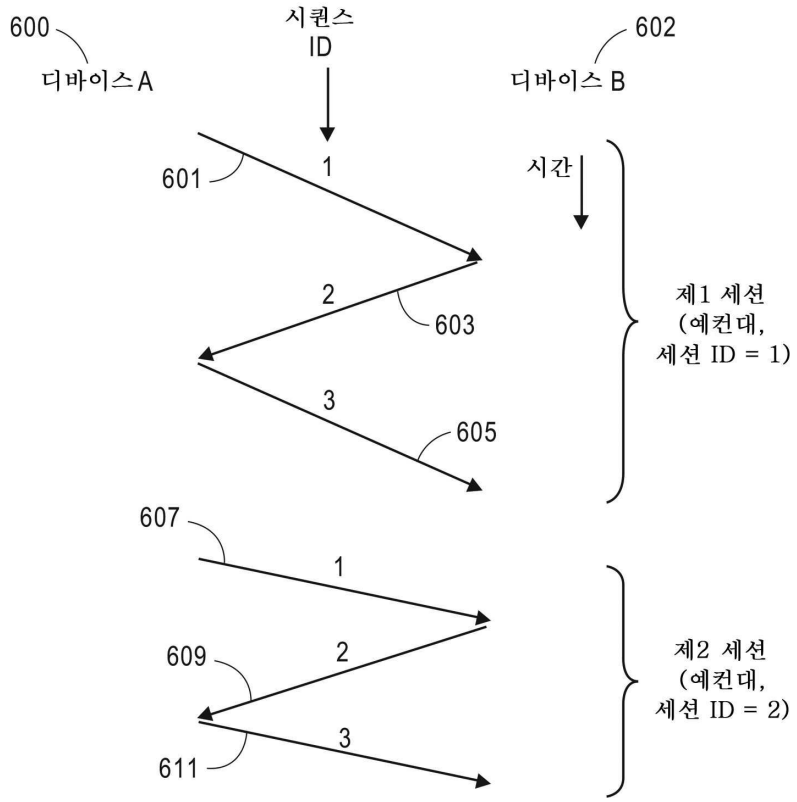
도면5a



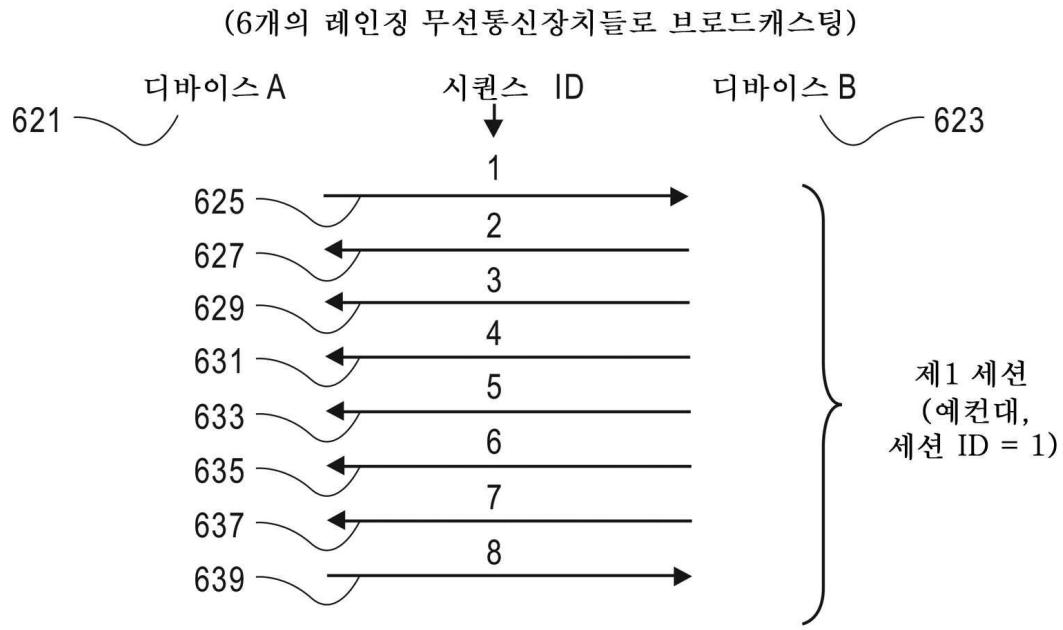
도면5b



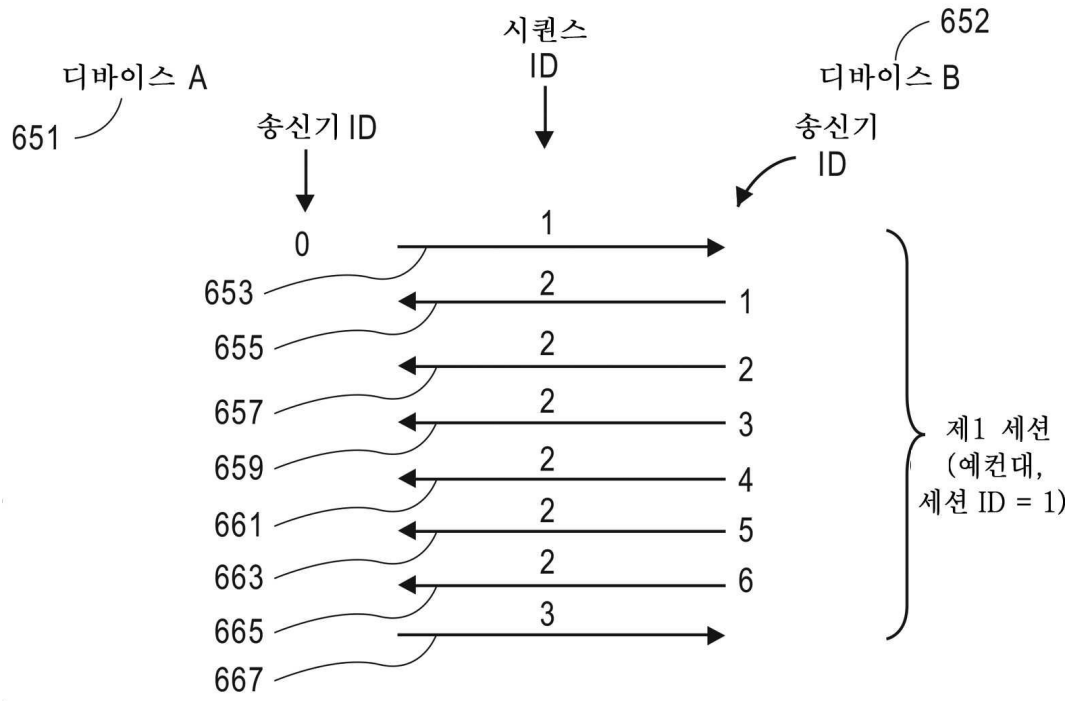
도면6a


600
디바이스 A
시퀀스 ID
602
디바이스 B
601
1
시간
2
603
제1 세션
(예컨대,
세션 ID = 1)
3
605
607
1
609
2
제2 세션
(예컨대,
세션 ID = 2)
3
611

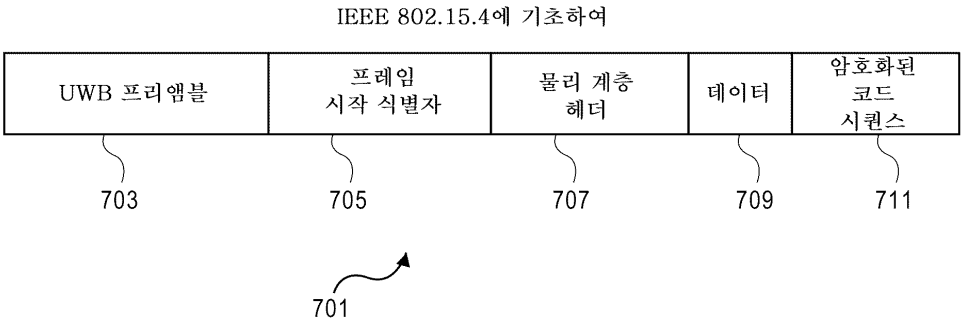
도면6b


(6개의 레인징 무선통신장치들로 브로드캐스팅)
디바이스 A
621
시퀀스 ID
디바이스 B
623
1
625
2
627
3
629
4
631
5
633
6
635
7
637
8
639
제1 세션
(예컨대,
세션 ID = 1)

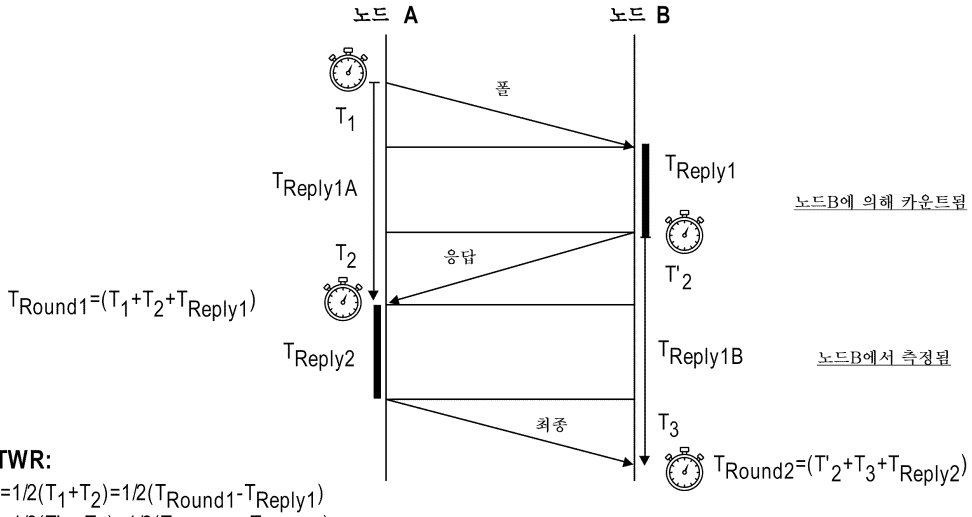
도면6c


디바이스 A
651
송신기 ID
시퀀스 ID
디바이스 B
652
송신기 ID
0
653
655
657
659
661
663
665
667
1
2
2
2
2
2
2
3
1
2
3
4
5
6
제1 세션
(예컨대,
세션 ID = 1)

도면7


IEEE 802.15.4에 기초하여
UWB 프리앰블
프레임 시작 식별자
물리 계층 헤더
데이터
암호화된 코드 시퀀스
703
705
707
709
711
701

도면8



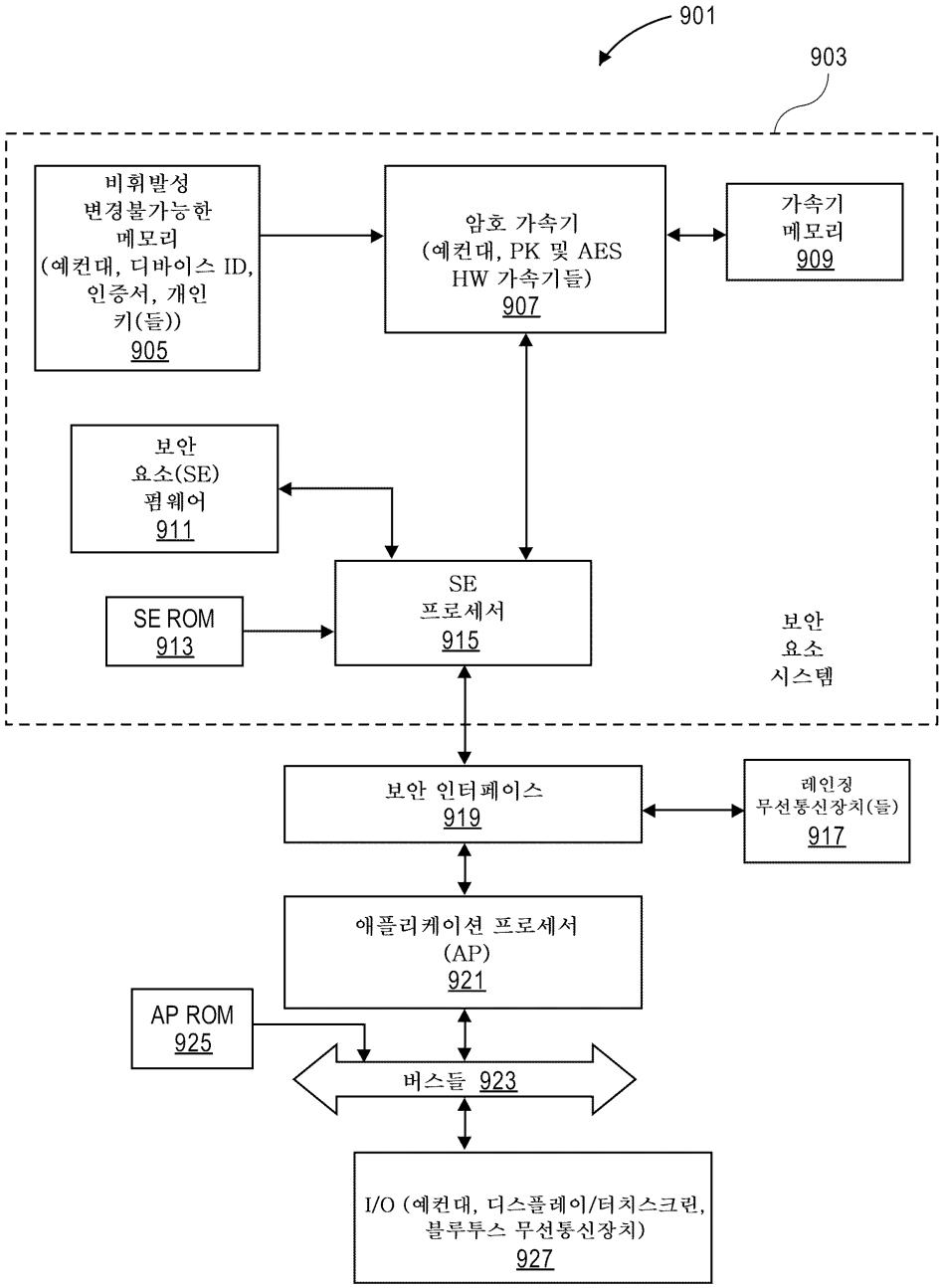
SS-TWR:

$ToF_1=1/2(T_1+T_2)=1/2(T_{Round1}-T_{Reply1})$

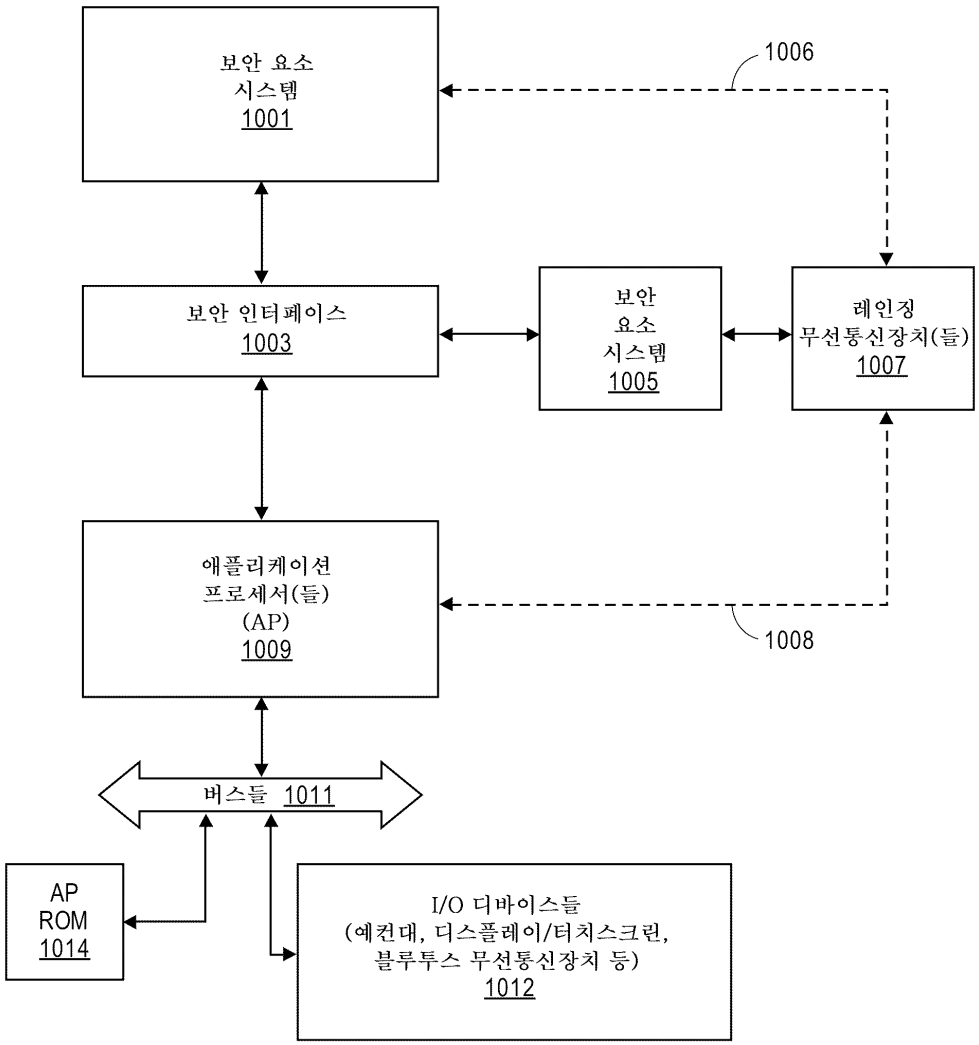
$ToF_2=1/2(T'_2+T_3)=1/2(T_{Round1}-T_{Reply2})$

SDS-TWR: $ToF=1/4(T_1+T_2+T'_2+T_3)=1/4(T_{Round1}+T_{Round2}-T_{Reply1}-T_{Reply2})$

도면9


901
903
비휘발성
변경불가능한
메모리
(예컨대, 디바이스 ID,
인증서, 개인
키(들))
905
암호 가속기
(예컨대, PK 및 AES
HW 가속기들)
907
가속기
메모리
909
보안
요소(SE)
펌웨어
911
SE ROM
913
SE
프로세서
915
보안
요소
시스템
보안 인터페이스
919
레인징
무선통신장치(들)
917
애플리케이션 프로세서
(AP)
921
AP ROM
925
버스들 923
I/O (예컨대, 디스플레이/터치스크린,
블루투스 무선통신장치)
927

도면10


보안 요소
시스템
1001
1006
보안 인터페이스
1003
보안
요소
시스템
1005
레인징
무선통신장치(들)
1007
애플리케이션
프로세서(들)
(AP)
1009
1008
버스들 1011
AP
ROM
1014
I/O 디바이스들
(예컨대, 디스플레이/터치스크린,
블루투스 무선통신장치 등)
1012