(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0008303
(43) 공개일자 2021년01월21일

(51) 국제특허분류(Int. Cl.)
G06F 21/35 (2013.01) *G06F 21/46* (2013.01)
G06F 3/0488 (2013.01) *H04L 29/06* (2006.01)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06F 21/35 (2013.01)
G06F 21/46 (2013.01)
(21) 출원번호 10-2020-0082739
(22) 출원일자 2020년07월06일
심사청구일자 2020년07월06일
(30) 우선권주장
16/509,063 2019년07월11일 미국(US)

(71) 출원인
슬림 에이치엠아이 테크놀로지
대만 타이페이 시티 105 송산 디스트릭트 푸싱 엔 로드 넘버 33 11층
(72) 발명자
시웅-쿠앙 차이
대만 타이페이 시티 115 난강 디스트릭트 징마오 세컨드 로드 레인157 넘버70 11층
(74) 대리인
김경희

전체 청구항 수 : 총 15 항

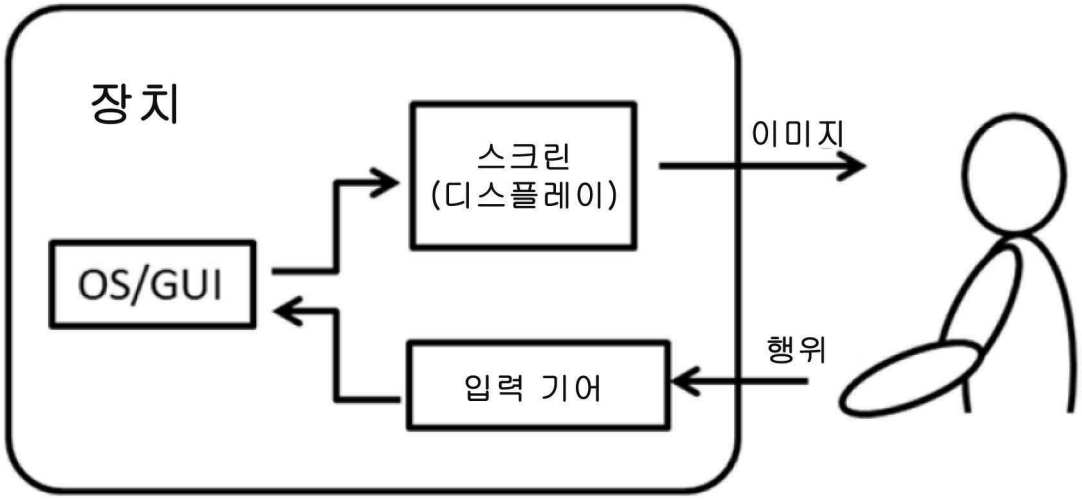
(54) 발명의 명칭 **안전한 상호작용 시스템 및 통신 디스플레이 장치**

(57) 요 약

시스템은 통신 디스플레이 장치 식별자를 갖는 통신 디스플레이 장치, 및 이동형 계산 장치 식별자를 갖는 이동형 계산 장치를 포함한다. 상기 이동형 계산 장치는, 제1 송수신기를 포함한다. 상기 통신 디스플레이 장치는 디스플레이 행렬 및 제2 수신기를 포함하는 ARC 모듈을 포함한다. 상기 디스플레이 행렬의 적어도 일부는 무선으로

(뒷면에 계속)

대 표 도 - 도1



보이지 않는 스트링을 송신하고 상기 보이지 않는 스트링과 관련된 사용자에게 보이는 지시를 형성하도록 구성된다. 상기 사용자에게 보이는 지시가 선택된 때, 채널은 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부, 상기 제1 송수신기 및 상기 제2 수신기를 연결하도록 형성된다. 상기 보이지 않는 스트링은 상기 채널을 통해 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부로부터 상기 제1 송수신기 및 상기 제2 수신기에 무선으로 결합되고, 상기 이동형 계산 장치는 상기 보이지 않는 스트링에 따라 태스크를 실행한다.

(52) CPC특허분류
G06F 3/04842 (2013.01)
G06F 3/0488 (2013.01)
H04L 63/0876 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/3236 (2013.01)
H04L 9/3247 (2013.01)

명 세 서

청구범위

청구항 1

시스템에 있어서,

이동형 계산 장치 식별자를 갖는 이동형 계산 장치. 상기 이동형 계산 장치는, 무선으로 데이터를 송신 및 수신하도록 구성되는, 제1 송수신기; 및 상기 제1 송수신기에 결합된, 제1 저장부를 포함하고; 및

통신 디스플레이 장치 식별자를 갖는 통신 디스플레이 장치를 포함하고. 상기 통신 디스플레이 장치는, ARC(행위 범위 통신) 모듈을 포함하고, 상기 ARC 모듈은, 디스플레이 행렬. 여기서 상기 디스플레이 행렬의 적어도 일부는 무선으로 보이지 않는 스트링을 송신하고 상기 보이지 않는 스트링과 관련된 사용자에게 보이는 지시를 형성하도록 구성되고; 및 무선으로 데이터를 수신하도록 구성된 제2 수신기를 포함하고;

상기 디스플레이 행렬의 일부 상의 상기 사용자에게 보이는 지시가 선택된 때, 채널은 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부, 상기 제1 송수신기 및 상기 제2 수신기를 연결하도록 형성되고,

상기 보이지 않는 스트링은 상기 채널을 통해 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부로부터 상기 제1 송수신기 및 상기 제2 수신기에 무선으로 결합되고, 상기 이동형 계산 장치는 상기 보이지 않는 스트링에 따라 태스크를 실행하는, 시스템.

청구항 2

제 1 항에 있어서, 상기 제1 송수신기는 상기 동일한 채널을 통해 상기 제2 수신기로 출력 스트링을 송신하도록 구성되고, 상기 제2 수신기는 상기 보이지 않는 스트링 및 상기 출력 스트링을 수신하도록 구성되는, 시스템.

청구항 3

제 2 항에 있어서, 상기 통신 디스플레이 장치는 상기 출력 스트링에 따라 상기 사용자에게 보이는 지시를 선택하는 사용자를 인식하도록 구성되는, 시스템.

청구항 4

제 2 항에 있어서,

상기 보이지 않는 스트링은 명령 및 데이터 스트링을 포함하고;

상기 데이터 스트링은 상기 이동형 계산 장치 식별자를 포함하고;

상기 명령에 따른 태스크는 상기 이동형 계산 장치에게 레코드를 생성 및 저장하고, 또한 상기 출력 스트링으로서 응답 스트링을 출력하도록 요청하고;

상기 이동형 계산 장치는 상기 제1 저장부 상에 상기 레코드를 생성하고 상기 보이지 않는 스트링 내의 상기 데이터 스트링에 따라 상기 응답 스트링을 생성하고; 및

상기 레코드는 상기 응답 스트링 및 상기 보이지 않는 스트링의 데이터 스트링의 적어도 일부를 포함하는, 시스템.

청구항 5

제 4 항에 있어서,

상기 사용자에게 보이는 지시는 상기 통신 디스플레이 장치 상에 또는 상기 통신 디스플레이 장치에 연결되고 서버-식별자에 의해 참조되는 서버 상에 계정을 생성하는 것을 나타내고, 상기 보이지 않는 스트링의 데이터 스트링은 상기 통신 디스플레이 장치 식별자 또는 상기 서버-식별자를 포함하고;

상기 레코드는 상기 통신 디스플레이 장치 식별자 또는 상기 서버-식별자를 포함하고, 상기 응답 스트링은 생성된 상기 계정에 로그인하기 위한 로그-인 스트링을 포함하고; 및

상기 통신 디스플레이 장치는 상기 제2 수신기를 통해 상기 로그-인 스트링을 수신하여 상기 계정을 생성하거나, 또는 상기 서버로 상기 로그-인 스트링을 제공하여 상기 서버 상에 상기 계정을 생성하는, 시스템.

청구항 6

제 4 항에 있어서,

상기 사용자에게 보이는 지시는 상기 이동형 계산 장치 상에 서버를 등록하는 것을 나타내고, 상기 서버는 상기 통신 디스플레이 장치에 연결되고 또한 서버-식별자에 의해 참조되고; 및

상기 데이터 스트링은 상기 서버-식별자, 및 상기 서버의 식별 스트링을 포함하고 상기 명령에 따른 태스크는 상기 이동형 계산 장치에게 상기 제1 저장부 상에 상기 서버-식별자 및 상기 식별 스트링을 저장하도록 요청하는, 시스템.

청구항 7

제 4 항에 있어서,

상기 사용자에게 보이는 지시는 적어도 하나의 파일을 암호화 또는 복호화하는 것을 나타내고;

상기 데이터 스트링은 상기 파일의 파일명을 포함하고;

상기 레코드는 상기 파일명을 포함하고, 상기 출력 스트링은 상기 파일을 암호화 또는 복호화하기 위한 키이고; 및

상기 통신 디스플레이 장치는 상기 제2 수신기로부터 상기 키를 수신하고 상기 파일을 암호화 또는 복호화하기 위해 상기 키를 이용하는, 시스템.

청구항 8

제 4 항에 있어서,

상기 사용자에게 보이는 지시는 상기 통신 디스플레이 장치 상의 또는 상기 통신 디스플레이 장치에 연결되고 또한 서버-식별자에 의해 참조되는 서버 상의 계정을 로그아웃하는 것을 나타내고;

상기 레코드는 상기 통신 디스플레이 장치 식별자 또는 상기 서버-식별자 및 다음에 상기 계정에 로그인하기 위한 새로운 로그-인 스트링을 포함하고;

상기 응답 스트링은 상기 새로운 로그-인 스트링을 포함하고; 및

상기 통신 디스플레이 장치는 상기 제2 수신기를 통해 상기 로그-인 스트링을 수신하고 상기 계정을 로그아웃하거나, 또는 상기 서버로 상기 로그-인 스트링을 보내고 상기 서버 상의 상기 계정을 로그아웃하는, 시스템.

청구항 9

제 2 항에 있어서,

상기 보이지 않는 스트링은 명령 및 데이터 스트링을 포함하고;

상기 명령에 따른 태스크는 상기 이동형 계산 장치에게 상기 제1 저장부 내에 저장된 레코드를 검색하도록 요청하고; 및

상기 이동형 계산 장치는 상기 데이터 스트링의 일부에 따라 상기 제1 저장부 내에서 상기 레코드를 발견하고 상기 출력 스트링 내의 상기 레코드의 적어도 일부로 출력하는, 시스템.

청구항 10

제 2 항에 있어서,

상기 보이지 않는 스트링은 명령 및 데이터 스트링을 포함하고; 및

상기 명령에 따른 태스크는 상기 이동형 계산 장치에게 상기 이동형 계산 장치 내에 저장된 데이터에 따라 상기 데이터 스트링을 암호화 또는 복호화하도록 요청하는, 시스템.

청구항 11

제 2 항에 있어서,

상기 사용자에게 보이는 지시는 상기 통신 디스플레이 장치에 연결되고 또한 서버-식별자에 의해 참조되는 서버를 인증하는 것을 나타내고;

상기 보이지 않는 스트링은 명령 및 데이터 스트링을 포함하고, 상기 데이터 스트링은 상기 서버-식별자 및 상기 서버의 식별 스트링을 포함하고;

상기 이동형 계산 장치는 상기 서버-식별자 및 상기 식별 스트링을 포함하는 상기 이동형 계산 장치 내에 저장된 레코드를 계산하는 계산 결과에 따라 상기 서버를 인증하고; 및

상기 이동형 계산 장치는 인증 결과를 보여주도록 구성되는 지시자를 더 포함하는, 시스템.

청구항 12

제 2 항에 있어서,

상기 이동형 계산 장치 및 상기 통신 디스플레이 장치 각각은, 데이터 전송을 위한 비대칭적 암호화를 수행하기 위해 공용 키 인프라스트럭쳐(PKI)에 의해 할당된 공용 키(pk) 및 비밀 키(sk)를 포함하는 한 쌍의 키들을 가지고;

상기 ARC 모듈은 프로세싱 블록을 더 포함하고 상기 프로세싱 블록은 다른 한 쌍의 키들, 상기 프로세싱 블록을 이용한 데이터 전송 상에서 비대칭적 암호화를 수행하기 위해 동일한 PKI에 의해 할당된 다른 공용 키 및 다른 비밀 키를 가지는, 시스템.

청구항 13

제 1 항에 있어서, 상기 ARC 모듈은

제2 저장부를 포함하고 또한 상기 디스플레이 행렬 및 상기 제2 수신기에 결합되는 프로세싱 블록을 더 포함하고;

상기 프로세싱 블록은 상기 디스플레이 행렬에 의해 상기 보이지 않는 스트링을 출력하고 상기 디스플레이 행렬에 의해 상기 사용자에게 보이는 지시를 디스플레이하기 위해 하나 또는 그 이상의 정보 소스들로부터 소스 데이터를 처리하도록 구성되고;

상기 하나 또는 그 이상의 정보 소스들은 상기 제2 수신기, 상기 통신 디스플레이 장치의 작동 시스템 및 상기 제2 저장부 중 적어도 하나를 포함하는, 시스템.

청구항 14

제 13 항에 있어서, 상기 프로세싱 블록은 상기 제2 수신기에 의해 수신되는 데이터에 따라 하나 또는 그 이상의 정보 소스들을 선택하도록 설정되거나; 또는 상기 프로세싱 블록은 상기 프로세싱 블록이 소정 시간 간격 동안 상기 제2 수신기로부터 또는 상기 작동 시스템으로부터 데이터를 수신하지 않은 후 정보 소스로서 상기 제2 저장부를 설정하는, 시스템.

청구항 15

통신 디스플레이 장치 식별자를 갖는 통신 디스플레이 장치에 있어서, 상기 통신 디스플레이 장치는, ARC(행위 범위 통신) 모듈을 포함하고, 상기 ARC 모듈은,

디스플레이 행렬. 여기서 상기 디스플레이 행렬의 적어도 일부는 무선으로 보이지 않는 스트링을 송신하고 상기 보이지 않는 스트링과 관련된 사용자에게 보이는 지시를 형성하도록 구성되고;

무선으로 데이터를 수신하도록 구성된 제2 수신기; 및

제2 저장부를 포함하고 또한 상기 디스플레이 행렬 및 상기 제2 수신기에 결합되는 프로세싱 블록을 포함하고;

상기 디스플레이 행렬의 일부 상의 상기 사용자에게 보이는 지시가 선택된 때, 채널은 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부, 이동형 계산 장치의 제1 송수신기 및 상기 제2 수신기를 연결하

도록 형성되고,

상기 보이지 않는 스트링은 상기 채널을 통해 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부로부터 상기 제1 송수신기 및 상기 제2 수신기에 무선으로 결합되고, 상기 이동형 계산 장치는 상기 보이지 않는 스트링에 따라 태스크를 실행하고,

상기 프로세싱 블록은 상기 디스플레이 행렬에 의해 상기 보이지 않는 스트링을 출력하고 상기 디스플레이 행렬에 의해 상기 사용자에게 보이는 지시를 디스플레이하기 위해 하나 또는 그 이상의 정보 소스들로부터 소스 데이터를 처리하도록 구성되고;

상기 하나 또는 그 이상의 정보 소스들은 상기 제2 수신기, 상기 통신 디스플레이 장치의 작동 시스템 및 상기 제2 저장부 중 적어도 하나를 포함하는, 통신 디스플레이 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 안전한 상호작용 시스템 및 통신 디스플레이 장치에 관한 것이다.

배 경 기 술

[0002] 사용자-장치 상호작용(user-device interaction, UDI)의 현재 메카니즘은 사용자를 전자 장치와 상호작용하기 위해 정보를 수신하고 제공하는 독립적인 당사자(party)로서 고려한다. 이 UDI에서 2 가지의 주요한 정보 경로들이 있다: 장치(device)로부터 사용자(user)로의 이미지(image), 및 사용자로부터 장치로의 행위(action). 장치 측면에서, 이것들은 또한 데이터를 광학적 이미지로 및 행위를 데이터로 각각 변환할 수 있는, 구성요소들, 디스플레이 및 사용자 입력을 나타낸다.

[0003] 이 메카니즘은 사용자가 제공할 수 있는 정보를 암시적으로 제한한다. 사용자는 정보를 기억하고 이를 복수의 행위들, 즉 한 글자씩(character by character) 제공해야 한다. 예를 들어, 비밀번호 응용 분야들에 있어서, 비밀번호 크기 및 무작위성(randomness)은 보호의 효율성에 영향을 미치는 것으로 알려져 있다. 하지만, 우리는 보호와 인간이 실제로 충분히 할 수 있는 기억 및 행위들을 절충해야 한다. 오늘날, 최소한의 6 내지 8 알파벳 글자들(또는 48 내지 64 비트들)을 갖는 비밀번호를 흔히 요구한다. 대조적으로, AES(Advanced Encryption Standard)는 정보 보호를 위해 128, 192, 또는 256 비트들의 키 길이를 제안한다. 길이 및 무작위성 모두는 인간 뇌가 이러한 데이터를 기억하도록 요구한다. 이러한 데이터를 재현하는 데 필요한 복잡한 행위들은 실제 적용에 있어서 다른 장벽이다.

[0004] 이 메카니즘의 다른 문제는 계산에 있어서 인간 뇌의 취약성에 관련된다. 사용자는 그의 입력, 예를 들어 비밀번호를 선택하기 위해 이미지를 비교하는 것과 같이, 응답하기 위해 단순한 동작만 수행할 수 있다. 디지털 서명에 있어서, 예를 들어, 암호화 해쉬 함수에 의해 문서의 해쉬 값을 생성할 필요가 있을 수 있다. 사용자는 그의 서명을 비밀 키로 사용하여 해쉬를 암호화하는 것은 고사하고, 문서를 보는 것으로써 해쉬를 생성할 수 없다. 사용자가 입력으로서 제공할 수 있는 정보는 현재 상호작용 메카니즘 하에서 제한된다. 이것은 인간 뇌의 기억 및 계산 제한조건들 및 재현을 위해 필요한 행위들의 복잡성으로 인한 제한들을 암시한다.

[0005] 몇몇의 경우들에 있어서, 단지 허용된 사용자만 UDI를 수행할 수 있다. 사람들은 이러한 비밀번호, 지문, 또는 안면 인식과 같은 인증에 의해 사용자를 인식하기 위해 다양한 메카니즘들을 채택한다. 이러한 메카니즘들은 장치가 어느 순간에 사람을 인식하는 것에 도움을 줄 수는 있지만, 인증된 사람을 지속적으로 추적할 수 없다. 이러한 메카니즘들은 사람을 인식하기 위해 일시적으로 눈을 뜨고, 그후 눈을 감고 동일한 사람과 상호작용하는 것으로 가정하는 것과 동일하다. 이에 더하여, 단지 한 명의 인증된 사람이 있을 수 있다. 다시 말하면, 현재 장치는 한 사람 이상을 인식할 수 없는 메카니즘을 위한 개인용 장치일 수 있다. 이것은 복수의 사용자들이 이 장치를 협력하여 작동시키는 것과 같은 더 일반적인 시나리오들에서는 장치의 응용을 제한한다.

발명의 내용

[0006] 시스템은 이동형 계산 장치(mobile computing device) 및 통신 디스플레이 장치(communication display device)를 포함한다. 상기 이동형 계산 장치는, 무선으로 데이터를 송신 및 수신하도록 구성되는, 제1 송수신기(first transceiver), 상기 제1 송수신기에 결합된 제1 저장부(first storage), 및 이동형 계산 장치 식별자(mobile computing device identifier)를 포함한다. 상기 통신 디스플레이 장치는 통신 디스플레이 장치 식별

자(communication display device identifier) 및 ARC(action range communication) 모듈을 포함한다. 상기 ARC 모듈은 디스플레이 행렬(display matrix) 및 무선으로 데이터를 수신하도록 구성되는 제2 수신기(second receiver)를 포함한다. 상기 디스플레이 행렬의 적어도 일부는 무선으로 보이지 않는 스트링(invisible string)을 송신하고 상기 보이지 않는 스트링과 관련된 사용자에게 보이는 지시(user-visible indication)를 형성하도록 구성된다. 상기 디스플레이 행렬의 일부 상의 상기 사용자에게 보이는 지시가 선택된 때, 채널은 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부, 상기 제1 송수신기 및 상기 제2 수신기를 연결하도록 형성된다. 상기 보이지 않는 스트링은 상기 채널을 통해 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부로부터 상기 제1 송수신기 및 상기 제2 수신기에 무선으로 결합되고, 상기 이동형 계산 장치는 상기 보이지 않는 스트링에 따라 태스크(task)를 실행한다.

[0007] 일 실시예에 있어서, 상기 제1 송수신기는 상기 동일한 채널을 통해 상기 제2 수신기로 출력 스트링(output string)을 송신하도록 구성된다. 상기 제2 수신기는 상기 보이지 않는 스트링 및 상기 출력 스트링을 수신하도록 구성된다.

[0008] 일 실시예에 있어서, 상기 보이지 않는 스트링 및 상기 출력 스트링은 상기 채널을 통해 신호들에 의해 전달되고, 상기 제2 수신기는 크기, 위상, 주파수, 신호 레벨 또는 시간에 있어서의 신호들의 특성을 구별하는 것에 의해 상기 보이지 않는 스트링 및 상기 출력 스트링을 인식하도록 구성된다.

[0009] 일 실시예에 있어서, 상기 통신 디스플레이 장치는 상기 출력 스트링에 따라 상기 사용자에게 보이는 지시를 선택하는 사용자를 인식하도록 구성된다.

[0010] 일 실시예에 있어서, 상기 보이지 않는 스트링은 명령(command) 및 데이터 스트링을 포함한다. 상기 데이터 스트링은 상기 이동형 계산 장치 식별자를 포함한다. 상기 명령에 따른 태스크는 상기 이동형 계산 장치에게 레코드(record)를 생성 및 저장하고, 또한 상기 출력 스트링으로서 응답 스트링(reply string)을 출력하도록 요청한다. 상기 이동형 계산 장치는 상기 제1 저장부 상에 상기 레코드를 생성하고 상기 보이지 않는 스트링 내의 상기 데이터 스트링에 따라 상기 응답 스트링을 생성한다. 상기 레코드는 상기 응답 스트링 및 상기 보이지 않는 스트링의 데이터 스트링의 적어도 일부를 포함한다.

[0011] 일 실시예에 있어서, 상기 사용자에게 보이는 지시는 상기 통신 디스플레이 장치 상에 또는 상기 통신 디스플레이 장치에 연결되고 서버-식별자에 의해 참조되는 서버 상에 계정(account)을 생성하는 것을 나타내고, 상기 보이지 않는 스트링의 데이터 스트링은 상기 통신 디스플레이 장치 식별자 또는 상기 서버-식별자를 포함한다. 상기 레코드는 상기 통신 디스플레이 장치 식별자 또는 상기 서버-식별자를 포함하고, 상기 응답 스트링은 생성된 상기 계정에 로그인하기 위한 로그-인 스트링을 포함한다. 상기 통신 디스플레이 장치는 상기 제2 수신기를 통해 상기 로그-인 스트링을 수신하여 상기 계정을 생성하거나, 또는 상기 서버로 상기 로그-인 스트링을 제공하여 상기 서버 상에 상기 계정을 생성한다.

[0012] 일 실시예에 있어서, 상기 사용자에게 보이는 지시는 상기 이동형 계산 장치 상에 서버를 등록(registering)하는 것을 나타내고, 상기 서버는 상기 통신 디스플레이 장치에 연결되고 또한 서버-식별자에 의해 참조된다. 상기 데이터 스트링은 상기 서버-식별자, 및 상기 서버의 식별 스트링을 포함하고 상기 명령에 따른 태스크는 상기 이동형 계산 장치에게 상기 제1 저장부 상에 상기 서버-식별자 및 상기 식별 스트링을 저장하도록 요청한다.

[0013] 일 실시예에 있어서, 상기 사용자에게 보이는 지시는 적어도 하나의 파일(file)을 암호화(encrypting) 또는 복호화(decrypting)하는 것을 나타낸다. 상기 데이터 스트링은 상기 파일의 파일명(filename)을 포함한다. 상기 레코드는 상기 파일명을 포함하고, 상기 출력 스트링은 상기 파일을 암호화 또는 복호화하기 위한 키(key)이다. 상기 통신 디스플레이 장치는 상기 제2 수신기로부터 상기 키를 수신하고 상기 파일을 암호화 또는 복호화하기 위해 상기 키를 이용한다.

[0014] 일 실시예에 있어서, 상기 이동형 계산 장치는 데이터 스트링 내의 데이터에 기초하여 난수 발생기(random number generator)를 통해 랜덤 스트링을 생성한다. 레코드 및 응답 스트링은 각각 랜덤 스트링을 포함한다.

[0015] 일 실시예에 있어서, 상기 사용자에게 보이는 지시는 상기 통신 디스플레이 장치 상의 또는 상기 통신 디스플레이 장치에 연결되고 또한 서버-식별자에 의해 참조되는 서버 상의 계정을 로그아웃하는 것을 나타낸다. 상기 레코드는 상기 통신 디스플레이 장치 식별자 또는 상기 서버-식별자 및 다음에 상기 계정에 로그인하기 위한 새로운 로그-인 스트링을 포함한다. 상기 응답 스트링은 상기 새로운 로그-인 스트링을 포함한다. 상기 통신 디스플레이 장치는 상기 제2 수신기를 통해 상기 로그-인 스트링을 수신하고 상기 계정을 로그아웃하거나, 또는 상기 서버로 상기 로그-인 스트링을 보내고 상기 서버 상의 상기 계정을 로그아웃한다.

[0016] 일 실시예에 있어서, 상기 보이지 않는 스트링은 명령 및 데이터 스트링을 포함한다. 상기 명령에 따른 태스크는 상기 이동형 계산 장치에게 상기 제1 저장부 내에 저장된 레코드를 검색하도록 요청한다. 상기 이동형 계산 장치는 상기 데이터 스트링의 일부에 따라 상기 제1 저장부 내에서 상기 레코드를 발견하고 상기 출력 스트링 내의 상기 레코드의 적어도 일부로 출력한다.

[0017] 일 실시예에 있어서, 상기 보이지 않는 스트링은 명령 및 데이터 스트링을 포함한다. 상기 명령에 따른 태스크는 상기 이동형 계산 장치에게 상기 이동형 계산 장치 내에 저장된 데이터에 따라 상기 데이터 스트링을 암호화 또는 복호화하도록 요청한다.

[0018] 일 실시예에 있어서, 상기 사용자에게 보이는 지시는 상기 통신 디스플레이 장치에 연결되고 또한 서버-식별자에 의해 참조되는 서버를 인증하는 것을 나타낸다. 상기 보이지 않는 스트링은 명령 및 데이터 스트링을 포함하고, 상기 데이터 스트링은 상기 서버-식별자 및 상기 서버의 식별 스트링을 포함한다. 상기 이동형 계산 장치는 상기 서버-식별자 및 상기 식별 스트링을 포함하는 상기 이동형 계산 장치 내에 저장된 레코드를 계산하는 계산 결과에 따라 상기 서버를 인증한다. 상기 이동형 계산 장치는 인증 결과를 보여주도록 구성되는 지시자(indicator)를 더 포함한다.

[0019] 일 실시예에 있어서, 상기 이동형 계산 장치 및 상기 통신 디스플레이 장치 각각은, 데이터 전송을 위한 비대칭적 암호화를 수행하기 위해 공용 키 인프라스트럭처(public key infrastructure, PKI)에 의해 할당된 공용 키(pk) 및 비밀 키(sk)를 포함하는 한 쌍의 키들을 가진다.

[0020] 일 실시예에 있어서, 상기 ARC 모듈은 프로세싱 블록(processing block)을 더 포함하고 상기 프로세싱 블록은 다른 한 쌍의 키들, 상기 프로세싱 블록을 이용한 데이터 전송 상에서 비대칭적 암호화를 수행하기 위해 동일한 PKI에 의해 할당된 다른 공용 키 및 다른 비밀 키를 가진다.

[0021] 일 실시예에 있어서, 상기 ARC 모듈은 제2 저장부를 포함하고 또한 상기 디스플레이 행렬 및 상기 제2 수신기에 결합되는 프로세싱 블록을 더 포함한다. 상기 프로세싱 블록은 상기 디스플레이 행렬에 의해 상기 보이지 않는 스트링을 출력하고 상기 디스플레이 행렬에 의해 상기 사용자에게 보이는 지시를 디스플레이하기 위해 하나 또는 그 이상의 정보 소스들로부터 소스 데이터를 처리하도록 구성된다. 상기 하나 또는 그 이상의 정보 소스들은 상기 제2 수신기, 상기 통신 디스플레이 장치의 작동 시스템 및 상기 제2 저장부 중 적어도 하나를 포함한다.

[0022] 일 실시예에 있어서, 상기 프로세싱 블록은 상기 제2 수신기에 의해 수신되는 데이터에 따라 하나 또는 그 이상의 정보 소스들을 선택하도록 설정된다.

[0023] 일 실시예에 있어서, 상기 프로세싱 블록은 상기 프로세싱 블록이 소정 시간 간격 동안 상기 제2 수신기로부터 또는 상기 작동 시스템으로부터 데이터를 수신하지 않은 후 정보 소스로서 상기 제2 저장부를 설정한다.

[0024] 통신 디스플레이 장치 식별자를 갖는 통신 디스플레이 장치는, ARC(행위 범위 통신) 모듈을 포함한다. 상기 ARC 모듈은 디스플레이 행렬, 제2 수신기 및 프로세싱 블록을 포함한다. 상기 디스플레이 행렬의 적어도 일부는 무선으로 보이지 않는 스트링을 송신하고 상기 보이지 않는 스트링과 관련된 사용자에게 보이는 지시를 형성하도록 구성된다. 상기 제2 수신기는 무선으로 데이터를 수신하도록 구성된 다. 상기 프로세싱 블록은 제2 저장부를 포함하고 또한 상기 디스플레이 행렬 및 상기 제2 수신기에 결합된다. 상기 디스플레이 행렬의 일부 상의 상기 사용자에게 보이는 지시가 선택된 때, 채널은 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부, 이동형 계산 장치의 제1 송수신기 및 상기 제2 수신기를 연결하도록 형성된다. 상기 보이지 않는 스트링은 상기 채널을 통해 상기 사용자에게 보이는 지시를 형성하는 상기 디스플레이 행렬의 일부로부터 상기 제1 송수신기 및 상기 제2 수신기에 무선으로 결합되고, 상기 이동형 계산 장치는 상기 보이지 않는 스트링에 따라 태스크를 실행한다. 상기 프로세싱 블록은 상기 디스플레이 행렬에 의해 상기 보이지 않는 스트링을 출력하고 상기 디스플레이 행렬에 의해 상기 사용자에게 보이는 지시를 디스플레이하기 위해 하나 또는 그 이상의 정보 소스들로부터 소스 데이터를 처리하도록 구성된다. 상기 하나 또는 그 이상의 정보 소스들은 상기 제2 수신기, 상기 통신 디스플레이 장치의 작동 시스템 및 상기 제2 저장부 중 적어도 하나를 포함한다.

[0025] 상기에서 설명된 본 개시의 실시예들에 따르면, 사용자가, 사이보그(cyborg)로서, 디지털 서명을 제공하는 것과 같은 복잡한 계산을 수행하고 비밀번호 또는 파일 암호화를 위해 마음대로 긴 랜덤 스트링을 이용하는 것이 가능하다. 랜덤 스트링을 제공하거나 계산을 하거나 결과를 출력하기 위해 단지 하나의 행위로 충분하다. 통신 디스플레이 장치는 복수-사이보그 상호작용들을 제공하기 위해 서로 다른 사이보그들로부터의 입력들을 인식할 수 있다(입력자 인식). 다시 말하면, 이것은 지속적인 인증 방식(way of continuous authentication)인데, 장치는 모든 입력을 인증할 수 있다. 우리는 장치 및 사용자 모두에 대하여 더 안전한 상호작용 방식을 가질 수 있다.

도면의 간단한 설명

[0026] 실시예들은 본 개시를 한정하지 않고 단지 설명을 위해 주어진, 상세한 설명 및 첨부된 도면들로부터 더 잘 이해될 것이다.

도 1은 사용자-장치 상호작용을 구현하기 위한 전통적인 메카니즘이다.

도 2는 사용자-장치 상호작용의 행위 범위 통신(ARC) 메카니즘이다.

도 3은 (a) DEGE 개념 및 (b) DEGE를 생성하기 위한 디스플레이 행렬을 위한 방식이다.

도 4는 닫힌 2 개의 전극들 (타입-1 AFDT)을 움직이는, 그리고 인체(타입-2 AFDT)와 같이, 전도성 매체를 통해 하나의 전극으로부터 다른 전극으로 신호를 연결하는, 용량성 결합을 시작하는 2 가지의 서로 다른 방법들을 보여준다.

도 5는 방송기-수신기 배치들(broadcaster-receiver arrangements) 및 다른 AFDT들로서의 ARC 플랫폼 상에 통합될 수 있는 응용들(applications)을 보여준다.

도 6은 ARC 메카니즘에 기초한 (a) 인간 입력 및 (b) 사이보그 입력을 비교한다.

도 7은 사이보그 입력을 보다 상세하게 도시한다. (a) 방송기 상에서 DEGE를 즉 도시된 바와 같이 'Login' DEGE를 선택할 때, ARC 모듈의 수신기는, UDi에 더하여, 사이보그에 의해 제공되는 추가의 UDe를 수신한다. (b) 이 사이보그 입력 프로세스 내에서 신호 흐름을 보여준다. (c) 이동형 계산 장치(WD)의 기능도 및 WD 내에 저장된 레코드의 포맷을 보여준다.

도 8은 스크린 장치와 WD 사이에 프로토콜들을 구현하기 위해, 동일한 GE 및 서로 다른 UD들을 가지고, 사이보그가 2 가지의 DEGE들을 이용해 계정을 생성하는 방법을 보여준다.

도 9는 계정에 로그인하기 위한 사용자명 및 비밀번호를 사이보그에게 제공하는 DEGE를 보여준다.

도 10은 사이보그가 (a) 비밀번호로서 랜덤 스트링을 생성하고 또한 (b) 다음에 로그인하기 위한 다른 랜덤 비밀번호를 설정하면서 계정을 로그아웃하는 DEGE를 보여준다.

도 11은 태그를 갱신, 즉 다음에 로그인에 필요한 데이터를 변경할 수 있는 로그아웃하는 흐름을 보여준다. 로그인하기 위해, 매번 서로 다른 태그를 필요로 할 것이다.

도 12는 양방향 인증(bidirectional authentication)을 위한 흐름을 보여준다. 서버 및 사이보그는 미리 서로 안다. 즉 서로의 신원(identity, 태그)을 교환 및 저장하는 것에 의해 서로 등록한다. 이후에 서로 인식하기 위해, 사이보그 및 서버는 증명(verify)을 위해 서로의 신원을 보내고 서로의 신원을 증명하는 것에 의해 서로 로그인할 수 있다.

도 13은 본 인증 메카니즘을 보여준다. 스크린 장치만이 서버 및 사용자의 신원들 모두를 확인(confirm)할 수 있다.

도 14는 사이보그가 문서에 서명하는, 즉 디지털 서명을 제공하는 흐름을 보여준다.

도 15는 (a) 재구성할 수 있는 ARC 모듈(reconfigurable ARC module, Re-ARC mod.)의 구조 및 Re-ARC mod.의 다양한 작동 모드들, (b) 사용자/사이보그가 스크린 장치와 상호작용을 하는 정상 장치 모드(normal device mode), (c) 사용자가 WD와 상호작용하는 가상 장치 모드 1(virtual device mode 1), 및 (d) 사용자/사이보그가 Re-ARC mod.과 상호작용하는 가상 장치 모드 2를 보여준다.

도 16은 (a) Re-ARC mod. 및 (b) PKI에 의해 발행되는, 한 쌍의 공용 키 및 비밀 키(pk_a, sk_a) 및 (pk_c, sk_c), 를 각각 가지는 WD를 보여준다. (c) 가상 장치 모드 3 작동을 보여준다.

도 17은 사이보그에 의한 암호화의 흐름을 보여준다.

도 18은 사이보그에 의한 복호화의 흐름을 보여준다.

도 19는 지속적인 인증 또는 입력자 인식을 위한 방법을 보여주는데, 스크린 장치는 매 입력에 대하여 사이보그를 인증한다.

도 20은 에코 모드 기능을 갖는 WD의 도면, 에코 신호(ES)를 생성하기 위한 명령, 및 WD를 인식하기 위한 수신기에 대한 방식을 포함하여, 지속적인 인증 또는 입력자 인식을 구현하기 위한 다른 방식을 보여준다.

도 21은 입력자 인식의 일 예를 보여준다. 시나리오는 디스플레이되는 스크린 상에 입력을 제공하기 위해 하나의 스크린 장치와 상호작용하는 3 개의 사이보그들이다. 단계들에 따라, 스크린 장치는 또한 입력을 제공하는 것이 허용되는 사이보그들을 결정할 수 있다.

발명을 실시하기 위한 구체적인 내용

[0027] 개시의 실시예들은, 첨부된 도면들을 참조하여 진행되는, 이하의 상세한 설명으로부터 명백해질 것이다. 이때 동일한 참조부호들은 동일한 요소들에 관련된다. 설명을 단순화시키기 위해, 우리는 이동형 계산 장치를 예를 들기 위해, 상세화되는 기능들을 가지는, 웨어러블 장치(WD), 및 통신 디스플레이 장치를 나타내기 위해 컴퓨터 또는 휴대폰과 같이 네트워크 및 디스플레이 기능을 가지는 스크린 장치를 이용할 것이다.

[0028] 상세한 설명은 이하의 주제들을 포함한다. 우리는 먼저 ARC(action range communication)의 메카니즘 및 요소들을 도입한다. ARC는 사용자 입력 및 단거리 데이터 전송(short-range data transmission, SRDT)을 위해 기능하는 보편적인 메카니즘이다. ARC에 있어서, 우리는 사용자/스크린 장치 상호작용, 즉 사용자 입력을 스크린 장치에, 결합하고, 또한 입력 정보를 제공하는 데 있어서 사용자를 보조하는 다른 장치(WD와 같은)를 가질 수 있다. 이런 의미에서, ARC의 셋업을 통해, 인간과 WD는 사이보그로 결합되어 스크린 장치와 상호작용하기 위해 하나의 유닛으로 작동할 수 있다. 이것은 UDI를 사이보그-장치 상호작용(cyborg-device interaction, CDI)으로 변환시킨다. 다시 말하면, ARC 셋업을 통해, WD는 UDI 프로세스를 결합하고 또한 사용자가 이러한 행동들을 수행하는 것처럼 데이터를 생성, 저장, 또는 계산과 같이, 디지털 데이터를 취급하는 데 있어서 사용자를 보조할 수 있다. 보다 상세하게, WD는 비밀번호를 기억해서 사용자가 비밀번호를 설정하고 잊어버리거나, 비밀번호에 대한 긴 랜덤 스트링을 생성하거나, 또는 로그아웃할 때 새로운 비밀번호를 설정하는 것과 같이 자주 비밀번호를 변경할 수 있다. 서버/장치는 사용자명/비밀번호, 지문, 또는 얼굴에 의해서가 아니라, 신원으로서 스트링에 의해서 사이보그를 인식할 수 있다. 각각의 입력에 대하여, 사이보그는 그의 신원을 제공하여 장치/서버가 입력을 제공하는 사람을 증명할 수 있다. 입력자 인식 또는 지속적인 인증. 따라서, 서버/장치는 단지 하나의 사이보그뿐만 아니라 ARC를 통해 복수의 사이보그들과 함께 상호작용할 수 있다. 사이보그는 인간이 하는 것과 같이 인증되지 않고 서버/장치를 인증할 수 있다. 양방향 인증. 사이보그는 데이터를 기억하는 것에 한정되지 않기 때문에, 서로 다른 긴 랜덤 스트링들을 가지고, 파일들을 자유로이 암호화/복호화할 수 있다. 우리는 사이보그/사용자와 상호작용하는 다양한 가상 장치들로서 UDI를 생성하고 또한 내재된 기능들로서 인증 또는 스크린 잠금을 수행하기 위해 재구성가능한 ARC 송수신기 모듈을 가질 수 있다.

[0029] ARC의 일반적인 개념은 새로운 정보 전달자 DEGE(data embedded graphic element)에 의해 수행되는 정보의 전송을 보여준다. DEGE는 정보를 표현하기 위해 2 가지 부분들, 이미지(GE) 및 데이터(UD)을 이용한다. DEGE의 전송은 DEGE 방송기로부터 수신기까지 UD를 전송하기 위한 채널을 설립하기 위해 사용자가 GE에 의존하는 것을 의미한다. 우리는 이러한 전송 프로세스를 기술하기 위해 행위 제공 데이터 전송(AFDT: action facilitating data transmission)를 이용한다. 전통적인 디스플레이는 DEGE 방송기로 변형될 수 있다. 이 주요 요소들 및 전체 메카니즘은 이하에서 설명될 것이다.

[0030] UDI의 전통적인 메카니즘(도 1)과 비교하여, ARC (도 2)는 (사용자에 의해 선택되는) 이미지 및 데이터 (선택의 내용 또는 입력 내용)를 방송기로부터 수신기로 전송되는 하나의 단일 정보 유닛으로 통합하고, 또한 방송기 및 수신기 모두는 동일한 장치 상에 위치된다. 장치 관점에서, 정보 유닛은 그 자체로 장치-내 전송(intra-device transmission)을 다시 귀환(loop)한다. 방송 때문에, 이러한 장치-내 전송은 모든 정보 유닛이 다 복귀하지는 않을 것이므로 사소한 전송은 아니다. 복귀된 유닛은 선택되어졌는지 또는 선택되었는지에 대한 메시지를 준다. 이러한 메카니즘에 있어서, 사용자는 도 1에서와 같이 그 자신의 정보를 제공하는 정보 소스로서 행동하지 않는다. 사용자는 방송기로부터 수신기로의 정보 유닛을 연결하는 데 도움을 주는 채널의 일부이다. 또는, 사용자 관점에서, 방송기로부터의 정보 유닛을 선택하고 이를 수신기로 전송한다. 우리는 이를 행위 제공 데이터 전송(action facilitating data transmission, AFDT)로서 선택-전송 프로세스(select-transfer process)로 명명한다. 방송기 및 수신기는 데이터 통신에서 송수신기 모듈과 같은 기능을 하는 ARC 송수신기 모듈(ARC mod.)을 형성한다. 하지만, 방송기는 통합된 정보 유닛, 데이터만이 아닌 이미지 및 데이터를 제공할 것이고, 정보는 동일한 송수신기의 수신기로 다시 귀환한다. 장치-내 전송.

[0031] 이 메카니즘은 근거리 통신 또는 NFC의 작동과 같이, UDI 뿐만 아니라 단거리 데이터 통신(SRDT)에 적용가능하

다. NFC에서, 사람들은 데이터 통신에만 집중하는데, 이것은 완성된 프로세스를 묘사하기에는 불충분하다. 작동을 완료하기 위해 사용자의 행위를 안내하기 위한 이미지를 필요로 한다. 이미지 및 행위는 NFC에서 필수불가결한 인자들이지만 무시되어 왔다. 우리는 이들을 데이터 통신과 함께 고려해야 한다. 전체 프로세스는 사용자가 방송기로부터 수신기로의 정보 유닛을 선택하는 UDI의 ARC 메카니즘과 동일하다. UDI와 달리, 방송기 및 수신기는 NFC 또는 SRDT 내의 2 개의 별도의 분리된 장치들 상에 위치한다. 이것은 장치-외 전송(extra-device transmission)이다. 따라서, 우리는 프로세스를 완료하기 위해 SRDT 및 UDI를 3 개의 주요 요소들, 이미지, 행위, 및 데이터 전송에 의존하는, 새로운 타입의 정보 전송으로서 취급할 수 있다. 이것들은 수신기에 대한, 방송기의 배치에 있어서 다른데, 별도로 분리된 장치들은 SRDT이고 동일한 장치는 UDI이다. 하나의 방송기는 장치-내 및 장치-외 전송을 위해 기능할 수 있다. 이것은 하나의 전송 플랫폼 ARC 내에서 UDI와 SRDT를 통합하기 위한 기초가 된다. 이하에서, 우리는 정보 전달자 DEGE, 전송 프로세스 ARDT, 및 방송기를 보다 상세하게 설명할 것이다.

[0032] DEGE

[0033] ARC에서, 정보는 오직 데이터에 의해서만이 아니라, 데이터 임베디드 그래픽 요소(data embedded graphic element, DEGE)로 명명되는, 이미지-데이터 통합 구조에 의해 표현된다. DEGE는 2 개의 부분들, 그래픽 요소(GE) 및 사용자 데이터(UD)를 포함하고, (GE, UD)로 표현될 수 있다. GE 및 UD는 사용자에 대해서는 GE이고 UD는 데이터 수신기에 대한 것으로, 서로 다른 정보 수신자들에 대한 것만 제외하고 동일한 정보 컨텐츠를 나타낸다. DEGE는 텍스트(GE로서)가 하이퍼링크(UD로서)와 연관되는, 하이퍼텍스트와 비슷하지만, 동일하지는 않다. 하이퍼텍스트는 실제로 텍스트와 하이퍼링크와 결합되지 않는다. 연관(association)은 그래픽 사용자 인터페이스(GUI)의 해석에 의존한다. 현재의 UDI 메카니즘에서, 텍스트는 그 위치에 의해 표현되고 텍스트를 선택하는 것은 GUI에 위치를 제공하는 것을 의미한다. GUI는 그후 위치를 하이퍼링크로 번역한다. 이것은 텍스트와 하이퍼링크를 함께 연결하기 위해, 텍스트를 기술하는 메타데이터, 즉 위치를 이용한다. 이 메카니즘은 위치로부터 하이퍼링크를 추출하기 위해 텍스트-위치 매핑에 의존한다는 점에서 장치-외 케이스에는 적용불가할 수 있다. 위치만으로는 의미가 없다. 한편, 우리는 위치 메타데이터에 의존하지 않고 UD(하이퍼링크)와 GE(텍스트)를 직접 동일한 위치에 부착하는 것에 의해 DEGE를 형성한다. UD는 메타데이터가 아니고 다른 장치가 인식할 수 있는 정보를 나타내는 데이터이다. 그러므로, 이것은 장치-외 케이스들 내에서 정보를 전달하기 위해 기능할 수 있다. 나아가, DEGE는 텍스트-하이퍼링크 조합에 한정되지 않기 때문에 더 일반적이다. 우리는 어떠한 아이콘(GE)과 데이터(UD)를 하나의 유닛으로서 함께 결합할 수 있다. 이것은 사용자 및 장치 모두가 이해할 수 있는 정보를 나타내는 일반적인 방법을 제공한다.

[0034] DEGE의 3 개의 특징들에 유의해야 한다. GE로 인해, DEGE에 의해 전달되는 정보는 실제 엔터티(tangible entity)와 같은 소정의 물리적 공간을 차지할 것이다. 동일한 정보는 GE 및 UD로서 표현되기 때문에, DEGE는 구조에 있어서 리던던시를 포함한다. 인간 및 장치와 같은, 이종의 당사자들에 정보를 분배할 때, 이러한 리던던시는 분배 프로세스를 단순화시킬 수 있다. DEGE는 데이터 및 이미지보다 정보를 표현하는 데 더 일반적이다. 우리는 데이터 및 이미지를 하나의 요소가 '널(null)'인, 즉 데이터와 이미지가 ('null', UD) 및 (GE, 'null') 종류들의 DEGE에 각각 대응하는, 특정한 DEGE로서 고려할 수 있다. 이것은 장치-인간 사회에 대한 정보를 표현하는 보편적인 방법이다.

[0035] 우리는 DEGE를 키보드 상의 키(key)로서 예를 들 수 있다: GE는 문자 'A'이고 UD는 아스키 코드(ASCII code) 41H이다. 또는, 우리는 이 개념을 일반화시킬 수 있고 또한 GE에 대해서는 텍스트 아이콘 '이것은 바이올린의 소리입니다' 및 UD는 바이올린을 연주하는 오디오 파일과 같이, 더 세련된 DEGE로 구축할 수 있다. 우리는 스크린 이미지가 키보드 배치와 유사한 DEGE들의 수집인 것으로 고려할 수 있다. ARC에 있어서 스크린은, 전통적인 의미에서 이미지 요소들을 단지 디스플레이하는 대신, DEGE들을 '디스플레이(display)'할 수 있다. 정보 측면에서, 프로세스는 라디오 방송국과 같이 사용자가 선택하도록 다양한 정보들을 제공하기 때문에, 단어 '디스플레이'를 '방송'으로 교체하는 것이 더 적당하다.

[0036] 방송기

[0037] DEGE 방송기를 만들기 위해, 우리는 디스플레이를 재구축할 필요가 있다. 이 변형을 설명하기 위한 단순한 방법은 디스플레이가 광학적 이미지 프레임 및 전기적 데이터 프레임을 교대로 '디스플레이'할 때 디스플레이는 DEGE 방송기가 되는 것이다. 공간 내에 이러한 2 가지 프레임들의 중첩은 DEGE들의 수집을 형성하고 또한 스크린은 사용자가 선택하도록 다양한 DEGE들을 제공할 수 있다(도 3(a)). 디스플레이 행렬은 교대 프레임들(alternate frames)을 생성하기 위해 2 가지 서로 다른 종류들의 신호들, 즉 광학적 이미지(GE)를 생성하기 위

한 하나 및 전기적 데이터(UD)를 위한 다른 하나를 전달할 필요가 있다. ARC에서, 디스플레이 행렬은 인간의 눈들(GE) 그리고 데이터 수신기들(UD)로 정보를 전송하기 위해 공유되는 안테나로서 기능한다. 도 3(b)에 도시된 바와 같이, 우리는 추상적으로 디스플레이 행렬이 아닌, 디스플레이의 모든 구성요소들이 수신된 전기적 신호들을 광학적 이미지(GE)로 변환하기 위해, 전자-광학적 변환(electro-optical conversion, EOC)을 위한 수신기를 형성하는 것으로 고려할 수 있다. 데이터 수신기는 UD의 신호들을 수신하는 것이 필요하고 또한 우리는 장치-내 및 장치-외 전송에 적합하도록 이 데이터 수신기를 유연하게 배치될 수 있다. 사실, 방송기가 2 개의 신호들, EOC 수신기를 위한 하나(수신되어 GE로 변환되는) 및 데이터 수신기를 위한 하나(UD로서 수신되는)을 전송하는, 데이터 통신에서의 배치와 유사하다.

[0038] 이러한 프레임 구조는 단지 설명을 위한 것이다. 디스플레이 행렬에 의해 DEGE를 생성하는 더 상세하고 일반적인 방법은 참고문헌("Action range communication (ARC): A digital architecture for user and device interaction", JOURNAL OF THE SOCIETY FOR INFORMATION DISPLAY, Volume25, Issue8, August 2017, Pages 486-495)를 참조할 수 있다. 참고문헌은 그 전체로서 참조에 의해 여기에 반영된다. 여기서 우리는 DEGE를 생성하기 위한 행렬에 대한 일반적인 가이드라인들을 요약할 수 있다. 행렬은 적절한 신호들이 행렬로 전달될 때만 GE들을 생성할 수 있다. 이것들은 이미지를 생성하기 위해 현재까지 행렬에 적용되었던 디스플레이 신호들이다. '부적절한' 신호들이 이용된다면, 우리는 이미지들을 가질 수 없지만 데이터, 또는 UD를 위한 전기적 데이터 프레임을 전송하기 위한 전기적 신호들을 방사한다. 이러한 '부적절한' 신호들의 예들은 이하와 같다: 1MHz보다 큰 신호 주파수 또는 신호들은 화소들로 진입하지 않고 라인 전극들 등 상에서만 나타난다. 이로써, 우리는 데이터 통신을 위해 UD를 전송하기 위해 이러한 신호들을 이용할 수 있다. 데이터 통신에서 서로 다른 주파수들을 갖는 혼합 신호들과 유사하게, 우리는 이 신호들을 함께 결합하여 행렬로 전송할 수 있다. 도 3(b)의 구조에 따르면, EOC 수신기는 디스플레이 신호들만을 이미지로 변환하고 UD 프레임을 위한 신호들은 폐기할 것이다. 한편, 채널이 설립된 때, 데이터 수신기는 '부적절한' 신호들로부터 UD를 추출할 수 있다. 이러한 방식으로, 디스플레이 행렬은 DEGE를 방송하기 위해 기능한다.

[0039] GE 및 UD가 널이 아닌 DEGE로부터 널인 이들 중 하나로(이미지 또는 데이터), 다양한 DEGE들을 전송하기 위해 방송기를 조정하는 것이 유연하다. 이것은 동적으로 데이터를 전송하기 위한 대역폭을 서로 다른 수신기들, 이 경우에 있어서, EOC 수신기 및 데이터 수신기로 할당하는 데이터 전송기와 유사하다. 행렬이 (GE, 'null') 또는 ('null', UD) 종류들의 DEGE들만 방송하는 극한 상황들에서, 방송기는 디스플레이(TV 또는 모니터) 및 데이터 전송기 각각이 된다. 이러한 극한 경우들 사이에서, 방송기는 브라우징 또는 텍스트 편집과 같은, UDI에 대한 DEGE들을 방송할 수 있다. 우리는 2 개의 수신기들에 대하여 방송 컨텐츠들을 동적으로 할당하는 것에 의해 방송기의 역할을 변경할 수 있다. 하지만, 우리는 컨텐츠를 할당할 때 가이드라인을 따라야 한다. 할당은 GE 프레임들 사이의 현저한 랙(lag)과 같이, 눈들의 시감각에 영향을 주지 않아야 한다. 실제 기준은 시나리오에 따라 달라질 수 있다. 예를 들어, 비디오 컨텐츠는 텍스트에 기반한 컨텐츠보다 더 랙에 민감하고 또한 간단한 UD만 전송할 수 있다.

[0040] AFDT

[0041] DEGE를 전송하는 프로세스는 2 가지 단계들을 포함한다: 선택 및 전송, 즉 먼저 채널을 설립하고 그후 신호들을 전송한다. 우리는 먼저 채널을 설정할 필요가 있다. DEGE를 선택하는 사용자의 행위는 방송기로부터 수신기로 UD를 전송하기 위한 채널을 설립할 것이다. 단거리 신호는 용량성 또는 유도성 커플링에 의해 2 가지의 비접촉 전극들 사이의 공간을 통해 전송할 수 있다. 우리는 이하에서 용량성 커플링(capacitive coupling)에 집중해야 한다. 사용자는 행위에 의해 2 개의 전극들 사이의 거리를 단축할 수 있어 주요한 신호가 시그널링되지 않은 전극 상에서 검출될 수 있다. 다시 말하면, '거리 단축(shrinking distance)'은 선택하는 것을 의미하고 또한 행위에 의해 채널을 설립하는 단계이다. 채널이 설립되기만 하면, 데이터를 전송하는 것은 사람들이 이미 알고 있는 신호 전파를 겪을 것이다. 비교하여, Wi-Fi와 같은 원거리 신호에 기초하는 데이터 전송은 신호 전파만 고려한, 한 단계 프로세스이다. 이것은 2-단계 프로세스의 특별한 경우인데, 이것은 채널이 미리 설립되어 있다. 하지만, 우리는 정보를 전송하는 일반적인 방법으로서 이 2-단계 프로세스로 복귀할 것이다. 이러한 2-단계 프로세스는 실제로 매우 보편적이다. 예를 들어, 지불 또는 출입 제어를 위한 스마트카드를 이용할 때, 우리는 행위에 의해 전송을 활성화시킬 필요가 있다. 본질적으로는, 행위는 전송을 위한 채널을 셋업하는 것이다. 우리는 이러한 2-단계 프로세스를 행위 제공 데이터 전송 또는 AFDT로서 명명한다는 것이 명백하다. AFDT는 ARC에서 DEGE를 전송하는 기능을 한다. 사실, 우리는 전체 DEGE(GE, UD)를 전송할 필요는 없다. 리던던시 때문에 UD만으로도 전체 정보를 나타낼 수 있다. 따라서, UD를 전송하기 위한 채널은 당연히 DEGE를 전송하는 것을 의미한다.

[0042] 도 4에 도시된 바와 같이, 사용자는 거리를 단축시키기 위한 2 가지의 서로 다른 방법들을 가질 수 있다. 하나

는 2 개의 전극들을 가까이 움직이는 것이고(타입-1) 다른 하나는 몸체와 같은 전도체를 통해 신호를 연결하는 것이다(타입-2). 회로 관점에서, 신호는 제1 경우에 있어서는 하나의 커패시터를 통해 그리고 제2 경우에 있어서는 2 개의 직렬 연결된 커패시터들을 통해 결합된다. 타입-2 경우에 있어서, 몸체는 용량성 터치 센싱에 있어서의 역할과 유사하게 전도성 있는 와이어와 같이 행동할 수 있다.

[0043] ARC 메카니즘

[0044] DEGE, 방송기, 및 AFDT에 기초하여, ARC 메카니즘은 이하의 단계들을 포함한다. 방송기는 사용자가 선택하도록 DEGE들을 보내고; DEGE를 선택하는 사용자의 행위는 UD를 수신기로 전송하기 위한 채널을 셋업하고; 그리고 수신기는 UD로부터 사용자의 선택을 학습한다. 수신기의 관점에서, 전체 프로세스가 데이터 전송보다는 더 복잡하지만 그 결과는 데이터 전송과 동일하다. 스크린 상에 보여지는 모든 DEGE들에도 불구하고, 결국, 우리는 선택된 DEGE에 집중하고 선택되지 않은 것들은 폐기할 필요가 있다. 이 메카니즘은 다양한 응용들에서 기능할 수 있다(도 5). UDI의 측면에서, 손가락 터치에 의한 온-스크린 입력은 타입-2 AFDT를 통한 DEGE의 장치-간 전송이고 스타일러스 입력은 타입-1 AFDT이다. SRDT는 타입-1 또는 타입-2 AFDT를 통한 장치-외 전송이다. NFC는 데이터 통신이 이용가능함을 지시하고 또한 위치를 표시하기 위해 사람들이 라벨(NFC 기호)을 GE로서 이용하는 타입-1 AFDT를 통한 SRDT에 속한다. 라벨은 정지된 GE인데, 이것은 쉽게 변할 수 없고 사용자가 암시적으로 전송을 목적으로 한다는 것을 말해준다. (전송될) 데이터와 결합한 라벨은 사용자가 선택하도록 하나의 단일 DEGE를 형성한다. 이 경우에 있어서, 사용자는 2 개의 선택들만 가질 수 있다, 선택하거나 또는 선택하지 않거나. 우리는 선택을 풍부하게 하고 또한 동적으로 변화가능한 선택들을 가지도록 이러한 하나의 고정된 DEGE(고정 목적으로 데이터를 전송하는 데 전용되는 고정된 라벨 및 기어들)를 더 일반적인 DEGE 방송기에 의해 교체할 수 있다. 도 5는 ARC는 UD와 SRDT를 통합하는 방식을 암시한다. 우리는 UDI에 대한 터치 센서 및 SRDT에 대한 데이터 송수신기와 같이, UDI와 SRDT에 대하여 하드웨어를 분리할 필요가 없다. 방송기는 예를 들어, 인코딩에 의해 모두에 대해 기능할 수 있고 또한 특정 수신기만이 UD를 디코딩할 수 있다. 우리는 ARC 메카니즘에서 전통적인 UDI 작동을 포함할 수 있다. 사실, 위치는 장치-내 수신기에서만 인식할 수 있는 UD를 암호화하는 특정 방법이다. 우리는 터치 센서와 같은 기어들에 의해 선택의 위치를 추출할 필요가 없다. 우리는 사용자가 선택하도록 (GE, 위치) DEGE를 방송하기 위해 스크린을 가질 수 있다. 선택된 UD는 장치-내 수신기에서만 의미있는 위치이다. 이것은 SRC 프레임워크 하에서 UDI와 SRDT를 통합하고 또한 장치 구조를 단순화시킨다.

[0045] 본 개시를 설명하기 위해, 우리는 사용자가 웨어러블 장치(WD)를 입는 것(예. 손목밴드)을 고려하고 스크린 장치 상에 UDI를 수행한다. 도 5에 도시된 바와 같이, UDI(손가락 입력) 및 SRDT 모두는 타입-2 AFDT에서 함께, 즉 사용자 관점에서 하나의 선택으로, 발생할 수 있다. 이 경우에 있어서, WD는 사용자 행위로 움직일 수 있고 모든 거리들은 함께 단축시킬 수 있기 때문에 물론 우리는 타입-1 AFDT를 통해 손가락 입력(타입-2 AFDT)을 SRDT와 혼합할 수 있다. 하지만, 타입-2 AFDT를 통한 모두는 설명을 위해 더 쉬울 수 있고 또한 UDI를 수행하기 위해 손에 차는 WD에 의존할 필요가 없다. SRDT가 UDI와 관련없는 데이터를 전송하도록 하는 대신, 우리는 이 2 가지의 전송들은 하나의 목적을 위한 하나의 전송으로서 함께 작동하는 것으로 고려할 수 있다. 이들은 무관한 전송보다는 관련 있다. 예를 들어, 사용자는 UDI에서 서버에 로그인하기 위해 선택할 때, 행위는 SRDT를 환기시킬 수 있고 또한 WD가 그의 사용자명 및 비밀번호를 제공하도록 해준다. 데이터 복잡도에 상관없이, 단지 하나의 행위는 전체 스트링을 입력해야 한다. 사용자 및 WD는, 사용자의 일부와 같은 WD가 UDI에서 사용자 행위와 협력하여 작동할 수 있는, 사이보그를 형성한다. WD의 작동을 처리하는 데 추가의 행위가 필요치 않기 때문에, 장치(WD)는 복잡한 데이터를 기억하거나 또는 계산하는 것과 같이, 정보를 처리하는 데, 간결하고 실제적으로, 사용자를 보조할 수 있다. 사이보그는 20 개의 랜덤 문자들을 갖는 비밀번호를 사용하는 것과 같이, 인간이 관리할 수 있는, 데이터 범위를 넓히고, 또한 정보 보안을 향상시킨다.

[0046] 도 6은 ARC에 기초한 (a) 인간 입력 및 (b) 사이보그 입력 사이의 차이를 보여준다. 도시된 바와 같이, 스크린 장치(3)는 프로세싱 블록(Proc.Block, 43), DEGE 방송기(41), 및 수신기(42)를 포함하는, 모듈, ARC mod.(4)을 통한, ARC 작동을 제공한다. 프로세싱 블록(43)은 작동 시스템(32)으로부터 입력 데이터를 DEGE로 그리고 수신된 데이터를 작동 시스템(32)에 대한 출력 데이터로 처리한다. 사용자는 DEGE를 터치하는 것에 의해 방송기 상에서 DEGE(도 6(a) 및 도 6(b) 각각에서 DEGE2' 및 DEGE2(411))를 선택할 수 있고 방송기와 수신기 사이의 채널(5)(몸체를 통한 타입-2 AFDT)를 셋업할 수 있다. UD2' 및 UD2(4112)의 신호들은 도 6(a)의 수신기(42)로 도 6(b)의 수신기(42)로 각각 채널(5)을 통해 지나갈 수 있다. 이것은 도 6(a)에서 인간에 의한 UD2'의 입력으로 이어진다. 사이보그의 경우에 있어서(도 6(b)), 우리는 선택된 UD2(4112)에서 WD(2)에 대한 명령(COMMAND) 및 데이터(DATA)와 같은, 정보를 포함시키는 것에 의해, 입력을 풍부하게 할 수 있다. WD(2)는 UD2(4112)에 따르면 출력($UD2_{WD}$, 211)을 제공한다. 수신기(42)는 채널(5)로부터 신호들을 결합하고 선택된 UD2(4112)(인간 입력과

동일한 방송기로부터) 및 $UD2_{WD}$(211)(WD(2)로부터) 모두를 수신한다. 스크린 장치(3)는 사이보그로부터의 입력으로서, 2 가지의 정보, UD2(4112) 및 $UD2_{WD}$(211)를 수신한다. 따라서, 사이보그 입력은 전통적인 사용자 입력에서 UD2' 대신 (UD2(4112) + $UD2_{WD}$(211))의 입력으로 이어질 것이다.

[0047] UD2(4112)는 스크린 장치(3) 내에서 전송되고(장치-내 전송) 또한 모든 DEGE들이 구별가능한 한 임의적으로 인코딩될 수 있다. 이것은 우리는 UD2(4112)로서 GE2(4111)의 위치를 이용하기 위해 제한하기보다 UD2(4112)로서 WD(2)에 대한 COMMAND/DATA를 이용할 수 있음을 정당화시킨다. 따라서, UD2(4112)를 통해, 스크린 장치(3)는 WD(2)에 데이터를 저장하도록 요청하거나 또는 WD(2)로부터 저장된 데이터를 요청하는 정보를 보낼 수 있고 WD(2)는 $UD2_{WD}$(211)로서 저장된 데이터를 복귀시킨다.

[0048] ARC 메카니즘을 통한 사이보그 작동의 더 상세사항은 도 7(a) 내지 도 7(c)에 도시되어 있다. 도 7(a)는 스크린 장치(3) 및 WD(2)를 갖는 사용자를 보여준다. 장치(3)은 사용자가 선택하도록 스크린(40)을 방송하는 행렬(41) 및 수신기(42)을 포함한다. 로그인 DEGEi(411)은 사용자의 선택을 보조하기 위해 GEi(4111)을 가지고 또한 선택 행위는 행렬(41), WD(2) 및 수신기(42)를 연결하도록 채널(5)을 설립할 것이다. UDi(4112)는 입력(COMMAND/DATA)으로서 WD(2)로 사용자 입력으로서 5 내지 42를 통해 이동할 수 있다. WD(2)는 UDe(211)를 출력하기 위해 4112에 반응할 수 있다. 도 7(b)는 이 사이보그/ARC 메카니즘에 있어서의 신호 흐름을 보여주는데, DEGE를 선택하는 행위는 방송기(행렬(41)), WD(2), 및 수신기(42)을 연결하기 위해 타입-2 AFDT로 귀결된다. 수신기(42)는 행렬을 둘러싸는 수신 안테나(421) 및 신호 프로세싱(422)를 포함한다. 도 7(c)는 다양한 실시예들에 대한 설명을 단순화시키는, WD(2)의 저장부에 저장된 레코드의 포맷 및 사이보그/ARC 메카니즘과 관련된 WD(2)에 있어서의 기능 블록들을 묘사한다. 도시된 바와 같이, WD(2)는 데이터 입력 및 출력을 위한 송수신기(21), 데이터를 저장하기 위한 저장부(22), 및 데이터 작동의 결과 또는 WD(2)의 상태를 보여주기 위한 지시자(23)를 포함한다. 지시자(23)는, 지시 램프, 전자 라벨, 또는 세그먼트 디스플레이, 수동 행렬 디스플레이, 또는 능동 행렬 디스플레이 등과 같은 다양한 종류의 디스플레이와 같은, 제어가능한 시각적 지시들을 제공할 수 있는 어떠한 수단이든 될 수 있다. WD(2)는 명령들의 세트를 가지고 송수신기(21)를 통한 COMMAND/DATA 입력에 기초하여 작동한다.

[0049] 도 7(a)에 도시된 바와 같이, 사용자 및 WD(2)는 하나의 유닛, 즉, 사이보그(8)로서 취급될 수 있다. 이 사이보그 작동에 있어서, 모든 전송들(사용자 입력 및 WD(2)의 입력 및 출력)이 데이터를 교환하는, 즉 사용자 입력과 데이터 전송을 하나의 행위로 결합하는, 행위에 의해 설립되는 채널(5)을 이용하는 사용자 활동을 단순화시키는 것이 필수적이다. 현재 데이터 통신만이 Wi-Fi 또는 블루투스와 같은, 장치들 사이의 전송을 고려하고 사용자 입력과 통합할 수 없다. 따라서, 전화(phone)를 가진 사람은 사이보그를 형성하지 않는다. 그는 블루투스를 통해 컴퓨터로부터 데이터를 가져오기 위해 전화를 작동시킬 수 있다. 하지만, 그는 전체 프로세스를 하나의 행위에 의해 완료하기보다는, 컴퓨터를 연결하고, 데이터를 검색하고, 데이터를 선택하고 이를 이동시키는, 단계별로 진행할 필요가 있다. 다시 말하면, 현재의 UDI는 하나의 전송으로 병렬로 데이터 전송과 함께 통합되지 않고, 기껏해야, 사용자 입력 및 데이터 전송을 연속으로 이어지고 사용자는 모든 COMMAN/DATA를 제공해야 한다.

[0050] 네트워크 작동과 유사하게, 스크린 장치(3)(WD(2))가 명칭 Alice(31) (Bob(24))을 가지는 것으로 가정하면, 이 명칭은 식별자로서 정보 소스 또는 수신자를 지정하기 위해 이용된다. SD-ID 및 WD-ID는 일반적인 경우들에 있어서 이 명칭들을 나타내는 데 이용된다. 다양한 실시예들을 설명하기 위해, WD(2)는 표 1에 도시된 바와 같이 지시 세트를 가지는 것으로 가정한다. 스크린 장치는 수신자의 명칭 WD-ID(Bob(24))을 어드레싱하는 것에 의해 WD로 정보를 보낼 수 있다. WD는 각각의 레코드가 적어도 3 개의 필드들, 소스 명칭(SN), 데이터 특성(DA), 및 데이터를 포함할 수 있는 레코드로 정보를 저장한다(도 7(c)). SN은 SD-ID 또는 서버의 명칭 등과 같은 이 레코드와 연관된 당사자의 명칭을 지시하고 또한 DA는 USERNAME 또는 PASSWORD 등과 같은 데이터의 특성을 특정한다. 예를 들어, 서버(ServN) 상의 계정의 사용자명(X) 및 비밀번호(Y)는 하나의 레코드 'ServN, USERNAME, X, PASSWORD, Y'로서, 또는 2 개의 분리된 레코드들, 'ServN, USERNAME, X' and 'ServN, PASSWORD, Y'로서 저장될 수 있다. 'GSO' 명령은, 상세화하자면, 크기 s를 갖는 랜덤 수 RN을 생성, 저장, 및 출력할 것이다. 'GET'은 WD 상에 저장된 레코드를 출력할 것이고, 'ST'는 WD 상에 레코드를 저장하고, 'WHO'는 그 명칭, 즉 WD-ID에 대해서 WD에 문의할 것이다. 단순함을 위해, 전송에 있어서 구분자들(delimiters)(전송의 시작 또는 끝)을 생략한다. 우리는 이하에서 설명될 디지털 서명과 같은, 세련된 프로토콜들을 위한 더 많은 명령들을 추가할 수 있지만; 하지만 기본적인 개념은 동일하다. 명령이 이 개시의 초점이 아니라 WD(2)를 위한 사용자 입력 내에 COMMAND/DATA를 임베딩하는 방식 및 이러한 복합적인 프로세스의 이득들이다.

표 1

[0051] WD의 지시 세트

입력	출력	설명
GSO(WD-ID, SN, DA, s)	RN	SN은WD-ID가 크기 s(옵션)를 갖고 랜덤 수 RN을 생성 및 출력하고, DA로서 사용되도록 하여 WD-ID 상에 레코드(SN, DA, RN)로서 저장하도록 요청한다.
GET(WD-ID, SN, DA)	데이터	SN은 WD-ID가 SN과 연관된 레코드를 출력하고 DA로서 이용되도록 요청한다.
ST(WD-ID, SN, DA, data)	---	SN은 WD-ID가 레코드(SN, DA, 데이터)를 기록하도록 요청한다.
ENCRYPT(WD-ID, SN, h1)	Encrypted h1	SN은 WD-ID가 비밀 키에 의해 h1을 암호화하고 또한 그 결괄르 출력하도록 요청한다.
WHO(SN)	WD-ID	SN은 WD가 그 명칭 WD-ID를 출력하도록 요청한다.

[0052] 채널(5)이 길이가 긴 UD의 전송을 지원할 수 있음을 정당화하기 위해, 우리는 채널 존재 기간(즉, 사용자가 몸체를 통해 타입-2 AFDT로서 그의 행위를 유지함)을 방송기 데이터 속도와 비교할 수 있다. UD는 1MHz 주파수 또는 초당 대략 1M 비트 데이터 속도를 갖는 신호들에 의해 전달됨을 가정하는 것은 합리적이다. 사용자의 행위의 시간 크기는 ~msec (10^{-3} 초) 범위 내에 있기 때문에, 사용자의 이목을 끌지 않더라도 하나의 행위에서 수 K비트 데이터를 충분히 전송할 수 있다. 행위와 데이터 속도 사이의 시간 크기 차이는 하나의 행위에서 길이가 긴 정보(UD로서 COMMAND 및 DATA)의 전송을 정당화한다. 우리는 채널 존재 기간을 연장하기 위해 또는 프로세스를 단순화시키기 위해 하나의 프로세스에서 수 개의 DEGE들을 결합할 수 있다. 예를 들어, 우리는 전송이 완료될 때까지 더 긴 데이터를 전송하기 위해 행위를 연장하는 것을 사용자에게 알리기 위해 GE(즉, 다른 DEGE)를 변경할 수 있다. 또는, 제1 DEGE는 사용자 입력을 위해 전용되고 제2 DEGE(동일한 GE지만 다른 UD)는 WD(2)와 데이터를 교환하기 위한 것이다. 이 2 개의 DEGE들은 동일한 위치에서 사용자의 행위 기간 내에서 발생된다. 사실, 시간 크기 차이 및 채널(5)를 연장하는 방식으로 인해, 우리는 단일 전송 뿐만 아니라 스크린 장치(3)과 WD(2) 사이에서 연속된 프로토콜들을 구현할 수 있다. 이것은 2 가지의 장치들이 채널(5)이 존재할 때 복잡한 태스크를 완료하기 위해 대화할 수 있음을 의미한다.

[0053] 우리는 사이보그를 인증하는 상황을 고려하고 2 가지 실시예들을 설명하는데, 첫번째는 사이보그는 스크린 장치 상에 계정을 등록할 것이고 두번째는 생성된 계정에 로그인하는 것이다. WD는 사용자명 또는 비밀번호와 같이 인증을 위한 정보를 제공하는 데 사용자를 보조한다. 우리는 서버에 의해 스크린 장치를 대체하고(즉, 명령 내에서 소스 명 SD-ID로서 서버명 ServN을 사용하고) 사이보그를 인증하기 위해 스크린 장치에 연결된 서버에 대한 실시예들을 적용할 수 있다. 우리는 WD는 계정을 생성하거나 또는 로그인할 때 자동으로 정보를 기억하고 기억된 정보를 제공하도록 사용자와 협력할 수 있는 방식임을 강조한다.

[0054] 실시예 1 - 사이보그 등록

[0055] 등록 동안, 사이보그는 서버 또는 스크린 장치(3) 상에 계정을 생성하고 미래에 로그인하기 위해 정보(로그인 정보)를 '기억'(WD(2) 상에 저장)할 것이다. 중요한 단계는 로그인 정보를 '기억'하는 것이다. WD(2) 상에 로그인 정보를 설정 및 저장하는 방법은 여럿 있다. 사용자는 현재(present)로서 정보를 설정하고 그후 최종 단계에서 WD(2) 상의 모든 정보를 저장(즉, 사용자가 'Create Account" DEGE를 클릭할 때 모든 정보를 저장)할 수 있다. 동일한 프로세스가 주소 등과 같은 다른 정보를 포함하기 위해 적용가능하지만, 우리는 사용자가 이후에 로그인하기 위한 정보, 즉 사용자명 및 비밀번호에만 집중한다. 마지막 행위를 제외한, 모든 사용자 행위들은, 전통적인 UDI 또는 ARC에서 장치-내 전송으로서 입력된다. UD는 스크린 장치만을 위한 것이기 때문에, 우리는 현재의 UDI 메카니즘이 하듯이 DEGE를 나타내기 위해 GE의 위치를 이용(위치로서 DEGE를 인코딩)할 수 있다. 그 결과는 터치 센싱을 위한 기어가 필요없는 것을 제외하고 전통적인 사용자 입력과 동일하다. 하지만, 'Create Account' DEGE의 UD(도 8)는 더 복잡하다. 이 UD는 2 가지 기능들을 달성할 필요가 있다: 스크린 장치(3)에 사용자가 계정을 생성하기 원함을 알리는 것(장치-내) 및 WD(2) 상에 로그인 정보를 저장하는 것(장치-외). 도 8에 도시된 바와 같이, 우리는 GE(4112)로서 아이콘 'Create Account"를 그리고 UD(4111)로서 WD(2)를 위한 COMMAND/DATA를 이용하는 것에 의해 이 DEGE(411)를 구축할 수 있다. 상기에서 언급된 바와 같이, COMMAND/DATA는 스크린 장치(3)에 이를 위해 선택된 것이 단지 DEGE를 인코딩하는 다른 방법임을 알리는 기능을 할 수 있고 스크린 장치(3)는 장치-내 전송으로 인해 그 의미를 이해할 수 있다.

[0056] WD(2) 상에 정보를 저장하기 위해, 우리는 스크린 장치(3) 및 WD(2)가 서로의 명칭을 알지 못하고 2 개의 단계들로 프로세스가 분리됨을 가정한다. 각각의 단계는 이하와 같이 WD(2)를 위한 COMMAND/DATA를 발생시키기 위해 동일한 GE 및 UD를 나타낸다:

[0057] a. 'WHO(Alice)': 스크린 장치(3) 'Alice'는 WD(2)의 명칭을 문의하고 WD(2)로부터 WD-ID(Bob(24))을 얻는다.

[0058] b. 'ST(Bob, Alice, USERNAME, X, PASSWORD, Y): 스크린 장치(3)는 WD(2) 'Bob'에게 스크린 장치(3) 'Alice' 상의 계정의 사용자명(X)와 비밀번호(Y)를 포함하는 레코드를 저장하도록 명령한다.

[0059] 단계 b는 단계 a로부터 정보 WD-ID(Bob(24)) 및 또한 사용자에 의해 설정된 사용자명(X) 및 비밀번호(Y)를 필요로 한다. 도 8에 열거된 바와 같이, 이것은 프로토콜들을 완료하기 위해 동일한 위치에서 2 개의 DEGE들을 이용하는 것에 대응한다. 이러한 방식으로, 사이보그는 인간이 하듯이 계정을 생성하는 스크린 장치에 정보를 주는 행위를 하면서 로그인 정보를 '기억'할 수 있다. 사용자는 정보를 기억하는 것에 관심을 둘 필요가 없기 때문에, 긴 랜덤 스트링들을 이용할 수 있다. 이것은 입력 데이터의 범위를 확장시키고 또한 사이보그 및 ARC에 의한 프로세스에서 행위의 역할을 단순화시키는 방법을 묘사한다.

[0060] 동일한 위치에서의 DEGE들을 통한 모든 프로토콜들을 구현하는 대신, 우리는 다른 위치들에서의 DEGE들로 프로토콜들을 세분할 수 있다. 예를 들어 'WHO' 명령은 하나의 위치에서 하나의 DEGE일 수 있거나, 또는 사용자명 및 비밀번호를 저장하는 것은 서로 다른 위치들의 2 개의 DEGE들에 의해 수행되고 WD(2) 상에 2 개의 레코드들을 생성할 수 있다. 하나의 위치는 선택하는 하나의 행위, 즉 전송 채널을 설립하기 위한 타입-2 AFDT를 필요로 한다. 서로 다른 위치들의 DEGE들로 분할하는 것은 프로세스를 복잡하게 만드는 것처럼 보일 수 있지만 사용자는 프로토콜들의 상세사항들 및 어떠한 정보가 교환되는지를 알 수 있다. 하나의 행위가 이 프로세스에서 복수의 전송들을 유발함은 명백하다: 방송기로부터 수신기 및 WD로 그리고 WD로부터 수신기로. 이들은 행위에 의해 형성되는 일시적인 네트워크(타입-2 AFDT는 방송기, 수신기, 및 WD를 연결함) 상에서 발생하는 전송들이고 하나의 UD에 의해 시작되는 전송들에 의존적이거나 또는 관련된다. GE 및 UD의 리던던시는 이러한 네트워크(GE 상에의 행위)를 형성하고 이러한 전송들(UD에 의한 일련의 전송들의 시작)을 실현하는 데 중요한 역할을 한다.

[0061] 실시예 2 - 사이보그 로그인

[0062] 로그인 세션에 있어서, 사용자가 등록된 계정에 로그인하려고 할 때, 스크린 장치(3)는 WD로부터 데이터를 추출하는 유사한 프로세스에 기초할 수 있다. 도 9에 도시된 바와 같이, 우리는 WD로부터 저장된 레코드를 추출하기 위한 UD로서 명령 'GET(Bob, Alice, USERMANE, PASSWORD)'과 함께 스크린 상에 'Login' DEGE를 생성할 수 있다. 사용자가 이 DEGE를 선택한 때, WD(2)는 저장부 내에서 레코드(Alice, USERNAME, X, PASSWORD, Y)를 찾고 그 레코드를 출력하기 위해 UD를 수신할 것이다.

[0063] 스크린 장치(3)에 연결된 서버 상에 계정을 등록하고 로그인하기 위해 사이보그를 위한 실시예들을 적용할 준비가 되었다. 우리는 서버를 지칭하는 명칭, 소위 ServN에 의한 명령들에서, 스크린 장치(3)의 명칭, Alice(31)를 교체할 수 있다. WD(2)는 서버 상의 계정에 대한 로그인 정보를 기억할 것이고 프로토콜들은 스크린 장치(3)에 의해 데이터를 저장 및 검색하는 것과 동일하다. 이러한 등록 및 로그인 실시예들에 있어서, 사용자는 프로세스를 시작할지 말지 여부만을 결정할 필요가 있고 복잡한 스트링을 기억하거나 또는 문자를 일일이 입력해야 하는 일을 겪지 않을 것이다. 그가 프로세스를 유발시키려고 결정하고 상기의 'Login' DEGE를 선택하기만 하면, WD는 상세한 정보를 제공하고 로그인 프로세스를 완료할 것이다. 사이보그는 정보를 취급하는 데 있어서는 사용자를 능가하고 계정 인증을 위한 사이보그의 적용은 프로세스를 나타내기 위해 몇 가지 기본적인 변화들을 가져온다. 먼저, 계정-생성 행위는 WD에 이를 저장하기 때문에, 사용자는 비밀번호와 같은, 정보를 기억할 필요가 없다. 인간의 관점에서, 이것은 비밀번호를 설정하고 잊어버리는 것과 동일하다. 사용자는 계정을 보호하기 위해 길고 랜덤한(LR), 예. 20 개의 문자들로, 비밀번호를 설정할 수 있다.

[0064] 두번째로, 사람이 LR 비밀번호를 설정하도록 하는 대신, 사용자는 랜덤하게 WD에 의해 생성되는 비밀번호를 가질 수 있다. 우리는 'Gen. Password' DEGE를 구축하기 위해 명령 'GSO(Bob, Alice, PASSWORD)'을 사용할 수 있다(도 10(a)). 사용자가 이 DEGE를 선택한 때, 스크린 장치는 사이보그에 의해 기억되는(WD 상에 저장되는) 비밀번호로서 랜덤 데이터를 수신할 것이다. 사용자는 스트링을 기억하는 것에 신경을 쓸 필요가 없을 뿐만 아니라 (20-문자 비밀번호에 대한 20 개의 행위들 대신) 하나의 행위에 의해 전체 스트링을 입력할 수 있다. 우리는 랜덤 데이터를 생성하면서, 그 크기, 랜덤 데이터 생성기를 위한 시드(seed), 또는 서로 다른 의사랜덤(pseudorandom) 수 생성기들을 선택하는 것과 같이, 더 많은 매개변수들을 포함시키기 위해 'GSO' 명령을 세분

화할 수 있다. 이런 방식으로, 사이보그의 계산 능력은 인간 범위를 넘어 정보를 생성할 수 있다.

[0065] 세번째로, 사용자는 스트링을 기억하는 것이 문제가 안 되기 때문에 비밀번호를 자주 변경할 수 있다. 도 10(b)에 도시된 바와 같이, 'GSO' 명령은 'Logout' DEGE 내에 포함될 수 있어 로그아웃을 위해 이 DEGE를 선택할 때마다 미래를 위해 로그인하기 위한 새로운 비밀번호가 설정될 수 있다.

[0066] 실시예 3 - 태그 인증

[0067] 우리는 사이보그를 인증하기 위해 사용자명/비밀번호가 필요하지 않다. 긴 스트링(태그)은 인증을 위한 신원(identity)으로서 기능할 수 있고 또한 보호의 효율성을 증가시킨다. 스크린 장치/서버는 계정 소유자를 인식하고 당사자가 인증을 위한 태그를 제공하도록 요청하기 위한 신원으로서, 분리된 사용자명 및 비밀번호 대신, 식별 스트링(태그)를 이용할 수 있다. 태그는 일시적으로 (상기에서와 같이 자주 변경될 수 있기 때문에) 그리고 지엽적으로 (특정 스크린 장치/서버만 인식할 수 있음) 효과적이다. 사이보그는 사용자명으로 LR 스트링을 이용할 수 있고 또한 비밀번호와 결합하는 것은 더 긴 LR 스트링과 균등하기 때문에, 우리는 태그를 사용자명-비밀번호의 병합(concatenation)으로 간주할 수 있다. 따라서, 우리는 계정에 접근하기 위한 사이보그를 인증하기 위해, 즉 계정에 로그인하는 방법으로서, 태그를 이용할 수 있다. 태그 인증 프로세스는 상기에서 언급된 등록 및 로그인 프로세스와 동일하다. 등록시, 우리는 태그로서 스트링을 설정하고 또한 미래에 사이보그를 인증하기 위해 WD(2) 상에 저장하기 위해, 즉 사이보그에 태그를 달기 위해, DEGE를 이용할 수 있다. 로그인 세션은 WD(2)로부터 저장된 태그를 검색하기 위해 DEGE를 이용할 것이다.

[0068] 이 태그 인증에서, 우리는 태그로부터 계정을 도출한다. 태그는 특정 응용분야에서 사이보그를 식별하기 위해 기능하는 사이보그의 '지문'과 유사하다. 이것은 서버/스크린 장치 관점에서 사이보그의 신원과 균등하다. 사이보그(8)가 서버 상에 복수의 계정들을 생성할 필요가 있을 때, 우리는 WD(2) 상의 레코드로서 태그를 저장하기 위해 더 많은 정보를 부가할 수 있다. 동일한 서버 명을 갖는 레코드가 이미 존재한다면 일련번호와 같은 새로운 필드가 부가될 수 있다. 따라서, 스크린 장치/서버는 사이보그 뿐만 아니라 그의 특별한 계정까지 확인할 수 있다. 이것은 사용자명과 같은 고정된 정보가 로그인할 때 필요치 않은 사용자명/비밀번호 메카니즘과는 다르다. 고정된 사용자명을 잠그고 공격하는 것은 쉽다. 비교하여, 태그는 일회용 비밀번호와 같이 변경가능하고 교체가능하다. 한편, 우리는 시작시, 사이보그가 실제인지, 가상이거나 또는 가짜인지 컨펌하기 위해 스크린 장치/서버를 위한 식별 시스템(예. public key infrastructure, PKI)이 필요하다. 이 초기 컨펌 후, 태그는 후속하는 인증을 위해 할당된다. 이것은 그룹 내에 개별 당사자 각각에 대하여 데이터베이스를 구축하는 것에 의해 중간자 공격(man-in-the-middle attack)을 피하는 것과 유사하다. PKI와 같은 식별 시스템은 기본적인 데이터베이스로서 행동하여 서로 처음 만났을 때 일 당사자가 다른 당사자의 신원을 점검할 수 있다. 그후, 이들은 미래에 인식을 위해 태그들을 교환할 수 있다.

[0069] 태그에 의한 사용자명/비밀번호의 교체는 2 가지 문제들을 완전히 분리할 수 있다: 계정의 명명 및 계정 소유자를 확인하는 방법. 스크린 장치/서버는 공개적으로 개시하지 않고 사적인 방식으로 계정을 명명할 수 있다. 태그는 소유자를 인식하기 위한 이들에 대한 계정의 가명(alias)이다. 계정은 다른 가명들을 가질 수 있고, 그 각각은 특정 목적 또는 응용을 위한 것일 수 있다. 예를 들어, 이메일 주소는 계정에 메일들을 보내기 위해서만 다른 가명으로 취급될 수 있다. 이것은 인간이 쉽게 기억할 수 있는 짧은 스트링일 수 있다. 또는, 우리는 이메일 주소로서 태그를 이용하고 WD(2)에/로부터 저장/검색하기 위해 유사한 프로세스를 적용할 수 있다. 우리는 이메일 주소를 포함하는 레코드를 상세화하기 위한 특성으로서 'EMAILADD'를 이용할 수 있다. 이 태그는 단지 메일을 보내는 것만을 목적으로 하고 어떻게 계정에 로그인하는지에 대한 정보는 개시하지 않는다. 오늘날, 사용자명으로서 이메일 주소를 이용하는 것은 로그인 정보(사용자명)를 개시할 뿐만 아니라 (이메일 주소로부터) 계정 소유자를 드러내고 비밀번호를 추측하기 쉽게 해준다.

[0070] 서버는 또한 모든 태그들이 동시에 서로 다름을, 또는 충돌 없음(no-collision)을 보장할 필요가 있다. 서버는 충돌 없음 조건을 보장하기 위해 다양한 방법들을 이용할 수 있다. 이것은 새로운 태그가 항상 데이터베이스 내의 태그들과 다름을 보장하기 위해 WD(2) 대신 미래에 로그인하기 위해 태그를 생성할 수 있다. 도 11은 새로운 태그를 새로운 로그인 정보로서 생성하기 위한 서버(6)에 대한 '로그아웃' 흐름을 보여준다. 도시된 바와 같이, 스크린 장치(3)는 채널(5 및 5a)(네트워크 연결)을 통해 WD(2) 및 서버(6)에 각각 연결된다. 'logout' 요청이 수신된 때, 서버(6)는 태그를 생성하고 WD(2) 상에 태그를 저장하기 위한 'ST' 명령을 발행할 수 있다. logout DEGE를 선택하는 것에 의해 설립되는 채널(5)(즉, 사용자가 'logout' DEGE를 선택한 때 데이터 채널)은 도 11에 도시된 바와 같이 2 가지 방향들로 일련의 명령들을 전송한다. WD(2)가 서버 대신 태그를 생성하는 것이 가능하다. 추가적인 프로토콜들은 서버(6)가 충돌이 없음을 컨펌할 때까지 연결들을 통해 WD(2)와 서버(6) 사이에서

반복(loop)하는 것이 필요하다.

[0071] 실시예 4 - 양방향 인증

[0072] WD(2)는 장치-대-장치 인증이기 때문에 역시 스크린 장치/서버를 인증할 수 있다. 이것은 사이보그가 스크린 장치/서버를 인증할 수 있음을 의미한다. 이것은 2 당사자들이 서로를 인증하는 양방향 인증이다.

[0073] 우리는 태그 인증에 기초하여 양방향 인증을 설명할 수 있다. 스크린 장치/서버는 실시예 3에서 언급된 바와 같이 사이보그(8)를 인증할 수 있다. 태그 인증은 양 측들에 상호적이어서 WD(2)(사이보그(8))가 서버/스크린 장치를 인증하기 위해 동일한 방법을 적용할 수 있다. ARC에서, 행위는 전통적인 사용자 입력에서와 같이 일 방향으로 정보를 제공하지 않는다. 이것은 양방향 전송을 위한 채널을 설립한다. 이것은 2 당사자들에 대한 상호성(reciprocity)이 서로를 입증하도록 해준다. 우리는 도 12에 도시된 바와 같은 시나리오를 고려한다. 사용자가 로그인하기 위해 DEGE를 선택한 때, 채널(5 및 5a)은 스크린 장치(3)를 통해 서버(6)와 WD(2)를 연결하기 위해 설립된다. 2 개의 새로운 데이터 특성들, 'IDW' 및 'IDS'는 레코드가 WD(2) 및 서버(6) 각각을 위한 태그인 것을 나타내는 데 이용된다. 언급된 바와 같이, DEGE의 UD를 통해, 서버(6)는 WD(2)에게 인증을 위한 태그(tag-W)를 제공하도록 요청할 수 있다. 유사하게, 동일한 채널을 통해, WD(2)는 서버(6)에게 인증을 위한 태그(tag-S)를 제공하도록 요청할 수 있다. 태그를 수신한 후, WD(2) 및 서버(6)는 수신된 태그와 지엽적으로 저장된 태그를 비교하는 것에 의해 서로 인증할 수 있다. 이들이 일치하면, 신원은 컨펌된다. WD(2)는 증명이 참, 거짓 또는 진행중인지 보여주기 위해 지시자(23)를 이용할 수 있다. 도 12는 이 프로토콜들을 보여준다. 서버(6) 및 WD(2)(사이보그(8))는 등록 동안 각각의 저장부 내에 레코드들을 생성하기 위해 tag-W와 tag-S를 교환할 필요가 있다. 이 프로세스는 실시예 1과 유사하다. 예를 들어, 등록시, 서버(6)는 'ST' 명령에 의해 그 태그(tag-S)를 WD(2) 상에 저장하고 WD(2)가 'GSO' 명령, ST(Bob. ServN, IDS, tag-S) 및 GSO(Bob, ServN, IDW)에 의해 태그를 생성하도록 요청할 수 있다.

[0074] 연결(채널(5 및 5a))에 기초하여, 비대칭 암호화 기술과 같이, 사람들이 장치-장치 인증에 대하여 개발해 왔던 모든 방법들은, 서버-사이보그 인증에 대하여 적용가능하다. 서버(6) 및 사이보그(WD(2))는 공용 키 인프라스트럭쳐(PKI)의 인증 기관(Certificate Authority, CA)에 의해 발행되는 증명서들을 가질 수 있다. 증명서들에 기초하여, 서버 및 사이보그는 첫 대면에 서로를 인증할 수 있다(등록으로서). 이후에, 이들은 공용 키 암호화 기술을 이용하여, 언급한 바와 같이, 랜덤 태그로 변환하거나, 또는 인증을 위한 하이브리드 스킴(hybrid scheme)에 양자를 결합할 수 있다. 이것은, 사이보그들로서, 사람들 및 서버들이 첫 대면에서 서로의 신원을 증명하기 위해, 2 당사자들, 즉 사이보그-사이보그, 사이보그-서버, 및 서버-서버를 위해 기능할 수 있는 것을 포함하는 전역적 PKI를 제안한다. 우리는 WD(2)의 명령 세트를 확장하는 것에 의해 이러한 기능들을 구현할 수 있음이 명백하다. 저장된 데이터를 단순히 검색하는 것에 더하여, WD는 암호화 또는 복호화와 같은 계산에 있어서 사용자를 보조할 수 있다.

[0075] 도 12에 있어서, 스크린 장치(3)는 서버와 사이보그 사이에서 정보를 전달하는 채널 역할을 한다. 이것은 테더링(tethering) 또는 모뎀으로서의 전화(phone-as-modem)와 유사한데, 이것은 휴대폰(mobile phone)이 연결된 컴퓨터와 그 인터넷 연결을 공유하는 것이다. 이것은 장거리(서버(6)와) 및 단거리(사이보그 또는 WD(2)와) 연결들을 중간에서 연결한다. 서버(6) 및 WD(2)(사이보그(8))는 이 테더링 구조를 통해 서로 직접 인증할 수 있다. 이것은 현재 사용자-서버 인증과는 다르다(도 13). 스크린 장치는 비밀번호, 지문, 안면 인식 등에 의해, 즉 일방향 인증을 통해 사용자를 인증하고, 또한 서버와 상호 인증하기 위해 CA에 의해 발행된 증명서를 이용해 PKI에 의존한다. 일방향 인증 때문에, 스크린 장치는 프로세스를 제어하고(사용자 및 서버로부터 모든 필요한 정보를 얻고) 또한 채널로서 양자로 정보를 전달하기보다는 양자를 인증하기 위해 중재자(arbitrator)처럼 행동한다. 본 개시의 또 다른 차이는 인증 프로세스를 수행하기 위해 자식 노드(child node)에 대한 부모 노드(parent node)에 의존한다는 것이다. WD(2)는 도 13의 스크린 장치가 부모 노드로서 사용자를 위한 유사한 프로세스를 수행하는 동안 자식 노드로서 인증 프로세스(사용자를 위한)를 수행한다. 사용자는 그 부모 노드에 대해서는 제어할 수가 없다. 다른 당사자가 스크린 장치를 해킹하고 사용자가 알아챌 수 없는 활동을 양도받을 수 있기 때문에, 이러한 인증을 채택하는 것은 위험성이 있다. 한편, WD(2)는 연결을 위해 사용자에 의존하는 사용자의 자식 노드이다. 위반(breach)은 사용자를 거쳐야 한다.

[0076] 실시예 5 - 사이보그가 메세지에 사인함

[0077] 이 실시예에 있어서, 우리는 사용자가 사이보그로서 직접 디지털 서명(DS)을 수행하는, 즉 사이보그가 그 자신의 서명을 생성하고 다른 이의 서명을 증명하는, 방법을 묘사한다. WD(2)는 증명이 참, 거짓, 또는 진행중인지 보여주기 위해 지시자(23)를 이용할 수 있다. 우리는 공용 키 암호화 기술의 현재 구현과 동일하게, 한 쌍의 키

들, 공용 키(pk) 및 비밀 키(sk)(증명서들)을 당사자에게 할당하는, PKI 및 CA를 가정한다.

[0078] DS는 공용키 암호화(public-key encryption, PKE)에 기초하는데, 이것은 pk에 의해 암호화된 메세지가 복호화를 위해 sk를 필요로 하고 그 역도 마찬가지이다. 따라서, 이 실시예는 PKE에 기초한 다른 프로세스에도 적용가능하다. 예를 들어, 발신자의 신원을 컨펌하기 위해 PKE를 이용하면 sk 소유자로부터 오는 메세지는 부인할 수 없다, 즉 부인 방지(non-repudiation). 도 13에서와 유사하게, 전통적인 DS는 pk-sk 쌍을 보유하고 사용자를 위해 DS를 생성하는 스크린 장치이다. 장치가 사용자 대신 DS를 수행하는 것처럼 보이지만, 실제로는 장치가 DS를 담당한다. 정보를 증명하는 능력의 부족으로, 사용자(인간)은 스크린 장치로부터 정보를 수용만 할 수 있고 어떠한 판단도 할 수 없다. 이것은 또한 부모 노드가 DS를 수행하는 인증에서와 동일한 문제를 가진다. 한편, 사이보그는 사용자, WD(2)의 자식 노드에 기초하여 DS를 수행한다.

[0079] 도 14는 사이보그가 메세지에 사인하는 프로세스를 보여준다. 서버(6a), WD(2a) 및 스크린 장치(3a) 각각은 채널(5 및 5a)을 통해 연결되고 또한 서로 다른 아래첨자들을 가지고 상세화되는 그 자체의 pk-sk 쌍을 가진다. 시나리오는 서버(6a)가 사이보그(8a)가 검토하고 사인하도록 문서(DOC)를 장치(3a)로 보내는 것이다. 전통적인 DS는 사용자가 'sign' 아이콘을 클릭할 때, 스크린 장치가 문서로부터 해쉬를 생성하고, sk_d로 해쉬를 암호화하고(사용자로부터의 서명으로서) 서버로 보낸다. 서버는 pk_d를 이용하여 다시 해쉬로 서명을 복호화하고 DOC로부터 지역적으로 생성된 해쉬와 비교할 수 있다. 양자가 일치하면, 사용자는 DOC에 서명한다. 도 14에 도시된 바와 같이, WD(2a)는 스크린 장치(3a) 대신 서명을 생성, 즉, WD(2a)로 해쉬를 암호화하는 작동을 이동시킨다. 해쉬가 sk_d (스크린 장치(3a)) 대신 sk_c (WD(2a))에 의해 암호화되기 때문에, 이것은 WD(2a), 사용자의 자식 노드에 의해 서명되는 서명인데, 이것은 사용자가 능동적으로 이를 위해 입력을 제공해야만 한다. 이것은 사용자에 의해 제공되는 것과 같이 서명을 간주하는 것을 정당화한다. 사용자에게, 이것은 행위에 의해 문서에 서명하는 것과 유사하다. 프로세스는 이하와 같다. 스크린 장치(3a)는 UD로서 명령 ENCRYPT (Bob, ServN, hash) 으로 WD(2a)가 DEGE를 통해 해쉬를 암호화하도록 요청할 수 있다. WD(2a)는 sk_c에 의해 암호화된 해쉬를 스크린 장치(3a)로 그후에 서버(a)로 출력한다. 그후, 서버(6a)는 서명으로부터 해쉬를 추출하기 위해 pk_c를 이용하고 또한 이 해쉬를 서버(6a)에 의해 DOC로부터 생성되는 해쉬와 비교한다. 양자가 일치하면, 사용자는 DOC에 서명한다. 유사한 방식으로, 사이보그는 문서가 서버에 의해 발행되었는지, 즉 서버의 서명을 증명하기 위해 증명할 수 있다. 이 경우에 있어서, 서버(6a)는 그 sk_s 및 pk_c에 의해 연속적으로 서명으로서 해쉬를 암호화하고 문서와 함께 스크린 장치(3a)로 보낼 수 있다. 스크린 장치(3a)는 이 암호화된 해쉬를 그 자체에 의해 생성되는 암호화되지 않은 해쉬와 함께 WD(2a)로 보낸다. WD(2a)는 서버(6a)에 의해 생성되는 해쉬를 얻기 위해 sk_c 및 pk_s 이용에 의해 연속적으로 암호화된 해쉬를 복호화할 수 있다. WD(2a)는 서버(6a)에 의해 그리고 스크린 장치(3a)에 의해 생성되는, 이 2 가지 해쉬들을 비교할 수 있다. 2 개가 일치하면, DOC는 서버(6a)로부터 온 것이다. 이것은 WD(2a)에서 새로운 명령을 필요로 하고, 실제로, 모든 프로토콜들은 'SIGN'과 같이 하나의 명령으로 통합될 수 있다. 'SIGN'은 먼저 DOC가 서버(6a)로부터 온 것인지 점검하고 이것이 컨펌될 때에만 서명을 제공할 것이다.

[0080] 이 DS 프로세스는 사이보그에 의해 인간 계산 능력을 확장시키는 일 예이다. 또한 인증과 유사하게, pk-sk 쌍은 첫 대면에서만, 즉 서버(6a)와 사이보그(8a)가 처음으로 만날 때 필요하다. 이후에, 이들은 그후의 암호화를 위해 (서버와 사이보그 사이에서만 효과적인) 태그들 또는 pk-sk 쌍을 교환할 수 있다. 나아가, 서버 및 사이보그는 서로를 인증하기 위해 서명에 기초할 수 있다. 이들은 (로그아웃과 같이) 떠나기(leave) 전에 스트링을 교환하고 그후, 다음 번에, 인식(서로에 로그인하는 것과 같이)을 위한 서명으로서 (암호화 해쉬 함수를 통해) 스트링의 해쉬를 보낼 수 있다. 수신자는 서명이 동일한 함수를 통한 스트링의 변환의 결과와 일치하는지 증명할 수 있다. 이것은 서명에 기반한 인증을 설립한다.

[0081] 실시예-6 가상 장치 상호작용

[0082] 도 14에서, 스크린 장치(3a)는 2 가지 역할들을 한다: 정보의 (서버(6a)와 WD(2a) 사이) 전달 및 (사이보그와 상호작용하기 위한 해쉬 또는 DEGE들과 같이) 정보 생성. 이 기능들은 작동 시스템(OS)(도 6(b))의 32) 하에서 중앙집중화되는 데 이용된다. 이 중앙집중화된 구조는, 도 14와 같이, 작동 시스템에서의 누출 또는 버그가 서버(6a)와 WD(2a) 사이의 정보의 유효성(effectiveness)에 영향을 줄 수 있기 때문에, 작동의 강건함(robustness)을 위협한다. 사용자 또는 사이보그와 상호작용하기 위해, 스크린 장치(사실은 OS)는 서버(6a)로부터 정보를 복호화하고 이미지 또는 GE로 변환할 필요가 있다. 정보는 목적지에 도달하기 전에 복호화되어 잠재적으로 조작될 수 있다. OS의 무결성(integrity)이 보장되지 않는 것을 고려하면 상황은 더 나쁘다; 하지만, 이것은 무결성이 기대치(expectation)이며 현재로서는 달성가능하지 않음을 암시한다.

[0083] 이 실시예에 있어서, 우리는 OS로부터 사용자/사이보그와 상호작용하기 위한 기능들을 분리하고 이러한 기능들을 재구성가능한 ARC 송수신기 모듈, Re-ARC mod. (4b) 내에 구현한다(도 15(a)). 이 기능들을 DEGE를 생성하고 수신된 UD를 처리하는 것을 포함한다. 재구성가능한(reconfigurable)은 이 송수신기 모듈이 다양한 소스들로부터 입력을 수신하고(도 6(b)에 도시된 ARC mod.(4)로서 OS(32)로부터뿐만 아니라) 또한 사용자/사이보그와 상호작용하기 위해 DEGE로 변환할 수 있음을 의미한다. 우리는 소스 및 Re-ARC mod.(4b)를, 함께, 스크린 장치(3) 내의 ARC mod.(4)로 입력을 제공하는 OS(2)와 유사한, 가상 장치로서 간주할 수 있다(도 6(b)). 이것은 OS가 전통적인 장치에서 모든 정보를 제어하도록 하는 것보다 더 안전하다. Re-ARC mod.(4b)는 계속해서 갱신할 필요가 없는, 단순한 기능들을 가진다. 이것은 사용자/사이보그를 위한 DEGE들로서 출력하기 위해서만 그 입력 데이터를 처리할 것이다. 우리는 OS에 의존하지 않으면서 데이터를 복호화하기 위해 Re-ARC mod.(4b)를 더 가질 수 있다. 도 15(a)에 도시된 바와 같이, Re-ARC mod.(4b)는 Pro.Block(43b), 행렬(41) 및 수신기(42)를 포함한다. Pro.Block(43b)은, 입력 데이터를 DEGE로 처리하고 행렬(41)로 전달하는, DEGE Pro.Block(431b), 수신기(42)로부터 데이터를 처리하는, Rec.Pro.Block(432b), 저장부(433b), 및 입력 소스들 및 출력 데이터를 선택하는 Sel-M block(434b)를 포함한다. 도시된 바와 같이, 431b로, IN으로부터(433b), 및 P1으로부터(즉, 432b로부터) 입력을 제공할 수 있는, 3 가지 서로 다른 소스들이 있다. 434b는 Re-ARC mod.(4b)의 출력, OUT이 되도록, 또는 P1을 통해 431b의 입력이 되도록, 432b로부터 데이터를 설정할 수 있다. 434b는 431b로의 입력으로서 서로 다른 소스들을 동적으로 선택할 수 있다. 예를 들어, 잠시동안 어떠한 소스들로부터도 데이터를 수신하지 않은 후(1분 후 절전을 위한 화면 잠금과 같이) 또는 처음에 전원을 켠 후, 434b는 화면 잠금(screen lock) 또는 전원을 켰을 때 초기 인증 또는 하이버네이션으로부터 복귀하기 위한 로그인 화면(431b)로의 입력으로서 433b를 선택할 수 있다. 433b로부터의 데이터는 IN 또는 432b를 또는 양자를 431b로의 입력으로 선택하는 것과 같이, 서로 다른 소스들로 절환하기 위한 사용자/사이보그를 인증하는 DEGE들을 포함할 수 있다. 다시 말하면, 434b는 432b로부터의 데이터, 즉 수신기(42)를 통한 사이보그로부터의 데이터에 따라 소스들을 선택할 수 있다. 따라서, 434b에 따라, 431b는 이 소스들 중 하나 또는 그 이상으로부터 입력을 가질 수 있다. 도 15(b) 내지 도 15(d)는 434b가 431b로의 입력으로서 이 소스들 중 하나를 선택할 때 Re-ARC mod.(4b)의 작동 모드를 보여준다. 복수의 소스들이 431b로의 입력으로서 선택된 때, 우리는 사용자/사이보그와 더 복잡한 상호작용들을 가질 수 있다; 하지만 기본적인 원리는 하나의 소스 경우와 동일하다.

[0084] 도 15(b)는 434b가 431b로의 입력 소스로서 IN을 선택하고 432b의 출력이 OUT에 연결되는 정상 모드 작동을 보여준다. 이것은 OS(32b 및 4b)가 사용자/사이보그와 상호작용하기 위해 협력하는 스크린 장치(3b)의 작동에 대응한다. 도 15(c)는 434b가 431b로의 입력으로서 P1으로의 432b의 출력을 설정하는 가상 장치 모드(1)를 보여준다. 이 모드에서, WD(2b)는DEGE들로 변환하기 위해 Re-RC mod.(4b)에 대해 데이터를 제공하는 소스로서 행동한다. DEGE가 선택된 때, UD는 WD(2b)로 복귀할 것이다. 이것은 가상 장치(점선으로 둘러싸인 4b 및 2b)의 장치-내 전송인데, 사용자는 가상 장치에 입력을 제공한다. WD(2b)는 DEGE를 생성하거나 또는 화면을 새로고침(refreshing)하기 위해 43b로 데이터 전송을 계속할 필요가 없다. 43b는 433b에서 데이터를 절약하고 그것만으로 화면을 새로고침할 수 있다. 이 모드에서, 사용자는 스크린 장치(3b)를 통해서조차 WD(2b) 상에서 데이터를 안전하게 유지할 수 있다. 도 15(d)에서, 434b는 431b에 대하여 데이터를 제공하기 위해 433b를 소스로서 설정하고 43b 내에서 432b의 출력을 유지한다. 이것은 4b는 DEGE를 생성하기 위해 43b가 그 저장부(433b) 내의 데이터를 이용하는 사용자/사이보그와 상호작용하기 위해 가상 장치로서 행동하고 또한 선택된 UD를 수신하는 것을 의미한다. 이 가상 장치 모드(2)에서, 433b의 데이터는 인증을 위한 스크린일 수 있고 43b는 사용자/사이보그가 로그인하도록 요청하기 위해 화면 잠금으로서 행동한다. 이것은 인증되지 않은 사용자/사이보그가 3b의 네트워크 연결들 또는 억세스(32b)하는 것을 금지한다. 우리는 전원이 켜지거나 또는 하이버네이션으로부터 복귀할 때 이 모드를 434b의 디폴트 모드로서 가질 수 있다(즉, 434b는 잠시동안 소스들로부터 데이터를 수신하지 않으면 이 디폴트 모드로 진입함). 이 경우에 있어서, 사이보그 작동은 전통적인 UDI보다 더 낫다. 사이보그에 의한 선택은, 단지 스크린을 터치하고, 이전의 실시예에서 언급된 바와 같이 사이보그 인증을 유발시킬 수 있다. 동일한 행위는 사용자가 일일이 문자를 입력하도록 하는 대신 WD(2b)로부터 전체 로그인 정보를 제공할 수 있다. 434b가 로그인하기 위해 바른 스트링을 수신한 때, 이것은 정상 장치 모드 또는 가상 장치 모드(1) 등과 같이, 사용자/사이보그의 요청에 종속하는 431b의 입력을 재구성할 수 있다.

[0085] 우리는 Re-ARC mod.로의 정보 소스로서 네트워크 상의 스크린 장치에 연결하는 서버를 가지도록 이 가상 장치 개념을 확장할 수 있다. 도 16(a) 내지 도 16(c)에 도시된 바와 같이, Re-ARC mod.(4c), WD(2c), 서버(6c), 및 스크린 장치(3c)의 작동 시스템(32c) 각각은 동일한 PKI로부터 그 자체의 공용 및 비밀 키 쌍, 즉 74, 73, 71, 및 72를 각각 가진다. 우리는 74에 기초한 PKE 작동들을 수행하기 위해 4c를 위한 다양한 구조들을 가질 수 있다. 4c는 복호화 및 암호화 작동들을 수행하기 위해 43c 내부 또는 외부에서, 독립적인 블록들을 가질 수 있다.

복호화 (암호화) 블록은 434c(로부터 출력 후)로의 입력 전에 또는 431c로의 입력 바로 전에(432c로부터 출력 바로 후에) 위치할 수 있다. 또는, 우리는 도 16(a)에서 고려된 바와 같이 431c(432c) 내부에서 실행되는 복호화(암호화) 작동을 가질 수 있다. PKE에 기초하여, 서버(6c)는 DEGE로 변환하기 위해서만 데이터를 4c로 안전하게 전송하여 사용자/사이보그와 상호작용할 수 있다. 4c는 또한 데이터를 암호화하고 6c로 안전하게 출력하기 위해 PKE를 이용할 수 있다. 스크린 장치(3c)는 PKI로부터, OS(32c) 및 Re-ARC mod.(4c)에 각각 속하는, 적어도 2 개의 키 쌍들(72 및 74)을 가지고, 하나(74)는 사용자/사이보그 상호작용에 전용된다. 4c의 보안은 이것이 단순한 함수를 가지고 데이터가 DEGE로서 보내질 수 있기 때문에 전체 스크린 장치(3c)보다 더 쉽게 보장된다. 이것은 서버(6c)와 Re-ARC mod.(4c) 사이의 데이터 보안을 보장한다. 우리는 사용자/사이보그와 상호작용하기 위해 6c 및 4c가 가상 장치(93)를 형성하는 것으로 간주할 수 있다(도 16(c)). 이와 유사하게, WD(2c)는 DS의 실시예에서 기술된 바와 같이 6c와 데이터를 교환하기 위해 PKE를 수행할 수 있다.

[0086] 실시예 7 - 파일 암호화

[0087] 데이터를 암호화하는 것은 정보 프라이버시를 보호할 수 있다; 하지만, 사용자는 복호화를 위해 매번 전체 스트링의 종류 및 비밀번호들을 기억해야 한다. 더 긴 비밀번호는 보호를 증가시킬 수 있지만, 입력 프로세스를 복잡하게 하고 기억하는 것이 어렵다. 우리는 행위가 하나의 문자가 아니라 복수의 문자들을 전송하기 위한 채널을 제공하기 때문에 이 문제들을 해결하기 위해 사이보그 개념을 채택할 수 있다. WD(2)는 암호화를 위한 랜덤 키를 생성하여 WD(2) 상의 하나의 레코드로서 파일명 및 키를 저장할 수 있다. 파일을 여는 것은 WD(2)가 복호화를 위한 파일명에 대응하는 키를 제공하도록 요청하는 것을 의미한다. 이 프로토콜들은 계정을 등록하는 동안 비밀번호를 설정하고 이를 로그인하기 위해 검색하는 것과 유사하다. 도 17에 도시된 바와 같이, 스크린 장치(3)는 복호화를 위해 WD(2)로부터 랜덤 수 RN(211a)를 요청하기 위해 'GSO" 명령을 포함하는 UD(4112a)를 갖는 DEGE(411a)를 포함하는 스크린(40a)을 디스플레이한다. 411a의 GE는 명확하고 간결한 방식으로 이 활동들을 설명하여 사용자가 이 DEGE의 선택 결과를 예상할 수 있어야 한다. 도 18은 암호화된 파일을 열기 위한(복호화) 프로토콜들을 보여준다. 스크린 장치(3)는 'GET' 명령에 의해 WD(2)로부터 RN(211a)을 요청하기 위해 2 가지의 다른 방법들로 스크린(40b)을 디스플레이할 수 있다. 도 17에서와 같이, DEGE(411b)는 선택되었을 때 암호화된 파일을 열기 위해 GE로서 아이콘 'Open' 아이콘을, 또는 더블 클릭되었을 때 암호화된 파일을 열기 위해 GE로서 파일 아이콘을 이용할 수 있다. 후자는 더블 클릭의 장치-내 입력 후 'GET' 명령으로 UD(4112b)를 출력하는 것을 의미한다. 모든 경우들은 이하의 단계들을 갖는 파일을 여는 프로시져를 생성한다: 키의 요청, 복호화, 및 파일 열기.

[0088] 실시예 8 - 연속적인 인증 및 입력자 인식

[0089] 비밀번호, 지문, 또는 안면 인식과 같은, 현재의 모든 인증들은, 인증 프로세스 동안 사용자의 신원을 컨펌만 할 수 있다. 프로세스 후, 통과되거나, 실패하거나, 또는 아직 인증되지 않은 당사자를 구별할 수 없다. 다시 말하면, 사용자는 인증 후 구별되지 못한다. 이 방법들은 인증된 사람들을 구별하거나 또는 태그하는 메카니즘을 가지고 있지 않기 때문에 엄격한 의미에서 이후의 상호작용 또는 입력이 인증된 사용자로부터 비롯되었음을 보장할 수 없다.

[0090] 태그 메카니즘 없이, 인증의 효과는 순간적으로만 유효하고 지속될 수 없다. 이에 더하여, 태깅 또한 장치가 서로 다른 사람들로부터 입력을 인식할 수 있음을 의미한다. 이것은 입력자 인식을 위한 기능이다. 현재 개인용 장치는 이 기능을 가지고 있지 않은데 그 이유는 '개인용' 장치이기 때문이다. 사용자와 상호작용하는 것과 달리, 정보에 기초하여 그 원천(소스)을 인식하는 것은 장치-장치 상호작용 에서 잘 성립된 메카니즘이다(예. 기지국은 각 핸드셋으로부터의 입력을 인식한다). 따라서, 우리는 사이보그를 지속적으로 인증하거나 또는 서로 다른 사이보그들로부터의 입력을 인식하기 위해 WD(2)를 이용할 수 있다. 이 경우에 있어서, 이것은 사용자(WD(2))의 자식 노드이고, 사용자를 인증하기 위한, 사용자(핸드폰과 같은)의 부모 노드는 아니다. (정보 소스를 확인하기 위해 PKE를 이용하는 것과 같이) 데이터 통신으로부터 전체 메카니즘을 채택하는 대신, 우리는 이 연속적인 인증 및 입력자 인식을 위해 더 간단한 메카니즘을 이용할 수 있다.

[0091] 스크린 장치가 사이보그를 인증하는 간단한 방법은 매 DEGE에 대하여 UD 내에 'WHO' 명령을 추가하는 것이다. 예를 들어(도 19), 스크린 장치(3) 상에 보여지는 스크린(40c)은 문자 'A'(DEGE(411c))를 가진다. 그 UD(4112c)는 문자 'A'의 아스키 코드 41H 및 'WHO' 명령을 포함한다. 따라서, 사용자가 'A'를 선택할 때, WD(2)는 'WHO' 명령에 따라 그 명칭 'Bob'을 출력할 것이고 스크린 장치(3)의 수신기(42)는 아스키 코드 및 'Bob'을 수신할 것이다. 스크린 장치(3)는 Bob이 41H를 입력하는 것으로 결론지을 수 있다.

[0092] 우리는 'WHO' 명령에 의해 사이보그의 신원을 문의하는 것이 아닌 메카니즘들을 가질 수 있다. 모든 사이보그들

은 먼저 스크린 장치 상에서 상호작용하기 전에 등록될 수 있다. 모든 등록된 사이보그들은 함께 상호작용하는 그룹을 형성한다. 등록 동안, 스크린 장치는 누가 입력을 제공하는지 인식하기 위해, 즉 입력자를 인식하기 위해 각각의 그룹 멤버들에 대하여 태그를 할당할 수 있다. WD는 이 태그를 저장하고 스크린 장치로부터의 요청시 이를 제공할 수 있다. 스크린 장치는 매 DEGE의 UD 내에 태그를 요청하기 위한 명령들을 추가할 수 있다. 이것은 스크린 장치가 인증된 사람으로부터의 입력들만을 수용하고(지속적인 인증) 서로로부터의 입력을 인식하는 것에 의해 함께 복수의 사람들과 상호작용할 수 있도록(입력자 인식) 해준다.

[0093] 예를 들어(도 20), WD(2d)는 2131d, 2132d, 및 2133d에 의해, 데이터(UD)를 검출한 때 에코 신호(ES)를 출력하는, 에코 모드에서 작동할 수 있다. 이 에코 모드는 명령 "ECHO-ON(t_{lag})" 및 "ECHO-OFF" 각각에 의해 활성화되거나 또는 비활성화될 수 있다. "t_{lag}"는 에코 모드가 활성화되는 시간 매개변수이다. 이것은 검출된 UD와 ES 사이의 시간 랙을 나타낸다. 따라서 등록 동안, 스크린 장치는 이 에코 모드를 활성화시키고 각각의 인증된 WD t_{lag}를 사이보그를 구별하기 위한 태그로서 할당할 수 있다.

[0094] 도 21은 함께 스크린 장치(3) 상에서 상호작용하는 3 개의 사이보그들(81, 82, 및 83)에 대한 시나리오를 보여준다. 등록 동안, 스크린 장치(3)는 등록을 위해 DEGE 내에 "ECHO-ON(t_{lag})" 명령을 포함하고 또한 각각의 사이보그에 대하여 서로 다른 t_{lag}를 할당할 수 있다. 도시된 바와 같이, 2 개의 UD들은 모든 t_{lag}를 수용하기 위해 적절한 시간 분리(time separation)를 가질 수 있다. 이것은 모든 사이보그들이 동일한 UD를 선택하는 것을 허용한다. 장치-내 전송 때문에, 우리는 전송을 단순화시키기 위해 n-비트 데이터에 의해 모든 DEGE를 인코딩할 수 있다(즉, UD는 n-비트 데이터이다). 예를 들어, 화면 상에 255 개 이하의 DEGE들이 있을 수 있어 8 비트 데이터로 모든 DEGE들을 표현하기에 충분한 것으로 가정한다. 태그(t_{lag})를 할당하는 것에 의해, 각각의 사이보그는 추가적인 비트를 나타낸다. 도 21에서 고려되는 3 개의 사이보그 시나리오에 있어서, 입력을 나타내기 위해 11 비트들: 스크린 상의 DEGE를 나타내는 처음 8 비트들 및 입력자를 나타내는 마지막 3 비트들을 사용하는 것은 동일하다. 도시된 바와 같이, 스크린 장치(3)가 데이터 UDI+'101'을 수신한 때, 이것은 사이보그1 및 사이보그3가 입력으로서 DEGE1을 각각 선택한 것을 의미한다. 이것은 또한 스크린 장치가 매 입력을 지속적으로 인증할 수 있음을 암시한다.

[0095] 도시된 바와 같이, 이 방법은 지문 인증 및 터치 센싱을 결합하는 것과 같이, 사이보그들이 하나의 DEGE를 동시에 선택하는 것을 허용하는데, 이것은 현재의 방법들에서는 가능하지 않다. 하나의 행위에 의해 활성화되는 장치-내 및 장치-외 전송들은 이 프로세스에서 협력적으로 작동할 수 있고, 장치-외 전송(WD(2d)를 갖는 스크린 장치)는 그 소스를 확인하기 위해(즉, 입력 정보를 선택하는 전송 채널 또는 경로를 특정하기 위해) 장치-내 전송(스크린 장치(3)로의 사용자 입력)을 보조한다. 이 에코 모드 작동에 기초하여, 우리는 입력 프로세스에서 사용자를 인식하기 위해, 암호화 기술과 같이, 복잡한 스킴을 채택할 필요가 없다. 이것은 실제로 입력자 인식을 구현할 수 있다. 우리는 스크린 장치로의 매 입력을 증명하는 것에 의해 데이터 보안을 향상시킬 수 있고 또한 인증된 사이보그만이 장치를 작동시킬 수 있다. 이것은 방어 또는 금융 응용분야들을 위한 서버들과 같이, 민감한 데이터를 갖는 시스템에 대하여 엄격한 보호를 제공한다. 우리는 매 입력을 그 제공자와 확고히 연관시킬 수 있고 그 결과는 부인될 수 없다(부인방지). 이에 더하여, 입력자 인식은 하나의 입력자로부터 많은 입력자들로 장치 입력 시나리오를 확장시킨다. 스크린 장치는 개인용 장치에 한정되지 않는다. 이것은 실제 데스크탑처럼 기능하거나 또는 사이보그들 간의 상호작용들을 수행하기 위한 중재자, 심판, 또는 딜러로 행동할 수 있다. 우리는 문서 또는 아이디어 토론, 게임, 투표, 또는 계약 체결 등과 같이, 테이블-크기 스크린 장치를 둘러싸는 사이보그들에 대하여 그룹 상호작용들을 가능하게 할 수 있다.

[0096] 결론적으로, 우리는 사이보그로서, 기억, 계산, 또는 디지털 데이터의 출력과 같이, 디지털 정보를 취급하는 데 있어서의 인간 능력을 확장시키는 것에 의해 안전한 시스템을 개시한다. 사이보그는, 사용자의 부모 노드 대신, 자식 노드인 장치를 통해 이 기능들을 구현한다. 사용자의 행위는 2 개의 장치들을 연결하는 채널을 설립하는 것이다. 우리는 추가적인 사용자 행위들 없이 입력을 보조하기 위해 데이터 전송들에 동시에 동반되는 사용자 입력을 가질 수 있다. 사용자는 사용자에 의해 생성된 것처럼 복잡하고, 긴, 랜덤 스트링들을 이용할 수 있다. 이것은 인증 프로세스를 단순화시킬 뿐만 아니라 더 효과적으로 만들어준다. 우리는 사이보그를 인식하는 장치(인증 및 입력자 인식), 서버를 인식하는 사이보그(양방향 인증), 및 보호 프라이버시(파일 암호화)와 같은 상호작용들을 개시한다. 이에 더하여, 우리는 또한 다양한 가상 장치 모드 작동들을 구현하기 위한 재구성가능한 ARC 모듈(Re-ARC mod.)를 개시한다. 사용자/사이보그는 로컬 스크린 장치를 통해 연결되는, 원격 서버와 안전하게 상호작용할 수 있다. 이것은 암호화 및 복호화 프로세스들을 취급하기 위해 지속적으로 갱신이 필요한, 불완

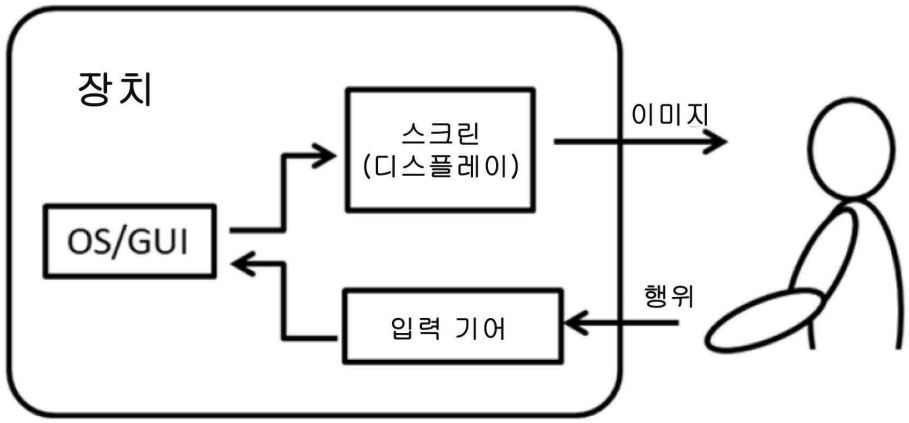
전한 작동 시스템에 의존하는 것을 막아준다.

[0097] 이로써 설명된 개시는 많은 방법들로 변경될 수 있음이 명백하다. 이러한 변경들은 본 개시의 사상 및 범위를 벗어나는 것으로 간주되지 않고, 당업자에게 명백할 수 있는 모든 이러한 변형들은 이하의 청구항들의 범위 내에 포함되어야 한다.

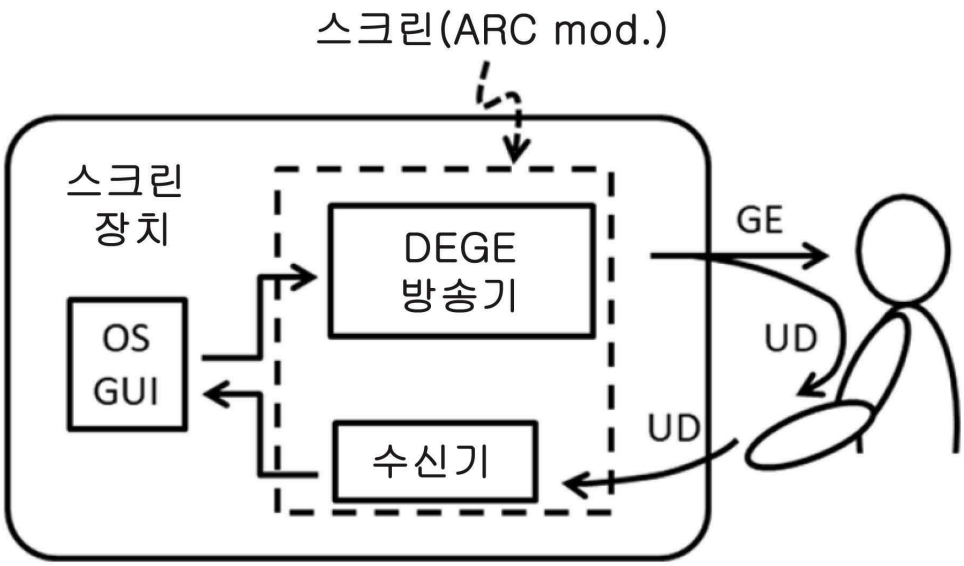
[0098] 본 개시는 특정 실시예들을 참조하여 설명되었지만, 이 설명은 한정하려는 의미로 해석되어서는 안된다. 개시된 실시예들의 다양한 변형들, 뿐만 아니라 다른 대안적인 실시예들은 당업자에게 명백할 것이다. 따라서, 첨부된 청구항들은 본 개시의 진정한 범위 내에 포함되는 모든 변형들을 커버하는 것으로 고려된다.

도면

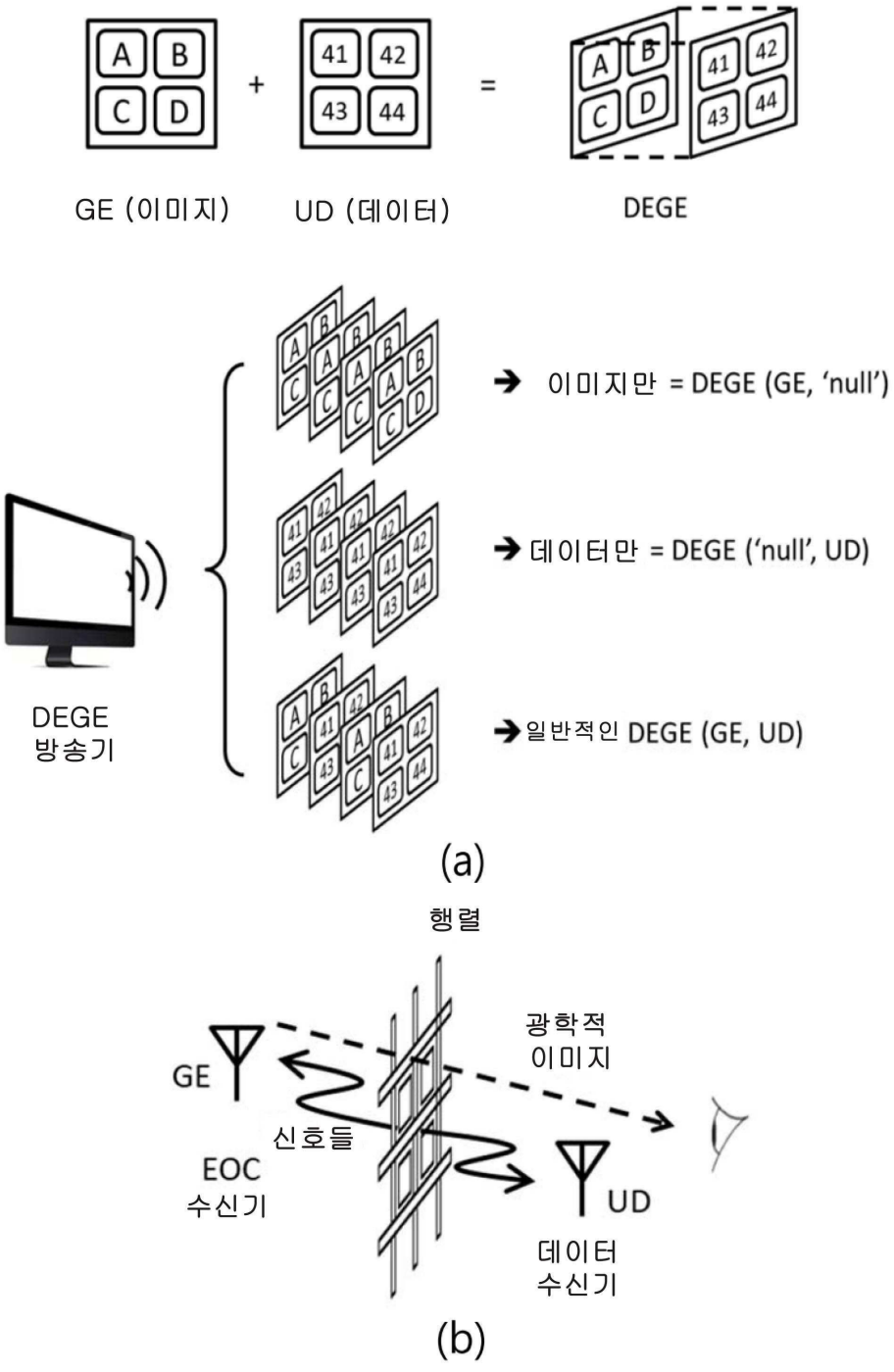
도면1



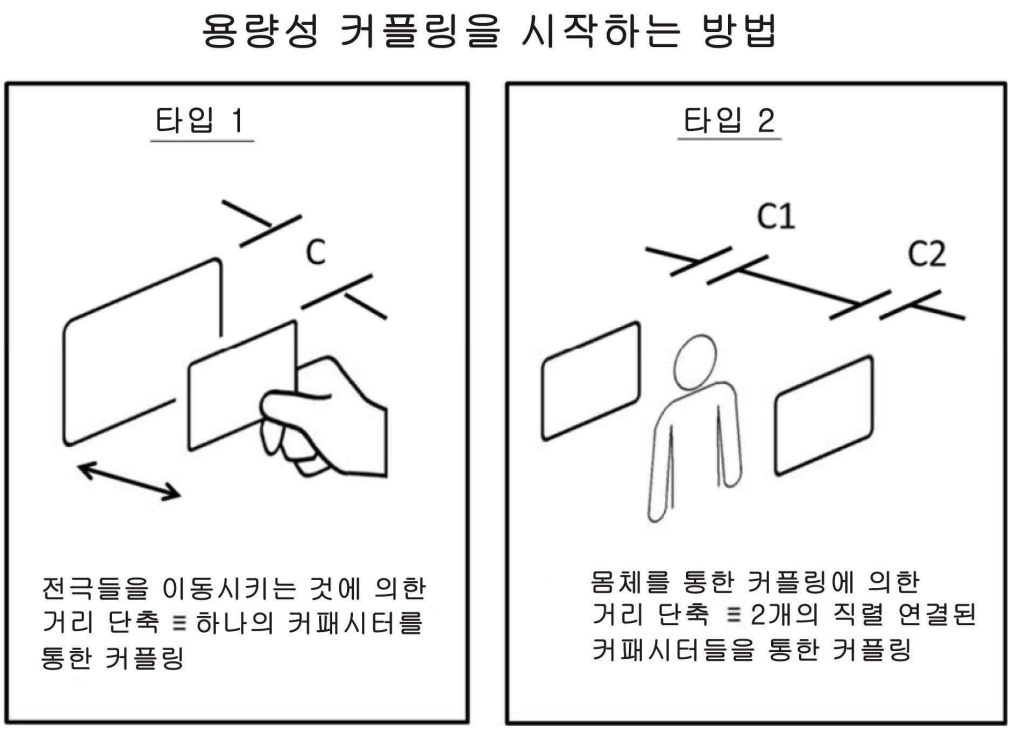
도면2



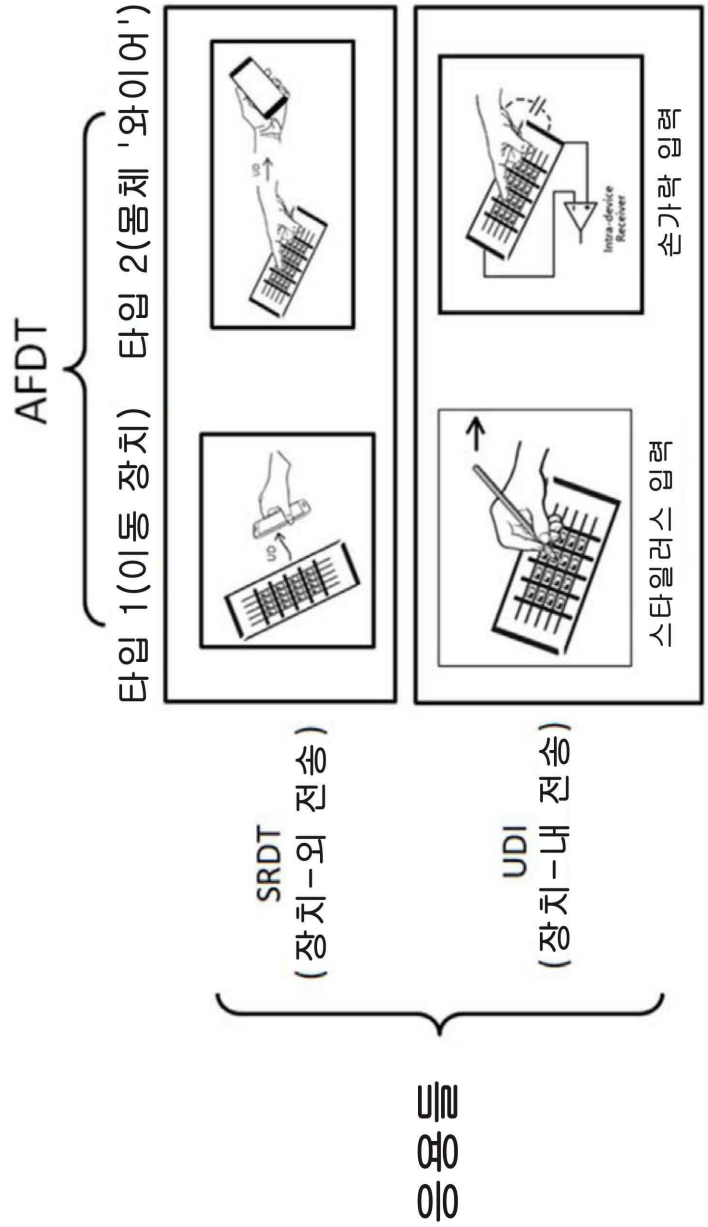
도면3


A
B
C
D
41
42
43
44
GE (이미지)
UD (데이터)
DEGE
DEGE
방송기
➔ 이미지만 = DEGE (GE, 'null')
➔ 데이터만 = DEGE ('null', UD)
➔ 일반적인 DEGE (GE, UD)
(a)
행렬
GE
광학적
이미지
신호들
EOC
수신기
UD
데이터
수신기
(b)

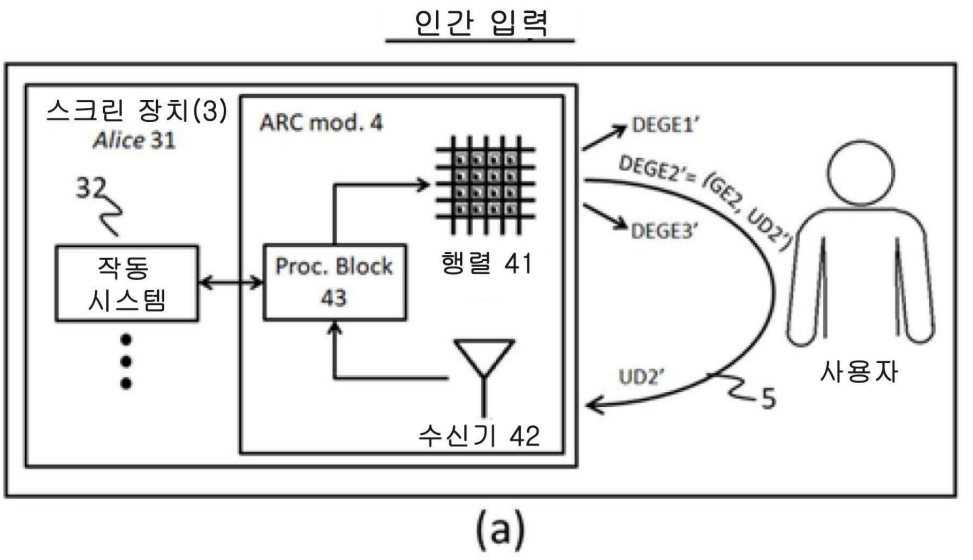
도면4

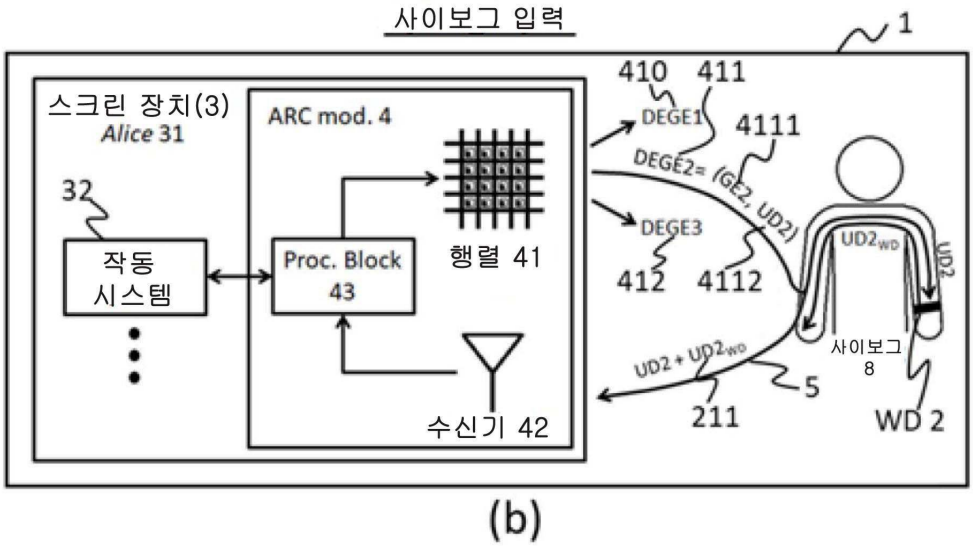

용량성 커플링을 시작하는 방법
타입 1
C
전극들을 이동시키는 것에 의한
거리 단축 ≡ 하나의 커패시터를
통한 커플링
타입 2
C1
C2
몸체를 통한 커플링에 의한
거리 단축 ≡ 2개의 직렬 연결된
커패시터들을 통한 커플링

도면5

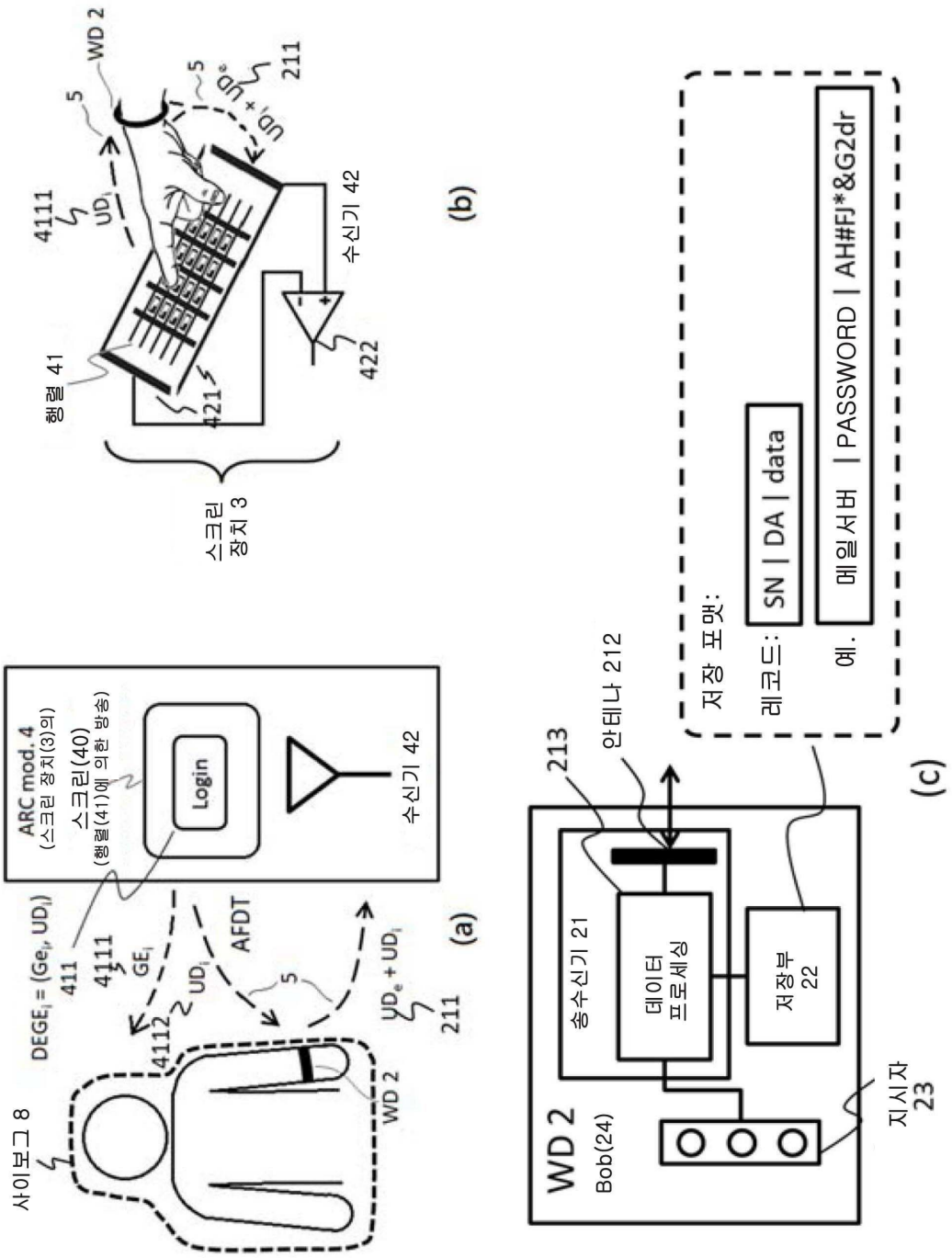

AFDT
타입 1(이동 장치)
타입 2(몸체 '와이어')
SRDT
(장치-외 전송)
UDI
(장치-내 전송)
손가락 입력
스타일러스 입력
Intra-device Receiver
음영들

도면6

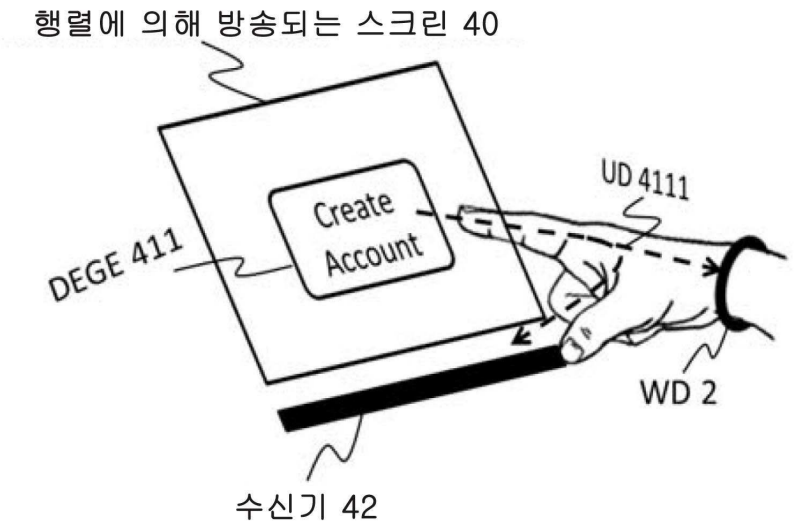

인간 입력
스크린 장치(3)
Alice 31
32
작동
시스템
ARC mod. 4
Proc. Block
43
행렬 41
수신기 42
DEGE1'
DEGE2'= (GE2, UD2')
DEGE3'
UD2'
5
사용자
(a)


사이보그 입력
1
스크린 장치(3)
Alice 31
32
작동
시스템
ARC mod. 4
Proc. Block
43
행렬 41
수신기 42
410
411
DEGE1
4111
DEGE2= (GE2, UD2)
DEGE3
412
4112
UD2WD
UD2
사이보그
8
UD2 + UD2WD
5
211
WD 2
(b)

도면7


WD 2
5
211
4111
UDi
수신기 42
행렬 41
422
421
스크린
장치 3
(b)
ARC mod. 4
(스크린 장치(3)의
스크린(40)
(행렬(41)에 의한 방송)
Login
수신기 42
DEGEi = (Gei, UDi)
411
4111
GEi
UDi
AFDT
5
4112
UDe + UDi
211
(a)
사이보그 8
WD 2
213
안테나 212
송수신기 21
데이터
프로세싱
저장부
22
WD 2
Bob(24)
지시자
23
저장 포맷:
레코드:
SN | DA | data
예.
메일서버 | PASSWORD | AH#FJ*&G2dr
(c)

도면8



계정을 생성하기 위한 DEGE들

	GE	UD
DEGE1	Create Account	'WHO(*Alice*)'
DEGE2		'ST(*Bob*, *Alice*, USERNAME, X, PASSWORD, Y)'

24 31

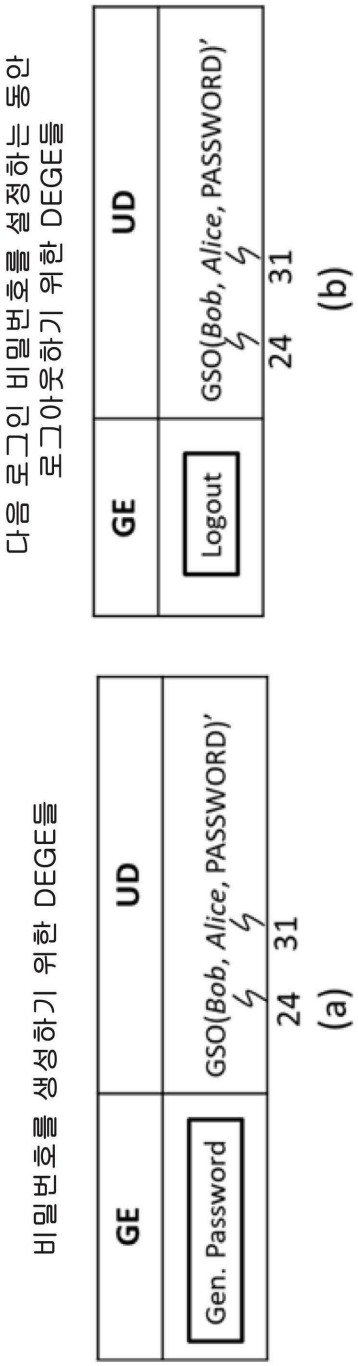
도면9

계정에 로그인하기 위한 DEGE들

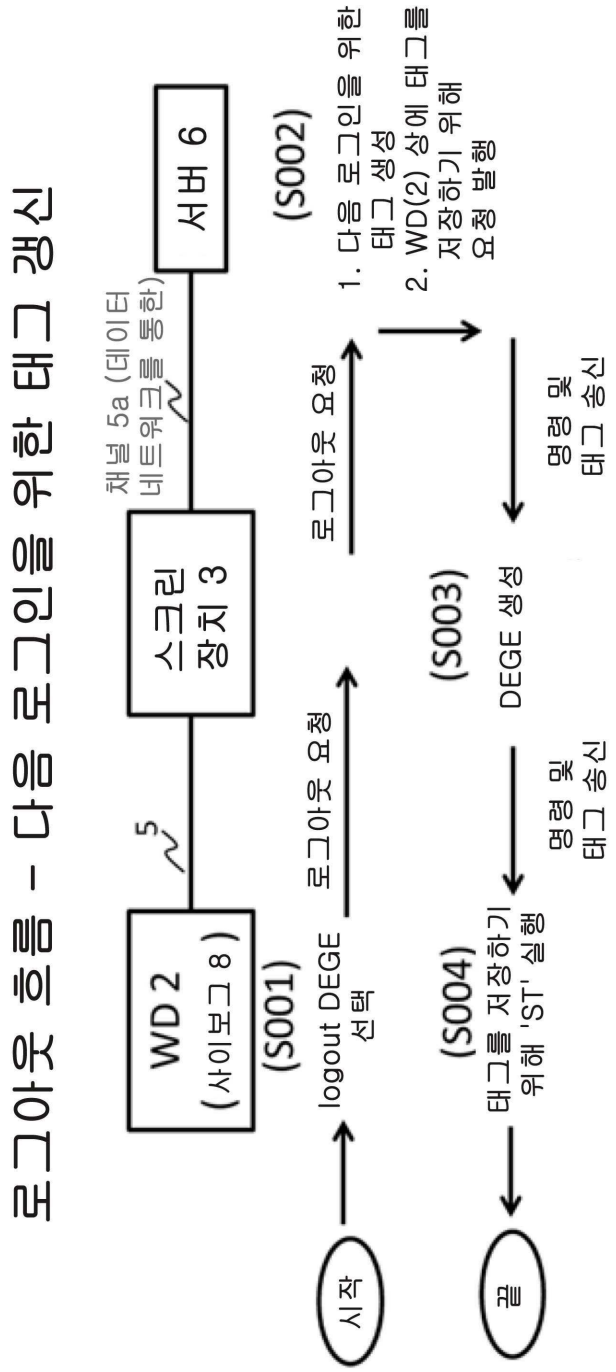
GE	UD
Login	'GET(*Bob*, *Alice*, USERNAME, PASSWORD)'

24 31

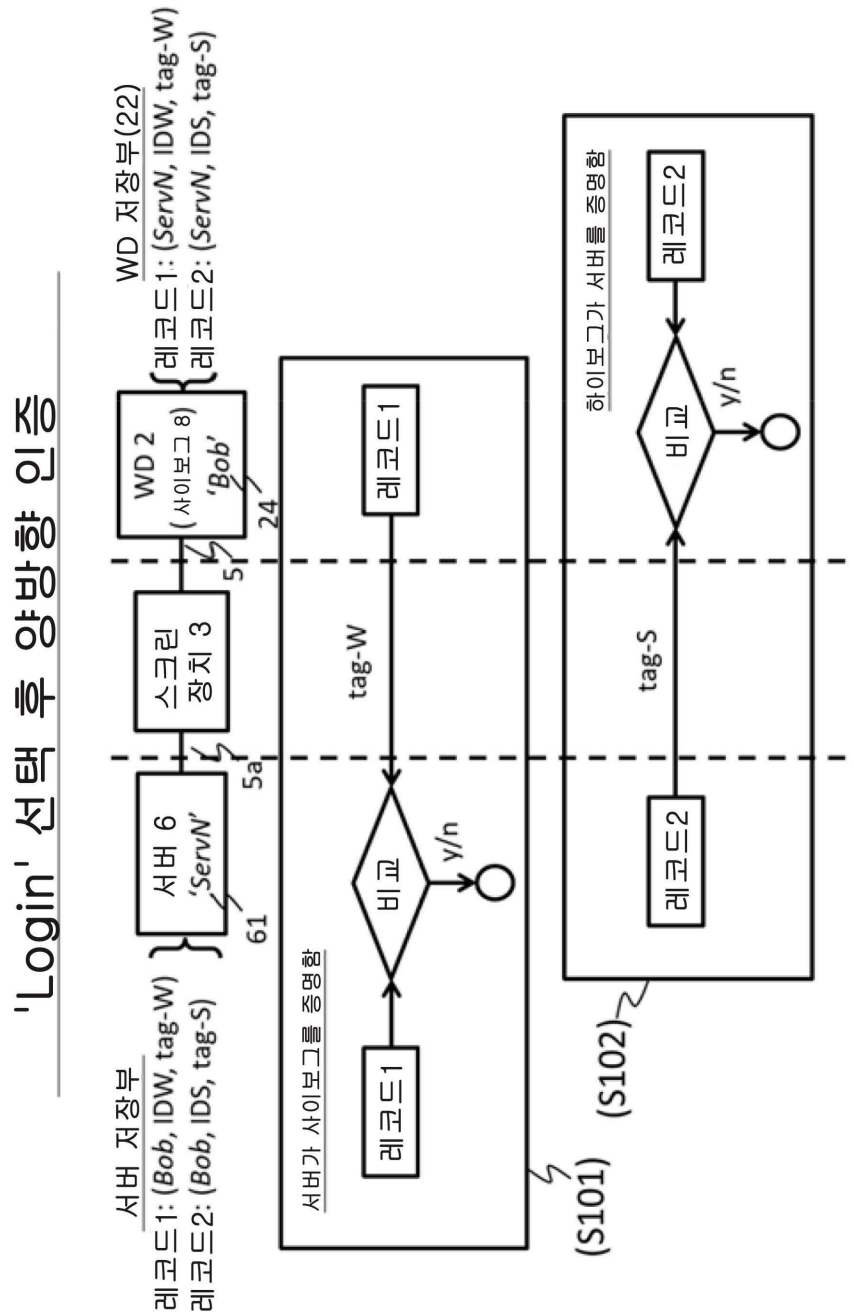
도면10


비밀번호를 생성하기 위한 DEGE들
GE
UD
Gen. Password
GSO(Bob, Alice, PASSWORD)'
24
31
(a)
다음 로그인 비밀번호를 설정하는 동안
로그아웃하기 위한 DEGE들
GE
UD
Logout
GSO(Bob, Alice, PASSWORD)'
24
31
(b)

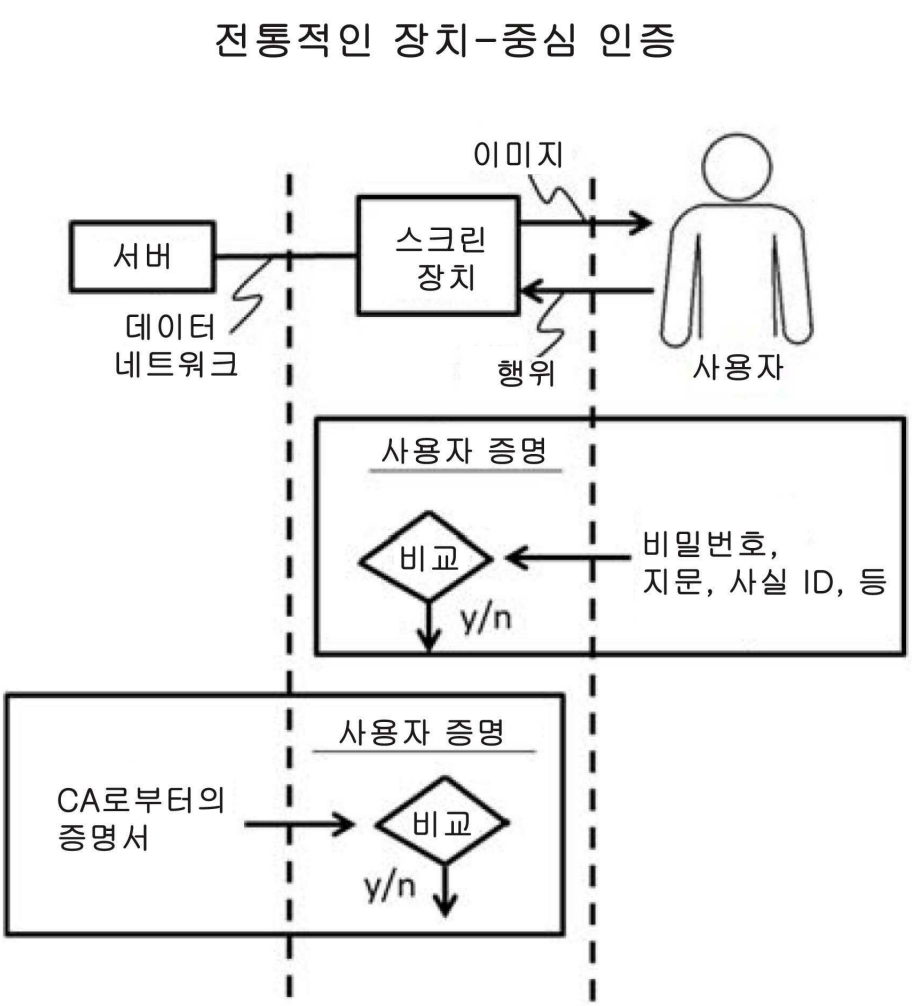
도면11


로그아웃 흐름 - 다음 로그인을 위한 태그 갱신
WD 2
(사이보그 8)
5
스크린
장치 3
채널 5a (데이터
네트워크를 통한)
서버 6
(S001)
logout DEGE
선택
로그아웃 요청
(S002)
1. 다음 로그인을 위한
태그 생성
2. WD(2) 상에 태그를
저장하기 위해
요청 발행
로그아웃 요청
(S003)
DEGE 생성
명령 및
태그 송신
명령 및
태그 송신
(S004)
태그를 저장하기
위해 'ST' 실행
시작
끝

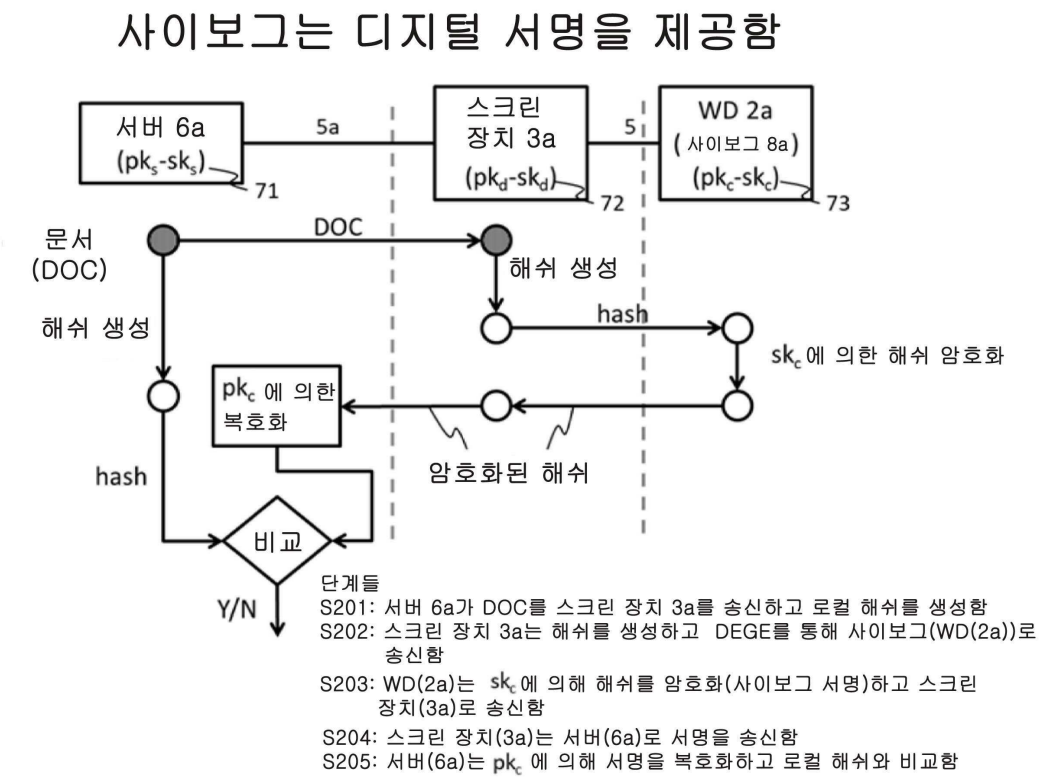
도면12


'Login' 선택 후 양방향 인증
서버 저장부
레코드1: (Bob, IDW, tag-W)
레코드2: (Bob, IDS, tag-S)
서버 6
'ServN'
61
스크린 장치 3
5a
WD 저장부(22)
레코드1: (ServN, IDW, tag-W)
레코드2: (ServN, IDS, tag-S)
WD 2
(사이보그 8)
'Bob'
24
5
서버가 사이보그를 증명함
tag-W
레코드1
비교
y/n
레코드1
(S101)
하이보그가 서버를 증명함
tag-S
레코드2
비교
y/n
레코드2
(S102)

도면13

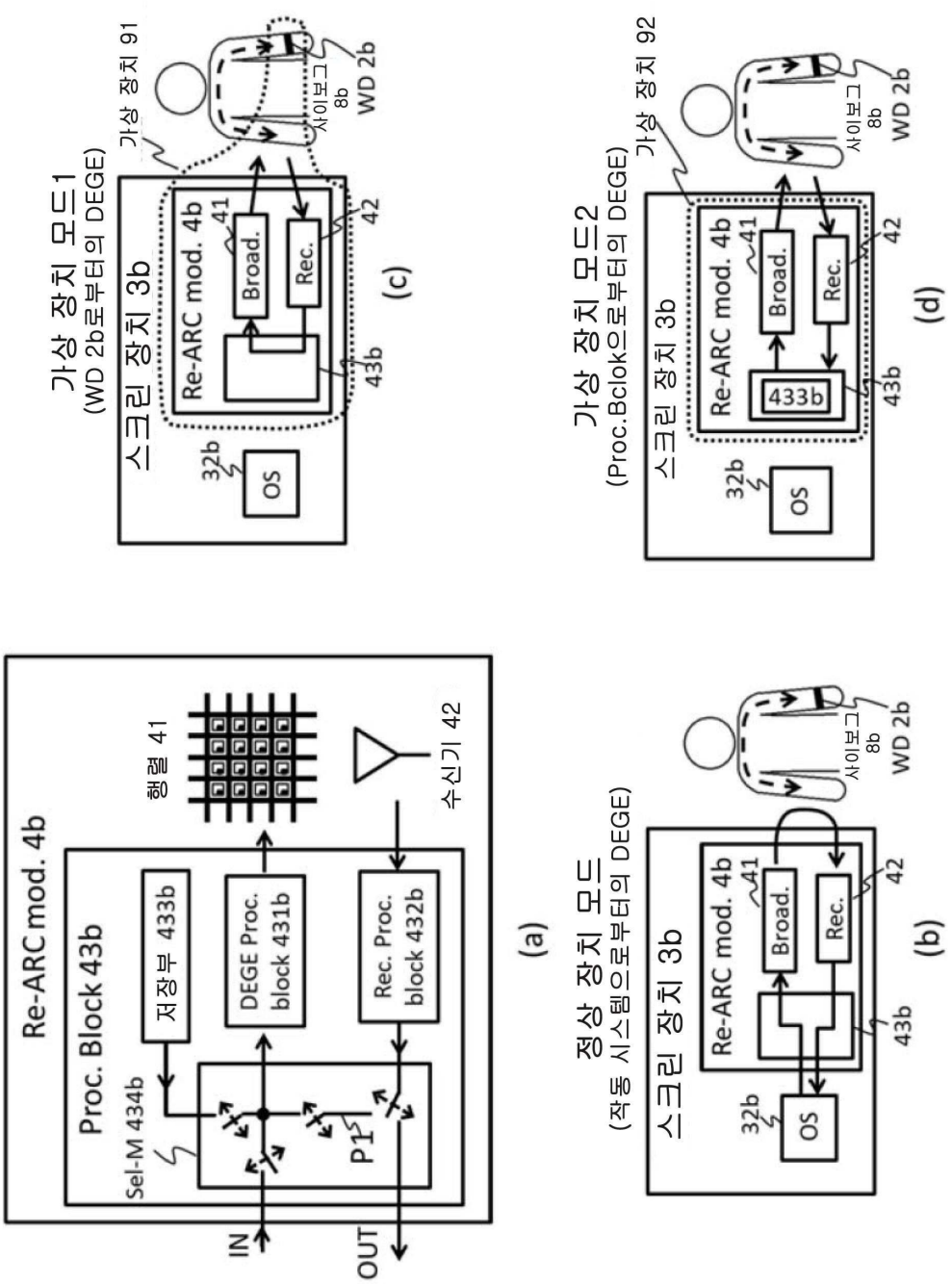

전통적인 장치-중심 인증
이미지
서버
스크린
장치
데이터
네트워크
행위
사용자
사용자 증명
비교
비밀번호,
지문, 사실 ID, 등
y/n
사용자 증명
CA로부터의
증명서
비교
y/n

도면14

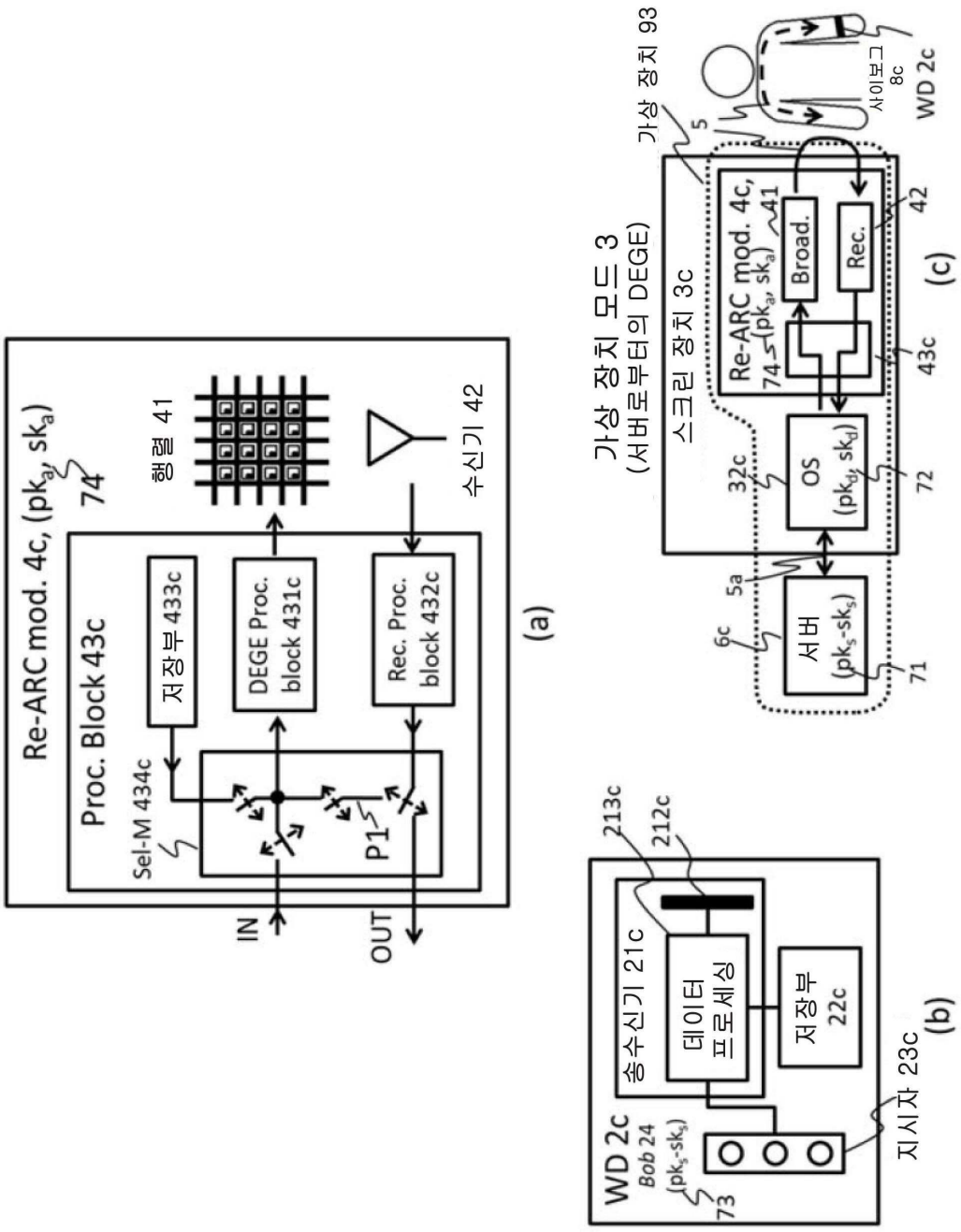


단계들
S201: 서버 6a가 DOC를 스크린 장치 3a를 송신하고 로컬 해쉬를 생성함
S202: 스크린 장치 3a는 해쉬를 생성하고 DEGE를 통해 사이보그(WD(2a))로 송신함
S203: WD(2a)는 sk_c에 의해 해쉬를 암호화(사이보그 서명)하고 스크린 장치(3a)로 송신함
S204: 스크린 장치(3a)는 서버(6a)로 서명을 송신함
S205: 서버(6a)는 pk_c 에 의해 서명을 복호화하고 로컬 해쉬와 비교함

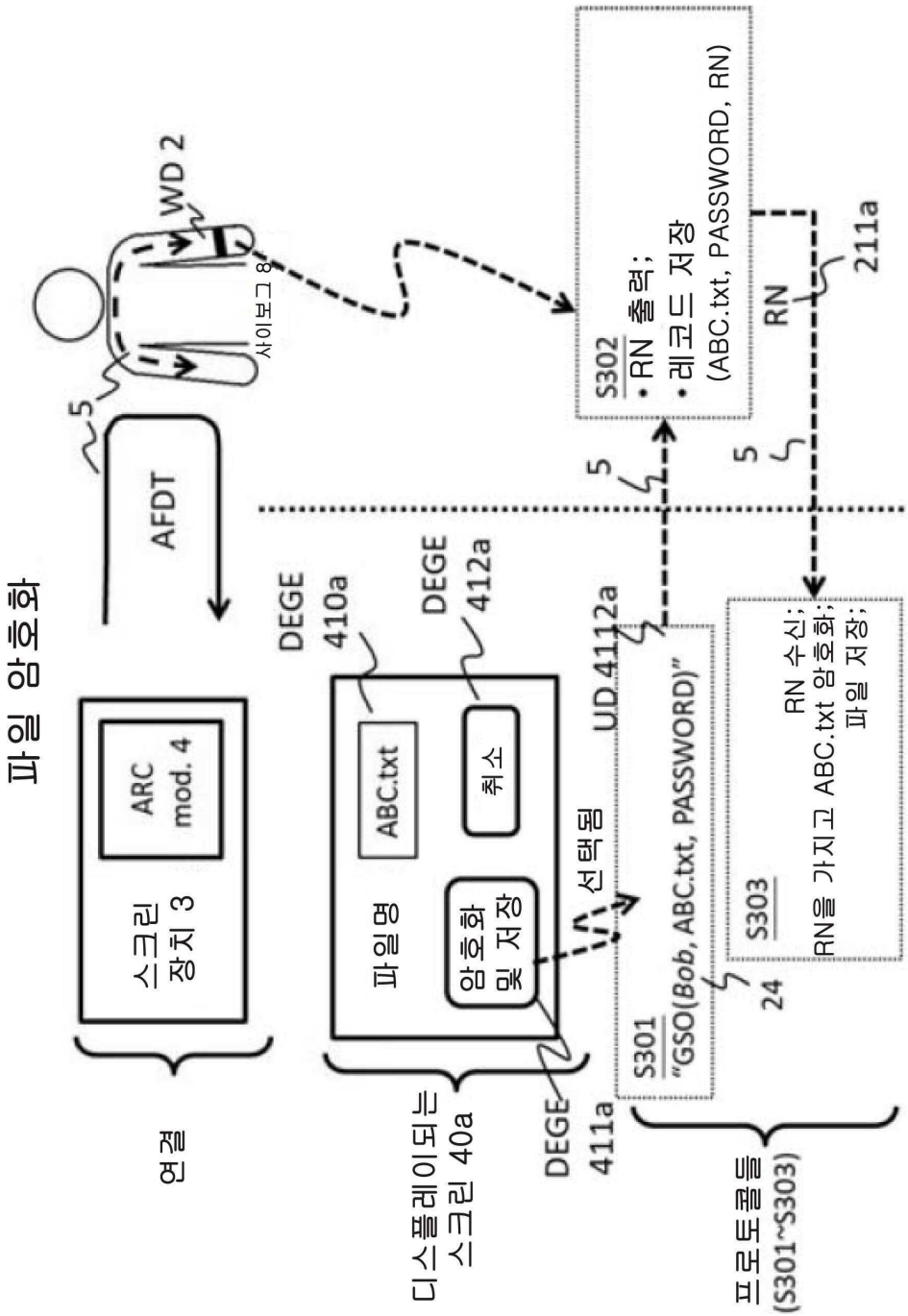
도면15


Re-ARC mod. 4b
Proc. Block 43b
Sel-M 434b
저장부 433b
DEGE Proc. block 431b
Rec. Proc. block 432b
P1
행렬 41
수신기 42
IN
OUT
(a)
가상 장치 모드1
(WD 2b로부터의 DEGE)
스크린 장치 3b
가상 장치 91
Re-ARC mod. 4b
41
Broad.
Rec.
42
43b
32b
OS
사이보그 8b
WD 2b
(c)
가상 장치 모드2
(Proc.Bclok으로부터의 DEGE)
가상 장치 92
433b
(d)
정상 장치 모드
(작동 시스템으로부터의 DEGE)
(b)

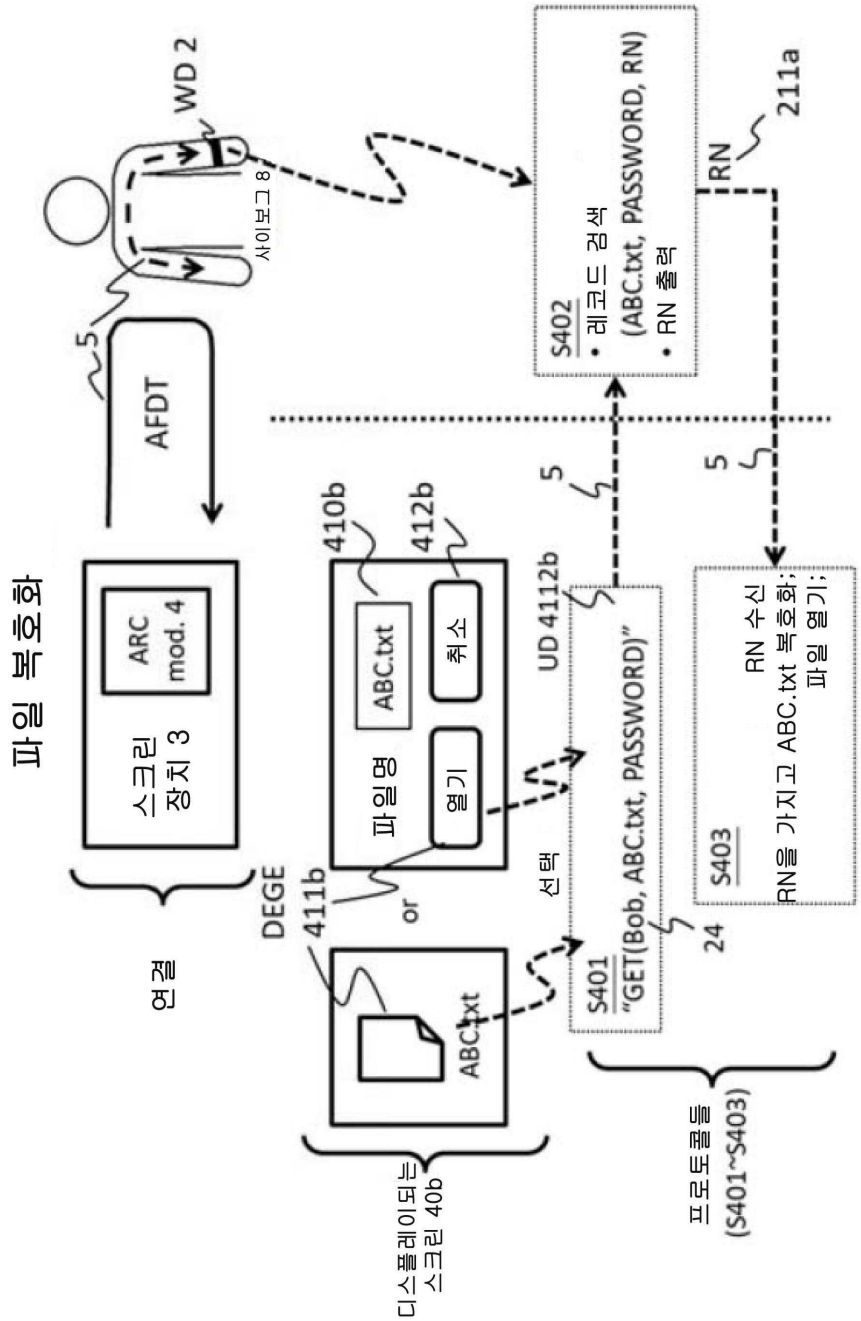
도면16


Re-ARC mod. 4c, (pk_a, sk_a)
74
Proc. Block 43c
Sel-M 434c
저장부 433c
DEGE Proc. block 431c
Rec. Proc. block 432c
P1
행렬 41
수신기 42
IN
OUT
(a)
가상 장치 모드 3
(서버로부터의 DEGE)
스크린 장치 3c
가상 장치 93
5
Re-ARC mod. 4c, (pk_a, sk_a)
74
41
Broad.
Rec.
42
43c
32c
OS (pk_d, sk_d)
72
5a
6c
서버 (pk_s-sk_s)
71
사이보그 8c
WD 2c
(c)
213c
212c
송수신기 21c
데이터 프로세싱
저장부 22c
WD 2c
Bob 24
(pk_s-sk_s)
73
지시자 23c
(b)

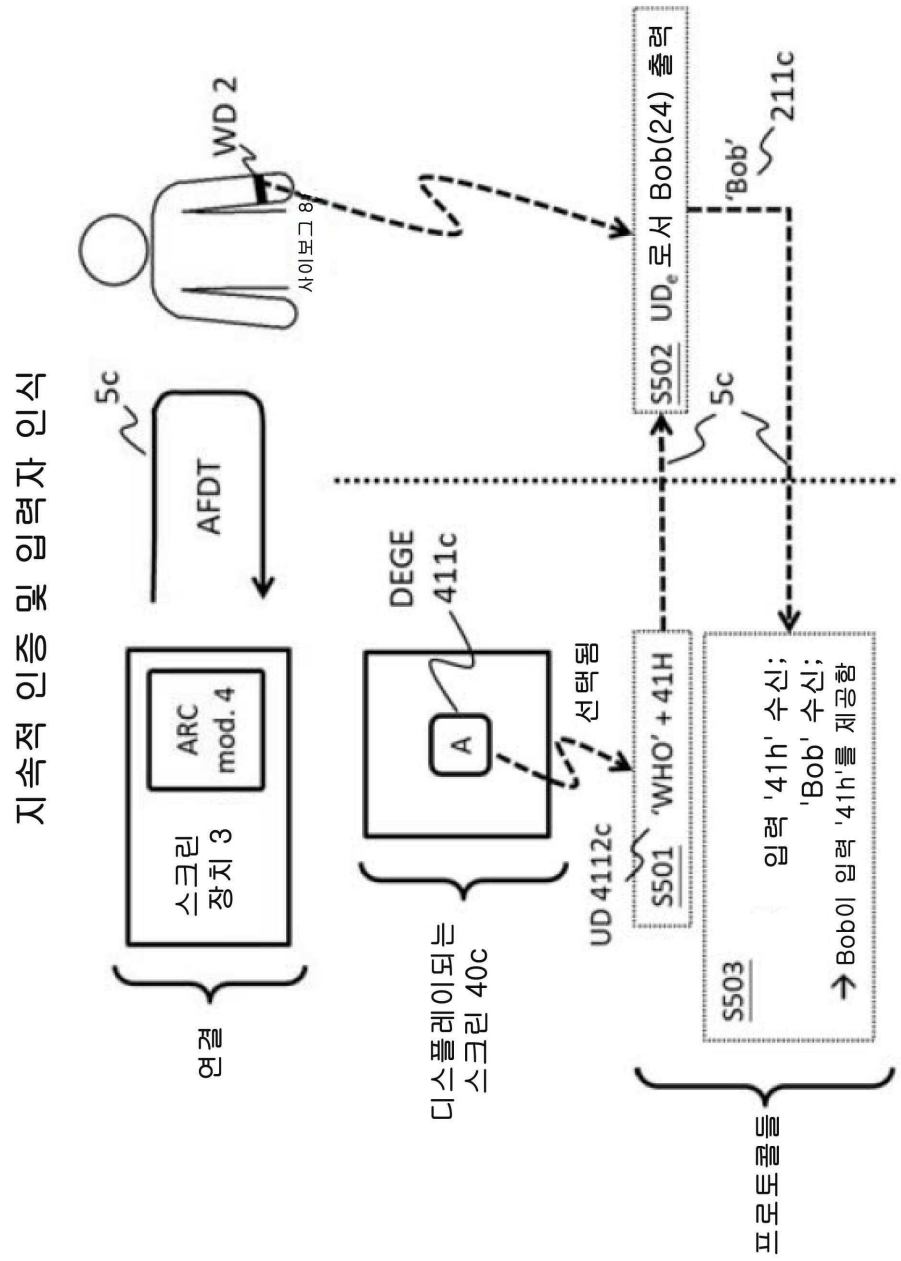
도면17


파일 암호화
WD 2
사이보그 8
5
AFDT
스크린 장치 3
ARC mod. 4
연결
DEGE 410a
DEGE 412a
파일명
ABC.txt
암호화 및 저장
취소
디스플레이되는 스크린 40a
DEGE 411a
선택됨
UD 4112a
S301
"GSO(Bob, ABC.txt, PASSWORD)"
24
S303
RN을 가지고 ABC.txt 암호화;
RN 수신;
파일 저장;
프로토콜들 (S301~S303)
5
S302
• RN 출력;
• 레코드 저장
(ABC.txt, PASSWORD, RN)
5
RN
211a

도면18

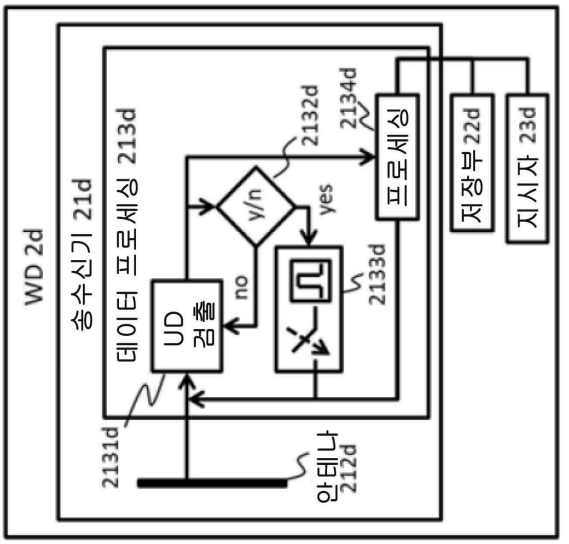

파일 복호화
WD 2
사이보그 8
5
AFDT
스크린
장치 3
ARC
mod. 4
연결
DEGE
411b
or
410b
412b
ABC.txt
취소
파일명
열기
선택
UD 4112b
ABC.txt
디스플레이되는
스크린 40b
S401
"GET(Bob, ABC.txt, PASSWORD)"
24
S402
• 레코드 검색
(ABC.txt, PASSWORD, RN)
• RN 출력
RN
211a
5
S403
RN 수신
RN을 가지고 ABC.txt 복호화;
파일 열기;
프로토콜들
(S401~S403)

도면19


지속적 인증 및 입력자 인식
WD 2
사이보그 8
5c
AFDT
211c
'Bob'
S502 UDe 로서 Bob(24) 출력
5c
DEGE
411c
A
선택됨
ARC
mod. 4
스크린
장치 3
연결
디스플레이되는
스크린 40c
UD 4112c
S501 'WHO' + 41H
S503
입력 '41h' 수신;
'Bob' 수신;
→ Bob이 입력 '41h'를 제공함
프로토콜들

도면20

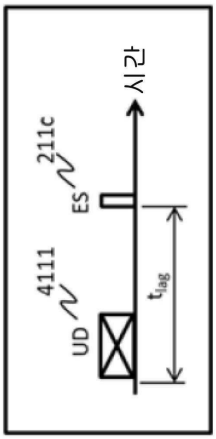
에코 모드를 갖는 WD 및 작동



에코 모드를 활성화 또는 비활성화시키기 위한 WD(2d)의 명령들

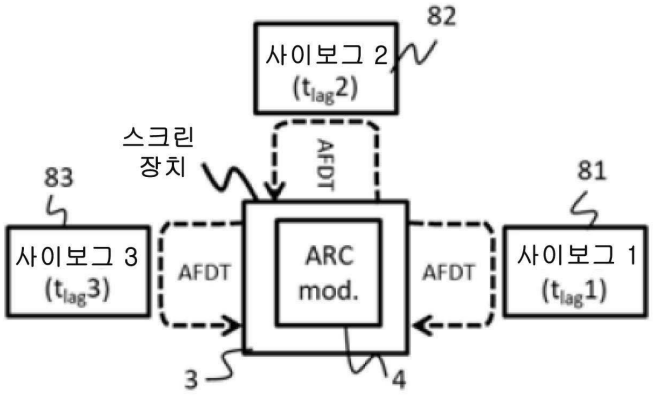
입력	출력	설명
ECHO-ON(t_{lag})	---	시간 랙 t_{lag}을 갖는 에코 모드를 활성화시킴;
ECHO-OFF	---	에코 모드를 비활성화시킴;

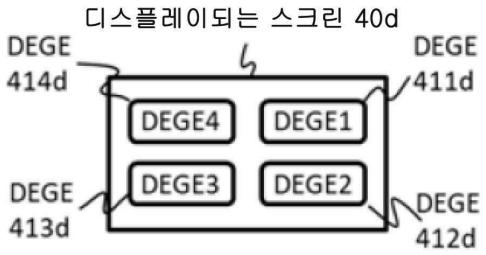
DEGE(411)이 선택된 때 수신기(42) 상의 신호들



입력자 인식의 예

시나리오:



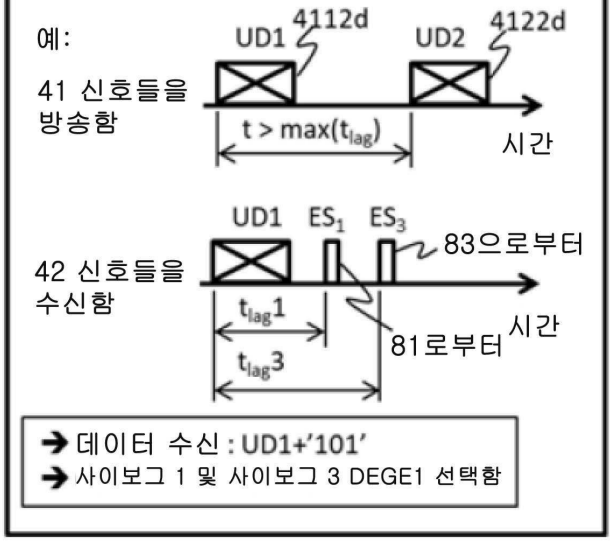


입력자 인식 단계들

단계 601. 등록

1. 'WHO': 각각의 사이보그로부터 WD의 WD-ID 문의;
2. 'ECHO-ON(t_{lag})':각각의 사이보그에 대하여 태그 할당
3. GE 표시: 사이보그에게 WD-ID가 등록됨을 알림

단계 502. 입력자 인식



➔ 데이터 수신 : UD1+'101'
➔ 사이보그 1 및 사이보그 3 DEGE1 선택함