(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년02월25일
(11) 등록번호 10-1016983
(24) 등록일자 2011년02월16일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2005-7001459
(22) 출원일자(국제출원일자) 2003년06월27일
심사청구일자 2008년06월27일
(85) 번역문제출일자 2005년01월26일
(65) 공개번호 10-2005-0027262
(43) 공개일자 2005년03월18일
(86) 국제출원번호 PCT/IB2003/002932
(87) 국제공개번호 WO 2004/014037
국제공개일자 2004년02월12일
(30) 우선권주장
02078076.3 2002년07월26일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
US05126746 A1*
WO1997039553 A1*
WO2001093434 A2
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
코닌클리케 필립스 일렉트로닉스 엔.브이.
네델란드왕국, 아인드호펜, 그로네보드스베그 1
(72) 발명자
캄퍼맨프랜시스커스엘.에이.제이.
네덜란드 엔엘-5656 아아 아인드호벤 프로프. 홀스틀란 6 내
(74) 대리인
장훈

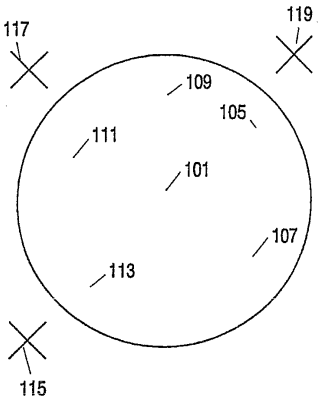
전체 청구항 수 : 총 10 항 심사관 : 김병우

(54) 보안 인증된 거리 측정

(57) 요 약

본 발명은 제 1 통신 디바이스가 제 1 통신 디바이스와 제 2 통신 디바이스 사이에서 인증된 거리 측정을 수행하는 방법에 관한 것으로서, 상기 제 1 및 제 2 통신 디바이스는 공통 비밀을 공유하고 상기 공통 비밀은 상기 제 1 통신 디바이스와 상기 제 2 통신 디바이스 사이의 거리 측정을 수행하기 위해 사용된다. 또한, 본 발명은 제 1 통신 디바이스에 저장된 데이터가 제 2 통신 디바이스에 의해 액세스 되는지를 판정하는 방법에 관한 것이다. 더욱이, 본 발명은 제 2 통신 디바이스에 대한 인증된 거리 측정을 수행하는 통신 디바이스에 관한 것이다. 또한, 본 발명은 통신 디바이스를 포함하는 멀티미디어 컨텐츠를 재생하기 위한 장치에 관한 것이다.

대 표 도 - 도1



특허청구의 범위

청구항 1

제 1 통신 디바이스에 저장된 멀티미디어 데이터가 제 2 통신 디바이스에 의해 액세스되는지를 판정하는 방법으로서, 상기 제 1 및 상기 제 2 통신 디바이스 사이의 인증된 거리 측정을 수행하는 단계를 포함하는 상기 판정하는 방법에 있어서,

상기 제 1 및 제 2 통신 디바이스는 공통 비밀(common secret)을 공유하고, 상기 공통 비밀은 상기 제 1 통신 디바이스와 상기 제 2 통신 디바이스 사이의 거리 측정을 수행하는데 사용되고, 공통 비밀은 상기 거리 측정을 수행하기 이전에 공유되고, 상기 공유는,

상기 제 2 통신 디바이스가 미리 정의된 순응 규칙들(compliance rules)의 세트에 순응하는지를 검사함으로써, 상기 제 2 통신 디바이스에 대한 인증 검사를 상기 제 1 통신 디바이스로부터 수행하는 단계와,

상기 제 2 통신 디바이스가 순응하는 경우, 상기 공통 비밀을 상기 제 2 통신 디바이스와 공유하는 단계와,

성공적인 인증 검사 및 거리 측정 이후에 상기 멀티미디어 데이터가 상기 제 1 통신 디바이스로부터 상기 제 2 통신 디바이스로 송신되는 보안 인증 채널의 생성에 있어 상기 공통 비밀을 이용하는 단계에 의해 수행되는 것을 특징으로 하는, 판정 방법.

청구항 2

제 1 항에 있어서,

인증된 거리 측정은,

제 1 시간(t1)에 상기 제 1 통신 디바이스로부터 상기 제 2 통신 디바이스로 제 1 신호를 송신하는 단계로서, 상기 제 2 통신 디바이스는 상기 제 1 신호를 수신하고, 상기 공통 비밀에 따라 상기 수신된 제 1 신호를 변경함으로써 제 2 신호를 생성하고, 상기 제 2 신호를 상기 제 1 통신 디바이스에 송신하게 되는, 상기 제 1 신호를 송신하는 단계와,

제 2 시간(t2)에 상기 제 2 신호를 수신하는 단계와,

상기 제 2 신호가 상기 공통 비밀에 따라 변경되었는지를 검사하는 단계와,

상기 t1과 t2 사이의 시간차에 따라 상기 제 1 및 상기 제 2 통신 디바이스 사이의 거리를 판정하는 단계에 따라 수행되는, 판정 방법.

청구항 3

제 2 항에 있어서,

상기 제 1 신호는 확산 스펙트럼 신호(spread spectrum signal)인, 판정 방법.

청구항 4

제 2 항에 있어서,

상기 제 2 신호가 상기 공통 비밀에 따라 변경되었는지를 검사하는 단계는,

상기 공통 비밀에 따라 상기 제 1 신호를 변경함으로써 제 3 신호를 생성하는 단계와,

상기 제 3 신호와 상기 수신된 제 2 신호를 비교하는 단계에 의해 수행되는, 판정 방법.

청구항 5

제 2 항에 있어서,

상기 제 1 신호 및 상기 공통 비밀은 비트 워드들이고, 상기 제 2 신호는 상기 비트 워드들 사이에서 XOR 연산을 수행함으로써 생성되는 정보를 포함하는, 판정 방법.

청구항 6

제 1 항에 있어서,

상기 인증 검사는 상기 제 2 통신 디바이스의 식별(identification)이 예상된 식별(expected identification)에 순응하는지를 검사하는 단계를 더 포함하는, 판정 방법.

청구항 7

제 1 항에 있어서,

상기 공통 비밀을 공유하는 단계는 키 전송 프로토콜(key transport protocol) 및 키 동의 프로토콜(key agreement protocol) 중 하나를 실행하는 단계를 포함하는, 판정 방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

제 1 통신 디바이스에 저장된 멀티미디어 데이터가 제 2 통신 디바이스에 의해 액세스되는지를 판정하도록 구성된 상기 제 1 통신 디바이스로서, 상기 제 1 통신 디바이스는 상기 제 1 및 상기 제 2 통신 디바이스 사이의 인증된 거리 측정을 수행하는 수단을 포함하는 상기 제 1 통신 디바이스에 있어서,

상기 제 1 통신 디바이스는 상기 제 2 통신 디바이스에 또한 저장되는 공통 비밀을 저장하는 메모리를 포함하고, 상기 공통 비밀은 상기 제 1 및 상기 제 2 통신 디바이스 사이의 상기 거리 측정을 수행하는데 사용되고, 상기 제 1 통신 디바이스는,

상기 제 2 통신 디바이스가 미리 정의된 순응 규칙들(compliance rules)의 세트에 순응하는지를 검사함으로써, 상기 제 2 통신 디바이스에 대한 인증 검사를 상기 제 1 통신 디바이스로부터 수행하는 단계와,

상기 제 2 통신 디바이스가 순응하는 경우, 상기 공통 비밀을 상기 제 2 통신 디바이스와 공유하는 단계와,

성공적인 인증 검사 및 거리 측정 이후에 상기 멀티미디어 데이터가 상기 제 1 통신 디바이스로부터 상기 제 2 통신 디바이스로 송신되는 보안 인증 채널의 생성에 있어 상기 공통 비밀을 이용하는 단계에 의해 상기 거리 측정을 수행하기 이전에 상기 공통 비밀을 공유하도록 구성되는 것을 특징으로 하는, 제 1 통신 디바이스.

청구항 12

제 11 항에 있어서,

상기 디바이스는,

제 1 시간(t1)에 상기 제 1 통신 디바이스로부터 상기 제 2 통신 디바이스로 제 1 신호를 송신하는 수단으로서, 상기 제 2 통신 디바이스는 상기 제 1 신호를 수신하고, 상기 공통 비밀에 따라 상기 수신된 제 1 신호를 변경함으로써 제 2 신호를 생성하고, 상기 제 2 신호를 상기 제 1 디바이스에 송신하게 되는, 상기 제 1 신호를 송신하는 수단과,

제 2 시간(t2)에 상기 제 2 신호를 수신하는 수단과,

상기 제 2 신호가 상기 공통 비밀에 따라 변경되었는지를 검사하는 수단과,

상기 t1과 t2 사이의 시간차에 따라 상기 제 1 및 상기 제 2 통신 디바이스 사이의 거리를 판정하는 수단을 포함하는, 제 1 통신 디바이스.

청구항 13

제 11 항 또는 제 12 항에 따른 제 1 통신 디바이스 및 상기 멀티미디어 데이터를 재생하는 수단을 포함하는 제 2 통신 디바이스를 포함하는 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 제 1 통신 디바이스가 제 1 통신 디바이스와 제 2 통신 디바이스 사이에서 인증된 거리 측정을 수행하는 방법에 관한 것이다. 또한, 본 발명은 제 1 통신 디바이스에 저장된 데이터가 제 2 통신 디바이스에 의해 액세스되는지를 판정하는 방법에 관한 것이다. 더욱이, 본 발명은 제 2 통신 디바이스에 대한 인증된 거리 측정을 수행하는 통신 디바이스에 관한 것이다. 또한, 본 발명은 통신 디바이스를 포함하는 멀티미디어 컨텐츠를 재생하기 위한 장치에 관한 것이다.

배 경 기 술

[0002] 디지털 미디어들은 여러 형태들의 데이터 정보에 대한 인기 있는 캐리어들(carriers)이 되어왔다. 컴퓨터 소프트웨어 및 오디오 정보는 예를 들면 광학 콤팩트 디스크들(CD들)에서 광범위하게 사용 가능하고 최근에는 DVD 역시 분배 점유율(distribution share)이 늘고 있다. CD 및 DVD는 데이터, 소프트웨어, 영상, 및 음성의 디지털 기록을 위해 공통적인 표준을 사용한다. 기록 가능한 디스크들, 고체 메모리 등의 부가적인 미디어들이 소프트웨어 및 데이터 분배 시장에서 현저히 증가하고 있다.

[0003] 아날로그 포맷에 비해 디지털 포맷의 실질적으로 우월한 품질은 디지털 포멧이 비인증된 복제 및 표절이 실질적으로 더 쉽게 되게 하였고, 또한 디지털 포맷은 복제하기가 보다 용이하고 보더 신속하다. 디지털 데이터 스트림의 복제는 압축, 비압축, 암호화 또는 비 암호화가 되었던 간에, 일반적으로 데이터의 뚜렷한 품질의 손실이 생기지 않는다. 따라서, 디지털 복제는 본질적으로 다-세대 복제의 견지에서 제한이 없다. 반면에, 매번 복제할 때마다 신호 대 잡음비 손실을 갖는 아날로그 데이터는 다-세대 복제 및 대량 복제의 견지에서 본질적으로 제한된다.

[0004] 디지털 포맷의 현재 유행의 도래는 많은 복제 방지 및 DRM 시스템과 방법들을 유발했다. 상기 시스템들 및 방법들은 암호화, 워터마킹 및 권리 기술(예컨대, 데이터에 대한 액세스 및 복제용 규칙) 등의 기술들을 사용한다.

[0005] 디지털 데이터의 형태의 컨텐츠를 보호하는 한 가지 방법은,

[0006] - 수신 디바이스가 순응 디바이스(compliant device)로서 인증받고,

[0007] - 컨텐츠의 유저가 그 컨텐츠를 다른 디바이스에 전송(이동, 복제)할 권리가 있는 경우에만 디바이스들 사이에서 전송된다는 것을 보장하는 것이다.

[0008] 컨텐츠의 전송이 허용되는 경우, 이는 컨텐츠가 유용한 포맷으로 불법적으로 포착될 수 없다는 것을 보장하는 암호화 방식으로 통상적으로 수행될 것이다.

[0009] 디바이스 인증 및 암호화된 컨텐츠 전송을 수행하기 위한 기술은 보안 인증 채널(SAC)이라 칭하며, 이용 가능하다. SAC상에서 컨텐츠의 복제가 허용될 수 있더라도, 컨텐츠 산업은 인터넷을 통한 컨텐츠 분배에 대해 매우 완고(bullish)하다. 이는, 예를 들면 이더넷과 같은 인터넷과 잘 정합하는 인터페이스상에서의 컨텐츠 전송에 대한 컨텐츠 산업의 반대(disagreement)를 초래한다.

[0010] 또한, 유저가 이웃집의 큰 텔레비전 스크린상에서 자기 소유의 영화를 보기 위해 이웃을 방문할 수 있다. 일반적으로, 컨텐츠 소유자는 이것을 금지할 것이지만, 그 영화의 라이센스 보유자(또는 그 라이센스 보유자가 소유하는 디바이스)가 상기 텔레비전 스크린 근처에 있다는 것이 증명될 수 있는 경우 수용 가능할 수 있다.

[0011] 따라서, 컨텐츠가 액세스되는지 또는 다른 디바이스에 의해 복제되는지를 결정할 때 인증된 거리 측정을 포함할 수 있다는 것에 흥미가 있다.

[0012] Stefan Brands 및 David Chaum 의 "Distance-Bounding protocols"(Eurocrypt '93(1993), 페이지 344 내지 359)이라는 항목에서, 공개키 식별 체계들의 거리 경계 프로토콜(distance-bounding protocols)의 집적화가 기술되어 있다. 여기서, 거리 측정은 시도와 응답(challenge and response) 비트들을 사용하는 시간 측정에 기초하고 책임 프로토콜(commitment protocol)의 사용에 의해 기술된다. 상기는 인증된 디바이스 순응 테스트를 허용하지 않고 2개의 디바이스가 서로를 인증해야 할 때 효과적이지 않다.

발명의 상세한 설명

[0013] 본 발명의 목적은 제한된 거리 내에서 컨텐츠의 보안 전송을 수행하는 문제점에 대한 해결책을 얻고자 하는 것이다.

[0014] 상기 목적은, 제 1 통신 디바이스가 제 1 통신 디바이스와 제 2 통신 디바이스 사이에서 인증된 거리 측정을 수행하는 방법에 의해 얻어지는데, 상기 방법에서, 제 1 및 제 2 통신 디바이스는 공통 비밀을 공유하고, 공통 비밀은 제 1 통신 디바이스와 제 2 통신 디바이스 사이의 거리 측정을 수행하기 위해 사용된다.

[0015] 공통 비밀이 거리 측정을 수행하기 위해 사용되고 있기 때문에, 제 1 통신 디바이스로부터 제 2 통신 디바이스까지의 거리를 측정할 때 측정되는 정당한 디바이스들 사이의 거리가 보장될 수 있다.

[0016] 상기 방법은 거리 측정 프로토콜을 인증 프로토콜과 조합한다. 이는 인증된 디바이스 순응성 테스트가 가능하게 하고, 어쨌든 보안 채널이 디바이스들 사이에서 보안 통신이 가능하게 하는데 요구되고 어떤 디바이스가 거리 측정이 수행되기 이전에 순응성에 대해 먼저 테스트될 수 있기 때문에 효과적이다.

[0017] 특정 실시예에 있어서, 상기 인증된 거리 측정은,

[0018] - 제 1 시간(t1)에 제 1 통신 디바이스로부터 제 2 통신 디바이스로 제 1 신호를 송신하는 단계로서, 제 2 통신 디바이스는 제 1 신호를 수신하고, 공통 비밀에 따라 수신된 제 1 신호를 변경함으로써 제 2 신호를 생성하고, 제 2 신호를 제 1 디바이스에 송신하도록 적응되는, 상기 송신하는 단계와,

[0019] - 제 2 시간(t2)에 제 2 신호를 수신하는 단계와,

[0020] - 제 2 신호가 상기 공통 비밀에 따라 변경되었는지를 검사하는 단계와,

[0021] - t1과 t2 사이의 시간차에 따라 제 1 및 상기 제 2 통신 디바이스 사이의 거리를 판정하는 단계에 따라 수행된다.

[0022] 신호를 송신하고 수신하는 시간차를 측정하며 제 2 통신 디바이스로부터 실제로 발생된 복귀 신호인지를 판정하기 위해 제 1 디바이스와 제 2 디바이스 사이에서 공유된 비밀을 사용함으로써, 거리를 측정할 때, 거리는 제 3 통신 디바이스(비밀을 알지 못함)에 대해 거리는 측정될 수 없다는 것을 보장하는 보안 인증 방식으로 측정된다. 신호를 변경하기 위해 공유된 비밀을 사용하는 것은 보안 인증된 거리 측정을 수행하는 간략한 방식이다.

[0023] 특정 실시예에 있어서, 제 1 신호는 확산 스펙트럼 신호이다. 그에 따라, 고해상도가 얻어지고, 불량한 전송 조건들(예를 들면, 많은 반사가 있는 무선 환경)에 대처할 수 있다.

[0024] 다른 실시예에 있어서, 제 2 신호가 상기 공통 비밀에 따라 변경되었는지를 검사하는 단계는,

[0025] - 공통 비밀에 따라 상기 제 1 신호를 변경함에 의해 제 3 신호를 생성하는 단계와,

[0026] 제 3 신호와 상기 수신된 제 2 신호를 비교하는 단계에 의해 수행된다.

[0027] 상기 방법은 검사 수행하는데 쉽고 간략한 방법이지만, 제 1 통신 디바이스와 제 2 통신 디바이스가 제 1 신호가 공통 비밀을 사용함으로써 어떻게 변경되었는지를 알아야 하다는 것이 요구된다.

[0028] 특정 실시예에 있어서, 상기 제 1 신호 및 상기 공통 비밀은 비트 워드들이고 제 2 신호는 상기 비트 워드들 사이에서 XOR 연산을 수행함으로써 생성되는 정보를 포함한다. 이에 의해, XOR 연산은 수행되어야 하는 매우 단순한 연산이며, 따라서 수행될 때 제 1 및 제 2 통신 디바이스에 의해 요구되는 자원이 거의 없다

[0029] 한 실시예에 있어서, 공통 신호는 리 측정을 수행하기 이전에 공유되고, 상기 공유는,

[0030] - 제 2 통신 디바이스가 미리 정의된 순응 규칙의 세트에 순응하는지를 검사함으로써, 제 2 통신 디바이스에 대한 인증 검사를 제 1 통신 디바이스로부터 수행하는 단계와,

[0031] - 제 2 통신 디바이스가 순응하는 경우, 비밀을 상기 제 2 통신 디바이스에 송신함으로써 공통 비밀을 공유하는 단계에 의해 수행되다.

[0032] 이는 순응 규칙에 순응하는 디바이스들만이 비밀을 수신할 수 있다는 것을 보장하는, 비밀의 공유를 수행하는 보안 방식이다. 더욱이, 공유된 비밀은 2개의 디바이스들 사이의 SAC 채널을 생성하는데 추후에 사용될 수 있다. 비밀은 예를 들면 ISO 11770-3에 기술된 키 전송 메커니즘들(key transport mechanisms)을 사용하여 공

유될 수 있다. 대안적으로, 예를 들면 ISO 11770-3에 기술된 키 동의(key agreement) 프로토콜이 또한 사용될 수 있다.

[0033] 다른 실시예에 있어서, 인증 검사는 상기 제 2 디바이스의 인증이 예상된 식별에 순응하는지를 검사하는 단계를 더 포함한다. 그에 따라, 제 2 디바이스가 실제로 그 디바이스인지가 보장된다. 동일성(identity)은 제 2 디바이스에 저장된 검증서(certificate)를 검사함으로써 얻어질 수 있다.

[0034] 또한, 본 발명은 제 1 통신 디바이스에 저장된 데이터가 제 2 통신 디바이스에 의해 액세스되는지를 판정하는 방법에 관한 것으로서, 상기 방법은 제 1 및 제 2 통신 디바이스 사이의 거리 측정를 수행하는 단계와, 측정된 거리가 미리 정의된 거리 간격 내에 있는지를 검사하는 단계를 포함하고, 거리 측정은 상술한 인증된 거리 측정이다. 디바이스들 사이의 공유 데이터와 관련하여 인증된 거리 측정을 이용함으로써, 비인증된 컨텐츠 분배는 감소될 수 있다.

[0035] 특정 실시예에 있어서, 제 1 디바이스에 저장된 데이터가 제 2 디바이스에 의해 액세스된다는 것이 판정되는 경우, 제 1 디바이스에 저장된 데이터는 상기 제 2 디바이스에 보내진다.

[0036] 본 발명은 제 1 통신 디바이스에 저장된 데이터가 제 2 통신 디바이스에 의해 액세스되는지를 판정하는 방법에 관한 것으로서, 상기 방법은 제 3 통신 디바이스와 제 2 통신 디바이스 사이의 거리 측정을 수행하는 단계와, 측정된 거리가 미리 정의된 거리 간격 내에 있는지를 검사하는 단계를 포함하고, 거리 측정은 상술한 인증된 거리 측정이다. 본 실시예에 있어서, 거리는 데이터가 저장되는 통신 디바이스와 제 2 통신 디바이스 사이에서 측정되지 않는다. 그 대신, 제 3 통신 디바이스와 제 2 통신 디바이스 사이에서 측정되고 제 3 통신 디바이스는 컨텐츠의 소유자에 대해 개인용 일 수 있다.

[0037] 본 발명은 제 2 통신 디바이스에 대해 인증된 거리 측정을 수행하는 통신 디바이스에 관한 것으로서, 상기 통신 디바이스는 제 2 통신 디바이스와 공통 비밀을 공유하고 통신 디바이스는 공통 비밀을 사용하여 제 2 디바이스에 대한 거리를 측정하는 수단을 포함한다.

[0038] 한 실시예에 있어서, 상기 디바이스는,

[0039] - 상기 디바이스는,

[0040] 제 1 시간(t1)에 제 1 통신 디바이스로부터의 제 1 신호를 제 2 통신 디바이스로 송신하기 위한 수단으로서, 상기 제 2 통신 디바이스는 제 1 신호를 수신하고, 공통 비밀에 따라 수신된 제 1 신호를 변경함으로써 제 2 신호를 생성하고, 제 2 신호를 제 1 디바이스에 송신하도록 적응되는, 상기 송신 수단과,

[0041] 제 2 시간(t2)에 제 2 신호를 수신하기 위한 수단과,

[0042] 제 2 신호가 상기 공통 비밀에 따라 변경되었는지를 검사하기 위한 수단과,

[0043] t1과 t2 사이의 시간차에 따라 제 1 및 제 2 통신 디바이스 사이의 거리를 판정하기 위한 수단을 포함한다.

[0044] 본 발명은 또한 상기에 다른 통신 디바이스를 포함하는 멀티미디어 컨텐츠를 재생하는 장치에 관한 것이다.

실 시 예

[0049] 도 1은 컨텐츠 보호를 위해 인증된 거리 측정이 사용되는 한 실시예를 도시한다. 서클(101)의 중심에 컴퓨터(103)가 배치된다. 상기 컴퓨터는 영상 또는 음성이며 예를 들면 하드디스크, DVD 또는 CD에 저장된 멀티미디어 등의 컨텐츠를 포함한다. 컴퓨터 소유자는 컨텐츠를 소유하고 그에 따라 컴퓨터는 멀티미디어 컨텐츠를 액세스하고 유저에 표시하도록 허가된다. 유저가 예를 들면 SAC를 통해 다른 디바이스에 컨텐츠의 합법적인 복제를 원하는 경우에, 다른 디바이스와 컴퓨터(103) 사이의 거리는 측정되고 서클(101) 내측의 디바이스(105, 107, 109, 111, 113)에 의해 표시된 미리 정의된 거리 내에 있는 디바이스만이 컨텐츠 수신이 허용된다. 반면에, 컴퓨터(101)까지의 거리가 미리 정의된 거리 보다 더 멀리 있는 디바이스(115, 117, 119)는 컨텐츠 수신이 허용되지 않는다.

[0050] 상기 예에서, 디바이스는 컴퓨터이지만, 디바이스가 거리 측정을 수행하기 위한 통신 디바이스를 포함하기만 하면 예를 들면 DVD 드라이브, CD 드라이브 또는 비디오이어도 무방하다.

[0051] 특정 실시예에서, 상기 거리는 데이터가 저장된 컴퓨터와 다른 디바이스 사이, 예를 들어 미리 정의된 거리내에 있는 컨텐츠의 소유자에 사적인 제 3 디바이스 사이에서 측정될 필요는 없다.

[0052] 도 2는 인증된 거리 측정을 수행하기 위해 통신 디바이스를 각각 포함하는 2개의 디바이스(201, 203) 사이에서 인증된 거리 측정을 수행하는 일반적인 개념을 도시한다. 상기 예에서, 제 1 디바이스(201)는 제 2 디바이스(203)가 요청한 컨텐츠를 포함한다. 인증된 거리 측정은 이하와 같다. 단계 205에서, 제 1 디바이스(201)는 제 2 디바이스(203)를 인증한다; 이는 제 2 디바이스(203)가 순응하는 디바이스인지를 검사하는 단계를 포함할 수 있고 또한 제 2 디바이스(203)가 실제로 제 1 디바이스(201)에 대해 인증된 디바이스인지를 검사하는 단계를 더 포함한다. 그 후, 단계 207에서, 제 1 디바이스는 비밀을 제 2 디바이스(203)와 교환하는데 이는 예컨대 랜덤하게 생성된 비트 워드를 제 2 디바이스(203)에 전송함으로써 수행될 수 있다. 상기 비밀은 예컨대 ISO 11770에 기술된 몇몇의 키관리 프로토콜에 따라 안전하게 공유되어야 한다.

[0053] 그 후, 단계 209에서, 거리 측정용 신호가 제 2 디바이스(203)에 전송된다; 제 2 디바이스는 비밀에 따라 수신된 신호를 변경하고 변경된 신호를 제 1 디바이스에 대해 재송신한다. 제 1 디바이스(201)는 발신되는 신호와 복귀하는 신호 사이의 왕복 시간을 측정하고 반환된 신호가 교환된 비밀에 따라 변경되었는지를 검사한다. 몇몇의 비밀에 따른 반환된 신호의 변경은 전송 시스템 및 거리 측정을 위해 사용된 신호에 대해 의존할 것이고, 즉, 이는 각각의 통신 시스템(1394, 이더넷, 블루투스, ieee 802.11, 등)에 대해 특별할 것이다.

[0054] 거리 측정을 위해 사용된 신호는 정규의 데이터(normal data) 비트 신호일 것이지만, 데이터 통신을 제외한 특별한 신호가 사용될 수 있다. 상기 실시예에서, 높은 고해상도를 얻을 수 있고 불량한 전송 조건들(예를 들면, 많은 반사가 있는 무선 환경)에 대처할 수 있도록, 확산 스펙트럼 신호가 사용된다.

[0055] 특정 실시예에 있어서, 직접 시퀀스 확산 스펙트럼 신호가 거리 측정을 위해 사용되었다; 이 신호는 비밀의 비트들(예를 들면, 비밀은 역시 127개의 비트들로 구성된다)로 직접 시퀀스 코드의 칩들을 XOR 연산함으로써(예를 들면, 127개의 칩으로 구성된 코드를 확산함에 의해) 변경될 수 있다. 또한, 다른 수학적인 연산들이 XOR로서 사용될 수 있다.

[0056] 단계 205의 인증 및 단계 207의 비밀 교환은 몇몇의 공지의 ISO 표준들(ISO 9798 및 ISO 11770)에서 기술된 프로토콜을 사용하여 수행될 수 있다. 예를 들면, 제 1 디바이스(201)는 이하의 통신 시나리오(scenario)에 따라 제 2 디바이스(203)를 인증한다:

[0057] 제 1 디바이스 -〉 제 2 디바이스: $R_B \| Text\ 1$

[0058] 여기서, R_B는 난수(random number)이다.

[0059] 제 2 디바이스 -〉 제 1 디바이스: $CertA \| TokenAB$

[0060] 여기서, CertA는 A의 검증서이다.

[0061] $TokenAB=R_A \| R_B \| B \| Text3 \| sS_A(R_A \| R_B \| B \| Text2)$

[0062] R_A는 난수이다.

[0063] 식별자 B는 옵션이다.

[0064] sS_A는 개인키 S_A를 사용하여 A에 의해 설정된 서명이다.

[0065] 만일, TokenAB가 ISO 11770-3에 의해 지정된 토큰(token)으로 대체되면 우리는 동시에 비밀키 교환을 할 수 있다. 우리는 상기를 Text2 대신에,

[0066] $Text2:= eP_B(A \| K \| Text2) \| Text3$

[0067] 를 치환함으로써 상기를 사용할 수 있다.

[0068] 여기서, eP_B는 공개키 B호 암호화된다.

[0069] A는 A의 식별자이고,

[0070] K는 교환될 비밀이다.

[0071] 이 경우에, 제 2 디바이스(203)는 키를 판정하고(즉, 키 제어를 한다), 이는 또한 키 전송 프로토콜이라고 하며 역시 키 동의 프로토콜이 사용될 수도 있다. 상기는 반전된 경우에는 바람직하지 않을 수 있어서 제 1 디바이스가 키를 판정한다. 비밀키는 이제 도 2의 단계 207에 따라 변경되었다. 재차, 비밀키는 예를 들면 키 전송 프로

토콜 또는 키 동의 프로토콜에 의해 교환될 수 있다.

[0072] 상기한 바와 같이 거리가 보안 인증된 방식으로 측정된 이후에, 컨텐츠와 데이터는 단계 211에서 제 1 및 제 2 디바이스 사이에 전송될 수 있다.

[0073] 도 3은 인증된 거리 측정을 수행하는 단계를 보다 상세하게 설명한다. 상기한 바와 같이, 제 1 디바이스(301) 및 제 2 디바이스(303)는 비밀을 교환하였다; 비밀은 제 1 디바이스의 메모리(305) 및 제 2 디바이스의 메모리(307)에 저장된다. 거리 측정을 수행하기 위해, 신호는 송신기(309)를 경유하여 제 2 디바이스에 전송된다. 제 2 디바이스는 수신기(311)를 통해 신호를 수신하고 313은 국부적으로 저장된 비밀을 이용하여 신호를 변경한다. 신호는 제 1 디바이스(301)에 의해 공지된 규칙에 따라 변경되고 송신기(315)를 경유하여 제 1 디바이스(301)에 재전송된다. 제 1 디바이스(301)는 변경된 신호를 수신기(317)를 통하여 변경하고, 319에 있어서, 수신된 변경된 신호는 국부적으로 변경된 신호와 비교된다. 국부적인 변경은 309에서 제 2 디바이스에 전송된 신호를 사용하고 그 후 제 2 디바이스에 의해 사용된 변경 규칙과 유사한 국부적으로 저장된 비밀을 사용하여 신호를 변경함으로써 321에서 수행된다. 수신된 변경 신호 및 국부적으로 변경된 신호가 동일한 경우, 수신된 신호는 인증되고 제 1 및 제 2 디바이스 사이의 거리를 판정하는데 사용될 수 있다. 2개의 신호가 동일하지 않으면, 수신된 신호는 인증되지 않고 따라서 325에 의해 도시된 바와 같이 거리를 측정하는데 사용될 수 없다. 323에서, 거리는 제 1 및 제 2 디바이스 사이에서 계산된다; 이는 예를 들면 신호가 송신기(309)에 의해 제 1 디바이스로부터 제 2 디바이스까지 전송된 경우의 시간을 측정함으로써, 그리고 수신기(317)가 제 2 디바이스로부터 신호를 수신한 경우를 측정함에 의해 수행된다. 전송된 시간과 수신 시간 사이의 시간차가 제 1 디바이스와 제 2 디바이스 사이의 물리적인 거리를 측정하는데 사용될 수 있다.

[0074] 도 4에 있어서, 인증된 거리 측정을 수행하는 통신 디바이스가 도시된다. 디바이스(401)는 수신기(403) 및 송신기(411)를 포함한다. 디바이스는, 통신 버스를 경유하여 메모리(417)에 접속된 마이크로 프로세서(413)를 사용하는 소프트웨어를 수행으로써, 상기한 단계들을 수행하기 위한 수단들을 더 포함한다. 통신 디바이스는 보호된 컨텐츠에 액세스하기 위해 DVD, 컴퓨터, CD, CD 레코더, 텔레비젼, 및 다른 디바이스 등과 같은 디바이스들 내에 배치될 수 있다.

산업상 이용 가능성

[0075] 본 발명에 따르면, 공통 비밀이 거리 측정을 수행하기 위해 사용되고 있기 때문에, 제 1 통신 디바이스로부터 제 2 통신 디바이스까지의 거리를 측정하는 경우에 측정되는 진정한 디바이스 사이들의 거리가 확보된다.

도면의 간단한 설명

[0045] 도 1은 컨텐츠 보호를 위해 사용되는 인증된 거리 측정을 도시하는 도면.

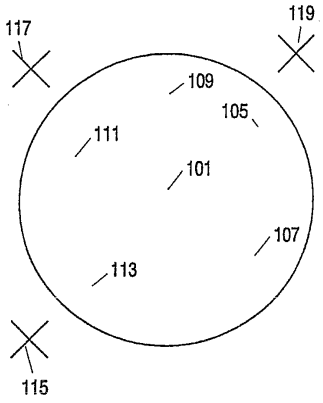
[0046] 도 2는 인증된 거리 측정을 수행하는 방법을 도시하는 흐름도.

[0047] 도 3은 도 2에 도시된 인증된 거리 측정을 수행하는 단계를 보다 더 상세히 도시하는 도면.

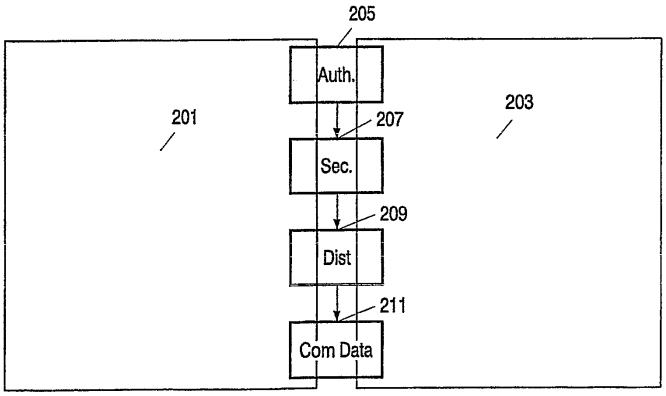
[0048] 도 4는 인증된 거리 측정을 수행하는 통신 디바이스를 도시하는 도면.

도면

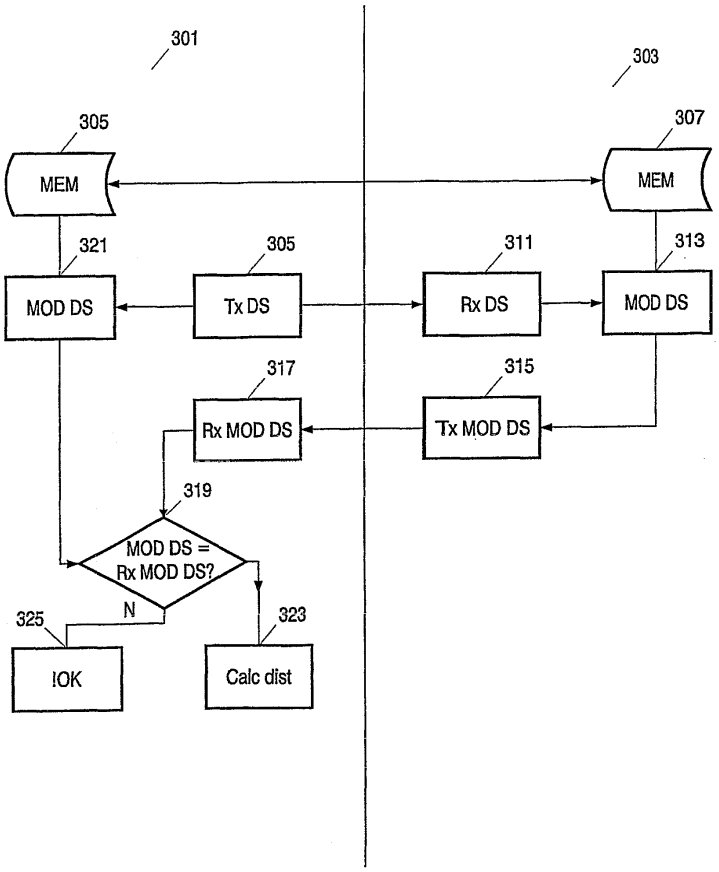
도면1


117
119
109
105
111
101
107
113
115

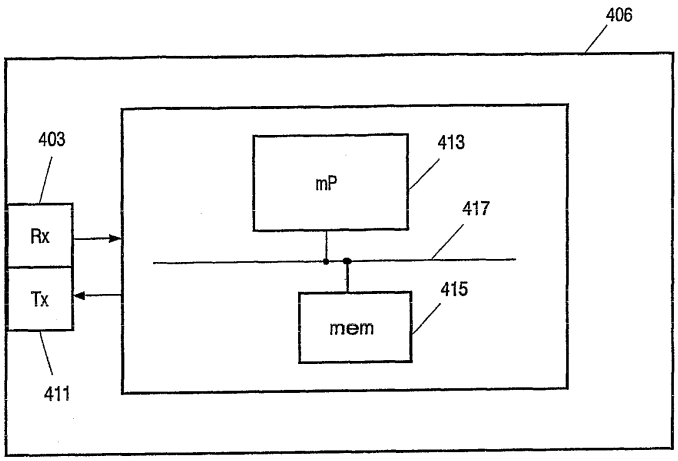
도면2


205
Auth.
201
203
207
Sec.
209
Dist
211
Com Data

도면3


301
303
305
MEM
307
MEM
321
MOD DS
305
Tx DS
311
Rx DS
313
MOD DS
317
Rx MOD DS
315
Tx MOD DS
319
MOD DS =
Rx MOD DS?
N
325
!OK
323
Calc dist

도면4


406
403
Rx
Tx
411
mP
413
417
mem
415