(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0030486
(43) 공개일자 2011년03월23일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04B 5/02* (2006.01)
(21) 출원번호 10-2010-7029154
(22) 출원일자(국제출원일자) 2008년11월03일
심사청구일자 2010년12월24일
(85) 번역문제출일자 2010년12월24일
(86) 국제출원번호 PCT/IB2008/054566
(87) 국제공개번호 WO 2009/144534
국제공개일자 2009년12월03일
(30) 우선권주장
08104094.1 2008년05월26일
유럽특허청(EPO)(EP)

(71) 출원인
엔엑스피 비 브이
네덜란드 엔엘-5656 아게 아인드호펜 하이 테크 캠퍼스 60
(72) 발명자
수에린거 피터
오스트리아 비엔나 에이-1102 구테일-쇼더-가세 8-12 인텔렉츄얼 프로퍼티 디파트먼트 엔엑스피 세미컨덕터스 오스트리아 게엠베하
드 종 한스
오스트리아 비엔나 에이-1102 구테일-쇼더-가세 8-12 인텔렉츄얼 프로퍼티 디파트먼트 엔엑스피 세미컨덕터스 오스트리아 게엠베하
(뒷면에 계속)
(74) 대리인
김원준, 김창세

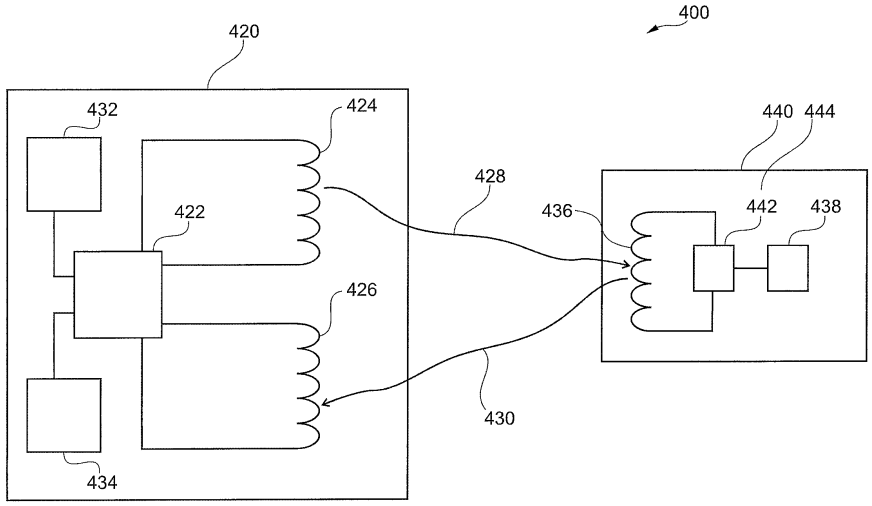
전체 청구항 수 : 총 29 항

(54) 판독기, 트랜스폰더, 접속 유효성 판정 방법 및 컴퓨터 판독가능한 매체

(57) 요 약

본 발명에 따르면, 트랜스폰더(440)에 대한 접속의 유효성을 판정하는 판독기(420)가 제공되며, 상기 판독기(420)는 두 개의 개별적인 단계들로 트랜스폰더(440)의 응답 시간을 측정하고 상기 트랜스폰더(440)를 인증하도록 구성된다. 판독기(420)에 대한 접속의 유효성을 판정하는 트랜스폰더(440)는, 두 개의 개별적인 단계들로 판독기(420)에게 응답 시간의 측정에 대한 정보를 제공하고 판독기(420)에게 인증을 위한 정보를 제공하도록 구성되며, 인증을 위해 사용되는 데이터의 적어도 일부가 응답 시간을 측정하는 동안에 판독기(420)와 트랜스폰더(440) 사이에서 전송되는 통신 메시지 내에 포함된다.

대 표 도



(72) 발명자

머레이 브루스

오스트리아 비엔나 에이-1102 구테일-쇼더-가세 8-12 인텔렉츄얼 프로퍼티 디파트먼트 엔엑스피 세미컨덕터스 오스트리아 게엠베하

노이만 헤이케

오스트리아 비엔나 에이-1102 구테일-쇼더-가세 8-12 인텔렉츄얼 프로퍼티 디파트먼트 엔엑스피 세미컨덕터스 오스트리아 게엠베하

홉메르 폴

오스트리아 비엔나 에이-1102 구테일-쇼더-가세 8-12 인텔렉츄얼 프로퍼티 디파트먼트 엔엑스피 세미컨덕터스 오스트리아 게엠베하

스턴 수산느

오스트리아 비엔나 에이-1102 구테일-쇼더-가세 8-12 인텔렉츄얼 프로퍼티 디파트먼트 엔엑스피 세미컨덕터스 오스트리아 게엠베하

특허청구의 범위

청구항 1

트랜스폰더(440)에 대한 접속의 유효성(validity)을 판정하는 판독기(420)로서,

상기 판독기(420)는 두 개의 개별적인 단계들로 트랜스폰더(440)의 응답 시간을 측정하고 상기 트랜스폰더(440)를 인증하도록 구성되며,

상기 인증을 위해 사용되는 데이터의 적어도 일부가 상기 응답 시간을 측정하는 동안에 상기 판독기(420)와 상기 트랜스폰더(440) 사이에서 전송되는 통신 메시지 내에 포함되는

판독기.

청구항 2

제 1 항에 있어서,

상기 트랜스폰더(440)에 제 1 커맨드(RAC1)를 전송한 시각과 상기 제 1 커맨드(RAC1)에 응답하여 상기 트랜스폰더(440)로부터 제 1 랜덤 넘버(RANDOM #1)를 수신한 시각 사이의 시간 간격에 기초하여 상기 응답 시간을 측정하도록 구성되는

판독기.

청구항 3

제 2 항에 있어서,

상기 응답 시간의 측정을 위해 상기 제 1 랜덤 넘버(RANDOM #1)가 수신된 후 상기 트랜스폰더(440)로부터 수신된 상기 제 1 랜덤 넘버(RANDOM #1)의 암호가, 상기 응답 시간의 측정을 위해 수신된 상기 제 1 랜덤 넘버(RANDOM #1)와 일치하는지 여부에 대한 평가에 기초하여 상기 트랜스폰더(440)를 인증하도록 구성되는

판독기.

청구항 4

제 1 항에 있어서,

제 1 커맨드(RAC1)와 제 2 랜덤 넘버(RANDOM #2)를 함께 상기 트랜스폰더(440)로 전송한 시각과 상기 제 1 커맨드(RAC1)에 응답하여 상기 트랜스폰더(440)로부터 제 1 랜덤 넘버(RANDOM #1)를 수신한 시각 사이의 시간 간격에 기초하여 상기 응답 시간을 측정하도록 구성되는

판독기.

청구항 5

제 4 항에 있어서,

상기 응답 시간의 측정을 위해 상기 제 1 랜덤 넘버(RANDOM #1)가 수신된 후 상기 트랜스폰더(440)로부터 수신된 상기 제 2 랜덤 넘버(RANDOM #2)의 암호 및 상기 제 1 랜덤 넘버(RANDOM #1)의 암호가, 상기 응답 시간의 측정을 위해 수신된 상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)와 일치하는지 여부에 대한 평가에 기초하여 상기 트랜스폰더(440)를 인증하도록 구성되는

판독기.

청구항 6

제 3 항 또는 제 5 항에 있어서,

상기 시간 간격이 사전결정된 시간 윈도우(time window) 내에 있고, 일치성을 만족하며, 상기 트랜스폰더(440)가 동작하는 통신 속도가 상기 판독기(420)가 상기 트랜스폰더(440)가 동작하는 통신 속도로 가정하는 것과 동일하다는 판정에 따라서만 상기 트랜스폰더(440)로의 접속이 유효하도록 구성되는

판독기.

청구항 7

제 1 항에 있어서,

복수의 통신 메시지들로 분할된 데이터를 인증을 위해 및/또는 근접 체크(a proximity check)를 위해 상기 트랜스폰더(440)와 교환하도록 구성되는

판독기.

청구항 8

제 4 항에 있어서,

순환 중복 검사(CRC; Cyclic Redundancy Check)로부터 자유롭게 상기 제 1 커맨드(RAC1)를 전송하도록 구성되는

판독기.

청구항 9

제 1 항에 있어서,

상기 트랜스폰더(440)로 전송된 메시지 및 상기 트랜스폰더(440)로부터 수신된 메시지에 대해 계산되는 상기 트랜스폰더(440)로부터의 순환 중복 검사를 포함하는 통신 메시지를 수신하고, 상기 순환 중복 검사를 포함하는 통신 메시지에서 통신 오류를 검출함에 따라 상기 트랜스폰더(440)와 교환된 메시지들의 비-유효성(non validity)을 가정하도록 구성되는

판독기.

청구항 10

제 4 항에 있어서,

상기 트랜스폰더(440)로부터의 순환 중복 검사를 포함하는 통신 메시지를 수신하도록 구성되되, 상기 순환 중복 검사는 상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)와 연관된 상기 판독기(420)로부터 수신된 메시지(RAC1)에 기초하여 상기 트랜스폰더(440)에 의해 발생되는

판독기.

청구항 11

판독기(420)에 대한 접속의 유효성(validity)을 판정하는 트랜스폰더(440)로서,

상기 트랜스폰더(440)는 두 개의 개별적인 단계들로 상기 판독기(420)에게 응답 시간의 측정에 대한 정보를 제공하고 상기 판독기(420)에게 인증을 위한 정보를 제공하도록 구성되며,

상기 인증을 위해 사용되는 데이터의 적어도 일부가 상기 응답 시간을 측정하는 동안에 상기 판독기(420)와 상기 트랜스폰더(440) 사이에서 전송되는 통신 메시지 내에 포함되는

트랜스폰더.

청구항 12

제 11 항에 있어서,

응답 시간의 측정을 위해 상기 트랜스폰더(440)로부터 수신된 제 1 커맨드(RAC1)에 응답하여 상기 판독기(420)에게 제 1 랜덤 넘버(RANDOM #1)를 전송하도록 구성되는

트랜스폰더.

청구항 13

제 12 항에 있어서,

응답 시간의 측정을 위해 비암호화된 상기 제 1 랜덤 넘버(RANDOM #1)를 상기 판독기(420)에게 전송하도록 구성되는

트랜스폰더.

청구항 14

제 12 항에 있어서,

제 2 랜덤 넘버(RANDOM #2)를 포함하는 상기 제 1 커맨드(RAC1)에 응답하여 상기 제 1 랜덤 넘버(RANDOM #1)를 전송하도록 구성되는

트랜스폰더.

청구항 15

제 14 항에 있어서,

추후의 세션을 위해 상기 제 1 랜덤 넘버(RANDOM #1)를 대체하도록 상기 제 2 랜덤 넘버(RANDOM #2)에 기초하여 제 3 랜덤 넘버(RANDOM #3)를 생성 및 저장하도록 구성되는

트랜스폰더.

청구항 16

제 14 항에 있어서,

상기 제 1 커맨드(RAC1)를 전송한 후에 전송된 상기 트랜스폰더(440)로부터의 제 2 커맨드(RAC2)의 수신 후에, 상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)의 암호를 전송하도록 구성되는

트랜스폰더.

청구항 17

제 11 항에 있어서,

상기 판독기(420)와 교환된 통신 메시지를 분석함으로써 상기 트랜스폰더(440)가 상기 판독기(420) 부근에 있는지 여부를 결정하고, 상기 트랜스폰더(440)가 상기 판독기(420) 부근에 있지 않다는 판정에 따라 통신을 종료하도록 구성되는

트랜스폰더.

청구항 18

제 11 항에 있어서,

복수의 통신 메시지들로 분할된 데이터를 인증을 위해 및/또는 근접 체크를 위해서 상기 판독기(420)와 교환하도록 구성되는

판독기.

청구항 19

제 12 항에 있어서,

상기 제 1 랜덤 넘버(RANDOM #1)를 순환 중복 검사와 함께 상기 판독기(420)로 전송하도록 구성되는

트랜스폰더.

청구항 20

제 11 항에 있어서,

타이밍을 나타내는 정보, 특히 상기 트랜스폰더(440)와 상기 판독기(420) 사이의 통신 속도를 나타내는 정보와 함께 통신 메시지를 상기 판독기(420)에 전송하도록 구성되는

트랜스폰더.

청구항 21

제 11 항에 있어서,

주파수를 검출 및 제한하도록 구성되되,

동작시에 상기 주파수가 범위를 벗어나면, 잔여 릴레이 어택 윈도우(residual relay attack window)를 제한하기 위해 상기 판독기(420)와의 통신을 중단시키는

트랜스폰더.

청구항 22

제 14 항에 있어서,

순환 중복 검사를 포함하는 통신 메시지를 생성하도록 구성되되, 상기 순환 중복 검사는 상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)와 연관된 상기 판독기(420)로부터 수신된 메시지(RAC1)에 기초하여 발생되는

트랜스폰더.

청구항 23

트랜스폰더(440)에 대한 접속의 유효성을 판정하는 판독기(420)의 방법으로서,

제 1 커맨드(RAC1)를 제 2 랜덤 넘버(RANDOM #2)와 함께 상기 트랜스폰더(440)로 전송하는 단계와,

상기 트랜스폰더(440)로부터 제 1 랜덤 넘버(RANDOM #1)를 수신하는 단계와,

상기 트랜스폰더(440)로부터 상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)의 암호를 수신하는 단계와,

상기 트랜스폰더(440)에 의해 사용된 것과 동일한 키로 상기 수신된 넘버를 복호화하거나, 또는 상기 키로 상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)를 암호화하는 단계와,

상기 트랜스폰더(440)로부터 수신된 상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)와, 상기 트랜스폰더(440)로부터 암호로서 수신된 상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)가 일치하는지 여부를 체크하는 단계와,

상기 제 1 랜덤 넘버(RANDOM #1)가 사전결정된 시간 윈도우 내에서 수신되었는지 여부를 체크하는 단계와,

상기 두 체크 단계의 결과가 모두 참인 경우에 상기 트랜스폰더(440)로의 접속을 유효한 것으로 인정하는 단계를 포함하는

접속 유효성 판정 방법.

청구항 24

제 23 항에 있어서,

상기 제 1 커맨드(RAC1)에 응답하여 상기 트랜스폰더(440)로부터 상기 제 1 랜덤 넘버(RANDOM #1)를 수신하는 단계와,

상기 제 1 커맨드(RAC1)를 전송한 후에 상기 트랜스폰더(440)로 제 2 커맨드(RAC2)를 전송하는 단계와,

상기 제 2 커맨드(RAC2)에 응답하여 상기 트랜스폰더(440)로부터 상기 제 1 랜덤 넘버(RANDOM #1)의 암호를 수신하는 단계를 더 포함하는

접속 유효성 판정 방법.

청구항 25

트랜스폰더(440)에 대한 접속의 유효성을 판정하는 판독기(420)의 방법으로서,

제 1 커맨드를 제 2 랜덤 넘버와 함께 상기 트랜스폰더(440)로 전송하는 단계와,

상기 트랜스폰더(440)로부터 제 1 랜덤 넘버를 수신하는 단계와,

상기 제 1 랜덤 넘버 및 상기 제 2 랜덤 넘버에 기초하여 생성된 제 1 메시지 인증 코드(MAC)를 상기 트랜스폰더(440)로 전송하는 단계와,

상기 제 1 랜덤 넘버 및 상기 제 2 랜덤 넘버에 기초하여 생성된 제 2 메시지 인증 코드(MAC)를 상기 트랜스폰더(440)로부터 수신하는 단계와,

상기 제 2 메시지 인증 코드(MAC)가 유효한지 여부를 체크하는 단계와,

상기 제 1 랜덤 넘버가 사전결정된 시간 윈도우 내에서 수신되었는지 여부를 체크하는 단계와,

만약 상기 두 체크 단계의 결과가 모두 참인 경우에 상기 트랜스폰더(440)로의 접속이 유효한 것으로 인정하는

단계를 포함하는

접속 유효성 판정 방법.

청구항 26

판독기(420)에 대한 접속의 유효성을 판정하는 트랜스폰더(440)의 방법으로서,

제 1 커맨드(RAC1)를 제 2 랜덤 넘버(RANDOM #2)와 함께 상기 판독기(420)로부터 수신하는 단계와,

제 1 랜덤 넘버(RANDOM #1)를 상기 판독기(420)로 전송하는 단계와,

상기 제 1 랜덤 넘버(RANDOM #1) 및 상기 제 2 랜덤 넘버(RANDOM #2)의 암호를 상기 판독기(420)로 전송하는 단계를 포함하는

접속 유효성 판정 방법.

청구항 27

판독기(420)에 대한 접속의 유효성을 판정하는 트랜스폰더(440)의 방법으로서,

제 1 커맨드와 제 2 랜덤 넘버를 상기 판독기(420)로부터 수신하는 단계와,

제 1 랜덤 넘버를 상기 판독기(420)로 전송하는 단계와,

상기 제 1 랜덤 넘버 및 상기 제 2 랜덤 넘버에 기초하여 생성된 제 1 메시지 인증 코드(MAC)를 상기 판독기(420)로부터 수신하는 단계와,

상기 제 1 메시지 인증 코드(MAC)가 유효한지 여부를 체크하는 단계와,

상기 제 1 메시지 인증 코드(MAC)가 유효한 경우, 상기 제 1 랜덤 넘버 및 상기 제 2 랜덤 넘버에 기초하여 생성된 제 2 메시지 인증 코드(MAC)를 전송하는 단계를 포함하는

접속 유효성 판정 방법.

청구항 28

컴퓨터 프로그램이 저장된 컴퓨터 판독가능한 매체로서,

상기 컴퓨터 프로그램은, 프로세서(422, 442)에 의해 실행되었을 때 청구항 제 23 항 및 제 25 항 내지 제 27 항 중 어느 한 항에 따른 방법을 실행 또는 제어하도록 구성되는, 컴퓨터 판독가능한 매체.

청구항 29

프로세서(422, 442)에 의해 실행되었을 때 청구항 제 23 항 및 제 25 항 내지 제 27 항 중 어느 한 항에 따른 방법을 실행 또는 제어하도록 구성되는 프로그램 요소.

명 세 서

기 술 분 야

[0001] 본 발명은 트랜스폰더에 대한 접속의 유효성을 판정하는 판독기에 관한 것으로, 이 판독기는 트랜스폰더의 응답 시간을 측정하고 트랜스폰더를 인증하도록 구성된다. 또한 본 발명은 판독기에 대한 접속의 유효성을 판정하는 트랜스폰더에 관한 것으로, 이 트랜스폰더는 판독기에게 응답 시간 측정에 대한 정보를 제공한다. 또한, 본 발명은 트랜스폰더에 대한 접속의 유효성을 판정하는 판독기의 방법 및 판독기에 대한 접속의 유효성을 판정하는 트랜스폰더의 방법에 관한 것이다. 이를 넘어서, 본 발명은 프로그램 소자와 관련된다. 또한, 본 발명은 컴퓨

터 판독가능한 매체와 관련된다.

배 경 기 술

[0002] 소위 "릴레이 어택 문제(relay attack problem)"는 트랜스폰더(특히 스마트 카드 및 RFID 태그)가 사용될 때 발생한다. 트랜스폰더는 일반적으로 자신에게 매우 근접한(근거리 통신) 판독기에 의해 판독된다. 릴레이 어택으로 인해 이러한 로컬 바인딩(Local Binding)이 범죄적 행위에 노출된다.

[0003] 예를 들어, 사람 A가 바에 있고 자신의 차를 바 앞에 주차했다고 가정하자. 차에는 키가 필요없는 진입 특징부가 장착되어 있다(즉 스마트 카드와 같은 트랜스폰더를 통해 차에 접근가능하다). 사람 B는 A가 자신의 주머니에 가지고 있는 트랜스폰더로부터 데이터를 판독하여, 이 데이터를 이동 전화를 통해서 차 옆에 서있는 사람 C에게 전송한다. 이러한 방식으로 사람 A가 자신의 차를 도난당한다는 것을 인지하지 못한 채로 사람 C가 A의 차문을 열 수 있다.

[0004] 트랜스폰더가 판독기에 의해 판독될 때, 예컨대 GSM을 통한 전송이 근거리 통신보다 더 오랜 시간을 소요하기 때문에, 응답 시간의 측정이 이러한 릴레이 어택을 검출하도록 측정될 수 있다. 만약 응답 시간이 사전결정된 시간 윈도우를 벗어나면, 액세스가 거부될 수 있다. 점점 더 빨라지는 전송 수단으로 인해서, 이러한 시간 윈도우는 가능한 한 작게 형성되어야 한다.

[0005] 그러나, 인증 동안에 암호화/복호화에 필요한 시간이 존재한다. 인증을 위한 알고리즘이 점점 더 복잡해지고 있기 때문에, 시간 윈도우에 대한 물리적 제한이 존재한다.

[0006] Hancke, G.P., Kuhn, M.G.에 의한 First International Conference on Security and Privacy for Emerging Areas in Communications Networks 2005, SecureComm 2005, pp.67-73의 "An RFID Distance Bounding Protocol"은, 비접촉 스마트카드와 같은 무선 주파수 식별 토큰이 근접 인증에 사용되는 경우 릴레이 어택에 취약하다고 개시하였다. 공격자는 더 긴 거리에 걸쳐 교환된 신호를 포워딩하는 트랜스폰더를 이용하여 무선 채널의 제한된 범위를 피할 수 있다. 무선 신호의 라운드-트립 지연을 정확하게 측정하는 암호 거리-바운딩 프로토콜은 가능한 대책을 제공한다. 이는 광속보다 더 빠르게 전파할 수 있는 정보는 없다는 사실로부터 판독기와 토큰 사이의 거리에 대한 상한을 추론한다. 극-광대역 펄스 통신에 기초하는 거리-바운딩 프로토콜이 개시되었다. 특히 패시브 저가 토큰, 소음이 많은 환경과 고속 애플리케이션에 사용하기에 적합하며, 토큰 내의 오직 단순한 비동기식 저전력 하드웨어만을 이용하여 구현가능해야 한다.

발명의 내용

과제의 해결 수단

[0007] 그러므로, 본 발명의 목적은 안전한 방식으로 동작가능한 판독기 및/또는 트랜스폰더를 제공하는 것이다.

[0008] 본 발명의 목적은 독립 청구항에 따르는 트랜스폰더, 판독기, 방법, 프로그램 소자 및 컴퓨터 판독가능한 매체에 의해 획득된다.

[0009] 예시적인 실시예에 따르면, 트랜스폰더(특히 판독기와 통신상 연결될 수 있는 권한이 주어진 트랜스폰더)에 대한 접속의 유효성(validity)을 판정하는 판독기(트랜스폰더에 통신상 연결될 수 있음)가 제공되며, 트랜스폰더의 응답 시간을 측정(특히 판독기의 상응하는 요청에 응답한 것이며, 상기 응답 시간은 판독기로부터 트랜스폰더로 요청을 전송한 시각과 트랜스폰더로부터 요청에 대한 응답을 수신한 시각 사이의 시간 간격일 수 있다) 및 트랜스폰더의 인증(특히 응답 시간 측정을 위해 다른 비-암호화된 통신 메시지가 앞서 전송된 후에 트랜스폰더로부터 판독기로 전송된 암호화된 통신 메시지에 의함)이 두 개의 개별적인 단계들로 수행된다. 인증을 위해 사용되는 (특히 추후에 사용되는) 데이터의 적어도 일부가 응답 시간을 측정하는 동안에 판독기와 트랜스폰더 사이에서 전송되는 (특히 인증 이전에 전송되는) 통신 메시지 내에 포함될 수 있다.

[0010] 다른 예시적인 실시예에 따르면, 판독기에 대한 접속의 유효성을 판정하는 트랜스폰더가 제공되며, 이때 응답 시간 측정을 위한 정보 및 인증을 위한 정보가 두 개의 개별적인 단계들로 판독기에 제공된다. 인증을 위해 (특히 추후에) 사용되는 데이터의 적어도 일부는 응답 시간을 측정하는 동안에 판독기와 트랜스폰더 사이에서 전송되는 (특히 인증 이전에 전송되는) 통신 메시지 내에 포함될 수 있다.

[0011] 또 다른 예시적인 실시예에 따르면, 트랜스폰더에 대한 (판독기의) 접속의 유효성을 판정하는 판독기의 방법(또는 판독기에 의해 수행되는 방법)이 제공되며, 이 방법은, 판독기에 의해 (제 1 통신 메시지와 같은) 제 1 커맨드를 제 2 랜덤 넘버와 함께 상기 트랜스폰더(440)로 전송하는 단계(단계 1)와,

[0012] 판독기에 의해, 트랜스폰더로부터 제 1 랜덤 넘버(특히 플레인텍스트 내의 랜덤 넘버)를 수신하는 단계(단계 2)와,

[0013] 판독기에 의해, 트랜스폰더로부터 제 1 랜덤 넘버 및 제 2 랜덤 넘버의 암호(특히 암호화된 형태)를 수신하는 단계(단계 3)와,

[0014] 판독기에 의해, 트랜스폰더에 의해 사용된 것과 동일한 키로 수신된 넘버(특히 암호화된 제 1 및 제 2 랜덤 넘버)를 복호화하거나, 또는 상기 키로 제 1 랜덤 넘버 및 제 2 랜덤 넘버를 복호화하는 단계(단계 4)와,

[0015] 판독기에 의해, 단계 2의 제 1 랜덤 넘버 및 제 2 랜덤 넘버와 단계 3의 제 1 랜덤 넘버 및 제 2 랜덤 넘버가 일치하는지 여부를 체크하는 단계(단계 5)와,

[0016] 판독기에 의해, 제 1 랜덤 넘버가 사전결정된 시간 윈도우 내에서 수신되었는지 여부를 체크하는 단계(단계 6)와,

[0017] 판독기에 의해, 단계 5에서의 체크 및 단계 6에서의 체크 결과가 참인 경우에 트랜스폰더로의 접속을 유효한 것으로 인정하는 단계(단계 7)를 포함한다.

[0018] 또 다른 예시적인 실시예에 따르면, 판독기에 대한 접속의 유효성을 판정하는 트랜스폰더의 방법이 제공되며, 이 방법은,

[0019] 트랜스폰더에 의해 제 1 커맨드를 제 2 랜덤 넘버와 함께 판독기로부터 수신하는 단계와,

[0020] 트랜스폰더에 의해 제 1 랜덤 넘버를 판독기로 전송하는 단계와,

[0021] 트랜스폰더에 의해 제 1 랜덤 넘버 및 제 2 랜덤 넘버의 암호를 판독기로 전송하는 단계를 포함한다.

[0022] 또 다른 예시적인 실시예(도 5 및 상응하는 설명에서 제공되는 상세한 설명)에 따르면, 트랜스폰더에 대한 접속의 유효성을 판정하는 판독기의 방법으로서,

[0023] 제 1 커맨드를 제 2 랜덤 넘버와 함께 트랜스폰더로 전송하는 단계와,

[0024] 트랜스폰더로부터 제 1 랜덤 넘버를 수신하는 단계와,

[0025] 제 1 랜덤 넘버 및 제 2 랜덤 넘버에 기초하여 생성된 제 1 메시지 인증 코드(MAC)를 상기 트랜스폰더로 전송하는 단계와,

[0026] 제 1 랜덤 넘버 및 제 2 랜덤 넘버에 기초하여 생성된 제 2 메시지 인증 코드(MAC)를 트랜스폰더로부터 수신하는 단계와,

[0027] 제 2 메시지 인증 코드(MAC)가 유효한지 여부를 체크하는 단계와,

[0028] 제 1 랜덤 넘버가 사전결정된 시간 윈도우 내에서 수신되었는지 여부를 체크하는 단계와,

[0029] 만약 두 체크 단계의 결과가 모두 참인 경우에 트랜스폰더로의 접속이 유효한 것으로 인정하는 단계를 포함한다.

[0030] 또 다른 예시적인 실시예(도 5 및 상응하는 설명에서 제공되는 상세한 설명)에 따르면, 판독기에 대한 접속의 유효성을 판정하는 트랜스폰더의 방법으로서,

[0031] 제 1 커맨드와 제 2 랜덤 넘버를 판독기로부터 수신하는 단계와,

[0032] 제 1 랜덤 넘버를 판독기로 전송하는 단계(특히 수신된 제 1 커맨드에 응답하여 특시 전송)와,

[0033] 제 1 랜덤 넘버 및 제 2 랜덤 넘버에 기초하여 생성된 제 1 메시지 인증 코드(MAC)를 상기 판독기로부터 수신하는 단계와,

[0034] 제 1 메시지 인증 코드(MAC)가 유효한지 여부를 체크하는 단계와,

[0035] 제 1 메시지 인증 코드(MAC)가 유효한 경우, 제 1 랜덤 넘버 및 제 2 랜덤 넘버에 기초하여 생성된 제 2 메시지 인증 코드(MAC)를 전송하는 단계를 포함한다(제 1 메시지 인증 코드(MAC)가 유효하지 않으면, 트랜스폰더는 예

컨대 인증 실패를 나타내도록 생성될 수 있는, 제 1 랜덤 넘버 및 제 2 랜덤 넘버에 기초하여 생성되지 않은 다른 메시지 인증 코드(MAC)를 판독기에 전송할 수 있다).

[0036] 본 발명의 또 다른 예시적인 실시예에 따르면, 프로그램 소자가 제공되며(예컨대, 예컨대 다운로드 가능한 프로그램과 같이 소스 코드 또는 실행가능한 코드로의 소프트웨어 루틴), 프로세서에 의해 실행되면, 전술된 특성들을 갖는 방법들 중 하나를 제어 또는 실행하도록 구성된다.

[0037] 본 발명의 또 다른 예시적인 실시예에 따르면, 컴퓨터 프로그램이 저장되는 컴퓨터 판독가능한 매체(예컨대 CD, DVD, USB 스틱, 플로피 디스크 또는 하드디스크)가 제공되고, 상기 컴퓨터 프로그램이 프로세서에 의해 실행되면 전술된 특성들을 갖는 방법들 중 하나를 제어 또는 실행하도록 구성된다.

[0038] 본 발명의 실시예에 따라 수행될 수 있는 데이터 프로세싱은 컴퓨터 프로그램, 즉 소프트웨어에 의해 구현될 수 있거나 또는 하나 이상의 특정한 전자 최적화 회로, 즉 하드웨어를 이용하여 구현될 수 있거나, 또는 소프트웨어 구성요소와 하드웨어 구성요소의 조합인 혼합 형태로 구현될 수 있다.

[0039] "트랜스폰더(transponder)"라는 용어는 특히 RFID 태그 또는 (예를 들어 비접촉) 스마트 카드를 나타낼 수 있다. 보다 일반적으로, 트랜스폰더는 인테로게이터(interrogator)로부터의 특정 신호에 의해 활성화되었을 때 소정의 (예컨대 코딩된) 데이터를 자동으로 전송할 수 있는 디바이스(예를 들어 칩을 포함함)일 수 있다.

[0040] "판독기(reader)"라는 용어는 트랜스폰더를 판독하고 반영 또는 생략된 신호를 다시 검출하기 위해 전자기적 복사 빔을 전송하도록 구성된 기지국을 특히 나타낼 수 있다. 판독기 디바이스는 판독 및/또는 입력 디바이스, RFID 판독기, 비접촉 칩 카드 판독기, 패시브 트랜스폰더 및 근거리 통신 디바이스로 이루어지는 그룹 중 하나로서 구성될 수 있다. 그러나, 통신은 유선 인터페이스 상에서도 이루어질 수 있다.

[0041] 하나 이상의 "애플리케이션"이 트랜스폰더 및 판독기에 의해 형성된 통신 시스템에 의해 제공될 수 있다. 이러한 애플리케이션은 특히 판독기 및 트랜스폰더에 의해 형성된 통신 시스템 내의 서비스를 나타낼 수 있으며, 이러한 서비스에 대해 트랜스폰더 및/또는 판독기가 기여할 수 있다. 이러한 기여의 제공은 저장 또는 계산된 데이터를 제공하고, 프로세싱 성능을 제공하는 등의 트랜스폰더의 성능을 포함할 수 있다. 이러한 서비스의 예시는 트랜스폰더의 사용자에 의한 대중 교통 수단의 사용에 대한 비용 지불, 무선 지불 시스템에 의한 상품의 구매 비용의 지불 등이다.

[0042] "메시지 인증 코드(MAC; message authentication code)"라는 용어는 메시지를 인증하는 데에 사용되는 정보의 짧은 조각을 특히 나타낼 수 있다. MAC 알고리즘은 인증될 임의 길이의 메시지 및 비밀 키를 입력으로서 수용할 수 있고, MAC을 출력할 수 있다. MAC 값은 입증가(비밀 키를 소유한 사람) 메시지 콘텐트에 대한 임의의 변화를 검출하도록 함으로써 자신의 진위뿐 아니라 메시지의 데이터 완전성도 보호할 수 있다.

[0043] 본 발명의 실시예는 판독기와 트랜스폰더 사이의 접속이 유효한지 여부에 대한 인정(즉 접속이 불법적인 것인지 아닌지에 대한 판정)이 응답 시간 측정을 위한 통신과 보안 목적의 통신을 시간적으로 분리시킴으로써 높은 확실성을 가지고 수행될 수 있다는 장점을 제공한다. 다시 말하면, 어택, 특히 릴레이 어택이 검출될 가능성이 높다. 이것은 트랜스폰더의 응답 시간 측정으로부터 암호화 동작에 필요한 시간을 분리시킴으로써 달성될 수 있다. 또한, 시간 측정 섹션 동안의 판독기와 트랜스폰더 간의 통신이 후에 인증을 위해 사용되는 코드를 전송하도록 공동으로 사용될 수 있다. 이것은 매우 효율적인 대역폭의 사용 및 신속한 초기화 페이즈를 가능케 할 수 있다. 또한, 이러한 코드를 교환함으로써, 두 엔티티 내의 이러한 코드들의 동시 생성이 방지될 수 있으며, 그에 따라 이러한 코드가 두 엔티티 중 하나에서만 생성되어도 충분하기 때문에, 시스템의 계산적 부담을 감소시킨다. 예를 들어, 판독기에게 응답 시간 측정에 즉시 응답할 것을 요청하는 트랜스폰더로부터 판독기로의 제 1 커맨드는 후속하는 암호화된 인증에 사용되는 코드의 일부로서 랜덤 넘버를 수반할 수 있다.

[0044] 본 발명의 실시예는 아래의 추가적인 장점을 가질 수 있다:

[0045] 예를 들어, 이러한 시스템은 대중 교통수단에 적용될 수 있지만, 차량의 키가 필요없는 진입 시스템 및 다수의 다른 애플리케이션에도 적용될 수 있다.

[0046] 상응하는 통신 시스템은 예를 들어 오직 특정한 위치에서만 소비되는 DRM 보호 콘텐트에 적용가능하다.

[0047] 상응하는 통신 시스템이 예를 들어 집에 있어야만 하는 가석방된 죄소에게 적용가능하다.

[0048] 그러므로, 본 발명의 실시예는 판독기와 트랜스폰더 간의 접속의 유효성을 판정하는 적절한 솔루션을 제공한다.

[0049] 아래에서, 판독기의 추가의 예시적인 실시예가 기술될 것이다. 그러나, 이러한 실시예는 트랜스폰더, 방법, 프

로그램 소자 및 컴퓨터 판독가능한 매체에도 적용된다.

[0050] 예시적인 실시예에 따르면, 판독기는 트랜스폰더에 제 1 커맨드를 전송한 시각과 제 1 커맨드에 응답하여 트랜스폰더로부터 제 1 랜덤 넘버를 수신한 시각 사이의 시간 간격에 기초하여 응답 시간을 측정하도록 구성된다. 다시 말하면, 응답 시간은 트랜스폰더가 판독기의 질의에 대한 응답을 전송하는 데에 요구되는 시간을 나타낼 수 있다. 판독기가 이러한 시간 간격을 측정할 때, 제 1 랜덤 넘버를 전송하기 위해 트랜스폰더에게 요청된 시간을 평가하는 것이 가능하다. 릴레이 어택 문제(어택으로 인한 추가 전송 경로를 포함)의 경우에, 이러한 시간은 사전결정된 문턱값보다 더 길 것이다. (암호화로 인한 지연이 예상되지 않도록) 트랜스폰더가 응답 시간 측정의 측면에서 판독기에게 제 1 랜덤 넘버를 전송하기 이전에 이를 암호화하지 않은 경우, 판독기와 트랜스폰더 간의 메시지들의 전파에 더하여 임의의 추가 지연이 릴레이 어택으로부터 발생할 가능성이 높다. 이러한 추가 지연의 부재는 판독기가 트랜스폰더와의 통신이 유효하다고 판정하도록 할 수 있다. 특히 플레인텍스트(plaintext) 또는 비암호화된 방식으로 제 1 랜덤 넘버가 (제 1 요청에 응답하여) 판독기에 의해 수신되는 시나리오에서, 트랜스폰더의 응답 시간은 릴레이 어택 문제가 존재하는지 여부를 판정하기 위한 적절한 수단이다. 예를 들어, 만약 측정된 응답 시간이 사전결정된 문턱값보다 더 작으면, 트랜스폰더와 판독기는 유효한 것으로 분류될 수 있다.

[0051] 앞서 기술된 실시예를 다시 참조하면, 판독기는 응답 시간 측정을 위해 제 1 랜덤 넘버가 수신된 후 트랜스폰더로부터 수신된 제 1 랜덤 넘버의 암호가, 응답 시간 측정을 위해 수신된 제 1 랜덤 넘버와 일치하는지 여부에 대한 평가에 기초하여 트랜스폰더를 인증하도록 구성된다. 다시 말하면, 제 1 커맨드에 응답하여 전송된 제 1 랜덤 넘버는 제 2 커맨드에 응답하여 전송된 제 1 랜덤 넘버(복호화 후, 암호화된 제 1 랜덤 넘버는 트랜스폰더로부터 판독기로 전송될 수 있다)와 비교될 수 있다. 따라서, 동일한 랜덤 넘버가 오직 응답 시간 측정을 목적으로 암호화되지 않고 전송되고, 후속하여 인증을 위해 암호화된 방식으로 재전송되기 때문에, 응답 시간 측정은 인증 입증으로부터 분리될 수 있다.

[0052] 바람직한 실시예에서, 제 1 커맨드와 제 2 랜덤 넘버를 함께 트랜스폰더로 전송한 시각과 제 1 커맨드에 응답하여 트랜스폰더로부터 제 1 랜덤 넘버를 수신한 시각 사이의 시간 간격에 기초하여 응답 시간을 측정하도록 구성된다. 다시 말하면, 제 1 요청의 전송과 함께, 판독기는 트랜스폰더에게 다음과 같은 두 가지 목적 중 적어도 하나를 위해 후속하여 사용될 수 있는 제 2 랜덤 넘버를 동시에 전송할 수 있다. 하나의 목적은 이후의 세션에서 트랜스폰더에 의해 사용될 수 있는 제 3 랜덤 넘버를 유도하기 위해서 수신된 제 2 랜덤 넘버가 트랜스폰더에 의해 사용될 수 있다는 것이다. 다른 목적은 인증을 위해 판독기로부터 트랜스폰더로 전송되는 제 2 랜덤 넘버가 (제 1 랜덤 넘버에 추가로) 사용될 수 있다는 것이며, 이는 아래에서 설명될 것이다.

[0053] 즉, 판독기 디바이스는 응답 시간 측정을 위해 제 1 랜덤 넘버가 수신된 후 트랜스폰더로부터 수신된 제 2 랜덤 넘버의 암호 및 제 1 랜덤 넘버의 암호가, 응답 시간 측정을 위해 수신된 제 1 랜덤 넘버 및 제 2 랜덤 넘버와 일치하는지 여부에 대한 평가에 기초하여 트랜스폰더를 인증하도록 구성된다. 이러한 시나리오에서, 판독기는 응답 시간 측정의 측면에서 트랜스폰더에게 제 2 랜덤 넘버를 전송할 수 있다. 이후의 절차에서, 전송기는 판독기로부터 수신된 제 2 랜덤 넘버 및 트랜스폰더 내에 이미 저장된 제 1 랜덤 넘버 모두를 갖는 인증 메시지를 암호화할 수 있다. 이들 두 랜덤 넘버는 특정한 키(판독기에게도 알려질 수 있음)를 이용하여 함께 암호화될 수 있다. 이것은 트랜스폰더를 안전하게 식별하고 동시에 오직 권한이 주어진 트랜스폰더만이 판독기와 통신하는 것을 보장함으로써 높은 안전도를 가지고 릴레이 어택 문제를 제거하도록 할 수 있다.

[0054] 이러한 판독기는 응답 시간 간격이 사전결정된 시간 윈도우(time window)(예를 들어 사전정의된 문턱값보다 작음) 내에 있고 트랜스폰더로부터 판독기로 인코딩된 형태로 전송되는 제 1 랜덤 넘버(및 선택적으로 추가의 제 2 랜덤 넘버) 사이에 일치가 존재한다는 판정에 따라서만 트랜스폰더로의 접속이 유효하도록 구성된다. 따라서, 두 기준 간의 로직 AND 조합이 트랜스폰더와 판독기 간의 접속을 유효한 것으로서 수용하는 데에 필요할 수 있다. 제 1 기준은 제 1 커맨드에 응답하는 트랜스폰더의 시간 간격이 사전결정된 문턱값보다 짧다는 것이다. 이것은 릴레이 어택 문제가 배제될 수 있음을 보장할 수 있다. 제 1 응답의 전송이 프로세싱 로드 또는 트랜스폰더에 의해 수행되는 태스크 없이 수행되기 때문에, 실제 전송 시간은 트랜스폰더와 판독기 간의 전송 경로의 길이에 대한 적절한 측정법이며, 릴레이 어택 문제의 경우에서 상당히 변화된다. 제 2 기준은 제 1 커맨드에 응답된 동일한 트랜스폰더가 제 1 랜덤 넘버(트랜스폰더 내에 저장됨) 및 제 2 랜덤 넘버(제 1 커맨드와 함께 판독기에 의해 전송됨)의 조합에 의해 형성될 수 있는 암호화된 패스워드를 제공한다.

[0055] 이러한 판독기는 복수의 통신 메시지들로 분할된 데이터를 인증을 위해 및/또는 근접 체크(a proximity check)를 위해 트랜스폰더와 교환하도록 구성된다. 그러므로, 모든 인증 정보 또는 모든 근접 체크(예를 들어 응답

시간 측정에 의함) 정보가 판독기와 트랜스폰다 사이에서 교환되는 단일 메시지 내에 포함될 필요는 없다. 반대로, 상응하는 코드가 판독기로부터 트랜스폰더로 전송되는 서로 다른 통신 메시지에 의해 전송될 수 있는 서로 다른 섹션으로 분할될 수 있거나, 그 역이 성립한다. 예를 들어, 근접성 체크는 정제된 시간 정보를 획득하기 위해서 복수의 조각들로 분할될 수 있다.

[0056] 판독기는 순환 중복 검사(CRC; Cyclic Redundancy Check)로부터 자유롭게 상기 제 1 커맨드(제 2 랜덤 넘버를 포함할 수 있음)를 전송하도록 구성된다. 이러한 컨셉은 판독기로부터 태그로 통신되는 데이터 섹션의 엔드에 부착된 CRC에 의존하는 ISO 14444-4 시스템과 비교하여 기본적으로 서로 다른 접근법이다. 본 발명의 실시예는 오류 보정을 위해 태그로부터 판독기로 전송되는 응답 메시지에 CRC를 부착할 수 있다. 판독기가 불법적인 통신이 발생하지 않았다는 판정을 하기 위해, CRC는 제 1 커맨드(제 2 랜덤 넘버를 포함함) 및 응답(제 1 랜덤 넘버를 포함함)을 포함할 수 있다.

[0057] 다음으로, 트랜스폰더의 다른 예시적인 실시예가 기술될 것이다. 그러나, 이들 실시예는 판독기, 방법, 프로그램 소자 및 컴퓨터 판독가능한 매체에도 적용된다.

[0058] 트랜스폰더는 자신으로부터 수신된 제 1 커맨드에 응답하여 응답 시간 측정을 위해 판독기에 제 1 랜덤 넘버를 전송하도록 구성될 수 있다. 이러한 제 1 랜덤 넘버는 비암호화된(또는 플레인텍스트) 형식으로 트랜스폰더로부터 판독기로 전송될 수 있다. 이러한 방법을 취함으로써, 암호화 절차의 성능이 인위적으로 응답 시간을 증가시키고 판독기와 통신하는 권한이 부여된 트랜스폰더의 보통 응답과 릴레이 어택 문제의 존재를 구별하는 것을 불가능하게 할 수 있기 때문에, 트랜스폰더로부터 응답을 수신하고 판독기에 의해 커맨드를 전송하는 시각 사이의 시간 간격의 측정이 트랜스폰더에 의해 수행될 암호화 절차에 의해 인위적으로 지연되지 않는 것이 가능해진다. 따라서, 비암호화된 방식으로 제 1 랜덤 넘버를 전송하는 것은 유효성과 관련된 판정의 신뢰가능성을 증가시킨다.

[0059] 특히, 트랜스폰더는 응답 시간 측정을 위해 판독기에게 지연되지 않은 제 1 랜덤 넘버를 전송하도록 구성될 수 있다. 따라서, 트랜스폰더는 제 1 커맨드에 응답하는 제 1 랜덤 넘버의 전송이 어떠한 추가의 프로세싱 등으로 인한 지연도 추가하지 않고 발생하는 것이 가능하도록 구성될 수 있다. 이것은 릴레이 어택 문제의 존재가 신뢰가능한 방식으로 검출가능한 가능성을 증가시킬 수 있다.

[0060] 트랜스폰더는 제 2 랜덤 넘버를 포함하는 제 1 커맨드에 응답하여 제 1 랜덤 넘버를 전송하도록 구성될 수 있다. 따라서, 제 1 커맨드는 제 1 랜덤 넘버를 포함하는 응답을 다시 전송하기 위해 트랜스폰더에 대한 트리거로서 사용될 수 있는 제2 넘버를 포함할 수 있다. 예를 들어, 제 1 랜덤 넘버를 판독기에 전송한 후에, 트랜스폰더는 이후의 세션(세션은 카드가 판독기의 무선 범위를 다시 남겨둘 때까지 지속된다)에서 제 1 랜덤 넘버를 대체하도록 제 2 랜덤 넘버에 기초하여 제 3 랜덤 넘버를 생성 및 저장할 수 있다. 예를 들어, 제 2 랜덤 넘버가 트랜스폰더에 저장되고, 소정의 알고리즘이 제 3 랜덤 넘버를 계산하도록 제 2 랜덤 넘버에 적용되는 것이 가능하다. 이 모든 것은 제 1 랜덤 넘버를 다시 판독기로 전송한 후에 수행될 수 있으며, 즉 트랜스폰더가 자유 프로세싱 용량을 갖는 간격에서 수행될 수 있다. 이러한 절차는 트랜스폰더와 판독기 디바이스 사이에서 통신을 위해 다른 세션을 위해서 제 1 랜덤 넘버를 업데이트하고, 그에 따라 응답 시간 측정 및 인증을 위해 트랜스폰더와 판독기 사이에서 교환되는 랜덤 넘버의 교환으로 인해 안전성을 추가로 증가시키도록 할 수 있다.

[0061] 트랜스폰더는 제 1 커맨드를 전송한 후에 트랜스폰더로부터 전송된 제 2 커맨드의 수신 후에 제 1 랜덤 넘버의 암호를 전송하도록 구성될 수 있다. 그러므로, 제 2 커맨드는 트랜스폰더로부터 비암호화된 방식으로 판독기가 제 1 랜덤 넘버를 수신한 후에 판독기에 의해 전송될 수 있다.

[0062] 그러나, 제 1 랜덤 넘버 및 제 2 랜덤 넘버의 암호화가 트랜스폰더에 의해 수행될 때, 트랜스폰더가 릴레이 어택 문제를 제외시키도록 충분히 빠른 방식으로만 응답하지 않음을 판독기에게 보장하지만, 이것은 제 1 및 제 2 랜덤 넘버뿐 아니라 암호화 키에 대한 인지를 필요로 하기 때문에 현재 통신하는 트랜스폰더는 이러한 통신에 대해 권한이 부여된 것이다.

[0063] 제 1 및 제 2 랜덤 넘버를 포함하는 암호화된 통신 메시지의 수신에 따른 인증을 위해서, 판독기는 두 가지 기회를 갖는다. 첫번째 기회는 트랜스폰더로부터 획득된 제 1 및 제 2 랜덤 넘버를 포함하는 암호화된 통신 메시지를 복호화하고 판독기의 메모리에 저장된 제 1 및 제 2 랜덤 넘버를 플레인텍스트로 갖는 복호화된 제 1 및 제 2 랜덤 넘버를 비교하는 것이다. 즉, 판독기는 트랜스폰더로부터의 제 1 응답 내에서 제 1 랜덤 넘버를 수신한다. 또한, 판독기는 제 1 커맨드를 이용하여 트랜스폰더에게 제 2 랜덤 넘버를 전송하였으며, 판독기는 이미 제 2 넘버를 알고 있다. 두번째 기회는 트랜스폰더에 의해 사용되는 알려진 키를 갖는 알려진 제 1 및 제 2

랜덤 넘버를 판독기가 암호화하는 것이다. 그 다음, 판독기에 의해 생성된 암호화된 통신 메시지는 트랜스폰더로부터 획득된 제 2 응답과 비교될 수 있다.

[0064] 트랜스폰더는 판독기와 교환된 통신 메시지를 분석함으로써 트랜스폰더가 판독기 부근에 있는지 여부를 결정하고, 트랜스폰더가 판독기 부근에 있지 않다는 판정에 따라 통신을 종료하도록 구성된다. 그러므로, 판독기가 판독기와 트랜스폰더 사이의 충분한 근접성을 분석할 수 있을 뿐 아니라(예를 들어 판독기와 트랜스폰더 간의 거리가 문턱값보다 작은지 또는 응답 시간이 문턱값보다 작은지), 판독기 또한 충분한 근접성과 관련된 사전정의된 기준이 만족되는지 여부의 체크를 수행할 수 있다. 입증 근접 체크(VPC) 메시지 및 응답이 근접을 판정하도록 할 수 있다(판독기는 트랜스폰더가 수신 및 전송한 것을 체크하고 시가나 측정을 수행하며, 트랜스폰더는 자신이 수신한 것과 판독기가 수신한 것을 체크한다).

[0065] 트랜스폰더는 복수의 통신 메시지들로 분할된 데이터를 인증을 위해 및/또는 근접 체크를 위해서 판독기와 교환하도록 구성될 수 있다. 따라서, 모든 인증 정보 또는 (예컨대 응답 시간 측정에 의한) 모든 근접 체크가 정보가 판독기와 트랜스폰더 사이에서 교환된 단일 메시지 내에 포함될 필요는 없다. 반대로, 상응하는 코드들이 판독기로부터 트랜스폰더로 전송되는 서로 다른 통신 메시지들에 의해 전송될 수 있는 서로 다른 섹션들로 분할될 수 있거나, 그 역이 가능하다. 예를 들어, 근접 체크는 정제된 시간 정보를 획득하기 위해 복수의 조각들로 분할될 수 있다.

[0066] 트랜스폰더는 제 1 랜덤 넘버를 순환 중복 체크(CRC)와 함께 판독기로 전송하도록 구성될 수 있다. 오류 복구는 커맨드를 포함하는 응답에 대해 CRC를 적용함으로써 수행될 수 있다. CRC는 RAC1 커맨드, Random #1 및 Random #2에 대해 계산될 수 있다.

[0067] 트랜스폰더는 타이밍을 나타내는 정보, 특히 트랜스폰더와 판독기 사이의 통신 속도를 나타내는 정보와 함께 통신 메시지를 판독기에 전송하도록 구성될 수 있다. 이러한 정보는 통신 파트너들 간의 동작 속도를 나타낼 수 있다. 상응하는 데이터 섹션은 판독기와 트랜스폰더 사이에서 교환되는 통신 메시지 내에 포함될 수 있고 PPSE 데이터 필드로서 표기될 수 있다. 판독기는 트랜스폰더와의 통신을 중단하기 위해서 이것을 이용할 수도 있다.

[0068] 트랜스폰더는 주파수를 검출 및 제한하도록 구성되되, 동작시에 상기 주파수가 범위를 벗어나면, 판독기와의 통신을 중단한다. 이것은 잔여 릴레이 어택 윈도우(residual relay attack window)를 제한하기 위해 수행될 수 있다.

[0069] 트랜스폰더 커맨드에 대한 응답은 선택적으로 CRC를 포함하여 RndR 외에 다수의 바이트를 포함할 수 있다. 트랜스폰더 커맨드는 CRC를 갖지 않는다. 다른 실시예에서, 이것은 트랜스폰더로부터 전송되는 부분 RndR이 부분 RndR를 이용하여 확장되어 수신된 것과 같은 트랜스폰더 커맨드(랜덤 넘버를 포함함) 상의 CRC에 의해 이어질 수 있도록 변경될 수 있다. 이전의 판독기는 근접 체크가 통신 오류 후에 실패할 수 있도록 통신 오류를 검출하여 그것을 복구하는 능력이 없고, 트랜스폰더가 필드 밖으로 나오거나 해제되어야만 했다. 트랜스폰더 커맨드에 대한 CRC는 잔여 릴레이 어택 윈도우를 넓힐 수 있기 때문에 수행되어서는 안된다. 이후의 실시예에서, 판독기는 통신 오류를 검출할 수 있고, 그 경우 근접 체크 동작을 재시작한다(코스의 새로운 RndC 및 RndR을 이용함).

[0070] 각각의 랜덤 넘버는 의사 랜덤 넘버(pseudo random number) 또는 진정한 랜덤 넘버(truly random number)일 수 있다. 의사 랜덤 넘버와는 반대로, 진정한 랜덤 넘버는 자신의 생성 기준과 무관하게 생성되는 넘버이다. 암호화를 위해서, 물리적 측정법에 기초하는 넘버들이 랜덤으로 간주될 수 있다. 의사 랜덤 넘버는 가능한 한 검출가능하지 않은 패턴을 갖지만 진정한 랜덤은 아닌 넘버들일 수 있다. 컴퓨터 프로그램은 진정한 랜덤 넘버를 만들 수 없기 때문에 의사 랜덤 넘버를 만들 수 있다. 랜덤 넘버 생성기는 트랜스폰더/판독기의 일부일 수 있다.

[0071] 임의의 랜덤 넘버와 키는 숫자 캐릭터의 시퀀스, 문자들의 시퀀스, 또는 알파벳-숫자 코드일 수 있다.

[0072] 본 발명의 실시예는 트랜스폰더와 관련되고, 특히 스마트 카드 및 RFID 태그와 관련된다. 명확성을 위해서, 본 명세서는 주로 스마트 카드를 참조로 설명되었지만, 당업자는 본 발명의 실시예가 일반적으로 RFID 태그 및 트랜스폰더 및 유선 또는 무선 접속 상에서 통신하는 일반적인 디바이스에도 동일하게 관련된다는 것을 이해할 것이다.

[0073] 본 발명의 이러한 측면들과 다른 측면들이 아래에서 실시예들을 참조로 하여 명백하게 설명될 것이다.

도면의 간단한 설명

[0074] 도 1은 릴레이 어택의 원리를 도시한 도면.

도 2는 본 발명의 예시적인 실시예에 따른 트랜스폰더와 판독기 간의 메시지 흐름도.

도 3은 본 발명의 실시예가 사용될 수 있는 예시적인 필드를 도시한 도면.

도 4는 본 발명의 예시적인 실시예에 따른 통신 시스템을 도시한 도면.

도 5는 본 발명의 다른 예시적인 실시예에 따른 판독기와 트랜스폰더 사이의 메시지 흐름도.

발명을 실시하기 위한 구체적인 내용

[0075] 본 발명은 첨부된 도면을 참조로 하여 예시적인 방식으로 아래에서 더욱 자세하게 기술될 것이다.

[0076] 본 발명의 도면은 개략적으로 도시되었다. 서로 다른 도면들에 걸쳐, 유사하거나 동일한 구성요소들에 대해 동일한 참조부호가 사용되었다.

[0077] 본 발명의 예시적인 실시예는 트랜스폰더 판독기 시스템(transponder reader system)의 릴레이 어택(relay attack)을 방지할 수 있게 한다.

[0078] 아래에서, 도 1 을 참조하여 릴레이 어택이 설명될 것이다.

[0079] 이러한 목적으로, 트랜잭션을 위한 것과 같이 근거리에 있지 않고 멀리 떨어진 보안 소자를 이용하는 트랜잭션이 고려된다.

[0080] 도 1은 트랜스폰더(120) 및 실물 판독기(140)가 근접하게 위치한 경우의 정상 동작을 나타내는 제 1 시나리오(100)를 도시한다. 트랜스폰더(120)는 예를 들어 스마트 카드 또는 NFC(Near Field Communication) 폰일 수 있다.

[0081] 도 1은 릴레이 어택의 존재를 나타내는 제 2 시나리오(150)를 도시한다. 트랜스폰더(120) 및 판독기(140)에 추가로, 인트루더(intruder)(160)의 제 1 통신 디바이스 및 인트루더(170)의 제 2 통신 디바이스가 트랜스폰더(120) 및 판독기(140)의 통신 경로 내에 도입된다. 추가적인 통신 디바이스(160, 170)의 존재가 트랜스폰더(120)와 판독기(140) 간의 통신 시간을 증가시키는 결과를 갖지만, 이것은 통상적으로 통신 디바이스(160, 170)가 원치 않는 방식으로 트랜스폰더(120) 또는 리더(140)를 동작시킬 수 있다.

[0082] 릴레이 어택(relay attack)은 이들 디바이스(160, 170)가 어떠한 키도 알지 못할 때 동작할 수 있다. 릴레이 어택은 특히 트랜잭션이 (대중 교통수단(mass transit)으로의 액세스와 같은) 사용자 동작을 요구하지 않고 이루어질 수 있을 때 잘 동작할 수 있다. 예를 들어, 만원 버스 또는 지하철에서, 공격자는 판독기(140)로서 동작하는 인트루션 디바이스(160, 170)에 반응하는 트랜스폰더를 가지고 있는 사람을 쉽게 발견할 수 있다. 지하철의 진입 역에서 자신의 전화기를 들고 있는 누군가에게 이동 전화(160 또는 170)를 통해 통신하는 것이 가능하다. 이렇게 통신하는 사람을 액세스를 획득할 수 있고, 버스 내에 있는 사람이 그 비용을 지불하게 된다. 이러한 릴레이 어택은 예를 들어 대중 교통수단뿐 아니라 승용차 내의 키가 없는 진입 시스템에도 적용가능하다.

[0083] 그러나, 전술된 시스템 설명은 단지 본 발명의 실시예가 성공적인 릴레이 어택을 방지하는 데에 사용될 수 있는 일례이다. 릴레이 어택을 시도하는 인트루더의 다른 시나리오로서, 본 발명의 예시적인 실시예를 다른 시스템에서 원거리의 서비스를 이용하고자 하지만 서비스는 단지 근접한 사용자에게만 사용가능한 경우의 적법한 사용자에게도 적용할 수 있다. 예를 들어, DRM 보호 콘텐트는 오직 특정한 위치에서 또는 집에서 지내야 하는 가석방된 죄수에 의해서만 소비된다. 따라서, 본 발명의 예시적인 실시예는 완전히 서로 다른 기술적 시나리오에 적용될 수 있다.

[0084] 본 발명의 예시적인 실시예의 요점은 트랜스폰더의 응답 시간을 측정하는 것이다. 릴레이 어택이 실행되면 이는 다소 시간이 소요될 것이다. 판독기가 응답 시간이 평소보다 더 긴 것을 검출하면(오차범위를 넘음), 릴레이 어택이 시작되었다고 결론내릴 수 있다. 트랜스폰더는 동일하게 수행할 수 있다.

[0085] 그러나, 이러한 시나리오는 비-어택 시스템의 응답이 올 수 있는 시간 윈도우(window of time)가 존재한다는 문제점을 발생시킬 수 있다. 만약 이러한 윈도우가 넓다면, (하나의 시스템 또는 시스템들 사이에서) 시스템 양상에서의 큰 변화를 수용하고, 고속 시스템은 어택을 시작할 시간을 남긴다. 본 발명의 예시적인 실시예에 따

른 솔루션은 시간 윈도우를 가장 빠른 릴레이 어택을 추가할 수 있는 시간의 양보다 더 작게 만드는 것이다. 따라서, 릴레이 어택 윈도우는 가능한 한 작게 형성되어야만 한다.

[0086] 도 2는 본 발명의 예시적인 실시예가 구현되는 통신 시스템을 도시한다. 도 4를 참조하면, 판독기는 참조번호(420)로 표기되고 트랜스폰더는 참조번호(440)로 표기되었다. 도 2는 또한 트랜스폰더(440)의 보안부(205)와 트랜스폰더(440)의 모뎀 칩 또는 기능(210)을 구별한다. 판독기(420)는 판독기 칩 부분(215)과 특정 애플리케이션(220)의 조합으로서 간주될 수 있다. 도 2의 수평 방향을 따라서, 트랜스폰더(440)와 판독기(420)에 의해 형성되는 통신 시스템에서의 이벤트가 도시되었다. 도 2의 수직 방향에 따라 시간이 플롯되었다.

[0087] 도 2는 본 발명의 실시예가 실시되는 방식을 상세하게 도시한다.

[0088] 단계 0에서, 그 자체가 알려져 있는 충돌 방지 절차(anti-collision procedure) 이후에, 판독기(420)는 추가의 통신을 위해 자신의 무선 범위 내에서 트랜스폰더들 중 하나를 선택할 수 있다. 트랜스폰더(440)에서, 릴레이 어택 체크 RAC1의 제 1 부분에 대한 커맨드가 도착할 때에 준비되어 있도록 제 1 랜덤 넘버 RANDOM #1가 기록 버퍼 내에 저장된다.

[0089] 단계 1에서, 애플리케이션(220)(예를 들어 판독기 칩(215)과 접속되는 마이크로컨트롤러 상에 위치됨)은 릴레이 어택 체크 RAC1의 제 1 부분에 대한 커맨드 및 제 2 랜덤 넘버 RANDOM #2를 판독기 칩(215)으로 전송한다. 판독기 칩(215)은 추가의 프로세싱 없이 트랜스폰더(440)의 칩(210)으로 데이터를 전송한다.

[0090] 단계 2에서, 카드(440)는 제 1 랜덤 넘버 RANDOM #1를 즉시 판독기(420)로 다시 전송하며, 이때 제 1 랜덤 넘버 RANDOM #1는 단계 0에서 카드 칩 내에 저장되어 있던 것이다.

[0091] 단계 3에서, 제 2 랜덤 넘버 RANDOM #2가 제 3 랜덤 넘버 RANDOM #3에 대한 베이스로서 제 2 랜덤 넘버를 취하는 트랜스폰더(440)의 암호 프로세서(205)로 전송된다. 그 다음 이러한 제 3 랜덤 넘버 RANDOM #3은 판독기(420)의 다음 요청을 위해 저장된다(제 1 랜덤 넘버 RANDOM #1은 그 다음에 겹쳐쓰기(overwritten)된다).

[0092] 단계 4에서, 애플리케이션(220)은 릴레이 어택 체크 RAC2의 일부에 대한 커맨드를 전송한다. 이러한 커맨드는 트랜스폰더(440)의 암호 프로세서(205)로 투명하게 포워딩된다.

[0093] 단계 5에서, 암호 프로세서(205)는 제 1 랜덤 넘버 RANDOM #1 및 제 2 랜덤 넘버 RANDOM #2를 암호화하여 그 결과인 MAC(RANDOM #1, RANDOM #2)을 판독기(420)로 다시 전송한다.

[0094] 단계 6에서, 애플리케이션(220)은 트랜스폰더(440)에 의해 사용되는 것과 동일한 키를 이용하여 수신된 데이터를 복호화하거나 또는 다시 동일한 키를 이용하여 제 1 랜덤 넘버 RANDOM #1 및 제 2 랜덤 넘버 RANDOM #2를 암호화한다. 본 발명의 실시예가 대칭적 키 암호화로 제한되는 것은 아님을 인지해야 한다. MAC는 공용 키 인프라구조 등을 이용하여 수행될 수도 있다. 그 다음 애플리케이션(220)은 이전에 전송되었던 제 2 랜덤 넘버 RANDOM #2 및 이전에 수신되었던 제 1 랜덤 넘버 RANDOM #1가 동시에 발생하였는지 여부를 체크한다.

[0095] 단계 7에서, 제 1 랜덤 넘버 RANDOM #1가 전용 시간 윈도우 내에서 수신되었는지 여부 및 트랜스폰더(440)가 유효하게 인증되었는지 여부에 대한 체크가 수행된다. 만약 두 가지 조건이 모두 만족되면, 판독기(420)와 트랜스폰더(440) 간의 접속이 변질되지 않으며, 이는

[0096] a) 제 1 랜덤 넘버 RANDOM #1이 유효 시간 프레임 내에서 수신되었고,

[0097] b) 제 1 랜덤 넘버 RANDOM #1이 확실히 유효한 트랜스폰더(440)로부터 왔기 때문이다.

[0098] 복잡한 계산이 필요하지 않기 때문에, 단계 2는 즉시 단계 1에 후속하여 실행된다. 또한, 응답 시간은 만약 포괄적인 암호화 절차가 존재하는 경우 발생할 수 있는 상당한 지터(jitter)를 겪지 않는다. 따라서, 유효 시간 윈도우는 매우 작게 형성될 수 있다. 시간 소비적인 인증 절차는 "여기(excitement) 없이" 실행될 수 있다. 따라서, 응답 시간 및 인증 절차의 측정은 완전히 분리된다.

[0099] 아래에서는, 일부 추가적인 고려사항이 설명될 것이다:

[0100] 본 발명의 실시예는 챌린지-응답 프로토콜에 기초하지만, 챌린지에 기초하는 응답을 계산하는 데에 시간이 필요하지 않다.

[0101] 타이밍은 전송된 메시지 RAC1 및 수신된 랜덤 넘버에 기초하여 정확하게 결정될 수 있다.

[0102] 체인 내에는 오직 낮은 지터를 갖는 구성요소들만이 존재한다. 따라서, 매우 작은 잔여 릴레이 어택 윈도우가

존재할 수 있다.

[0103] 메시지의 위조를 검출하기 위해서, MACed RANDOM #1 및 RANDOM #2가 전송된다. 응답은 SAM 또는 애플리케이션(220)에 의해 체크된다.

[0104] 인트루더는 MAC을 계산할 수 없다.

[0105] RAC2 커맨드는 이론적으로 필요하지 않다. MACed RANDOM #1 및 RANDOM #2는 요청 없이도 전송될 수 있다.

[0106] 프로토콜은 릴레이 어택 체크가 하나의 세션에서 다수 실행되는 것을 허용하며, 따라서 random #3도 실행되도록 한다. 만약 재체크(recheck)가 필요하지 않으면 이것은 배제될 수 있다. 그러나 예를 들어 디바이스의 적법한 소유자가 서비스를 이용하면서 근접하게 유지해야만 하는 다른 애플리케이션에 있어서, 주기적인 재체크가 수행될 수 있다.

[0107] 위조 불가능한 클록(non forgeable clock)은 예를 들어 이동 전화 및 판독기에 있어서 유효한 가정이다. 그러나, 배터리가 방전되었을 때에도 기능해야만 하기 때문에, 비접촉 카드에 있어서, 또는 예를 들어 이동 전화에서 정확한 클록이 이용가능하지 않을 때 문제가 될 수 있다. 이러한 경우에, 카드는 판독기 클록에 동기화할 수 있고 판독기는 더 빨리 실행하기 위해서 조작된 릴레이된 판독기일 수 있다.

[0108] 만약 인트루더가 예를 들어 2배의 속도로 카드를 실행하게 할 수 있으면, 카드는 자신이 생각하기에 약 80㎲가 지났다고 생각하지만 실제로는 40㎲ 후에 응답을 전송할 수 있다. 릴레이 어택 윈도우는 약 80㎲-40㎲ = 40㎲이 될 것이다. 이러한 시나리오에 대한 솔루션은 만약 카드가 주파수 범위를 벗어나서 동작할 때 카드를 스위칭 오프하는 주파수 센서를 카드에 삽입하는 것이다.

[0109] 도 3은 통신 시스템의 두 가지 서로 다른 예시를 도시한다.

[0110] 참조번호(300)로 표기된 제 1 예시에서, 카드 또는 이동 전화는 예를 들어 대중 교통수단 인프라구조와 상호작용한다.

[0111] 참조번호(350)로 표기된 제 2 예시에서, 카드 또는 이동 전화는 이동 전화와 상호작용한다.

[0112] 유선 및 신뢰가능/무선 및 비신뢰가능/유선 및 신뢰가능으로 분류된 이러한 시스템의 특성이 도 3에 도시되었다.

[0113] 아래에서, 도 4를 참조하면, 본 발명의 예시적인 실시예에 따른 통신 시스템(400)이 설명될 것이다.

[0114] 통신 시스템(400)은 도 2에 도시된 시나리오와 유사하고 판독기(420) 및 트랜스폰더(440)를 포함한다.

[0115] 판독기(420)는 방출 안테나(424) 및 수신기 안테나(426)와 통신상 연결되는 프로세서(422)(마이크로프로세서 또는 중앙 처리 유닛과 같은 프로세서)를 포함한다. 방출 안테나(424)는 통신 메시지(428)를 트랜스폰더(440)로 전송할 수 있다. 수신기 안테나(426)는 트랜스폰더(440)로부터 통신 메시지(430)를 수신할 수 있다. 전송 안테나(424) 및 수신기 안테나(426)가 도 4에서 두 개의 서로 다른 안테나들로 도시되었지만, 다른 실시예에서는 단일의 공통 공유 송수신기 안테나를 사용할 수도 있다.

[0116] 안테나(424, 426)는, 통신 메시지(428)와 같은 전송을 위해서 데이터가 프로세서(422)로부터 전송 안테나(424)로 전송될 수 있도록 프로세서(422)와 전기적으로 연결된다. 수신기 안테나(426)에 의해 수신되는 통신 메시지(430)는 또한 프로세서(422)에 의해 분석 및 프로세싱될 수도 있다.

[0117] 반도체 메모리와 같은 저장 유닛(432)은 프로세서(422)에 액세스 가능한 데이터를 저장하는 것을 허용하도록 프로세서(422)와 연결된다. 또한, 사용자가 판독기 디바이스(420)를 동작시킬 수 있게 하는 입력/출력 유닛(434)이 도시되었다. 입력/출력 디바이스(434)는 버튼, 키패드, 조이스틱 등과 같은 입력 디바이스를 포함할 수 있다. 이러한 입력 소자를 통해서, 사용자는 입력 커맨드를 판독기 디바이스(420)로 입력할 수 있다. 또한, 입력/출력 유닛(434)은 액정 디스플레이와 같은 디스플레이 유닛을 포함할 수 있으며 그에 따라 판독기 디바이스(420)의 판독 절차의 결과를 사용자가 볼 수 있게 디스플레이하도록 한다.

[0118] 도 4로부터 알 수 있는 것처럼, 트랜스폰더(440)는 전송 및 수신기 안테나(436), 마이크로프로세서와 같은 프로세서(442) 및 메모리(438)를 포함한다. 일 실시예에서, 메모리(328) 및 프로세서(442)는 안테나(436)에 접속될 수 있고 패브릭 조각과 같은 서포트(444)에 부착될 수 있는 집적 회로(IC) 내에 모놀리식으로 집적될 수 있다.

[0119] 통신 메시지(428, 430)는 엔티티(420, 440) 사이에서 무선 방식으로 교환될 수 있다.

[0120] 판독기(420)와 트랜스폰더(440) 사이 접속의 유효성을 판정하기 위해서(판독기(420)와 트랜스폰더(440) 사이의 접속이 유효한지 아닌지 여부를 결정하기 위한 것임), 판독기(420)는 먼저 제 2 랜덤 넘버(도 2에서 RAMDOM #2로 표기됨)와 함께 제 1 랜덤 넘버(도 2에서 RAC1로서 표기됨)를 트랜스폰더(440)로 전송할 수 있다. 예를 들어 도 4의 통신 메시지(428)와 같은 통신 메시지의 수신에 따라서, 트랜스폰더(440)는 즉시 플레인텍스트(plaintext) 내에 제 1 랜덤 넘버(도 2에서 1로 표기됨)를 포함하는 통신 메시지(430)를 다시 전송할 수 있다. 따라서, 트랜스폰더(440)는 릴레이 어택 윈도우를 감소시키기 위해서 지연되지 않고 암호화되지 않은 방식으로 답변할 수 있다. 통신 메시지(428)가 제 2 랜덤 넘버(도 2에 RANDOM #2로 표기됨)를 포함할 때, 이러한 넘버는 메모리(438) 내에 저장될 수 있고 판독기 디바이스(420)와 같은 판독기 디바이스와 트랜스폰더(440) 사이의 연속적인 통신 세션을 위해 새로운 제 1 랜덤 넘버를 유도하도록 하는 역할을 할 수 있다. 판기 디바이스(420)의 프로세서(422)는 이후에 사용하기 위해서 메모리(432) 내에 수신된 제 1 랜덤 넘버를 저장할 수 있다.

[0121] 후속하여, 판독기(420)가 트랜스폰더(440)에게 추가적인 통신 메시지를 전송할 것을 요청하는 제 2 요청을 암호화된 방식으로 트랜스폰더(440)에게 더 전송하는 것이 선택적으로 가능하다. 그러나, 트랜스폰더(440)가 동작 중에 제 2 통신 메시지를 판독기(420)로 전송하는 것이 가능하기 때문에 이러한 추가 요청은 불필요하다. 이러한 제 2 통신 메시지는 암호화된 방식 또는 MACed 방식으로 제 1 랜덤 넘버 및 제 2 랜덤 넘버(RANDOM #1, RANDOM #2)를 포함할 수 있다. 프로세서(422)에 의해 수신된 넘버(제 1 및 제 2 랜덤 넘버를 포함함)를 복호화하는 것은, 트랜스폰더(440)로부터 전송된 것과 같은 제 1 및 제 2 랜덤 넘버를 메모리(432) 내에 저장된 제 1 및 제 2 랜덤 넘버와 비교하도록 허용할 수 있다. MAC이 사용되는 경우에, 프로세서(422)는 동일한 메시지에 대해서 MAC을 계산하고 결과가 수신되며 그것을 MAC과 비교한다.

[0122] 제 1 요청에 대한 응답 시간이 사전정의된 문턱값보다 작고, 메모리(432) 내에 저장된 상응하는 제 1 및 제 2 랜덤 넘버를 갖는 제 2 응답을 갖는 트랜스폰더(440)에 의해 전송되는 제 1 랜덤 넘버와 제 2 랜덤 넘버 사이에 적절한 매칭이 존재하는 시나리오에서만, 판독기(420)와 트랜스폰더(440) 사이의 통신이 유효한 것으로 수용될 것이다.

[0123] 당업자는 예시적인 실시예에 따른 트랜스폰더, 판독기 및 방법이 비접촉 데이터 전송으로만 제한되지 않으며, 유선 통신에도 적용될 수 있음을 인지해야 한다.

[0124] 실시예에서, 근접 체크가 챌린지-응답 상호작용의 라운드 트립 시간(round trip time)을 측정함으로써 실행된다. 만약 공격자가 릴레이 어택을 시작하길 원하면, 공격자는 지연을 도입해야 할 것이다. 얼마나 큰 지연이냐에 따라서, 지연이 검출될 수 있다. 시간 측정의 정확도 및 남아있는 잔여 릴레이 어택 윈도우는 트랜스폰더(PD)의 CLF(비접촉 프론트-엔드)뿐 아니라 비접촉 통신을 다루는 판독기(PCD)의 일부인 PCD의 비접촉 프론트-엔드(PCD-CLF)의 구현에 따른다. 이동 전화를 이용함으로써 릴레이 어택을 시작하는 것은 이러한 구현에 의해 대응될 수 있다. 체크가 단일 커맨드 및 단일 응답으로 수행될 수 있지만, 기술된 프로토콜은 적어도 세 개의 커맨드-응답 쌍을 이용한다. PD 측에서의 랜덤 넘버 및 암호화 계산의 실제 드로잉(drawing)은 응답이 반환될 수 있는 시간보다 많은 시간을 소요할 수 있다. 따라서, 이들 세 요소들은 다음과 같이 분리된다:

[0125] 1. PD가 랜덤 넘버를 드로잉하고 이것이 수행되기 전에는 응답을 전송하지 않도록 한다.

[0126] 2. 챌린지 랜덤 넘버가 도착하면 응답 랜덤 넘버로 응답한다. 이 단계에서 PCD는 복수의 챌린지-응답 쌍으로 분할될 수 있다.

[0127] 3. 넘버들이 조작되지 않았음을 보장하도록 암호화 체크를 수행한다.

[0128] 도 5는 본 발명의 예시적인 실시예에 따른 판독기(420)와 트랜스폰더(440) 간의 메시지 흐름(500)을 도시한다.

[0129] 도 5는 근접 체크 프로토콜에 대한 오버뷰를 제공하고 근접 체크 동안 교환되는 메시지의 예시를 제공한다.

[0130] 먼저, PD는 PPC(Prepare Proximity Check; 근접 체크 준비) 커맨드를 전송한다. 이것은 PD가 7 바이트의 랜덤 넘버를 준비하도록 지시한다. PPC 커맨드는 커맨드 코드로만 구성된다. 이것은 예를 들어 성공 반환 코드를 이용하여 PD에 의해 응답될 수 있다. 그 후에, PCD는 부분적인 또는 전체 7 바이트 랜덤 챌린지를 갖는 근접 체크(PC) 커맨드를 전송한다. PCD는 한번에 전체 7 바이트 넘버를 전송할 수 있고, 한번에 오직 하나의 바이트만을 감소시킨다. 이러한 커맨드에서, ISO 14443-4에 의해 일반적으로 규정되는 CRC는 선택적으로 생략된다. 마지막 비트를 전송한 직후에, PCD가 타이머를 시작할 것이 제안된다. 그 다음 PD는 반드시 최소의 프레임 지연 시간 이후인, ISO 14443-4가 허용하는 가장 이른 정확한 정시에 동일한 길이의 준비된 랜덤 응답의 일부로 응답해야만 한다. 또한 ISO 14443-4에 의해 규정되는 모든 필드가 이러한 응답에서 생략된다.

[0131] PCD는 PD 응답의 제 1 비트를 수신하는 즉시 타이머를 중지시킨다. 측정된 시간은 랜덤 넘버를 전송한 시각과 응답 랜덤 넘버를 수신한 시각 사이의 시간, 즉 최소 프레임 지연 시간(FDT; Frame Delay Time)과 라운드-트립 시간(RTT; Round-Trip Time)의 합이다.

[0132] 이러한 챌린지-응답 쌍으로서 랜덤 넘버들의 일부를 전송하는 절차는 전체 7 바이트가 교환될 때까지 PCD에 의해 반복된다. 랜덤 넘버가 어떤 크기로 분할되는지, 결과적으로 얼마나 많은 근접 체크 커맨드가 PCD에 의해 사용되는지가 자유롭게 선택될 수 있다. 실시예에서, 챌린지-응답 쌍의 최대 개수는 7개일 수 있다. 양 단부에서 7 바이트 랜덤 넘버의 수신된 부분들을 수집하여 그들이 수신된 순서대로 기억한다.

[0133] 무엇이 실질적으로 가능한지는 PCD-CLF에 따를 것이기 때문에, 마지막 비트를 전송한 뒤에 시간을 시작하고 첫 번째 비트를 수신할 때 중지하는 것이 제안될 수 있다. 서로 다른 PCD-CLF의 구현이 서로 다른 시간 측정 기술에 대해 허용되며 따라서 서로 다른 잔여 릴레이 어택 윈도우가 가능하다. 제안된 방식의 작업과 미세한 입도의 시간 측정에 따라 가장 작은 잔여 릴레이 어택 윈도우가 형성될 것이다.

[0134] 측정된 시간은 사전정의된 문턱값에 대해 비교된다. 이것은 PCD-CLF 및 잔여 리스크의 평가가 가능한 시간 측정의 입도에 의존하는 비접촉 인프라구조 오퍼레이터에 의해 선택된다. PCD는 각 근접 체크 커맨드 이후에 측정된 시간을 체크할 수 있거나 (또는 문턱값을 초과할 때 타임-아웃하는 타이머를 이용하여), 또는 측정된 최대 시간을 기억할 수 있고 오직 단부에서만 체크를 수행할 수 있다. 만약 문턱값이 초과되면, 근접 체크 프로토콜이 실패한다.

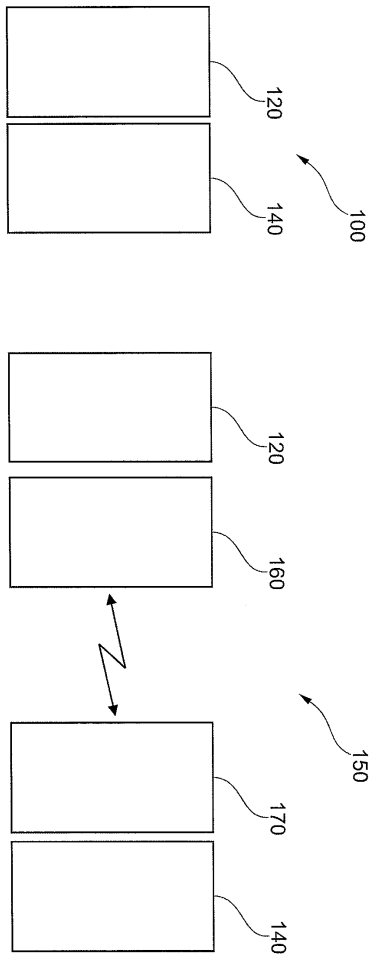
[0135] 완전한 n 바이트(예를 들어 7 바이트) 랜덤 챌린지가 근접 체크 커맨드로 프로세싱되면, PCD는 VPC(Verify Proximity Check) 커맨드를 전송한다. 이러한 커맨드는 PD 및 PCD가 동작하는 속도에 대한 일부 정보 및 완전한 7 바이트 랜덤 넘버에 대한 MAC을 포함하여(PPSE 바이트 내에 저장됨), 인트루더가 ISO 표준에 의해 허용되는 서로 다른 (더 높은) 속도로 카드를 동작시킬 수 없고 어택을 시작하는 데에 시간을 필요로 하게 한다(속도에 대한 다른 체크도 가능하다). MAC 입력에 대한 랜덤 넘버 순서화는 근접 체크 커맨드의 전송 동안 동일한 분할을 반영한다. PD는 인커밍 MAC을 확인해야 한다. 만약 MAC 확인이 실패하면, PD는 추가의 동작이 (더 이상) 수용되지 않는 상태로 갈 수 있다.

[0136] 본 발명의 예시적인 실시예에 따르면, 판독기 및 트랜스폰더의 전체 기능성이 반전될 수 있으며, 따라서 프로토콜 플로우가 다른 방향일 수 있다. 이것은 명시적으로 개시된 시스템과 균등한 솔루션이며, 본 발명의 특허청구범위에 의해 커버된다.

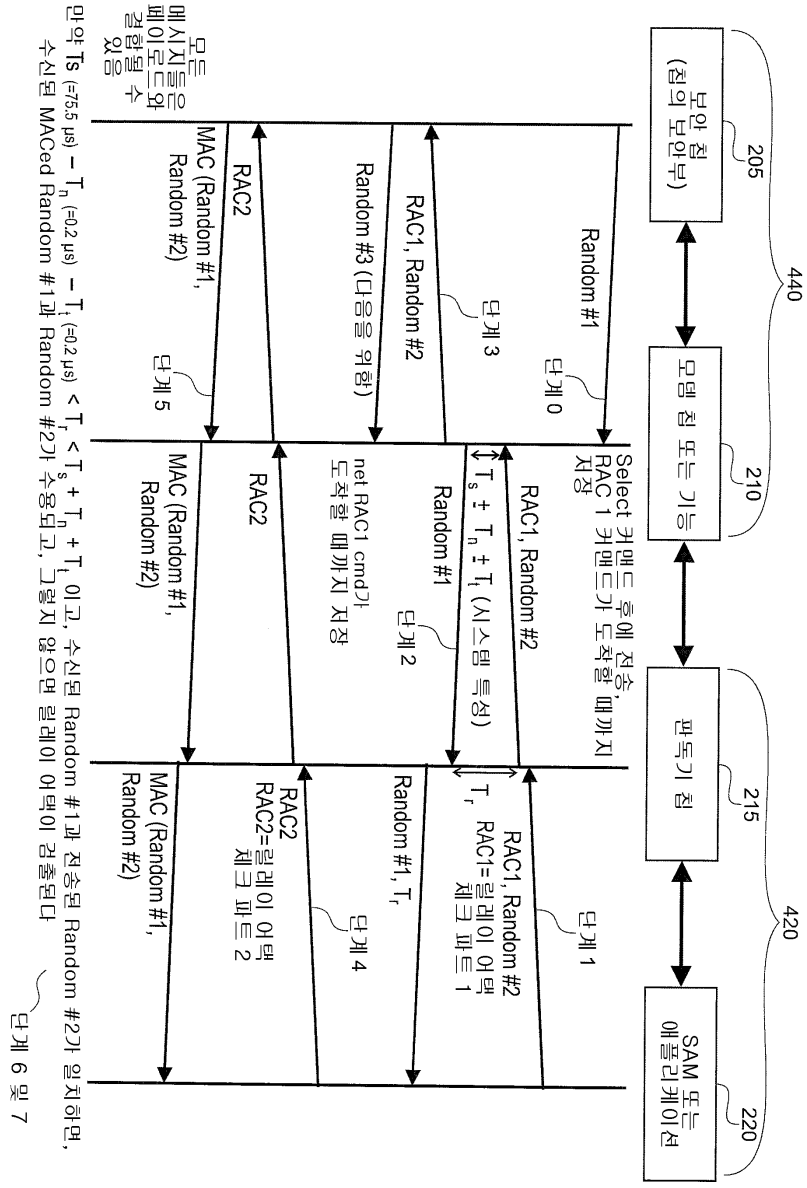
[0137] 마지막으로, 전술된 실시예는 단지 설명을 위한 것으로 본 발명을 제한하는 것이 아니며, 당업자는 첨부된 특허청구범위에 의해 정의된 본 발명의 범주로부터 벗어나지 않고 다수의 다른 실시예를 구성할 수 있을 것임을 인지해야 한다. 특허청구범위에서, 괄호 안의 참조 부호가 본 특허청구범위를 제한하는 것으로 해석되어서는 안된다. "포함하는" 및 "포함한다" 등과 같은 표현은 전체 청구항 또는 명세서 내에 나열되지 않은 다른 구성요소 또는 단계의 존재를 제외하는 것이 아니다. 또한 구성요소를 단수로 기재한 것이 이러한 구성요소가 복수개 존재하지 않음을 의미하는 것은 아니며, 그 반대 역시 마찬가지이다. 다수의 수단을 열거하는 디바이스 청구항에서, 이러한 다수의 수단들은 동일한 소프트웨어 또는 하드웨어에 의해 구현될 수 있다. 서로 다른 종속항에 기재된 단계들이 이들 단계들의 조합이 바람직하게 사용될 수 없음을 나타내는 것이 아님을 이해해야 한다.

도면

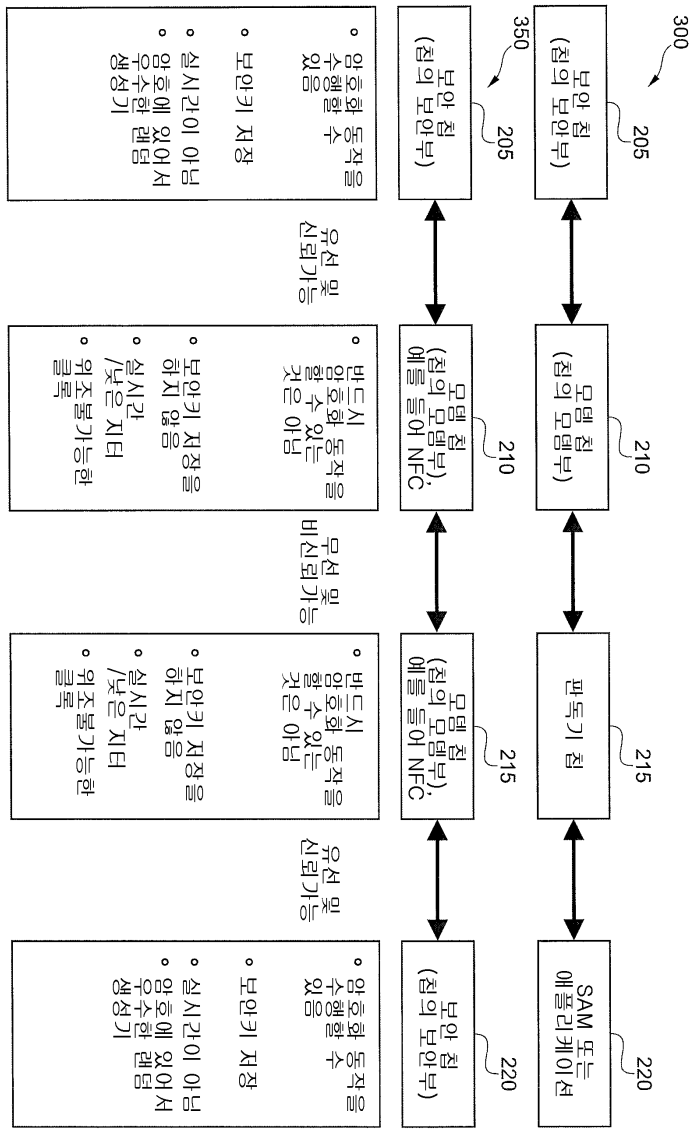
도면1



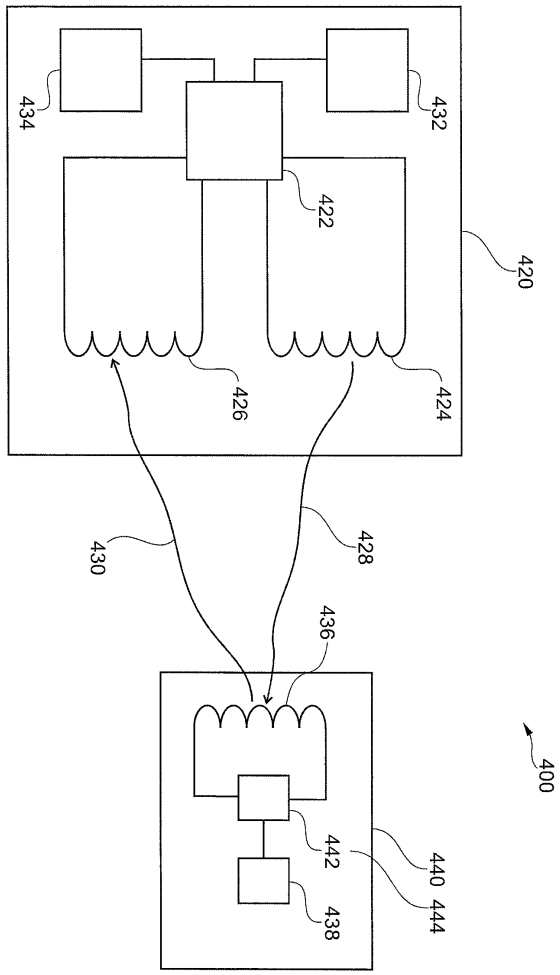
도면2


보안 칩
(칩의 보안부)
205
440
모뎀 칩 또는 기능
210
판독기 칩
215
420
SAM 또는
애플리케이션
220
단계 0
Random #1
단계 3
RAC1, Random #2
Random #3 (다음을 위함)
RAC2
MAC (Random #1,
Random #2)
단계 5
모든
메시지들은
페이로드와
결합될 수
있음
Select 커맨드 후에 전송,
RAC 1 커맨드가 도착할 때까지
저장
RAC1, Random #2
Ts ± Tn ± Tt (시스템 특성)
Random #1
단계 2
net RAC1 cmd가
도착할 때까지 저장
RAC2
MAC (Random #1,
Random #2)
단계 1
RAC1, Random #2
RAC1= 릴레이 어택
체크 파트 1
Tr
Random #1, Tr
단계 4
RAC2
RAC2= 릴레이 어택
체크 파트 2
MAC (Random #1,
Random #2)
단계 6 및 7
만 약 Ts (=75.5 μs) − Tn (=0.2 μs) − Tt (=0.2 μs) < Tr < Ts + Tn + Tt 이고, 수신된 Random #1과 전송된 Random #2가 일치하면,
수신된 MACed Random #1과 Random #2가 수용되고, 그렇지 않으면 릴레이 어택이 검출된다

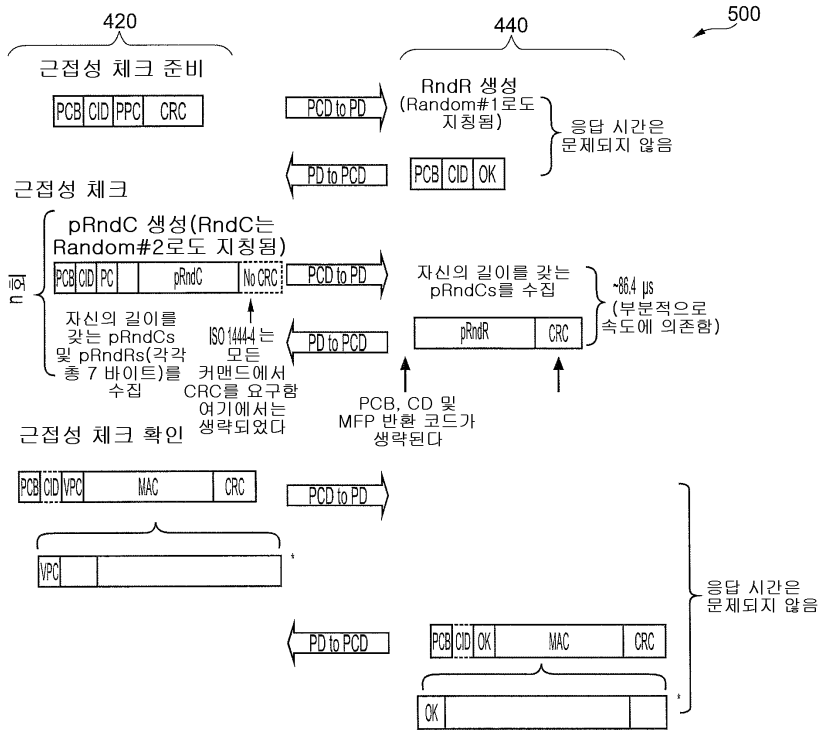
도면3


300
보안 칩
(칩의 보안부)
205
모뎀 칩
(칩의 모뎀부)
210
펌독기 칩
215
SAM 또는
애플리케이션
220
보안 칩
(칩의 보안부)
205
350
모뎀 칩
(칩의 모뎀부),
예를 들어 NFC
210
모뎀 칩
(칩의 모뎀부),
예를 들어 NFC
215
보안 칩
(칩의 보안부)
220
유선 및
신뢰가능
무선 및
비신뢰가능
유선 및
신뢰가능
• 암호화 동작을
수행할 수
있음
• 보안키 저장
• 실시간이 아님
• 암호에 있어서
우수한 랜덤
생성기
• 반드시
암호화 동작을
할 수 있는
것은 아님
• 보안키 저장을
하지 않음
• 실시간
/낮은 지터
• 위조불가능한
클록
• 반드시
암호화 동작을
할 수 있는
것은 아님
• 보안키 저장을
하지 않음
• 실시간
/낮은 지터
• 위조불가능한
클록
• 암호화 동작을
수행할 수
있음
• 보안키 저장
• 실시간이 아님
• 암호에 있어서
우수한 랜덤
생성기

도면4



도면5



PCD = 판독기 측

PD = 트랜스폰더 측

pRndC = 부분 RndC

pRndR = 부분 RndR

* PPSE, 랜덤 챌린지(RndC) 및 랜덤 응답(RndR)의 Concatentation