



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년05월31일
(11) 등록번호 10-0960064
(24) 등록일자 2010년05월19일

(51) Int. Cl.

H04L 9/32 (2006.01)

(21) 출원번호 10-2007-0114435

(22) 출원일자 2007년11월09일

심사청구일자 2007년11월09일

(65) 공개번호 10-2008-0044164

(43) 공개일자 2008년05월20일

(30) 우선권주장

06124154.3 2006년11월15일

유럽특허청(EPO)(EP)

(56) 선행기술조사문헌

KR1020000022249 A*

US20040158714 A1*

US20020078351 A1

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

리서치 인 모션 리미티드

캐나다 온타리오 워털루 필립 스트리트 295 (우편
번호 엔2엘 3더블유8)

(72) 발명자

서킨 알레그젠더

캐나다 온타리오 엘3엑스 2제이2 뉴마켓 헤들 크
레센트 430

셴필드 마이클

캐나다 온타리오 엘4씨 3에스9 리치몬드 힐 스톡
데일 크레센트 38

(74) 대리인

김태홍, 신정건

전체 청구항 수 : 총 35 항

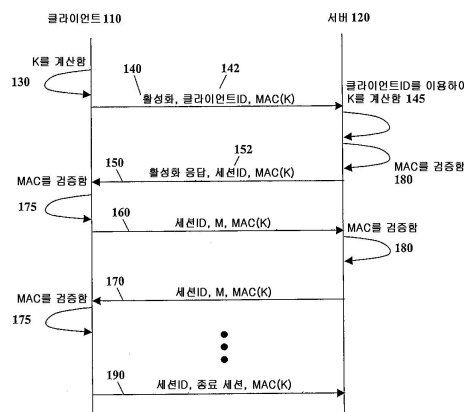
심사관 : 최수연

(54) 클라이언트 자격증명서 기반의 보안 세션 인증 방법 및 장치

(57) 요약

클라이언트와 서버 간 메시지의 클라이언트 자격증명서 기반 인증을 위한 방법 및 장치로서, 클라이언트와 서버 양측 모두는 상기 클라이언트 자격증명서를 인지하고 있고, 상기 방법은, 키를 생성하기 위해 상기 클라이언트 자격증명서를 사용하는 단계와; 상기 클라이언트와 상기 서버 간의 메시지를 인증하기 위해 상기 키를 사용하는 단계를 포함하는, 클라이언트 자격증명서 기반 인증을 위한 방법 및 장치가 제공된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

클라이언트 장치와 서버 간의 메시지들의 클라이언트 자격증명서(credential) 기반 인증을 위한 방법으로서, 상기 클라이언트 장치와 상기 서버 양측 모두는 상기 클라이언트 자격증명서를 인지하고 있는 것인, 상기 클라이언트 자격증명서 기반 인증 방법에 있어서,

키를 생성하기 위해 상기 클라이언트 자격증명서를 이용하는 단계;

시퀀스 넘버를 포함하는 메시지를 송신을 위하여 준비하는 단계;

상기 클라이언트 장치와 상기 서버 양측 모두에 알려진 메시지 인증 코드(MAC; Message Authentication Code) 함수(function)를 사용함으로써, 상기 메시지와 상기 키로 메시지 인증 코드(MAC)를 계산하는 단계; 및

상기 클라이언트 장치와 상기 서버 간의 메시지들을 인증하기 위해 상기 MAC를 사용하는 단계

를 포함하는 클라이언트 자격증명서 기반 인증 방법.

청구항 2

제1항에 있어서, 상기 클라이언트 자격증명서는 암호인 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 3

제2항에 있어서, 상기 키는 원하는 키 길이가 달성될 때까지 상기 암호를 반복함으로써 생성되는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 4

제1항 또는 제2항에 있어서, 상기 키는 상기 클라이언트 및 상기 서버 양측 모두에 알려진 해시 함수를 이용함으로써 생성되는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 5

제4항에 있어서, 상기 해시 함수의 결과물들은 원하는 키 길이로 절단되는(truncated) 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 6

제2항에 있어서, 상기 암호는 상기 키의 생성에 앞서 보안 토큰(security token)과 결합되는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 7

제6항에 있어서, 상기 보안 토큰은 상기 클라이언트 장치에 의해 상기 서버에 오프라인 상으로 제공되는 정보를 포함하고,

상기 정보는, 출생일자; 출생장소; 모친의 처녀시절 이름(maiden name); 보안 응답; 또는 이들의 조합 중 어느 하나를 포함하는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 8

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 클라이언트 자격증명서 이용단계는, 상기 키를 생성하기 위해 상기 클라이언트 자격증명서를 세션 식별자와 결합하는 것 또는 상기 클라이언트 자격증명서를 활성화 메시지로 부터의 난스(nonce)와 결합하는 것을 더 포함하는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 9

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 키의 생성은 보안 의사 난수(secure pseudo-random number) 생성기를 이용하는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 10

제9항에 있어서, 상기 보안 의사 난수 생성기는 상기 클라이언트 자격증명서를 시드(seed)로서 사용하는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 11

제6항에 있어서, 상기 키의 생성은 보안 의사 난수 생성기를 이용하고,

상기 보안 의사 난수 생성기는 상기 보안 토큰과 결합된 클라이언트 자격증명서를 시드로서 사용하는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 12

제8항에 있어서, 상기 키의 생성은 보안 의사 난수 생성기를 이용하고,

상기 보안 의사 난수 생성기는 상기 세션 식별자와 결합된 클라이언트 자격증명서를 시드로서 사용하거나, 상기 난수와 결합된 클라이언트 자격증명서를 시드로서 사용하는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 13

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 메시지들을 인증하기 위해 MAC를 사용하는 단계는,

보안 메시지를 생성하기 위해 상기 MAC를 상기 메시지에 추가하는 단계; 및

상기 보안 메시지를 송신하는 단계

를 포함하는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 14

제13항에 있어서, 상기 보안 메시지는, 상기 보안 메시지의 수신과 동시에 상기 MAC를 재생성(recreating)하고 이 재생성된 MAC를 수신된 상기 MAC와 비교함으로써, 인증된 것이고 변경되지 않은 것임이 검증되는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 15

제13항에 있어서, 상기 메시지는, 활성화 요청 메시지이고 클라이언트 식별자를 포함하는 것이거나, 활성화 응답이고 세션 식별자를 포함하는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 16

제13항에 있어서, 상기 메시지는 HTTP 메시지이고,

상기 MAC는 HTTP 꼬리말/footer)에 추가되는 것인 클라이언트 자격증명서 기반 인증 방법.

청구항 17

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 클라이언트 자격증명서 이용 단계를 수행하기 전에, 상기 메시지에 시퀀스 넘버를 추가하는 단계를 더 포함하는 클라이언트 자격증명서 기반 인증 방법.

청구항 18

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 클라이언트 자격증명서로 생성된 상기 키를 이용하는 대칭 키를 교섭(negotiating)하는 단계를 더 포함하는 클라이언트 자격증명서 기반 인증 방법.

청구항 19

클라이언트 장치와 서버 간의 메시지들의 클라이언트 자격증명서 기반 인증에 사용되는 상기 클라이언트 장치로서, 상기 클라이언트 장치와 상기 서버 양측 모두는 상기 클라이언트 자격증명서를 인지하고 있는 것인, 상기 클라이언트 장치에 있어서,

공유되는 자격증명서를 저장하기 위한 메모리;

상기 메모리와 통신하는 프로세서로서,

시퀀스 넘버를 포함하는 메시지를 송신을 위하여 준비하고,

키를 생성하기 위해 상기 클라이언트 자격증명서를 이용하고,

메시지 인증 코드(MAC; Message Authentication Code)를 생성하기 위해 상기 키 및 상기 메시지를 사용하며,

보안 메시지를 생성하기 위해 상기 MAC를 상기 메시지에 부가하도록 구성되는 상기 프로세서; 및
상기 보안 메시지를 송신하도록 구성되는 통신 서브시스템
을 포함하고,

상기 클라이언트 장치는 또한, 상기 서버로부터 수신한 메시지들을 인증하기 위해 상기 키와 상기 시퀀스 넘버를 사용하도록 구성되는 것인, 클라이언트 장치.

청구항 20

제19항에 있어서, 상기 클라이언트 자격증명서는 암호인 것인 클라이언트 장치.

청구항 21

제20항에 있어서, 상기 프로세서는, 원하는 키 길이가 달성될 때까지 상기 암호를 반복함으로써 상기 키를 생성하도록 구성되는 것인 클라이언트 장치.

청구항 22

제19항 또는 제20항에 있어서, 상기 프로세서는, 상기 클라이언트 장치와 상기 서버 양측 모두에 알려진 해시 함수를 이용함으로써, 상기 키를 생성하도록 구성되는 것인 클라이언트 장치.

청구항 23

제22항에 있어서, 상기 프로세서는 또한 상기 해시 함수의 결과물들을 원하는 키 길이로 절단하도록 구성되는 것인 클라이언트 장치.

청구항 24

제20항에 있어서, 상기 프로세서는 또한 상기 키의 생성에 앞서 상기 암호를 보안 토큰과 결합하도록 구성되는 것인 클라이언트 장치.

청구항 25

제24항에 있어서, 상기 보안 토큰은 상기 클라이언트 장치에 의해 상기 서버에 오프라인상으로 제공된 정보를 포함하고,

상기 정보는, 출생일자; 출생장소; 모친의 처녀시절 이름; 보안 응답; 또는 이들의 조합 중 어느 하나를 포함하는 것인 클라이언트 장치.

청구항 26

제19항 내지 제21항 중 어느 한 항에 있어서, 상기 프로세서는 상기 키를 생성하기 위해 상기 클라이언트 자격증명서를 세션 식별자와 결합하거나, 상기 클라이언트 자격증명서를 활성화 메시지에서부터의 난스(nonce)와 결합하도록 구성되는 것인 클라이언트 장치.

청구항 27

제19항 내지 제21항 중 어느 한 항에 있어서, 상기 프로세서는 보안 의사 난수 생성기를 이용하여 상기 키를 생성하도록 구성되는 것인 클라이언트 장치.

청구항 28

제27항에 있어서, 상기 보안 의사 난수 생성기는 상기 클라이언트 자격증명서를 시드로서 사용하는 것인 클라이언트 장치.

청구항 29

제24항에 있어서, 상기 프로세서는 보안 의사 난수 생성기를 이용하여 상기 키를 생성하도록 구성되고, 상기 보안 의사 난수 생성기는 상기 보안 토큰과 결합된 클라이언트 자격증명서를 시드로서 사용하는 것인 클라이언트 장치.

청구항 30

제26항에 있어서, 상기 프로세서는 보안 의사 난수 생성기를 이용하여 상기 키를 생성하도록 구성되고, 상기 보안 의사 난수 생성기는 상기 세션 식별자와 결합된 클라이언트 자격증명서를 시드로서 사용하거나 상기 난수와 결합된 클라이언트 자격증명서를 시드로서 사용하는 것인 클라이언트 장치.

청구항 31

제19항 내지 제21항 중 어느 한 항에 있어서, 상기 메시지는, 활성화 요청 메시지이고 클라이언트 식별자를 포함하거나, 활성화 응답이고 세션 식별자를 포함하는 것인 클라이언트 장치.

청구항 32

제19항 내지 제21항 중 어느 한 항에 있어서, 상기 프로세서는 또한 상기 메시지에 시퀀스 넘버를 부가하도록 구성되는 것인 클라이언트 장치.

청구항 33

제19항 내지 제21항 중 어느 한 항에 있어서, 상기 프로세서는 또한 상기 클라이언트 자격증명서로 생성된 상기 키를 이용하는 대칭 키를 교섭하도록 구성되는 것인 클라이언트 장치.

청구항 34

제19항 내지 제21항 중 어느 한 항에 있어서, 상기 클라이언트 장치는 이동 장치인 것인 클라이언트 장치.

청구항 35

컴퓨팅 장치 또는 시스템의 프로세서에서 실행되는 프로그램 코드로서, 상기 컴퓨팅 장치 또는 상기 시스템으로 하여금 제1항 내지 제3항 중 어느 한 항의 방법을 수행하도록 하기 위한 상기 프로그램 코드를 내장하는 컴퓨터 판독가능 매체.

명세서

발명의 상세한 설명

기술 분야

[0001] 본원의 개시사항은 일반적으로 보안 세션 인증과 관련되고, 더 자세하게는 현저한 계산상의 오버헤드 없이 보안 인증된 세션을 확립하는 것에 관련된다.

배경 기술

[0002] 클라이언트-서버 환경에서, 클라이언트와 서버 간의 통신은 종종 인증될 필요가 있다. 구체적으로, 어떤 서비스에 액세스하기 위해, 하나의 컴퓨팅 장치가 종종 네트워크를 통해 다른 컴퓨팅 장치(클라이언트 및 서버)와 통신한다. 클라이언트와 서버가 진정한 것임을 보증하고, 이에 의해 아이덴티티 및 데이터 무결성(integrity)을 유지하기 위하여, 인증이 요구된다.

[0003] 서버와 클라이언트 간의 통신을 인증하기 위한 몇가지 해결방안이 존재한다. 한 해결방안으로는, 간단한 인증으로 세션을 인증하는 것이 있을 수 있다. 오늘날의 인터넷 상의 대다수의 보안 웹 서버들은 세션을 인증하기 위하여 SSL/TLS(보안 소켓 계층/전송 계층 보안)을 통한 HTTP(하이퍼 텍스트 전송 프로토콜) 포스트-기반 인증

또는 기초 인증과 같은 몇 가지 형태의 간단한 인증을 사용한다. 그 후, 인증된 세션은 HTTP 쿠키 내의 클라이언트 내에 또는 클라이언트 상에 저장된 토큰에 의해 식별된다. 이러한 방식은 SSL/TLS를 요구하기 때문에 복잡하다. SSL 및 TLS를 적절하게 지원하기 위해서는, 클라이언트가 상대적으로 강력한(strong) 암호 성능을 포함할 필요가 있다. 예를 들어, 공용/개인 키 시스템이 이용될 수 있다. 그러나, 무선 데이터 장치 또는 개인 휴대용 정보 단말기(PDA)와 같은, 간단한 클라이언트에 대해 이러한 강력한 암호 성능을 사용하는 것은 장치에 따라 가능하지 않을 수도 있다. 또한, 무선 환경에서 사용되는 경우, 이러한 형태의 인증을 사용하는 것은 단지 채널 하나를 확립하기 위해 수많은 정보 교환을 요구한다. 무선 장치에서 사용하는 경우, 무선 공간에서의 지연, 네트워크 대역폭 관점에서의 비용, 배터리 수명, 및 데이터 송신 비용이 지나치게 클 수도 있다.

[0004] 다른 해결방법으로서, 더 간단한 암호 방법을 사용하는 것이 있다. 이러한 방식은 NTLM(윈도우즈 NT LAN 매니저)와 같은 시도-응답(challenge-response) 시퀀스를 포함한다. NTLM 인증법을 참조하면, 이는 TCP(전송 제어 프로토콜) 연결을 인증하는, 마이크로소프트 사유의 HTTP 기반 시도-응답 인증 메커니즘이다. NTLM 인증 연결을 통한 HTTP 트래픽의 데이터 무결성은 보호되지 않기 때문에, HTTP 메시지는 공격자에 의해 변화되거나, 제거되거나, 또는 주입될 수 있다. 따라서, 세션이 이미 인증된 적이 있더라도, HTTP 메시지에 대한 데이터 소스 인증이 보증되지는 않는다.

발명의 내용

해결 하고자하는 과제

[0005] 따라서, 상술한 간단한 암호 방법에 대해 보안성을 향상시킨 해결방안이 요구된다. 향상된 해결방안이 널리 구현되기 위해서는 계산의 측면에서 지나치게 강도가 높아서는 안 된다.

과제 해결수단

[0006] 본원 발명은, 클라이언트와 서버 양측 모두에 알려진 클라이언트 자격증명서(credential)을 이용함으로써 데이터 무결성을 유지하는, 보안 세션 인증 방법 및 장치를 제공함으로써 상술한 점을 극복할 수 있다. 구체적으로, 본원 발명은 특정한 형태의 통신을 위한 클라이언트 및 서버 양측 모두에 이미 알려진 공유된 비밀을 이용한다.

[0007] 일 실시형태에서, 서버가 이미 알고 있는 클라이언트 장치용 암호는 공유 자격증명서로서 사용될 수 있다.

[0008] 상기 사항에 대한 다양한 태양이 설명되며, 이러한 태양에는 세션의 생성, 해시 키를 생성하기 위해 암호와 결합된 그 밖의 알려진 정보의 사용, 공유 자격증명서를 확장하기 위한 보안 의사-난수 생성기의 사용, 어드레싱 재생 방식을 위한 시퀀스 넘버의 사용, 기타 다른 것들이 포함된다.

[0009] 따라서, 본원 발명은 클라이언트 장치와 서버 간의 메시지의 클라이언트 자격증명(credential) 기반 인증을 위한 방법으로서, 클라이언트 장치 및 서버 양측 모두는 상기 클라이언트 자격증명서를 인지하고 있는 방법에 있어서, 키를 생성하기 위해 상기 클라이언트 자격증명서를 이용하는 단계 및, 클라이언트 장치와 서버 간의 메시지를 인증하기 위해 상기 키를 이용하는 단계를 포함하는 방법을 제공할 수 있다.

[0010] 또한, 본원 발명은 클라이언트 장치와 서버 간의 메시지의 클라이언트 자격증명서 기반 인증에 사용되는 상기 클라이언트 장치로서, 클라이언트 장치와 서버 양측 모두는 상기 클라이언트 자격증명서를 인지하고 있는 클라이언트 장치에 있어서, 공유되는 자격증명서를 저장하기 위한 메모리; 상기 메모리와 통신하는 프로세서로서, 키를 생성하기 위해 상기 클라이언트 자격증명서를 이용하고, 메시지 인증 코드를 생성하기 위해 상기 키 및 메시지를 사용하며, 보안 메시지를 생성하기 위해 상기 메시지 인증 코드를 상기 메시지에 부가하도록 구성되는 프로세서; 상기 보안 메시지를 송신하도록 구성되는 통신 서브시스템을 포함하는 클라이언트 장치를 제공할 수 있다.

효 과

[0011] 본원 발명은, 클라이언트와 서버 양측 모두에 알려진 클라이언트 자격증명서(credential)를 이용함으로써 데이터 무결성을 유지하는, 보안 세션 인증 방법 및 장치를 제공함으로써 상술한 점을 극복할 수 있다.

발명의 실시를 위한 구체적인 내용

[0012] 이제 도 1을 참조한다. 도 1의 예시적인 프로세스에서, 클라이언트(110)는 서버(120)와 통신한다. 어느 한쪽

방향의 통신이 인증된 것이고 데이터의 삽입 또는 교체가 발생하지 않는다는 것을 보증하기 위하여, 본원 발명은 통신의 어느 일방향 종료시점에서 재생산될 수 있는 식별자가 메시지 텍스트에 부가되는 통신을 제공한다.

[0013] 바람직한 실시형태에서, 부가된 식별자는 메시지 인증 코드(MAC)이다. MAC는 당해 기술분야에 공지되어 있는 것으로, 두 개의 입력을 포함한다. 구체적으로, 이들 입력은 MAC가 부가되는 텍스트와, 비밀 키이다. 두 입력의 조합은 해시가 생성될 수 있도록 하여, 비밀 키를 알지 않고는 해시가 재생성될 수 없다. 당해 기술분야에서 통상의 지식을 가진 자에 의해 이해되는 바와 같이, 해시 값은 일반적으로 임의의 값이 유효하지 않을 정도로 충분히 크다.

[0014] 다양한 MAC 알고리즘이 사용될 수 있다. 한 가지 예는 HMAC 알고리즘이다. 이러한 알고리즘은, 예를 들어, 다음의 수학적 식 1일 수 있다.

수학적 식 1

[0015]
$$\text{HMAC}_K(m) = h((K \oplus \text{opad}) || h((K \oplus \text{ipad}) || m))$$

[0016] K는 키이고, opad 및 ipad는 상수이며, m은 메시지이다. h는 보안 해시 함수이다. 심볼 $\oplus$ 은 비트단위의 배타적 논리합(XOR)을 나타내고, 심볼 ||는 접합(concatenation)을 나타낸다.

[0017] "h"가 SHA1-알고리즘으로 선택되었다면, 알고리즘은 SHA1-HMAC가 되고, 이 알고리즘은 간단한 장치상에서 구현될 수 있다.

[0018] 다시 도 1을 참조하면, 클라이언트(110)는 세션이 활성화되기 전에 서버(120)와 통신하기를 희망한다. 단계 130에서, 클라이언트(110)는 키(K)를 계산한다. 이 키는 클라이언트(110) 및 서버(120) 양측 모두에 알려진 클라이언트 자격증명서에 기초한다. 예를 들어, 상기 키는 클라이언트(110)상의 암호에 기초할 수 있다. 서버는 이러한 암호를 이미 가지고 있을 것이고, 따라서 통신 채널을 통해 암호를 송신하는 것은 요구되지 않는다.

[0019] 당해 기술분야에서 통상의 지식을 가진 자가 이해하는 바와 같이, MAC 함수는 키가 일정한 길이가 되기를 요구한다. 따라서, 암호는 키로서 사용될 수 있기 전에, 원하는 길이의 키를 생성하기 위해 다양한 알고리즘을 거쳐 수정될 필요가 있을 수 있다. 그러한 결정론적인(deterministic) 알고리즘은 당업자에게 알려져 있을 것이고 다양한 알고리즘이 이용될 수 있다.

[0020] 다양한 알고리즘 중 하나로는 원하는 수의 비트에 도달할 때까지 인코딩된 암호 스트링을 반복하는 것이 있을 수 있다. 다른 알고리즘은, 일정한 수의 비트를 확장하고 생성하기 위해 SHA1과 같은 보안 해시 함수를 가지고 암호를 해싱한 후, 불필요한 임의의 초과 비트를 제거하는 것을 포함한다. 다른 접근법은 보안 의사-난수 생성기(PRNG)와 함께 암호 또는 기타 클라이언트 자격증명서를 사용하는 것이 될 수 있다. 이러한 암호 또는 다른 클라이언트 자격증명서는 보안 의사-난수 생성기에 대한 시드(seed)가 될 수 있고, 서버와 클라이언트 양측 모두가 동일한 의사-난수 생성기를 갖는 한 보안 PRNG에 의해 출력된 필요한 수의 비트로 키를 구성할 것이다. 그 밖의 알고리즘들이 당업자에게 알려져 있을 것이다.

[0021] 엔트로피(entropy)를 향상시키기 위해 기타 보안 정보가 암호에 부가될 수 있다. 예를 들어, 클라이언트와 서버 양측 모두에 알려진 정보 중에서 생일, 출생도시, 모친의 처녀시절 이름(maiden name)이 암호에 부가될 수 있고, 또한 이들은 PRNG를 시드(seed)하는 보안 토큰의 일부로서 또는 키를 생성하기 위한 보안 해시 함수의 인수(argument)로서 사용될 수 있다. 그러한 추가적인 보안 정보는 클라이언트에 의해 오프라인으로 제공된다.

[0022] 당업자에게 이해되는 바와 같이, 보안 해시 함수는 가역적(reversible)이지 않다. 보안 PRNG에 의해 생성된 임의의 바이트의 시퀀스가 주어진 경우, 이 시퀀스를 발생시키기 위해 PRNG에 의해 사용된 시드를 계산하는 것은 불가능하다. 그러므로, 보안 해시 함수 또는 보안 PRNG가 키 발생에 사용되는 경우, 주어진 세션을 위한 키가 일치하더라도(compromised), 암호가 즉각적으로 회복되지는 않을 것이다.

[0023] 이해되는 바와 같이, 키(K)에 대한 미리 규정된 길이로 암호의 확장은, 암호의 단지 일부를 사용하는 것과는 반대로 전체 암호를 사용하는 것이 바람직할 것이며, 이는 이러한 암호의 사용이 보다 안전한 키를 제공할 것이기 때문이다.

[0024] 다음으로, 프로세스는 단계 140으로 진행된다. 단계 140에서, 클라이언트(110)은 활성화 메시지를 서버(120)에 보낸다. 활성화 메시지는, 클라이언트 ID(142)와 같은, 클라이언트를 식별하는 식별자를 포함한다. 활성화 메시지는 자신을 위한 MAC를 더 포함한다. 당업자에게 이해되는 바와 같이, MAC는 단계 130에서 계산된 키(K)와

함께 메시지 정보를 포함한다.

- [0025] 일례에서, 활성화 메시지는 HTTP 메시지일 수 있다. 사용자가 HTTP를 통해 보안 세션을 확립하고자 시도하는 경우, MAC는 HTTP 꼬리말(footer)에 추가될 수 있다. 그러나, 이 예는 제한적이지 않고, 다른 메시지 타입이 고려될 수 있다.
- [0026] 단계 145에서, 서버(120)는 단계 140으로부터 수신된 메시지의 클라이언트 식별자에 대한 키를 계산한다. 서버(120)는 클라이언트(110)의 클라이언트 자격증명서로부터의 공통 비밀을 인지하고 있고, 따라서, 클라이언트 ID를 사용하여, 이러한 클라이언트 자격증명서를 찾고, 클라이언트(110)가 키(K)를 계산하는데 사용한 것과 동일한 알고리즘에 기초하여 키를 계산할 수 있다. 일단 단계 145에서 키가 계산되면, 클라이언트(110)으로부터 수신된 어떤 후속하는 메시지들에 대해서도 키를 다시 계산할 필요를 없애기 위하여, 계산된 키는 서버(120) 상에 지역적으로(locally) 저장되고 클라이언트 ID(142) 또는 세션 식별자와 관련될 수 있다.
- [0027] 단계 150에서, 서버(120)는 활성화 응답을, 세션 식별자(ID)(152)와 활성화 응답 메시지에 대한 MAC과 함께, 클라이언트(110)로 되돌려 보낸다. 다시, MAC는 공유된 키 및 활성화 응답 메시지의 콘텐츠에 기초하여 계산된다.
- [0028] 일단 클라이언트(110)가 세션 식별자(152)를 수신하면, 이 세션 식별자는 단계 160에 도시된 바와 같이 서버(120)에 보내지는 후속 메시지(M)에 포함될 수 있다. 유사하게, 서버(120)으로부터 클라이언트(110)로의 메시지 또한 단계 170에 도시된 바와 같이 세션 식별자를 포함할 수 있다.
- [0029] 세션의 일부로서의 후속 메시지 및 활성화 메시지를 포함하는, 어떠한 메시지도 검증될 필요가 있다. 클라이언트(110)가 메시지를 수신하는 때, 클라이언트는, 그 메시지가 인증된 것이라는 것을 보증하기 위하여, 메시지의 MAC를 검증할 필요가 있다. 이는 수신된 메시지를 취하여 클라이언트(110)의 키를 가지고 해싱함으로써 수행된다. 이러한 해시의 결과는 서버(120)로부터 보내질 MAC와 비교된다. 이는 단계 175로서 도시된다.
- [0030] 유사하게, 서버(120)가 클라이언트(110)로부터 메시지를 수신하는 때, 서버는 특정 클라이언트 ID용 키를 가지고 그 메시지를 해싱하고, 이것을 클라이언트(110)로부터 보내진 MAC와 비교한다. 이는 단계 180에 도시된다.
- [0031] 상기 검증 단계 175 또는 180이 각각, 서버(120) 또는 클라이언트(110)로부터 보내지는 MAC와 매칭되지 않는다는 결과를 각각 내놓는 경우, 메시지는 유효하지 않은 것으로 고려되고 스푸핑(spoof)일 수 있거나, 그러한 결과는 데이터를 삽입하거나 메시지에서 데이터를 제거하기 위한 누군가의 시도일 수 있다. 이 메시지는 무시될 수 있거나 예러가 기원자(originator)로 되돌려질 수 있다.
- [0032] 세션을 종료한 후, 서버(120) 또는 클라이언트(110) 중 어느 하나는, 단계 190에서 메시지를 다른 당사자에게 보냄으로써 그 세션을 파괴할 수 있다. 메시지는 세션 식별자 및 종료 세션 메시지를 포함한다. 이 종료 세션 메시지는 종료 세션용 MAC, 세션 식별자, 및 키(K)를 수반한다. 단계 190에서의 메시지가 검증되는 경우, 세션은 종료된다.
- [0033] 이제 도 2을 참조한다. 도 2는 클라이언트(110)와 서버(120) 간의 데이터흐름도를 도시하고, 도 1의 실시형태에 대한 대안적인 실시형태를 제공한다. 구체적으로, 도 1의 실시형태는 어드레싱 재생을 예방하지 않고, 만약 시스템의 설계자가 어드레싱 재생 공격을 염려한다면 도 2의 방법이 대신 사용될 수 있다.
- [0034] 당업자에게 이해되는 바와 같이, 도 1의 방법을 이용할 때, 클라이언트(110)와 서버(120) 간의 통신을 스누핑(snooping)하는 제3자는 메시지를 가로채어 그 메시지를 서버(120)로 다시 보낼 수 있다. 도 1의 방법에서, 서버(120)는 동일한 검증(180)을 수행하여 메시지가 유효하다고 판정하고 적절한 응답을 보낸다. 몇몇 경우에는, 그러한 어드레싱 재생 공격의 발생을 허용하는 것이 바람직하지 않다. 이러한 경우, 메시지의 일부로서 시퀀스 넘버를 사용할 수 있다.
- [0035] 구체적으로, 도 1에서와 마찬가지로 단계 130에서 클라이언트(110)는 키(K)를 계산한다. 다음으로 단계 210에서, 활성화 메시지, 클라이언트 식별자(ID)(142), 시퀀스 넘버(244) 및 MAC(248)을 포함하는 메시지가 보내진다. MAC(K)(248)은 이제 시퀀스 넘버(244)를 포함하는 메시지에 기초하여 계산된다. MAC 계산에 시퀀스 넘버를 포함시키는 것은 누군가가 그 후에 클라이언트(110)를 속이려고 시도하기 위해 상이한 시퀀스 넘버를 삽입하는 것을 예방한다.
- [0036] 서버(120)가 단계 210으로부터 메시지를 수신하는 때, 서버는, 도 1의 방법에서와 마찬가지로 단계 145에서 클라이언트 ID(142)를 위한 키를 계산한다. 또한, 서버는 도 1에서와 마찬가지로 단계 180에서 MAC를 검증한다. 단계 215에서 프로세스는 또한 시퀀스 넘버를 검증한다. 이것은, 서버(120)가 이전에 특정 클라이언트 ID로부

터 시퀀스 넘버를 수신한 적이 있는지 없는지 여부를 검사하고, 만약 수신한 적이 있다면, 메시지를 무시하는 것을 포함한다. 당업자에게 이해되는 바와 같이, 클라이언트(110)가 도 2의 방법을 사용하여 메시지를 보낼 때마다, 그 메시지와 함께 고유 시퀀스 넘버가 보내져야 한다. 고유 시퀀스 넘버를 제공하는 다양한 방법들이 당업자에게 알려져 있다.

- [0037] MAC가 단계 180에서 검증되고 시퀀스 넘버가 단계 215에서 검증되면, 단계 220에서 서버(120)는 활성화 응답 메시지를 클라이언트(110)에 되돌려 보낸다. 이 활성화 응답 메시지는 MAC(K)(258)와 함께 응답, 세션 식별자(152), 시퀀스 넘버(254)를 포함한다.
- [0038] 도 1의 방식과 유사한 방식으로, 후속 메시지들은, 클라이언트(110)와 서버(120) 양측 모두에 알려진 키와 함께 세션 식별자, 메시지(M), 및 이들 모두에 대해 계산된 MAC를 갖는 시퀀스 넘버로 처리될 수 있다.
- [0039] 세션의 종료 시점에서, 서버(120) 또는 클라이언트(110) 중 어느 하나는, 세션 식별자, 시퀀스 넘버, 및 이들 모두에 대한 MAC를 포함하는, 종료 세션 메시지를 보냄으로써 세션을 파괴시킬 수 있다. 그 후, 세션은 종료된다.
- [0040] 키에 대해 암호가 사용된다면, 그 키가 열악한 엔트로피(entropy)를 가질지도 모른다는 염려가 있을 수 있다. 한가지 해결방안은, 암호가 최소 길이이고 글자와 숫자를 모두 가지고 있으며 흔한 단어가 아님을 확실히 하는 등에 의해, 원하는 암호 강도 레벨을 실현하는 것이다. 예를 들어, 보안 전문가들에게 용인가능한 정도의 합리적인 키 엔트로피를 달성하기 위해, 암호 또는 암호와 다른 보안 토큰의 조합을 20바이트 이상으로 할 수 있다.
- [0041] 클라이언트(110) 및 서버(120)에 의해 확립된 모든 세션에 대해 키가 동일한 상태로 남아 있다는, 보안 측면에서의 걱정이 있을 수 있다. 하나의 해결방안으로서, 클라이언트(110) 및 서버(120)에 의해 확립된 매 세션마다 고유 키를 사용할 수 있다. 그러므로, 어떤 방법은, 일단 세션 식별자가 수신되면, 키의 일부로서 세션 식별자를 사용할 수 있다.
- [0042] 도 3을 참조하면, 클라이언트(110)은 서버(120)와 통신한다. 착수시에, 키는 단계 130에서 계산되고, 단계 310에서 클라이언트 식별자 및 MAC를 포함하는 활성화 메시지가 서버에 보내진다. 단계 130에서 계산된 키는 암호와 같은 공유된 비밀에 기초한다. 그 후, 서버는 클라이언트 식별자용 키(K)를 계산할 수 있고, 단계 180에서 MAC를 검증할 수 있다. 그 후, 단계 315에서 서버(120)는 K2로 표시되는 제2키를 생성한다. 클라이언트(110)의 세션에 할당되는 세션 식별자와 함께, 암호와 같은 공유된 자격증명서들의 조합으로부터, K2가 유도될 수 있다. 공유 자격증명서의 조합과 세션 식별자를 위한 알고리즘은 클라이언트(110)와 서버(120) 양측 모두에 알려질 것이다.
- [0043] 단계 320에서 서버(120)는, 활성화 응답, 세션 식별자(152), 키(K2)로 생성된 MAC를 포함하는, 인증된 응답 메시지를 클라이언트(110)에 되돌려 보낸다. 단계 325에서 클라이언트(110)는, 단계 320의 메시지로 수신된 세션 식별자에 기초하여 키(K2)를 계산하고, 이 키(K2)를 저장한다. 그 후, 클라이언트(110)는 서버(120)와의 후속 통신들에 이 키(K2)를 사용한다.
- [0044] 이해되는 바와 같이, 도 3의 방법 또한 메시지 내의 시퀀스 넘버를 이용할 수 있고, 따라서 도 2와 도 3의 방법들은 결합될 수 있다.
- [0045] 키 내의 세션 식별자의 사용은 그 세션을 위한 고유 키를 제공한다.
- [0046] 다른 대안에서, 공유된 클라이언트 자격증명서에 기초한 키를 이용하는 클라이언트와 서버들 사이에, 보다 보안성 높은 대칭 키(symmetric key)가 교섭(negotiate)될 수 있고, 이에 의해 대칭 암호화가 가능해진다. 예를 들어, 클라이언트는 세션 활성화 메시지를 서버에 보낼 수 있다. 그 후, 서버는 공유된 키를 이용하여 암호화되는 대칭 키를 가지고 응답할 수 있다. 대안적으로, 클라이언트는 원래 메시지의 보안성 높은 키를 보낼 수 있으며, 이는 서버와 클라이언트 양측 모두가 상기 보안성 높은 키의 해독에 사용되는 공유 키를 알 것이기 때문이다. 그 후, 대칭 키는 클라이언트와 서버 간 메시지의 인증 및/또는 암호화에 사용될 수 있다. 그러나, 이러한 강화는 대칭 암호화/해독 능력을 요구한다.
- [0047] 당업자에게 이해되는 바와 같이, 상기 사항들은 데이터 송신에 적합한 어떤 프로토콜을 사용해서도 송신될 수 있지만, 무선 장치용으로는 UDP와 같은 데이터 기반의 프로토콜을 사용하는 것이 바람직하다.
- [0048] 따라서, 도 1, 2, 및 3은, 해싱용 키를 생성하기 위해 공유된 비밀을 이용하는, 클라이언트-서버 간 통신 방법을 도시한다. 해시는, 메시지의 진정성을 보증하고 스푸핑(spoofing) 또는 메시지로부터의 데이터의 삭제나 삽입을 예방하기 위하여, 키를 이용하고 메시지에 통합될 수 있다. 알려진 자격증명서는 암호와 같은 클라이언트

및 서버 양측 모두에 이미 알려진 아이템들을 포함할 수 있다. 다른 자격증명으로는, 클라이언트와 서버 양측 모두에 알려지는 키들을 클라이언트와 서버 양측 모두에 추가하는 것이 있다. 이것은, 이동 장치가 제조될 때 든 아니면 후속하는 규정 단계에서든, 규정을 공급하는 동안에 행해질 수 있다.

[0049] 상기 사항들에 기초하면, 메시지 무결성(integrity)이 MAC에 의해 보호되기 때문에, 메시지는 전송 중에 변경될 수 없다. 세션의 소유자만이 그 세션에 대한 유효한 메시지를 생산할 수 있다는 것을 알 수 있음은 당연하다. 따라서, 서버 또한 인증된다.

[0050] 클라이언트(110)는 서버(120)와 통신할 수 있는 어떠한 장치여도 된다. 컴퓨터와 같은 유선 장치가 이용될 수 있다; 그러나, 여기에서 설명된 방법들의 보호 특징과 간편한 계산 요건들에 의할 때, 이 방법은 제한된 계산 능력을 가진 장치들에서도 역시 이용될 수 있다. 그러한 장치들은, 예를 들어, 몇몇 무선 장치를 포함하고, 이 경우 핸드셰이킹(handshaking) 루틴을 위한 제한된 수의 통신을 갖는 것에 의해 더 큰 이득을 끌어낸다. 이하에서, 본 방법이 이용될 수 있는 하나의 예시적인 이동 장치가 도 4를 참조하여 설명된다. 이것은 한정하도록 의도된 것은 아니며, 설명의 목적을 위해 제공된 것이다.

[0051] 도 4는 본원의 장치 및 방법의 바람직한 실시형태와 함께 이용되기에 적합한 이동 장치를 도시하는 블록도이다. 이동 장치(400)는 바람직하게는 적어도 음성 및 데이터 통신 능력을 갖는 쌍방향 무선 통신 장치이다. 이동 장치(400)는 인터넷을 통해 다른 컴퓨터 시스템과 통신하는 능력을 갖는 것이 바람직하다. 제공되는 정확한 기능성에 따라, 무선 장치에는, 예를 들어, 데이터 메시징 장치, 쌍방향 무선통신기(pager), 무선 이메일 장치, 데이터 메시징 능력을 갖는 셀룰러 전화기, 무선 인터넷 기기, 또는 데이터 통신 장치가 있을 수 있다.

[0052] 이동 장치(400)가 쌍방향 통신용으로 작동(enable)되는 경우, 이동장치는, 하나 이상의 -바람직하게는 임베딩되거나 내부에 위치한- 안테나 소자(416 및 418), 국부발진기(LOs; 413), 및 디지털 신호 프로세서(DSP; 420) 등의 프로세싱 모듈과 같은 관련 부품들뿐 아니라, 수신기(412)와 송신기(414) 모두를 포함하는 통신 서브 시스템(411)을 포함할 것이다. 통신 분야에서 통상의 지식을 가진자에게 이해되는 바와 같이, 통신 서브시스템(411)의 상세한 설계는, 그 장치가 동작 되도록 의도된 통신 네트워크에 따를 것이다.

[0053] 네트워크 액세스 요건들 또한, 네트워크(419)의 유형에 따라 변화할 것이다. 몇몇 CDMA 네트워크에서 네트워크 액세스는 클라이언트 또는 이동 장치(400)의 사용자와 관련된다. CDMA 이동 장치는 CDMA 네트워크 상에서 동작하기 위해 제거가능 사용자 아이덴티티 모듈(RUIM) 또는 클라이언트 아이덴티티 모듈(SIM) 카드를 필요로 할 수도 있다. SIM/RUIM 인터페이스(444)는 일반적으로 -SIM/RUIM 카드가 디스켓이나 PCMCIA 카드처럼 삽입·제거될 수 있는- 카드 슬롯과 유사하다. SIM/RUIM 카드는 대략 64K의 메모리를 가질 수 있고, 많은 수의 키 구성(451), 및 ID(identification) 및 클라이언트 관련 정보와 같은 기타 정보(453)를 보유할 수 있다.

[0054] 필요한 네트워크 등록 또는 활성화 절차가 완료되었을 때, 이동 장치(400)는 네트워크(419)를 통해 통신 신호를 송신 및 수신할 수 있다. 도 4에 도시된 바와 같이, 네트워크(419)는 이동 장치와 통신하는 복수의 기지국으로 구성될 수 있다. 예를 들어, 하이브리드 CDMA 1x EVDO 시스템에서, CDMA 기지국 및 EVDO 기지국은 이동 장치와 통신하고, 이동 장치는 두 기지국 모두에 동시에 접속된다. EVDO 기지국 및 CDMA 1x 기지국은 이동 장치와 통신하기 위해 서로 다른 페이징 슬롯을 사용한다.

[0055] 통신 네트워크(419)를 거쳐 안테나(416)에 의해 수신된 신호는 수신기(412)에 입력되며, 이 수신기는 신호 증폭, 주파수 하향 변환, 필터링, 채널 선택 등과 같은 일반적인 수신기 기능들과, 도 4에 도시된 예시적인 시스템에서는, 아날로그-디지털(A/D) 변환을 수행할 수 있다. 수신된 신호의 A/D 변환은, DSP(420)에서 수행될 복조와 디코딩과 같은 보다 복잡한 통신 기능들을 가능케 한다. 유사한 방식으로, 송신될 신호는 DSP(420)에 의해, 예를 들어 변조 및 인코딩을 포함하는, 처리가 행해지고, 디지털-아날로그 변환, 주파수 상향 변환, 필터링, 증폭, 및 안테나(418)를 통한 통신 네트워크(419) 상으로의 송신을 위해 송신기(414)로 입력된다. DSP(420)는 통신 신호를 처리할 뿐 아니라, 수신기와 송신기 제어를 제공한다. 예를 들어, 수신기(412) 및 송신기(414)의 통신 신호에 적용되는 이득은, DSP(420)에 의해 구현되는 자동 이득 제어 알고리즘을 통해 적응적으로(adaptively) 제어될 수 있다.

[0056] 이동 장치(400)는 이동 장치의 전체 동작을 제어하는 마이크로프로세서(438)를 포함하는 것이 바람직하다. 적어도 데이터 및 음성 통신을 포함하는, 통신 기능들이 통신 서브시스템(411)을 통해 수행된다. 마이크로프로세서(438)는 또한, 디스플레이(422), 플래시 메모리(424), 랜덤 액세스 메모리(RAM; 426), 보조 입/출력(I/O) 서브시스템(428), 시리얼 포트(430), 하나 이상의 키보드 또는 키패드(432), 스피커(434), 마이크로폰(436), 단거리 통신 서브시스템과 같은 기타 통신 서브시스템(440), 및 도면부호 442로 지정된 임의의 기타 장치 서브시스

템과 같은 추가적인 장치 서브시스템들과 상호작용한다. 시리얼 포트(430)는 USB 포트 또는 당업자에게 알려진 기타 포트를 포함할 수 있다.

[0057] 도 4에 도시된 서브시스템들 중 몇몇은 통신-관련 기능들을 수행하는 반면, 나머지 서브시스템들은 "상주하는(resident)" 또는 온-디바이스 기능들을 제공할 수도 있다. 특히, 예를 들어 키보드(432) 및 디스플레이(422)와 같은, 몇몇 서브시스템들은, 통신 네트워크를 통한 송신용 텍스트 메시지의 입력(enter)과 같은 통신-관련 기능과, 계산기 또는 작업 리스트와 같은 장치-상주 기능에 모두 사용될 수도 있다.

[0058] 마이크로프로세서(438)에 의해 사용되는 동작 시스템 소프트웨어는 플래시 메모리(424)-플래시 메모리 대신 리드-온리 메모리(ROM) 또는 유사한 저장 소자(미도시)여도 됨-와 같은 영구 저장소에 저장되는 것이 바람직하다. 당업자는 동작 시스템, 특정 장치 애플리케이션, 또는 그것들의 일부가 RAM(426)과 같은 휘발성 메모리 내로 일시적으로 로딩될 수도 있다는 것을 이해할 것이다. 또한, 수신된 통신 신호는 RAM(426)에 저장될 수도 있다.

[0059] 도시된 바와 같이, 플래시 메모리(424)는 컴퓨터 프로그램(458) 및 프로그램 데이터 저장소(450, 452, 454, 456) 양측에 대해 상이한 영역으로 분리될 수 있다. 이러한 상이한 저장 유형들은 각 프로그램이 그들 자신의 데이터 저장 요건을 위해 플래시 메모리(424)의 일부를 할당할 수 있음을 나타낸다. 마이크로프로세서(438)는, 그것의 동작 시스템 기능에 추가하여, 이동 장치상에서의 소프트웨어 애플리케이션의 실행을 가능하게 하는 것이 바람직하다. 예를 들어 적어도 데이터 및 음성 통신 애플리케이션을 포함하는 기본 동작을 제어하는, 미리 결정된 세트의 애플리케이션은 일반적으로 제조 중에 이동 장치(400)상에 인스톨 될 것이다. 기타 애플리케이션은 후속하여 또는 동적으로 인스톨될 수 있다.

[0060] 바람직한 소프트웨어 애플리케이션으로는, 이메일, 달력 이벤트, 음성 메일, 약속, 및 작업 아이템들(이들에 제한되는 것은 아님)과 같은 이동 장치의 사용자에게 관련되는 데이터 아이템들을 조직하고 관리하는 능력을 갖는 개인 정보 관리기(PIM)가 있을 수 있다. 당연히, PIM 데이터 아이템의 저장을 용이하게 하기 위해, 하나 이상의 메모리 저장소가 이동 장치 상에서 이용가능할 것이다. 이러한 PIM 애플리케이션은 무선 네트워크(419)를 통해 데이터 아이템을 송신 및 수신하는 능력을 갖는 것이 바람직할 것이다. 바람직한 실시형태에서, PIM 데이터 아이템은, 무선 네트워크(419)를 통해, 호스트 컴퓨터 시스템에 저장되거나 그에 관련된 이동 장치 사용자의 대응 데이터 아이템과, 무결절성으로(seamlessly) 통합되고, 동기화되며, 업데이트된다. 네트워크(419), 보조 I/O 서브시스템(428), 시리얼 포트(430), 단거리 통신 서브시스템(440) 또는 임의의 기타 적절한 서브시스템(442)을 통해 추가적인 애플리케이션이 이동 장치(400) 상으로 로딩될 수 있고, 마이크로프로세서(438)에 의해 실행되도록 사용자에게 의해 RAM(426) 또는, 바람직하게는, 비휘발성 저장소(미도시)에 인스톨될 수 있다. 이러한 애플리케이션 인스톨의 융통성은 장치의 기능성을 향상시키고, 또한 강화된 온-디바이스 기능들, 강화된 통신-관련 기능들, 또는 양자 모두를 제공할 수 있다. 예를 들어, 보안 통신 애플리케이션은 전자 상거래 기능 및 그러한 기타 금전적인 거래가 이동 장치(400)를 이용하여 수행될 수 있도록 할 수 있다.

[0061] 데이터 통신 모드에서, 텍스트 메시지 또는 웹 페이지 다운로드와 같은, 수신된 신호는 통신 서브시스템(411)에 의해 처리될 것이고, -바람직하게는 디스플레이(422)(또는 보조 I/O 장치(428))에의 출력을 위해 수신된 신호를 추가적으로 처리하는- 마이크로프로세서(438)에 입력될 것이다.

[0062] 또한, 이동 장치(400)의 사용자는, -바람직하게는 완전한 문자숫자식(alphanumeric) 키보드 또는 전화기-타입 키패드인- 키보드(432)를 디스플레이(422) 및, 경우에 따라서는, 보조 I/O 장치(428)와 함께 이용하여, 예를 들어 이메일 메시지와 같은 데이터 아이템을 작성할 수 있다. 이렇게 작성된 아이템은 그 후 통신 서브시스템(411)을 통해 통신 네트워크 상으로 송신될 수 있다.

[0063] 수신된 신호가 스피커(434)로 출력되는 것이 바람직하고 송신용 신호가 마이크로폰(436)에 의해 생성될 것이라는 점을 제외하면, 음성 통신에 대해서도 이동 장치(400)의 전체적인 동작은 유사하다. 또한, 이동 장치(400) 상에서, 음성 메시지 기록 서브시스템과 같은, 대안적인 음성 또는 오디오 I/O 서브시스템이 구현될 수도 있다. 일차적으로 음성 또는 오디오 신호의 출력이 스피커(434)를 통해 달성되는 것이 바람직하나, 예를 들어 송신자의 아이덴티티, 음성 통화 지속시간, 또는 기타 음성 통화 관련 정보의 표시를 제공하기 위해 디스플레이(422) 또한 사용될 수 있다.

[0064] 도 4의 시리얼 포트(430)는 일반적으로 사용자의 데스크탑 컴퓨터(미도시)와 동기화되는 것이 바람직한 개인 휴대용 정보 단말기(PDA) 타입의 이동 장치에서 구현될 것이나, 이는 선택적인 장치 구성요소이다. 이러한 포트(430)는 사용자로 하여금 외부 장치 또는 소프트웨어 애플리케이션을 통해 선호(preferance)를 설정하는 것을 가능케 할 것이고, 무선 통신 네트워크를 통하지 않고도 이동 장치(400)로의 정보 또는 소프트웨어 다운로드를

제공함으로써 이동 장치(400)의 기능을 늘릴 것이다. 이 대안적인 다운로드 경로는 예를 들어, 직접적이고 따라서 믿을 수 있고 신뢰성 있는 접속을 통해 이동 장치상으로 암호화 키를 로딩하는데 이용될 수 있고, 이에 의해 보안 장치 통신을 가능하게 한다. 당업자에게 이해되는 바와 같이, 시리얼 포트(430)는 추가적으로, 모뎀으로서, 작동하는 컴퓨터에 이동 장치를 접속하는데 사용될 수 있다.

[0065] 단거리 통신 서브시스템과 같은 기타 통신 서브시스템(440)은, 이동 장치(400)와 -반드시 유사한 장치일 필요는 없는- 상이한 시스템 또는 장치 간의 통신을 제공할 수 있는 추가적인 선택적 구성요소이다. 예를 들어, 서브시스템(440)은, 유사하게 작동되는 시스템 및 장치들과의 통신을 제공하기 위한, 적외선 장치와 관련 회로 및 부품 또는 블루투스(Bluetooth)TM 통신 모듈을 포함할 수 있다.

[0066] 도 4의 실시형태는 여기에서 설명된 방법을 구현하는데 이용되는 장치에 대해 필수적이지 않을 수 있는 많은 양태를 포함하고 있다.

[0067] 더 기본적인 장치는 프로세서, 메모리, 및 통신 서브시스템만을 포함할 수도 있다. 구체적으로, 장치는 키(K)와 키(K)에 기초한 MAC를 생성하는 프로세서를 필요로 한다. 메모리는 암호와 같은 공유되는 자격증명서를 저장하는데 이용될 수 있다. 통신 서브시스템은, 셀룰러 네트워크 또는 무선 근거리 통신망(WLAN)과 통신하는 무선 서브시스템과 같은 무선 통신 시스템, 또는 유선 통신을 위한 모뎀 또는 케이블 접속을 포함할 수 있다. 도 4로부터의 몇가지 특징들의 조합을 갖는 통신 서브시스템, 메모리, 및 프로세서를 가지는 기타 장치들 또한 사용될 수 있다.

[0068] 여기에서 설명된 실시형태들은 본원의 기술들의 구성요소에 대응하는 구성요소를 갖는 구조, 시스템, 또는 방법들의 예시이다. 여기에 쓰여진 기재로부터 당업자는 본원의 기술들의 구성요소에 마찬가지로 대응하는 대안적인 구성요소들을 갖는 실시형태들을 만들고 사용할 수 있다. 따라서, 본원의 기술들의 의도된 범위는, 여기에서 설명된 바와 같은 본원의 기술들과 다르지 않은 그 밖의 구조, 시스템, 또는 방법을 포함하며, 여기에서 설명된 바와 같은 본원의 기술들과 실질적이지 않은 차이를 갖는 그 밖의 구조, 시스템, 또는 방법 또한 포함한다.

도면의 간단한 설명

[0069] 본원 발명은 도면을 참조하여 더 잘 이해될 수 있을 것이다.

[0070] 도 1은 클라이언트와 서버 간의 예시적인 통신을 도시하는 데이터 흐름도이다.

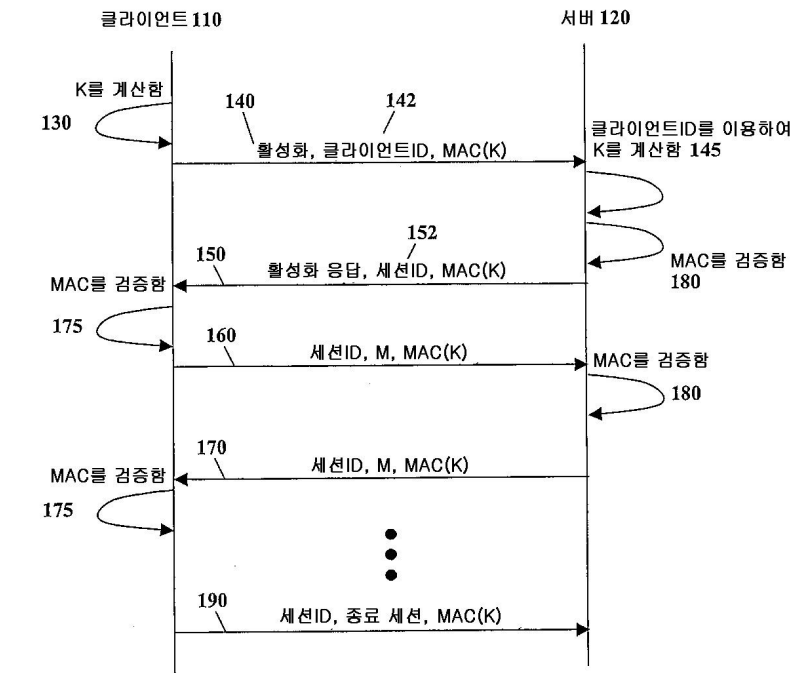
[0071] 도 2는 클라이언트와 서버 간의 다른 예시적 통신을 도시하는 데이터 흐름도이다.

[0072] 도 3은 클라이언트와 서버 간의 또 다른 예시적인 통신을 도시하는 데이터 흐름도이다.

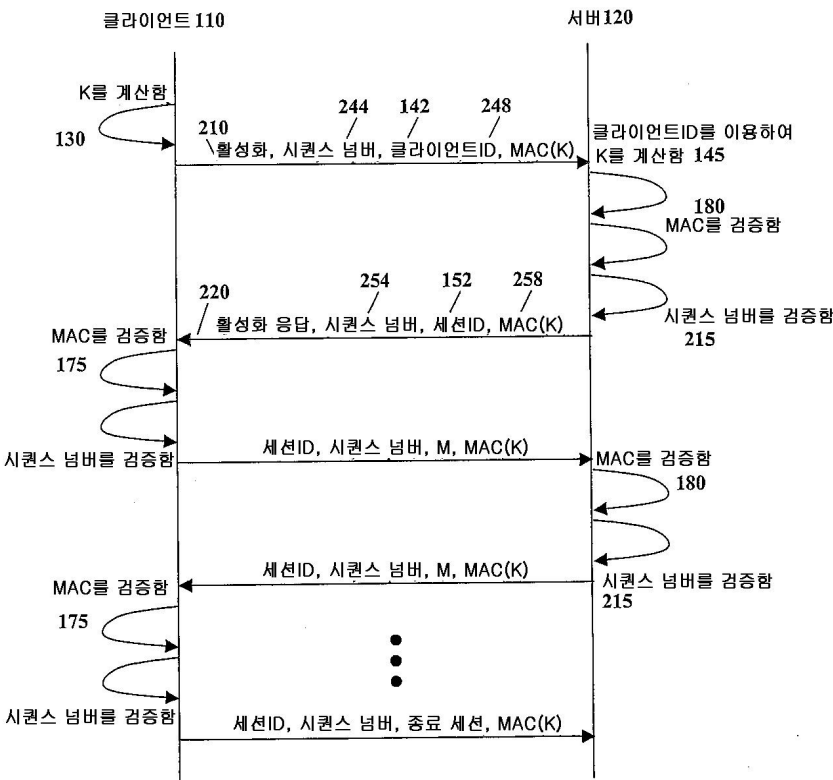
[0073] 도 4는 도 1 내지 도 3에 도시된 클라이언트와 서버 간의 통신과 관련되어 사용될 수 있는 예시적인 이동 장치를 도시하는 블록도이다.

도면

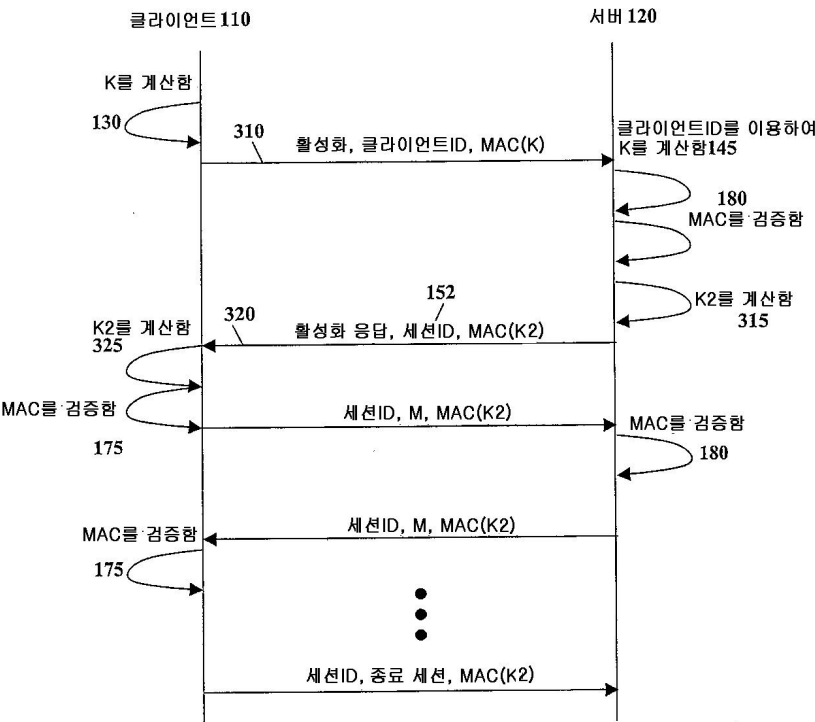
도면1



도면2



도면3



도면4

