(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년11월07일
(11) 등록번호 10-1459255
(24) 등록일자 2014년10월31일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04W 12/04* (2009.01)
(21) 출원번호 10-2013-7026955
(22) 출원일자(국제) 2012년03월14일
심사청구일자 2013년10월11일
(85) 번역문제출일자 2013년10월11일
(65) 공개번호 10-2014-0003593
(43) 공개일자 2014년01월09일
(86) 국제출원번호 PCT/US2012/029117
(87) 국제공개번호 WO 2012/125758
국제공개일자 2012년09월20일
(30) 우선권주장
13/420,420 2012년03월14일 미국(US)
61/452,317 2011년03월14일 미국(US)
(56) 선행기술조사문헌
US20050071645 A1
US20070028299 A1
US20070039042 A1
전체 청구항 수 : 총 17 항

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
뉴만 리차드 이
미국 95110 캘리포니아주 샌호세 테크놀로지 드라이브 1700
슈럼 시드니 비
미국 95110 캘리포니아주 샌호세 테크놀로지 드라이브 1700
용지 로렌스 더블유 3세
미국 95110 캘리포니아주 샌호세 테크놀로지 드라이브 1700
(74) 대리인
특허법인코리아나

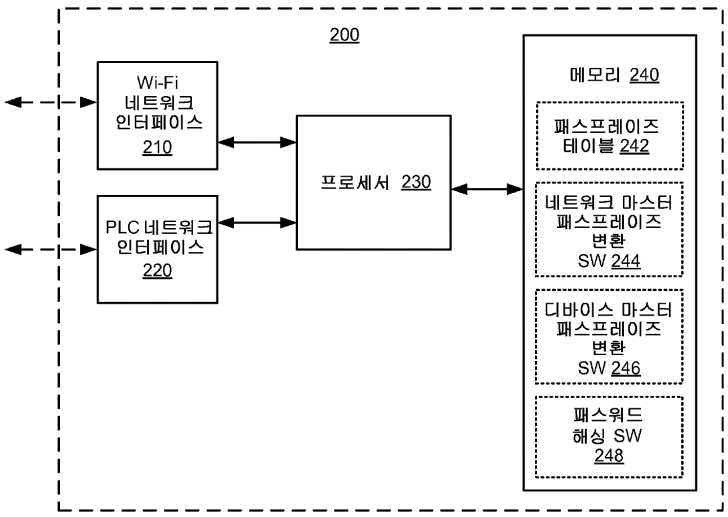
심사관 : 이상윤

(54) 발명의 명칭 **하이브리드 네트워킹 마스터 패스프레이즈**

(57) 요 약

하나 이상의 통신 매체들을 통해 통신하도록 구성된 다수의 네트워크 인터페이스들을 포함하는 하이브리드 네트워크에 대한 패스프레이즈 기반 보안 셋업을 제공하기 위한 방법 및 장치가 제공된다. 이 방법은 다수의 네트워크 인터페이스들의 네트워크 인터페이스에서 사용자로부터 패스프레이즈를 수신하는 단계를 포함한다. 수신된 패스프레이즈는 그 후에 하나 이상의 네트워크 인터페이스들에 대한 디바이스를 인증하기 위해 이용된다. 이 인증은 네트워크 인터페이스들에 의해 이용된 통신 매체에 상관없이 수행될 수 있다.

대 표 도



특허청구의 범위

청구항 1

제 1 및 제 2 통신 프로토콜들에 따라 각각 동작하는 제 1 및 제 2 서브-네트워크들을 갖는 하이브리드 네트워크로서,

상기 제 1 및 제 2 통신 프로토콜들은 상이하고, 홈플러그 (HomePlug) 프로토콜 및 WLAN (wireless local area network) 프로토콜로부터 선택되고,

상기 하이브리드 네트워크는 제 1 디바이스를 포함하고,

상기 제 1 디바이스는,

상기 제 1 통신 프로토콜의 제 1 네트워크 인터페이스;

제 1 프로세서; 및

상기 제 1 프로세서에 커플링되고 제 1 컴퓨터 실행가능 명령들을 저장하고 있는 제 1 메모리

를 포함하고,

상기 제 1 컴퓨터 실행가능 명령들은, 상기 제 1 프로세서에 의해 실행될 때, 상기 제 1 디바이스로 하여금,

사용자로부터 마스터 패스프레이즈 (master passphrase) 를 수신하게 하고;

상기 제 1 통신 프로토콜에 응답하여 제 1 패스워드를 발생시키기 위해 상기 마스터 패스프레이즈의 문자들을 선택적으로 절단, 부가, 또는 대체함으로써, 상기 마스터 패스프레이즈를, 상기 제 1 통신 프로토콜을 준수하는 상기 제 1 패스워드로 변환하게 하고;

상기 제 1 패스워드를 이용하여 상기 제 1 서브-네트워크에 대해 상기 제 1 디바이스를 인증하게 하고;

상기 제 1 패스워드를 해싱하여 상기 제 1 통신 프로토콜을 준수하는 제 1 키를 유도하게 하며;

상기 제 1 키를 이용하여 상기 제 1 디바이스를 상기 제 1 서브-네트워크에 합류시키게 하는, 하이브리드 네트워크.

청구항 2

제 1 항에 있어서,

상기 하이브리드 네트워크는 제 2 디바이스를 더 포함하고,

상기 제 2 디바이스는,

상기 제 2 통신 프로토콜의 제 2 네트워크 인터페이스;

제 2 프로세서; 및

상기 제 2 프로세서에 커플링되고 제 2 컴퓨터 실행가능 명령들을 저장하고 있는 제 2 메모리

를 포함하고,

상기 제 2 컴퓨터 실행가능 명령들은, 상기 제 2 프로세서에 의해 실행될 때, 상기 제 2 디바이스로 하여금,

상기 사용자로부터 상기 마스터 패스프레이즈를 수신하게 하고;

상기 제 2 통신 프로토콜에 응답하여 제 2 패스워드를 발생시키기 위해 상기 마스터 패스프레이즈의 문자들을 선택적으로 절단, 부가, 또는 대체함으로써, 상기 마스터 패스프레이즈를, 상기 제 2 통신 프로토콜을 준수하는 상기 제 2 패스워드로 변환하게 하고;

상기 제 2 패스워드를 이용하여 상기 제 2 서브-네트워크에 대해 상기 제 2 디바이스를 인증하게 하고;

상기 제 2 패스워드를 해싱하여 상기 제 2 통신 프로토콜을 준수하는 제 2 키를 유도하게 하며;

상기 제 2 키를 이용하여 상기 제 2 디바이스를 상기 제 2 서브-네트워크에 합류시키게 하는, 하이브리드 네트워크.

청구항 3

제 1 항에 있어서,

상기 제 1 메모리는 부가적인 컴퓨터 실행가능 명령들을 저장하고 있고,

상기 부가적인 컴퓨터 실행가능 명령들은, 상기 제 1 프로세서에 의해 실행될 때, 상기 제 1 디바이스로 하여금,

상기 제 1 디바이스로부터의 상기 마스터 패스프레이즈를, 상기 제 1 또는 제 2 통신 프로토콜의 네트워크 인터페이스를 갖는 제 3 디바이스에 송신하게 하는, 하이브리드 네트워크.

청구항 4

제 1 및 제 2 통신 프로토콜들에 따라 각각 동작하는 제 1 및 제 2 서브-네트워크들을 갖는 하이브리드 네트워크에 다수의 디바이스들을 부가하는 방법으로서,

상기 제 1 및 제 2 통신 프로토콜들은 상이하고, 홈플러그 (HomePlug) 프로토콜 및 WLAN (wireless local area network) 프로토콜로부터 선택되고,

상기 방법은,

마스터 패스프레이즈를 제 1 디바이스에 입력하는 단계로서, 상기 제 1 디바이스는 상기 제 1 통신 프로토콜의 제 1 네트워크 인터페이스를 포함하는, 상기 마스터 패스프레이즈를 제 1 디바이스에 입력하는 단계;

상기 제 1 디바이스에서의 제 1 변환 동작을 이용하여 상기 마스터 패스프레이즈를 변환하여 상기 제 1 통신 프로토콜을 준수하는 제 1 패스워드를 발생시키는 단계로서, 상기 제 1 변환 동작은, 상기 제 1 통신 프로토콜에 응답하여 상기 제 1 패스워드를 발생시키기 위해 상기 마스터 패스프레이즈의 문자들을 선택적으로 절단, 부가, 또는 대체하는 것을 포함하는, 상기 제 1 통신 프로토콜을 준수하는 제 1 패스워드를 발생시키는 단계;

상기 제 1 패스워드를 이용하여 상기 제 1 서브-네트워크에 대해 상기 제 1 디바이스를 인증하는 단계;

상기 제 1 패스워드를 해싱하여 상기 제 1 통신 프로토콜을 준수하는 제 1 키를 유도하는 단계; 및

상기 제 1 키를 이용하여 상기 제 1 디바이스를 상기 제 1 서브-네트워크에 합류시키는 단계를 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 방법.

청구항 5

제 4 항에 있어서,

상기 제 1 디바이스로부터의 상기 마스터 패스프레이즈를 암호화된 메시지로 제 3 디바이스에 전송하는 단계를 더 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 방법.

청구항 6

제 4 항에 있어서,

마스터 패스프레이즈를 제 2 디바이스에 입력하는 단계로서, 상기 제 2 디바이스는 상기 제 2 통신 프로토콜의 제 2 네트워크 인터페이스를 포함하는, 상기 마스터 패스프레이즈를 제 2 디바이스에 입력하는 단계;

상기 제 2 디바이스에서의 제 2 변환 동작을 이용하여 상기 마스터 패스프레이즈를 변환하여 상기 제 2 통신 프로토콜을 준수하는 제 2 패스워드를 발생시키는 단계로서, 상기 제 2 변환 동작은, 상기 제 2 통신 프로토콜에 응답하여 상기 제 2 패스워드를 발생시키기 위해 상기 마스터 패스프레이즈의 문자들을 선택적으로 절단, 부가, 또는 대체하는 것을 포함하는, 상기 제 2 통신 프로토콜을 준수하는 제 2 패스워드를 발생시키는 단계;

상기 제 2 패스워드를 이용하여 상기 제 2 서브-네트워크에 대해 상기 제 2 디바이스를 인증하는 단계;

상기 제 2 패스워드를 해싱하여 상기 제 2 통신 프로토콜을 준수하는 제 2 키를 유도하는 단계; 및

상기 제 2 키를 이용하여 상기 제 2 디바이스를 상기 제 2 서브-네트워크에 합류시키는 단계를 더 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 방법.

청구항 7

제 6 항에 있어서,

상기 제 1 디바이스로부터의 상기 마스터 패스프레이즈를, 상기 제 1 및 제 2 통신 프로토콜들의 네트워크 인터페이스들을 갖는 제 3 디바이스에 송신하는 단계를 더 포함하고,

상기 제 3 디바이스는, 상기 제 2 변환 동작을 이용하여 상기 마스터 패스프레이즈를 변환하여 상기 제 3 디바이스에서 상기 제 2 패스워드를 발생시키는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 방법.

청구항 8

제 7 항에 있어서,

상기 제 3 디바이스는,

상기 제 2 패스워드를 해싱하여 상기 제 2 키를 유도하고;

상기 제 2 키를 이용하여 상기 제 3 디바이스를 상기 하이브리드 네트워크에 합류시키는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 방법.

청구항 9

제 4 항에 있어서,

상기 하이브리드 네트워크의 기존의 멤버인 제 3 디바이스에서, 상기 제 3 디바이스를 상기 하이브리드 네트워크에 합류시키기 위해 이전에 이용된 제 3 패스워드를 선택하는 단계; 및

상기 제 3 디바이스에서의 역변환 동작을 이용하여, 상기 제 3 패스워드로부터 상기 마스터 패스프레이즈를 유도하는 단계를 더 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 방법.

청구항 10

제 4 항에 있어서,

상기 변환 동작들을 수행하지 않는 제 4 디바이스를 대신하여 상기 제 1 통신 프로토콜의 네트워크 인터페이스를 갖는 제 3 디바이스에서 상기 마스터 패스프레이즈를 유도하는 단계를 더 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 방법.

청구항 11

제 1 및 제 2 통신 프로토콜들에 따라 각각 동작하는 제 1 및 제 2 서브-네트워크들을 갖는 하이브리드 네트워크에 다수의 디바이스들을 부가하는 시스템으로서,

상기 제 1 및 제 2 통신 프로토콜들은 상이하고, 홈플러그 (HomePlug) 프로토콜 및 WLAN (wireless local area network) 프로토콜로부터 선택되고,

상기 시스템은,

마스터 패스프레이즈를 제 1 디바이스에 입력하는 수단으로서, 상기 제 1 디바이스는 상기 제 1 통신 프로토콜의 제 1 네트워크 인터페이스를 포함하는, 상기 마스터 패스프레이즈를 제 1 디바이스에 입력하는 수단;

상기 제 1 디바이스에서의 제 1 변환 동작을 이용하여 상기 마스터 패스프레이즈를 변환하여 상기 제 1 통신 프로토콜을 준수하는 제 1 패스워드를 발생시키는 수단으로서, 상기 제 1 변환 동작은, 상기 제 1 통신 프로토콜에 응답하여 상기 제 1 패스워드를 발생시키기 위해 상기 마스터 패스프레이즈의 문자들을 선택적으로 절단, 부가, 또는 대체하는, 상기 제 1 통신 프로토콜을 준수하는 제 1 패스워드를 발생시키는 수단;

상기 제 1 패스워드를 이용하여 상기 제 1 서브-네트워크에 대해 상기 제 1 디바이스를 인증하는 수단;

상기 제 1 패스워드를 해싱하여 상기 제 1 통신 프로토콜을 준수하는 제 1 키를 유도하는 수단; 및

상기 제 1 키를 이용하여 상기 제 1 디바이스를 상기 제 1 서브-네트워크에 합류시키는 수단을 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 시스템.

청구항 12

제 11 항에 있어서,

상기 제 1 디바이스로부터의 상기 마스터 패스프레이즈를 암호화된 메시지로 제 3 디바이스에 전송하는 수단을 더 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 시스템.

청구항 13

제 11 항에 있어서,

마스터 패스프레이즈를 제 2 디바이스에 입력하는 수단으로서, 상기 제 2 디바이스는 상기 제 2 통신 프로토콜의 제 2 네트워크 인터페이스를 포함하는, 상기 마스터 패스프레이즈를 제 2 디바이스에 입력하는 수단;

상기 제 2 디바이스에서의 제 2 변환 동작을 이용하여 상기 마스터 패스프레이즈를 변환하여 상기 제 2 통신 프로토콜을 준수하는 제 2 패스워드를 발생시키는 수단으로서, 상기 제 2 변환 동작은, 상기 제 2 통신 프로토콜에 응답하여 상기 제 2 패스워드를 발생시키기 위해 상기 마스터 패스프레이즈의 문자들을 선택적으로 절단, 부가, 또는 대체하는, 상기 제 2 통신 프로토콜을 준수하는 제 2 패스워드를 발생시키는 수단;

상기 제 2 패스워드를 이용하여 상기 제 2 서브-네트워크에 대해 상기 제 2 디바이스를 인증하는 수단;

상기 제 2 패스워드를 해싱하여 상기 제 2 통신 프로토콜을 준수하는 제 2 키를 유도하는 수단; 및

상기 제 2 키를 이용하여 상기 제 2 디바이스를 상기 제 2 서브-네트워크에 합류시키는 수단을 더 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 시스템.

청구항 14

제 13 항에 있어서,

상기 제 1 디바이스로부터의 상기 마스터 패스프레이즈를, 상기 제 1 및 제 2 통신 프로토콜들의 네트워크 인터페이스들을 갖는 제 3 디바이스에 송신하는 수단을 더 포함하고,

상기 제 3 디바이스는, 상기 제 2 변환 동작을 이용하여 상기 마스터 패스프레이즈를 변환하여 상기 제 3 디바이스에서 상기 제 2 패스워드를 발생시키는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 시스템.

청구항 15

제 14 항에 있어서,

상기 제 3 디바이스는,

상기 제 2 패스워드를 해싱하여 상기 제 2 키를 유도하고;

상기 제 2 키를 이용하여 상기 제 3 디바이스를 상기 하이브리드 네트워크에 합류시키는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 시스템.

청구항 16

제 11 항에 있어서,

상기 하이브리드 네트워크의 기존의 멤버인 제 3 디바이스에서, 상기 제 3 디바이스를 상기 하이브리드 네트워크에 합류시키기 위해 이전에 이용된 제 3 패스워드를 선택하는 수단; 및

상기 제 3 디바이스에서의 역변환 동작을 이용하여, 상기 제 3 패스워드로부터 상기 마스터 패스프레이즈를 유도하는 수단을 더 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 시스템.

청구항 17

제 11 항에 있어서,

상기 변환 동작들을 수행하지 않는 제 4 디바이스를 대신하여 상기 제 1 통신 프로토콜의 네트워크 인터페이스를 갖는 제 3 디바이스에서 상기 마스터 패스프레이즈를 유도하는 수단을 더 포함하는, 하이브리드 네트워크에 다수의 디바이스들을 부가하는 시스템.

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

명 세 서

기 술 분 야

[0001] 본 실시형태들은 일반적으로 네트워크 기술들에 관한 것으로, 상세하게는 하이브리드 네트워킹 솔루션들에 관한 것이다.

배 경 기 술

[0002] 고품질의 디지털 인코딩된 콘텐츠 (예를 들어, 데이터, 보이스, 및 비디오) 를 고정식 및 이동식 디바이스들 양쪽에 분배하고, 이들 디바이스들을 통해 많은 세트의 콘텐츠 관련 서비스들을 가능하게 하고 제어하도록 하는

서비스 제공자들 및 소비자들에 의한 요구가 점점 증가하고 있다. 그러나, 이러한 콘텐츠 관련 서비스들을 가능하게 할 수 있으면서도 또한 사용자 친화적 방법을 허용하여 상이한 네트워크 기술들에 따라 동작하는 다수의 디바이스들을 갖는 하이브리드 네트워크를 생성 및/또는 변경하도록 하는 통합된 네트워크 솔루션은 현재 존재하지 않는다.

[0003] 무선으로 및/또는 하드웨어 접속들을 통해 동작할 수도 있는 기존의 하이브리드 네트워크들은 통상적으로, 다양한 상이한 네트워킹 표준들에 기초하는 다수의 네트워크 기술들 (예를 들어, Wi-Fi, 홈플러그 (HomePlug) AV, 및 이더넷) 을 포함한다. 통상적으로, 이들 상이한 네트워크 기술들의 구성, 동작 및 통신 프로토콜들은 상이한 그룹들에 의해 생성되어 변할 수도 있다. 더욱 상세하게는, 서로 상이한 Wi-Fi, 홈플러그 AV, 및 이더넷 시스템들과 연관된 (예를 들어, 새로운 네트워크들을 생성하는 것, 디바이스들을 기존의 네트워크에 부가하는 것, 접속된 디바이스들을 발견하는 것, 다른 디바이스들/네트워크들에 브리지하는 것 등을 위한) 네트워크 접속 셋업 프로시저들이 존재할 뿐만 아니라, 이들 표준들 중 하나의 표준에 따라 동작하는 디바이스들은 통상적으로, 브리징 디바이스들 및/또는 복잡한 접속 셋업 동작들의 이용 없이 이들 표준들 중 또 다른 표준에 따라 동작하는 디바이스들에 접속하는 (그리고 그에 의해 디바이스들과 통신하는) 것에 대한 어려움을 갖고 있다. 사용자 관점에서, 다수의 상이한 네트워킹 기술들을 채용한 하이브리드 네트워크를 셋업 및/또는 변경하기 위한 단일의 단순화된 메커니즘을 갖는 것이 바람직하다. 또한, 이 하이브리드 네트워크가 사용자에게 완전히 투명한 방식으로 상이한 네트워크 기술들을 통합하는 단일의 끊김없는 네트워크로서 기능하는 것이 바람직하다.

[0004] 통상적으로, 네트워킹 기술들은, 비인가된 디바이스들이, 인가된 디바이스들과 네트워크들을 형성하는 것, 기존의 네트워크에 합류하는 것, 및 네트워크를 통해 전송된 데이터를 디코딩하는 것을 방지하기 위한 보안 메커니즘들을 포함한다. Wi-Fi 및 홈플러그 AV 는 이들 타입의 보안 메커니즘들을 지원하는 네트워크 통신 기술들 또는 프로토콜들의 예들이다.

[0005] 비인가된 디바이스들이 네트워크를 형성하거나 또는 네트워크에 합류하는 것을 방지하기 위한 하나의 기법은, 디바이스들이, 네트워크에 대해 합류하는 디바이스와 그 합류하는 디바이스를 인증하는 디바이스 양쪽에게 알려져 있는 비밀 보안 키 (예를 들어, "미리 공유된 키") 또는 패스워드를 소유한다는 것을 증명하는 것을 필요로 하는 것이다. 이러한 보안 키들은 단일 디바이스와 연관될 수도 있거나 (예를 들어, 디바이스 키) 또는 네트워크와 연관되어 네트워크 내의 모든 디바이스들에게 알려져 있을 수도 있다 (예를 들어, 네트워크 키).

[0006] 사용자 데이터를 암호화하여 이 데이터가 비인가된 디바이스들에 의해 디코딩되는 것을 방지하도록 하기 위해 이용되는 보안 키들은 인증 프로세스 동안 발생될 수 있다. 합류하는 디바이스와 인증하는 디바이스가 동일한 보안 키를 소유하는 것을 보장하는 통상 기법은, 사용자가, 합류하는 디바이스와 인증하는 디바이스 양쪽에 대해 동일한 패스워드를 입력하도록 하는 것을 필요로 하는 것이고, 그에 응답하여, 합류하는 디바이스와 인증하는 디바이스는 동일한 (예를 들어, 미리 공유된) 보안 키를 발생시킬 수도 있다.

[0007] 불행하게도, 패스워드들 및 보안 키들의 상세들 (예를 들어, 수용가능한 길이들, 포맷들, 및/또는 유효 문자 세트들) 이 통상적으로 상이한 네트워크 기술들 간에서 변한다. 예를 들어, 홈플러그 네트워크 프로토콜은 그의 패스워드들을 특정하여 허용가능한 문자들 (예를 들어, 프린트가능한 ASCII 문자들) 의 제 1 세트의 제 1 범위 (예를 들어, N 과 M 인스턴스들 사이) 를 포함하도록 할 수도 있지만, Wi-Fi 네트워크 프로토콜은 그의 패스워드들을 특정하여 허용가능한 문자들 (예를 들어, 모든 ASCII 문자들) 의 제 2 세트의 제 2 범위 (예를 들어, X 와 Y 인스턴스들 사이) 를 포함하도록 할 수도 있고, 여기서 $N \neq X$, $M \neq Y$ 이고, 문자들의 제 1 및 제 2 세트들은 동일하지 않다. 부가적으로, 홈플러그 패스워드들에 허용된 문자들의 최소 개수는 Wi-Fi 패스워드들에 허용된 문자들의 최소 개수보다 더 클 수도 있고, 홈플러그 패스워드들에 허용된 일부 문자들 (예를 들어, 문자들 "[" 및 "]") 은 Wi-Fi 패스워드들에 허용되지 않을 수도 있다. 그 결과, 현재 하이브리드 네트워크들은 통상적으로, 사용자가, 하이브리드 네트워크를 형성 및/또는 이 하이브리드 네트워크에 합류하려고 시도하는 각 타입의 네트워크 기술 디바이스에 대한 상이한 패스워드 및/또는 키를 입력하는 것을 필요로 하는데, 이는 부담스러울 뿐만 아니라 사용자가 각각의 디바이스가 채용한 네트워크 기술의 타입을 결정하는 것을 필요로 할 수도 있고 또는 더 나쁘게는, 상이한 기술들에 대한 상이한 패스워드들을 동일한 디바이스에 대해 입력하는 것을 필요로 할 수도 있다.

[0008] 따라서, 사용자가, 상이한 네트워크 기술들에 따라 동작하는 디바이스들을 이용하는 하이브리드 네트워크를 형성 및/또는 확장하게 하는 단순하고 단일화된 인증 메커니즘에 대한 필요성이 존재한다.

발명의 내용

과제의 해결 수단

[0009] 본 실시형태들에 따르면, 사용자가 단일 마스터 패스프레이즈 (master passphrase) 를 이용하여 상이한 네트워크 기술들에 따라 동작하는 디바이스들을 이용하는 하이브리드 네트워크를 안전하게 형성 및/또는 확장하게 하는 단순하고 단일화된 인증 메커니즘이 개시된다. 따라서, 본 실시형태들은, 다양한 상이한 네트워크 기술들 또는 통신 프로토콜들에 따라 동작하는 네트워크 인터페이스들을 갖는 디바이스들에 대한 패스워드 기반 인증 및 셋업 동작들을 단일화함으로써 하이브리드 네트워크들을 생성 및/또는 변경할 때 사용자들의 경험을 유리하게 개선시킨다. 예를 들어, 사용자가, 상이한 네트워크 기술들을 이용하여 통신하는 디바이스들에 다수의 상이한 기술-특정 패스워드들을 입력하는 것을 필요로 하기보다는, 본 실시형태들은, 단일 마스터 패스프레이즈가, 끊김없고 효율적인 방식으로 하이브리드 네트워크에 대한 상이한 네트워크 기술들에 따라 동작하는 다양한 디바이스들을 인증 및 접속하게 한다. 또한, 본 실시형태들은, 예를 들어, Wi-Fi 및 홈플러그 통신 프로토콜들에 의해 지원되는 다양한 "단순한 접속" 셋업 동작들과 관련하여 구현될 수도 있다.

[0010] 더욱 상세하게는, 제 1 및 제 2 통신 프로토콜들에 따른 데이터 통신을 용이하게 하는 하이브리드 네트워크에 다수의 디바이스들을 합류시키기 위해 단일 마스터 패스프레이즈를 이용하는 본 실시형태들에 따른 일 예시적인 방법이 다음과 같이 구현될 수도 있다. 우선, 사용자는 마스터 패스프레이즈를 제 1 통신 프로토콜의 제 1 네트워크 인터페이스를 갖는 제 1 디바이스에 입력하고, 마스터 패스프레이즈를 제 2 통신 프로토콜의 제 2 네트워크 인터페이스를 갖는 제 2 디바이스에 입력한다. 다음에, 마스터 패스프레이즈가 제 1 변환 동작을 이용하여 제 1 디바이스에서 변환되어, 제 1 통신 프로토콜을 준수하는 제 1 패스워드를 발생시킨다. 마스터 패스프레이즈가 제 2 변환 동작을 이용하여 제 2 디바이스에서 변환되어, 제 2 통신 프로토콜을 준수하는 제 2 패스워드를 발생시킨다. 그 후에, 제 1 패스워드가 이용되어 제 1 디바이스에서 제 1 통신 프로토콜을 준수하는 제 1 키를 유도할 수도 있고, 제 2 패스워드가 이용되어 제 2 디바이스에서 제 2 통신 프로토콜을 준수하는 제 2 키를 유도할 수도 있다. 이들 키들은 그 후에, 하이브리드 네트워크의 대응하는 서브-네트워크들에 대한 제 1 및 제 2 디바이스들을 인증하기 위해 이용될 수도 있다.

[0011] 다른 실시형태들에 대해, 인증 프로세스는 특정 패스워드가 의도되는 통신 프로토콜 또는 네트워크 기술에 따라 각각의 패스워드를 적합한 키로 변환하는 것을 더 수반할 수도 있다. 유도된 키들은 그 후에, 네트워크에 합류하는 것의 부분인 인증 및 키 분배를 수행하기 위해 이용될 수도 있다.

[0012] 이러한 방식으로, 사용자는 전체 하이브리드 네트워크에 대해 단일 패스프레이즈를 유리하게 이용하는 것이 가능할 수도 있어서, 네트워크 내의 각각의 디바이스가 채용한 네트워크 프로토콜(들) 을 알아야 할 필요성을 경감시킬 뿐만 아니라, 네트워크 인터페이스의 각 타입에 대한 분리된 패스워드들을 입력할 필요성을 경감시킨다.
또한, 제 1 네트워크 기술을 통한 또 다른 디바이스에 대한 제 1 네트워크 인터페이스에의 보안 접속을 통해 마스터 패스프레이즈가 획득되면, 마스터 패스프레이즈가 다른 디바이스에 대한 제 2 네트워크 인터페이스를 인증하기 위해 이용될 수도 있어서, 마스터 패스프레이즈를 다른 디바이스에 입력할 필요성이 없어진다.

[0013] 다른 실시형태들에 대해, 제 1 및 제 2 디바이스들은 동일한 통신 프로토콜에 따라 동작할 수도 있고, 및/또는 상이한 통신 프로토콜들에 따라 동작하는 다수의 네트워크 인터페이스들을 포함할 수도 있다.

도면의 간단한 설명

[0014] 첨부 도면들의 피처들에는 본 실시형태들이 제한이 아니라 예시로서 예시되어 있고, 동일한 도면부호들은 유사한 엘리먼트들을 지칭한다:

도 1 은 본 실시형태들이 구현될 수도 있는 하이브리드 네트워크의 블록도이다.

도 2 는 도 1 의 하이브리드 네트워크의 디바이스들 중 일 예시적인 디바이스의 블록도이다.

도 3 은 일부 실시형태에 따른, 단일 네트워크 마스터 패스프레이즈 (network master passphrase; NMPP) 로부터 복수의 상이한 기술-특정 네트워크 패스워드들 및 키들을 생성하기 위한 일 예시적인 동작을 나타낸 일 예시적인 플로차트이다.

도 4 는 일부 실시형태에 따른, 단일 디바이스 마스터 패스프레이즈 (device master passphrase; DMPP) 로부터 복수의 상이한 기술-특정 디바이스 패스워드들 및 키들을 생성하기 위한 일 예시적인 동작을 나타낸 일 예시적인 플로차트이다.

도 5 는 일 예시적인 실시형태 하에서 네트워크를 형성하는 인터페이스 디바이스들 간의 메시지 교환들을 예시

한 순서도이다.

도 6 은 또 다른 예시적인 실시형태 하에서 네트워크를 형성하는 인터페이스 디바이스들 간의 메시지 교환들을 예시한 순서도이다.

도 7 은 또 다른 예시적인 실시형태 하에서 디바이스가 네트워크에 합류하는 인터페이스 디바이스들 간의 메시지 교환들을 예시한 순서도이다.

도 8 은 또 다른 예시적인 실시형태 하에서 디바이스가 네트워크에 합류하는 인터페이스 디바이스들 간의 메시지 교환들을 예시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 다른 디바이스들과 통신하기 위해 각각의 디바이스가 채용한 네트워크 기술 또는 통신 프로토콜과 관계없이, 단일 마스터 패스프레이즈 (master passphrase) 가 디바이스들을 하이브리드 네트워크에 생성, 인증, 및/또는 부가하게 하는 하이브리드 네트워크에 대한 보안 메커니즘을 확립하기 위한 방법 및 장치가 개시되어 있다. 다음의 설명에서는, 본 개시물의 완전한 이해를 제공하기 위해 특정 컴포넌트들, 회로들, 및 프로세스들의 예들과 같은 다수의 특정 상세들이 제시된다. 또한, 다음의 설명에서 그리고 설명의 목적을 위해, 본 실시형태들의 완전한 이해를 제공하기 위해 특정 술어가 제시된다. 그러나, 당업자는 이들 특정 상세들이 본 실시형태들을 실시할 필요가 없을 수도 있다는 것을 인식할 것이다. 다른 경우들에 있어서, 잘 알려져 있는 회로들 및 디바이스들이 본 개시물을 불명확하게 하는 것을 회피하기 위해 블록도로 도시되어 있다. 여기에 사용된 용어 "커플링된" 은 직접 접속되거나 또는 하나 이상의 개재하는 컴포넌트들 또는 회로들을 통해 접속된다는 것을 의미한다. 여기에 설명된 다양한 버스들을 통해 제공된 신호들 중 임의의 신호는 다른 신호들과 시간-다중화될 수도 있고 하나 이상의 공통 버스들을 통해 제공될 수도 있다. 용어 "버스" 는 유선 및 무선 통신 기술들 양쪽을 포함하고, 통신 매체에 접속된 디바이스들의 개수에 의존하지 않는다. 부가적으로, 회로 엘리먼트들 또는 소프트웨어 블록들 간의 상호접속은 버스들 또는 단일 신호 라인들로서 도시될 수도 있다. 버스들 각각은 대안적으로 단일 신호 라인일 수도 있고, 단일 신호 라인들 각각은 대안적으로 버스들일 수도 있으며, 단일 라인 또는 버스는 컴포넌트들 간의 통신을 위한 무수한 물리적 또는 논리적 메커니즘들 중 임의의 하나 이상을 나타낼 수도 있다. 본 실시형태들은 여기에 설명된 특정 예들로 제한되는 것으로 해석되어서는 안되며, 오히려 첨부된 특허청구범위로 정의된 모든 실시형태들의 범위 내에 포함된다.

[0016] 여기에 사용되는 바와 같이, Wi-Fi 디바이스는 WLAN (Wireless Local Area Network) 을 통해 다른 Wi-Fi 디바이스들과 통신할 수도 있다. 용어들 Wi-Fi 및 WLAN 은 IEEE 802.11 계열의 표준들, 블루투스, HiperLAN (유럽에서 주로 사용되는, IEEE 802.11 표준과 비교되는 무선 표준들의 세트), 및 비교적 짧은 무선 전파 범위를 갖는 다른 기술들에 의해 관리되는 통신들을 포함할 수 있다. 따라서, 용어들 "Wi-Fi 디바이스" 및 "WLAN 디바이스" 는 본 개시물에서 상호교환가능하고, 그 모두는 IEEE 802.11 계열의 표준들, 블루투스, HiperLAN, 및 비교적 짧은 무선 전파 범위를 갖는 다른 기술들에 의해 관리되는 통신들을 허용하는 네트워크 인터페이스들을 갖는 디바이스들을 지칭한다.

[0017] 또한, 용어 홈플러그 AV (HomePlug AV; HPAV) 는, TV 의 가정내 분배, 게이밍 및 인터넷 액세스와 같은 애플리케이션들을 위해, 그리고 전기 시스템들과 전기 기구들 사이의 가정내 통신들 및 스마트 파워 미터들을 위해, (예를 들어, 홈플러그 계열의 표준들 및 IEEE 1901 계열의 표준들에 기재되어 있는 바와 같이) 홈플러그 전력선 연합 (HomePlug Powerline Alliance) 에 의해 개발된 표준들의 콜렉션 및 IEEE 1901 표준 그룹에 의해 개발된 표준들의 콜렉션을 지칭한다. 여기서 PLC (Powerline Communications) 표준들이라고도 또한 지칭될 수도 있는 HPAV 표준들은, 기존의 가정 전기 배선이, 다양한 가정내 디바이스들 간의 통신을 용이하게 하는 것 및/또는 인터넷에 접속하는 것을 용이하게 하는 것을 위해 이용되게 한다. 따라서, 용어들 "홈플러그 AV 디바이스", "HPAV 디바이스", 및 "PLC 디바이스" 는 본 개시물에서 상호교환가능하고, 그 모두는 PLC 표준들 및/또는 다양한 홈플러그 표준들 (예를 들어, 홈플러그 1.0, 홈플러그 AV, 홈플러그 AV2 등) 에 의해 관리되는 통신들을 허용하는 네트워크 인터페이스들을 갖는 디바이스들을 지칭한다.

[0018] 또한, 본 실시형태들은 MoCA (Multimedia over Coax Alliance) 네트워킹 표준들 및 다른 네트워킹 표준들을 지원한다. 예를 들어, MoCA 는, 동축 케이블들을 이용하여 소비자 전자장치와 가정들 내의 네트워킹 디바이스들을 접속하고, 준수 디바이스들 간의 오디오 및 비디오 스트림들의 데이터 통신 및 전송 양쪽을 허용하는 표준을 촉진하는 트레이드 그룹이다. 따라서, 여기에 사용되는 바와 같이, 용어 "MoCA 디바이스" 는 MoCA 표준들에 따라 통신하는 디바이스들을 지칭한다.

[0019] 여기에서의 설명의 목적을 위해, 용어 "푸시버튼" 은 임의의 버튼, 스위치, 터치, 스와이프 (swipe), 또는 활성화되었을 때 관련 디바이스가 네트워크 접속 셋업 동작들을 개시하게 하는 다른 적합한 사용자 인터페이스를 지칭할 수도 있다. 또한, 여기에 사용되는 바와 같이, 용어 "합류 디바이스" 는 현재는 네트워크의 멤버가 아닐 수도 있지만 (예를 들어, 디바이스의 푸시버튼의 활성화에 응답하여) 디바이스가 단순한 접속 셋업 동작들을 개시하여 네트워크에 합류하게 하는 "합류 상태" 에 진입하는 디바이스를 지칭한다. 용어 "부가 디바이스" 는 현재는 네트워크의 멤버이고 (예를 들어, 디바이스의 푸시버튼의 활성화에 응답하여) 디바이스가 네트워크에의 또 다른 디바이스 (예를 들어, 합류 디바이스) 의 부가를 용이하게 하는 "부가 상태" 에 진입하는 디바이스를 지칭한다.

[0020] 또한, 여기에 사용되는 바와 같이, 용어들 "패스프레이즈" 및 "패스워드" 는 디바이스들 및/또는 네트워크들 사이의 보안 링크를 확립하는데 이용될 수도 있는 문자들 또는 심볼들 (예를 들어, ASCII 문자들) 의 시퀀스를 지칭하고, 그에 따라 여기에서의 설명의 목적을 위해 상호교환가능할 수도 있다. 용어 "키" 는 새로운 네트워크를 형성하는 것, 기존의 네트워크에 합류하는 것, 및/또는 네트워크와 연관된 하나 이상의 디바이스들을 인증하는 것을 위해 하나 이상의 디바이스들에 의해 이용될 수도 있는 문자들 또는 심볼들 (예를 들어, ASCII 문자들) 의 시퀀스 또는 비트들의 시퀀스를 지칭한다. 여기에 설명된 일부 실시형태들에 대해, 네트워크 패스워드들 및 디바이스 패스워드들은 비교적 단순한 변환 동작들 (예를 들어, 문자 절단, 문자 패딩 (padding), 문자 대체 동작들, 및/또는 문자 인코딩 동작들) 을 이용하여 마스터 패스프레이즈들로부터 유도될 수도 있고, 네트워크 키들 및 디바이스 키들은 비교적 복잡한 변환 동작들 (예를 들어, 해싱 기법들) 을 이용하여 네트워크 패스워드들 및 디바이스 패스워드들 각각으로부터 유도될 수도 있다.

[0021] 상기 언급된 바와 같이, 본 실시형태들에 따르면, 하나 이상의 상이한 네트워크 기술들 또는 통신 프로토콜들에 따라 동작하는 네트워크 인터페이스들을 갖는 디바이스들을 인증하기 위한 보안 크리덴셜들 (예를 들어, 패스워드들 및/또는 보안 키들) 을 발생시키기 위해 단일 마스터 패스프레이즈가 이용될 수도 있다. 패스워드들 및 보안 키들의 상세들 (예를 들어, 수용가능한 길이들, 포맷들, 및/또는 유효 문자 세트들) 은 통상적으로 상이한 네트워크 기술들 간에서 변하기 때문에, 이러한 패스워드들 및 보안 키들을 발생시키기 위한 특정 기법들은 상이한 네트워크 기술들에 따라 변한다. 따라서, 본 실시형태들에 따르면, 비교적 단순한 변환 동작의 상이한 타입들이 공통 마스터 패스프레이즈에 대해 수행되어 상이한 네트워크 기술-특정 패스워드들 및 보안 키들을 발생시키도록 할 수도 있다. 일부 실시형태들에 대해, 주어진 디바이스에서 이러한 패스워드들 및/또는 보안 키들을 유도하기 위해 공통 마스터 패스프레이즈에 대해 수행된 변환 동작의 타입은, (예를 들어, 디바이스가, Wi-Fi 통신 프로토콜들, PLC 프로토콜들, MoCA 프로토콜들, 또는 이러한 프로토콜들의 조합에 따라 동작하는 네트워크 인터페이스를 갖고 있든지 간에) 주어진 디바이스에 의해 채용된 네트워크 인터페이스(들) 의 타입에 응답하여 선택될 수도 있다.

[0022] 일부 실시형태에서, 하이브리드 네트워크를 생성 및/또는 변경할 때 마스터 패스프레이즈들의 2개의 타입이 이용될 수도 있다: "디바이스 마스터 패스프레이즈" 및 "네트워크 마스터 패스프레이즈". 디바이스 마스터 패스프레이즈 (device master passphrase; DMPP) 는 주어진 디바이스가 네트워크에 합류하는데 이용될 수도 있고, 네트워크에 합류하는 디바이스 및 인증하는 디바이스에 의해 미리 공유될 수도 있다. 일부 실시형태에 대해, DMPP 는 (예를 들어, 디바이스의 제조자에 의해) 디바이스에 부착되고 또한 이 디바이스 내의 비휘발성 메모리에 저장된 라벨 상에 프린트될 수도 있다. 그 후에, 디바이스가 하이브리드 네트워크에 합류하기 위해, 사용자는 라벨 상에 나타낸 DMPP 를 (예를 들어, 이미 네트워크의 멤버일 수도 있는) 인증하는 디바이스에 입력한 후에, 합류 디바이스 및 인증하는 디바이스가 DMPP 에 대한 동일한 변환 동작을 수행하여 동일한 네트워크 기술 특정 패스워드를 발생시키고, 그 동일한 네트워크 기술 특정 패스워드는 이어서 2개의 디바이스들 간의 보안 링크를 확립 (예를 들어, 인증) 하고 합류 디바이스가 네트워크에 합류하는 것을 용이하게 위해 이용될 수 있다.

[0023] 하이브리드 네트워크 내의 모든 디바이스들에게 알려져 있는 네트워크 마스터 패스프레이즈 (network master passphrase; NMPP) 는 다양한 기법들을 이용하여 네트워크 디바이스들에게 분배될 수도 있다. 예를 들어, 하나의 실시형태에서, 사용자는 NMPP 를 발생시킨 후에, 그 NMPP 를, 네트워크에 합류하게 될 각각의 디바이스에 입력할 수도 있다. 또 다른 실시형태에서, 주어진 디바이스는 NMPP 를 자동적으로 발생시키고 사용자에게 그 NMPP 를 (예를 들어, 주어진 디바이스에 제공된 적합한 UI 에) 디스플레이할 수도 있고, 그 사용자는 이어서 NMPP 를 네트워크에 합류하려고 시도하는 다른 디바이스들에 입력한다. 또 다른 실시형태에서, 인증 동작 동안, 다른 미리 공유된 디바이스 키들 또는 패스워드들을 이용하여, NMPP 가, 인증하는 디바이스로부터 합류 디바이스로 송신될 수도 있다. NMPP 는 그 후에 각각의 디바이스에 의해 변환되어 동일한 네트워크 기

술 특정 패스워드들을 발생시킬 수도 있고, 그 동일한 네트워크 기술 특정 패스워드들은 이어서 2개의 디바이스들 간의 보안 링크를 확립 (예를 들어, 인증) 하기 위해 이용될 수도 있다.

[0024] 도 1 은 본 실시형태들이 구현될 수도 있는 하이브리드 네트워크 (100) 의 블록도이다. 시스템 (100) 은 Wi-Fi 디바이스 (110), PLC 디바이스 (111), 및 하이브리드 디바이스 (112) 를 포함하도록 도시되어 있다. Wi-Fi 디바이스 (110) 는 IEEE 802.11 계열의 표준들에 따라 동작할 수도 있는 Wi-Fi 인터페이스 (WL0) 를 포함하고, PLC 디바이스 (111) 는 HPAV 표준들, PLC 표준들, 및/또는 IEEE 1901 계열의 표준들에 따라 동작할 수도 있는 PLC 인터페이스 (PL1) 를 포함하며, 하이브리드 디바이스 (112) 는 Wi-Fi 인터페이스 (WL2) 및 PLC 인터페이스 (PL2) 를 포함한다. 단순화를 위해 단지 3개의 디바이스들 (110 내지 112) 만이 도 1 에 도시되어 있지만, 네트워크 (100) 는, 임의의 적합한 네트워크 통신 기술 또는 프로토콜에 따라 동작하는 하나 이상의 네트워크 인터페이스들을 갖는 임의의 개수의 디바이스들을 포함할 수도 있다는 것을 이해해야 한다. 또한, 단순화를 위해 도 1 에 도시되어 있지는 않지만, 네트워크 (100) 는, MoCA 표준들에 의해 관리되는 통신들을 허용하는 MoCA-준수 네트워크 인터페이스들을 포함하는 다른 디바이스들을 포함할 수도 있다.

[0025] 디바이스들 (110 내지 112) 각각은, 예를 들어, 셀 폰, PDA, 태블릿 컴퓨터, 랩톱 컴퓨터, 무선 액세스 포인트, 모뎀, 라우터, PLC 네트워크 어댑터, 인터넷 프로토콜 (IP) 텔레비전, 또는 Wi-Fi 프로토콜들, HPAV 프로토콜들, MoCA 프로토콜들, 이더넷 프로토콜들, 및/또는 다른 프로토콜들을 이용하여 다른 디바이스들과 통신하는 것이 가능한 다른 적합한 디바이스를 포함하는 임의의 적합한 디바이스일 수 있다. 또한, 이러한 디바이스들의 Wi-Fi 인터페이스들이 하이브리드 네트워크 (100) 의 WLAN 서브-네트워크 (단순화를 위해 미도시) 에서 서로 통신할 수도 있고, 이러한 디바이스들의 PLC 인터페이스들이 하이브리드 네트워크 (100) 의 PLC 서브-네트워크 (단순화를 위해 미도시) 에서 서로 통신할 수도 있다는 것 등에 주목한다.

[0026] 도 2 는 도 1 의 하이브리드 디바이스 (112) 의 하나의 실시형태인 디바이스 (200) 를 도시한 것이다. 디바이스 (200) 는 Wi-Fi 네트워크 인터페이스 (210), PLC 인터페이스 (220), 프로세서 (230), 및 메모리 (240) 를 포함한다. Wi-Fi 네트워크 인터페이스 (210) 는, Wi-Fi (즉, WLAN) 프로토콜들을 이용하여 네트워크 (100) 와 연관된 다른 디바이스들과 데이터를 교환하는데 이용될 수 있는 수신기/송신기 회로 (단순화를 위해 미도시) 를 포함한다. PLC 네트워크 인터페이스 (220) 는, HPAV 프로토콜들 및/또는 다른 PLC 프로토콜들을 이용하여 네트워크 (100) 와 연관된 다른 디바이스들과 데이터를 교환하는데 이용될 수 있는 수신기/송신기 회로 (단순화를 위해 미도시) 를 포함한다.

[0027] 메모리 (240) 는, 네트워크 (100) 와 연관된 다른 디바이스들과의 보안 링크들을 확립하는 것, 네트워크 (100) 와 연관된 다른 디바이스들을 인증하는 것, 네트워크 (100) 에의 디바이스 (200) 의 합류를 용이하게 하는 것, 및/또는 네트워크 (100) 에의 다른 디바이스들의 합류를 용이하게 하는 것을 위해 이용될 수도 있는 다양한 패스워드들, 패스프레이즈들, 키들, 및/또는 PIN들을 저장한 패스프레이즈 테이블 (242) 을 포함한다. 예를 들어, 테이블 (242) 은 네트워크 마스터 패스프레이즈 (NMPP), 디바이스 마스터 패스프레이즈 (DMPP), HPAV 네트워크 멤버십 키들 (network membership keys; NMKs), HPAV 디바이스 액세스 키들 (device access keys; DAKs), Wi-Fi 네트워크 패스워드들 (Wi-Fi network passwords; WLNPs), Wi-Fi 미리 공유된 키들 (pre-shared keys; PSKs), 및 임의의 적합한 네트워크 기술에 특정한 다른 적합한 패스워드들을 저장할 수도 있다.

[0028] 또한, 메모리 (240) 는, 다음의 소프트웨어 모듈들을 저장하는 비일시적 컴퓨터 판독가능 매체 (예를 들어, 하나 이상의 비휘발성 메모리 엘리먼트들, 예컨대, EPROM, EEPROM, 플래시 메모리, 하드 드라이브 등) 를 포함한다:

[0029] • 테이블 (242) 에 저장될 수도 있고, 사용자에 의해 적합한 UI 를 통해 입력될 수도 있고, 및/또는 하이브리드 네트워크 (100) 와 연관된 또 다른 디바이스로부터 제공될 수도 있는 네트워크 마스터 패스프레이즈 (NMPP) 에 응답하여 네트워크-기술 특정 네트워크 패스워드들을 발생시키는 네트워크 마스터 패스프레이즈 변환 소프트웨어 (SW) 모듈 (244);

[0030] • 테이블 (242) 에 저장될 수도 있고, 사용자에 의해 적합한 UI 를 통해 입력될 수도 있고, 및/또는 하이브리드 네트워크 (100) 와 연관된 또 다른 디바이스로부터 제공될 수도 있는 디바이스 마스터 패스프레이즈 (DMPP) 에 응답하여 네트워크-기술 특정 디바이스 패스워드들을 발생시키는 디바이스 마스터 패스프레이즈 변환 소프트웨어 모듈 (246); 및

[0031] • 네트워크-기술 특정 패스워드들에 응답하여 네트워크-기술 특정 키들을 발생시키는 패스워드 해싱 소프트웨

어 모듈 (248).

[0032] 각각의 소프트웨어 모듈은, 프로세서 (230) 에 의해 실행될 때, 디바이스 (200) 로 하여금 대응하는 기능들을 수행하게 하는 명령들을 포함한다. 그에 따라, 메모리 (240) 의 비일시적 컴퓨터 판독가능 매체는, 도 3 및 도 4 와 관련하여 후술되는 방법들의 동작들의 전부 또는 일부를 수행하기 위한 명령들을 포함한다.

[0033] Wi-Fi 네트워크 인터페이스 (210), PLC 네트워크 인터페이스 (220), 및 메모리 (240) 에 커플링되는 프로세서 (230) 는, 디바이스 (200) (예를 들어, 메모리 (240) 내) 에 저장된 하나 이상의 소프트웨어 프로그램들의 스트립트들 또는 명령들을 실행하는 것이 가능한 임의의 적합한 프로세서일 수 있다. 예를 들어, 프로세서 (230) 는 네트워크 마스터 패스프레이즈 변환 소프트웨어 (SW) 모듈 (244), 디바이스 마스터 패스프레이즈 변환 소프트웨어 (SW) 모듈 (246), 및 패스워드 해싱 소프트웨어 모듈 (248) 을 실행할 수 있다.

[0034] 더욱 상세하게는, 프로세서 (230) 는 네트워크 마스터 패스프레이즈 변환 SW 모듈 (244) 을 실행하여 본 실시형태들에 따른 다양한 변환 동작들을 이용하여 NMPP 로부터 임의의 개수의 상이한 네트워크-기술 특정 네트워크 패스워드들을 발생시킬 수도 있다. 예를 들어, SW 모듈 (244) 의 실행은 NMPP 에 대한 제 1 변환 동작을 수행하여 HPAV 네트워크 패스워드 (network password; NPW) 를 발생시킬 수도 있고, NMPP 에 대한 제 2 변환 동작을 수행하여 WLAN 네트워크 패스워드 (WLAN network password; WLNP) 를 발생시킬 수도 있고, 및/또는 NMPP 에 대한 다른 변환 동작들을 채용하여 다른 서브-네트워크 기술들에 대한 네트워크 패스워드들을 발생시킬 수도 있다.

[0035] 이와 유사하게, 프로세서 (230) 는 디바이스 마스터 패스프레이즈 변환 SW 모듈 (246) 을 실행하여 본 실시형태들에 따른 다양한 변환 동작들을 이용하여 DMPP 로부터 임의의 개수의 상이한 네트워크-기술 특정 디바이스 패스워드들을 발생시킬 수도 있다. 예를 들어, SW 모듈 (246) 의 실행은 DMPP 에 대한 제 1 변환 동작을 채용하여 HPAV 디바이스 패스워드 (device password; DPW) 를 발생시킬 수도 있고, DMPP 에 대한 제 2 변환 동작을 채용하여 WLAN 디바이스 패스워드 (WLAN device password; WLDP) 를 발생시킬 수도 있고, 및/또는 DMPP 에 대한 다른 변환 동작들을 채용하여 다른 서브-네트워크 기술들에 대한 디바이스 패스워드들을 발생시킬 수도 있다.

[0036] 프로세서 (230) 는 패스워드 해싱 SW 모듈 (248) 을 실행하여, 네트워크 기술의 각 타입에 대해, 패스프레이즈 변환 SW 모듈들 (244 및/또는 246) 에 의해 발생된 대응하는 패스워드(들) 로부터 보안 키를 발생시킬 수도 있다. 더욱 상세하게는, HPAV 네트워크 기술들에 대해, 패스워드 해싱 SW 모듈 (248) 은 HPAV 네트워크 패스워드 (network password; NPW) 로부터 HPAV 네트워크 멤버십 키 (NMK) 를 유도할 수도 있고, 및/또는 HPAV 디바이스 패스워드 (DPW) 로부터 HPAV 디바이스 액세스 키 (DAK) 를 유도할 수도 있다. WLAN 네트워크 기술들에 대해, 패스워드 해싱 SW 모듈 (248) 은 WLAN 네트워크 패스워드 (WLNP) 로부터 WLAN 미리 공유된 키 (PSK) 를 유도할 수도 있고, 및/또는 WLAN 디바이스 PIN (WLDP) 으로부터 WLAN 디바이스 키 (WLAN device key; WLDK) 를 유도할 수도 있다.

[0037] 도 1 의 Wi-Fi 디바이스 (110) 및 PLC 디바이스 (111) 의 실시형태들은, 네트워크 인터페이스들의 개수 및/또는 타입을 제외하고는, 도 2 의 하이브리드 디바이스 (200) 와 유사할 수도 있다는 것에 주목한다. 예를 들어, Wi-Fi 디바이스 (110) 의 실시형태들은 PLC 인터페이스 (220) 를 제외하고는 하이브리드 디바이스 (200) 의 모든 엘리먼트들을 포함할 수도 있는 한편, PLC 디바이스 (111) 의 실시형태들은 Wi-Fi 인터페이스 (210) 를 제외하고는 하이브리드 디바이스 (200) 의 모든 엘리먼트들을 포함할 수도 있다.

[0038] 도 3 은 일부 실시형태에 따른, 단일 네트워크 마스터 패스프레이즈 (NMPP) 로부터 복수의 상이한 기술-특정 네트워크 패스워드들 및 키들을 생성하기 위한 일 예시적인 동작을 나타낸 일 예시적인 플로차트 (300) 이다. 우선, 사용자는 하이브리드 네트워크 (100) 와 연관된 하나 이상의 디바이스들에 NMPP 를 입력한다 (302). NMPP 는, 더욱 상세히 설명되는 바와 같이, HPAV 네트워크 패스워드 (NPW) 및 Wi-Fi 네트워크 패스워드 (WLNP) 의 슈퍼세트일 수도 있다는 것에 주목한다.

[0039] 그 후에, NMPP 가 입력되었고 및/또는 이전에 저장된 디바이스들에서 비교적 단순한 변환 동작들의 하나 이상의 타입이 수행될 수도 있다 (304). 일부 실시형태에 대해, 이들 비교적 단순한 변환 동작들이 (예를 들어, 디바이스가 채용한 네트워크-기술 인터페이스(들) 의 타입에 따라) 선택적으로 수행되어 하나 이상의 기술-특정 네트워크 패스워드들을 발생시킬 수도 있다 (306). 일부 실시형태에 대해, 비교적 단순한 변환 동작들이 선택적으로 NMPP 의 문자들을 절단하고, NMPP 를 패딩하고 (예를 들어, NMPP 에 문자들을 부가하고), NMPP 의 문자들을 대체하고, 및/또는 NMPP 의 문자들의 세트들을 인코딩하여 다양한 기술-특정 네트워크 패스워드들을 발

생시키도록 할 수도 있다 (306). 예를 들어, NMPP 에 대해 제 1 변환 동작이 수행되어 HPAV 네트워크 패스워드 (NPW) 를 발생시킬 수도 있고 (306A), NMPP 에 대해 제 2 변환 동작이 수행되어 WLAN 네트워크 패스워드 (WLNP) 를 발생시킬 수도 있고 (306B), 및/또는 NMPP 에 대해 제 3 변환 동작이 수행되어 다른 네트워크 기술들에 대한 네트워크 패스워드들 (NTPP) 을 발생시킬 수도 있다 (306C).

[0040] 상기 언급된 바와 같이, 패스워드들 및 보안 키들의 상세들 (예를 들어, 수용가능한 길이들, 포맷들, 및/또는 유효 문자 세트들) 은 통상적으로 상이한 네트워크 기술들 간에서 변한다. 예를 들어, 하나의 네트워크 기술 (예를 들어, HPAV) 은 임의의 프린트가능한 ASCII 문자의 (임의의 프린트가능한 ASCII 문자를 포함하는) 8개와 64개의 인스턴스들 사이를 갖는 패스워드들을 허용할 수도 있는 한편, 또 다른 네트워크 기술 (예를 들어, Wi-Fi) 은 단지 알파뉴메릭 문자들의 (알파뉴메릭 문자들을 포함하는) 4개와 20개의 인스턴스들 사이를 갖는 패스워드들을 허용할 수도 있다. 따라서, 본 실시형태들에 따르면, 타깃 네트워크 기술이 그의 패스워드들이 논-알파뉴메릭 문자들 (예를 들어, 스페이스, 탭, 구두점 등) 을 포함하게 하지 않으면, 이러한 논-알파뉴메릭 문자들을 포함하는 네트워크 마스터 패스프레이즈 (NMPP) 가, 이러한 논-알파뉴메릭 문자들을 미리 결정된 알파뉴메릭 문자들 및/또는 미리 결정된 문자들의 시퀀스들로 대체하는 변환 동작을 이용하여 변환될 수도 있어서, NMPP 로부터 발생된 기술-특정 패스워드가 타깃 네트워크 기술을 준수하도록 한다 (예를 들어, 결과적인 네트워크 기술-특정 패스워드가 단지 타깃 네트워크 기술에 의해 허용된 문자들 및/또는 심볼들을 포함하도록 한다).

역으로, NMPP 가 타깃 네트워크 기술에 의해 허용되지 않는 어떠한 문자들도 포함하고 있지 않으면, NMPP 로부터 네트워크 패스워드를 발생시킬 때 NMPP 의 임의의 문자들을 대체시키기 위해 기술-특정 네트워크 패스워드를 발생시키도록 채용된 변환이 필요하지 않을 수도 있다.

[0041] NMPP 가 타깃 네트워크 기술에 의해 허용된 최소 개수의 패스워드 문자들보다 더 적은 문자들을 포함하면 (예를 들어, NMPP 가 너무 짧으면), NMPP 는 (예를 들어, 타깃 네트워크 기술에 의해 허용된 "x" 와 같은 하나 이상의 문자들 또는 심볼들을 이용한) 결정론적인 방식으로 패딩될 수도 있다. 패딩 문자들은, NMPP 내의 문자들을 복제하는 것 및 또 다른 변환 동작을 이용한 단순한 문자 대체를 포함하여, NMPP 내의 문자들로부터 결정론적으로 유도된 문자들을 포함할 수도 있어서, NMPP 로부터 발생된 네트워크 패스워드가 타깃 네트워크 기술을 준수하도록 한다 (예를 들어, 결과적인 기술-특정 패스워드가 타깃 네트워크 기술에 의해 허용된 가장 짧은 길이로 되도록 한다).

[0042] NMPP 가 타깃 네트워크 기술에 의해 허용된 최대 개수의 패스워드 문자들보다 더 많은 문자들을 포함하면 (예를 들어, NMPP 가 너무 길면), 또 다른 변환 동작을 이용하여 NMPP 가 절단될 수도 있어서, NMPP 로부터 발생된 네트워크 패스워드가 타깃 네트워크 기술을 준수하도록 한다 (예를 들어, 결과적인 기술-특정 패스워드가 타깃 네트워크 기술에 의해 허용된 가장 긴 길이로 되도록 한다). 다른 실시형태들에 대해, 타깃 네트워크 기술에 의해 허용된 가장 긴 길이를 초과하는 다수의 NMPP 문자들이, 다르게는 절단되지 않은 NMPP 문자들과 조합되어, NMPP 의 모든 문자들로부터 (예를 들어, 타깃 네트워크 기술에 의해 허용된 가장 긴 길이를 갖는) 새로운 패스워드를 유도하도록 할 수도 있다. 따라서, 이러한 다른 실시형태들에 대해, NMPP 의 부분을 절단하기보다는, 적합한 문자 조합 또는 인코딩 알고리즘을 이용하여 NMPP 의 문자들의 하나 이상의 그룹들이 조합되어, 타깃 네트워크 기술에 의해 허용된 대응하는 개수의 단일 문자들 또는 심볼들을 생성하도록 한다.

[0043] 네트워크 패스워드들을 발생시키기 위해 NMPP 에 대해 수행된 변환 동작(들) 과 관계없이, 결과적인 기술-특정 네트워크 패스워드들이 대응하는 타깃 네트워크 기술들과 연관된 패스워드 요건들에 따르는 것, 및 네트워크 패스워드들이 결정론적인 방식으로 발생되어, 비교적 단순한 변환 동작들 (예를 들어, 문자 대체, 패딩, 절단, 및 인코딩) 중 특정한 것을 이용하여 주어진 NMPP 를 변환하는 것이, 디바이스가 NMPP 로부터 네트워크 패스워드(들) 를 유도하는 것에 상관없이, 동일한 패스워드를 생성하도록 하는 것은 중요하다.

[0044] 대안적인 실시형태들에 대해, 주어진 네트워크 기술에 대한 (예를 들어, 304 에서 비교적 단순한 변환 동작들을 이용한) 관련 NMPP 로부터의 네트워크 패스워드의 유도는, 주어진 네트워크 기술을 이용하는 제 2 디바이스를 대신하여, 주어진 네트워크 기술을 이용할 수도 있거나 이용하지 않을 수도 있는 제 1 디바이스에 의해 수행될 수도 있다. 이들 대안적인 실시형태들은, 제 2 디바이스가 본 실시형태들에 따라 NMPP 로부터 네트워크 패스워드의 유도를 구현하지 않는다는 상황들에 대해서 채용될 수도 있다. 이러한 대안적인 실시형태에서, 네트워크 패스워드는 제 1 디바이스의 UI 에 디스플레이될 수도 있어서, 사용자가 그 패스워드를 판독하게 하고 그 패스워드를 제 2 디바이스 상의 UI 에 입력하게 한다.

[0045] 본 실시형태들에 따라 비교적 단순한 변환 동작들을 이용하여 다양한 기술-특정 네트워크 패스워드들이 NMPP 로부터 유도되었다면, 네트워크 기술 타입에 응답하여, 그 유도된 네트워크 패스워드들에 대해 하나 이상의 비교

적 복잡한 변환 동작들이 수행되어 (308) 하나 이상의 네트워크 보안 키들을 발생시킬 수도 있다 (310). 일부 실시형태에 대해, 비교적 복잡한 변환 동작들이 선택적으로 네트워크 패스워드들을 해싱 또는 연결하여 네트워크 보안 키들을 유도할 수도 있고, 이 네트워크 보안 키들은 이어서 디바이스들을 인증하고 및/또는 이 디바이스들을 하이브리드 네트워크에 합류시키기 위해 이용될 수도 있다. 다른 실시형태들에 대해, 키들의 유도는, 적합한 변환 동작들과 함께 2개의 디바이스들 간의 메시지 교환들을 수반할 수도 있다. 예를 들어, 더 많은 보안을 달성하기 위해, 일시적인 키들의 유도는 2개의 디바이스들 간에서 기능적으로 분리될 수도 있고, 인증 메시지 교환들의 부산물로서 수행된다.

[0046] 더욱 상세하게는, HPAV 네트워크 패스워드 (NPW) 는 제 1 해싱 함수에 따라 해싱되어 HPAV 네트워크 멤버십 키 (NMK) 를 발생시킬 수도 있고 (310A), WLAN 네트워크 패스워드 (WLNP) 는 제 2 해싱 함수에 따라 해싱되어 WLAN 미리 공유된 비밀 키 (PSK) 를 발생시킬 수도 있으며 (310B), 다른 네트워크 패스워드 (NTTP) 는 제 3 해싱 함수에 따라 해싱되어 다른 네트워크 기술에 대한 미리 공유된 비밀 키 (NTPSK) 를 발생시킬 수도 있다 (310C). 일부 실시형태에 대해, 제 1, 제 2, 및 제 3 해싱 함수들이 상이할 수도 있지만, 다른 실시형태들에 대해서는, 제 1, 제 2, 및 제 3 해싱 함수들 중 하나 이상이 동일할 수도 있다.

[0047] 또한, 대안적인 실시형태들에 대해, 주어진 네트워크 기술에 대한 (예를 들어, 308 에서 비교적 복잡한 변환 동작을 이용한) 관련 네트워크 패스워드로부터의 네트워크 보안 키의 유도는, 주어진 네트워크 기술을 이용하는 또 다른 디바이스를 대신하여, 주어진 네트워크 기술을 이용하지 않는 디바이스에 의해 수행될 수도 있다. 이들 대안적인 실시형태들은, 다른 디바이스가, 사용자가 마스터 패스프레이즈들 또는 네트워크 패스워드들을 입력하게 하는 UI 를 갖고 있지 않은 상황들에 대해서 채용될 수도 있다.

[0048] 결과적인 기술-특정 네트워크 보안 키들이 그 후에 이용되어, 디바이스들 간의 보안 링크들을 인증하고, 네트워크를 형성하고, 및/또는 디바이스들을 하이브리드 네트워크에 부가하도록 할 수도 있다.

[0049] 도 4 는 일부 실시형태에 따른, 단일 디바이스 마스터 패스프레이즈 (DMPP) 로부터 복수의 상이한 기술-특정 디바이스 패스워드들 및 키들을 생성하기 위한 일 예시적인 동작을 나타낸 일 예시적인 플로차트 (400) 이다. 우선, 사용자는 하이브리드 네트워크와 연관된 하나 이상의 디바이스들에 DMPP 를 입력한다 (402). DMPP 는, 더욱 상세히 설명되는 바와 같이, HPAV 디바이스 패스워드 (DPW) 및 Wi-Fi 디바이스 패스워드 (WLDP) 의 슈퍼세트일 수도 있다는 것에 주목한다.

[0050] 그 후에, DMPP 가 입력되었고 및/또는 이전에 저장된 디바이스들에서 비교적 단순한 변환 동작들의 하나 이상의 타입이 수행된다 (404). 일부 실시형태에 대해, 이들 비교적 단순한 변환 동작들이 디바이스의 인터페이스들의 다양한 네트워크 기술 타입에 응답하여 선택적으로 수행되어 하나 이상의 기술-특정 디바이스 패스워드들을 발생시킬 수도 있다 (406). 일부 실시형태에 대해, 비교적 단순한 변환 동작들이 선택적으로 DMPP 의 문자들을 절단하고, DMPP 를 패딩하고 (예를 들어, DMPP 에 문자들을 부가하고), DMPP 의 문자들을 대체하고, 및/또는 DMPP 의 문자들의 세트들을 인코딩하여 다양한 기술-특정 디바이스 패스워드들을 발생시키도록 할 수도 있다 (406). 예를 들어, DMPP 에 대해 제 1 변환 동작이 수행되어 HPAV 디바이스 패스워드 (DPW) 를 발생시킬 수도 있고 (406A), DMPP 에 대해 제 2 변환 동작이 수행되어 WLAN 디바이스 패스워드 (WLDP) 를 발생시킬 수도 있고 (406B), 및/또는 DMPP 에 대해 제 3 변환 동작이 수행되어 다른 네트워크 기술들에 대한 디바이스 패스워드들 (NTDP) 을 발생시킬 수도 있다 (406C).

[0051] 상기 언급된 바와 같이, 패스워드들 및 보안 키들의 상세들 (예를 들어, 수용가능한 길이들, 포맷들, 및/또는 유효 문자 세트들) 은 통상적으로 상이한 네트워크 기술들 간에서 변한다. 예를 들어, 하나의 네트워크 기술 (예를 들어, HPAV) 은 임의의 프린트가능한 ASCII 문자의 (임의의 프린트가능한 ASCII 문자를 포함하는) 8개와 64개의 인스턴스들 사이를 갖는 패스워드들을 허용할 수도 있는 한편, 또 다른 네트워크 기술 (예를 들어, Wi-Fi) 은 단지 알파뉴메릭 문자들의 (알파뉴메릭 문자들을 포함하는) 4개와 20개의 인스턴스들 사이를 갖는 패스워드들을 허용할 수도 있다. 따라서, 본 실시형태들에 따르면, 타깃 네트워크 기술이 그의 패스워드들이 논-알파뉴메릭 문자들 (예를 들어, 스페이스, 탭, 구두점 등) 을 포함하게 하지 않으면, 이러한 논-알파뉴메릭 문자들을 포함하는 디바이스 마스터 패스프레이즈 (DMPP) 가, 이러한 논-알파뉴메릭 문자들을 미리 결정된 알파뉴메릭 문자들 및/또는 미리 결정된 문자들의 시퀀스들로 대체하는 변환 동작을 이용하여 변환될 수도 있어서, DMPP 로부터 발생된 기술-특정 패스워드가 타깃 네트워크 기술을 준수하도록 한다 (예를 들어, 결과적인 네트워크 기술-특정 패스워드가 단지 타깃 네트워크 기술에 의해 허용된 문자들 및/또는 심볼들을 포함하도록 한다). 역으로, DMPP 가 타깃 네트워크 기술에 의해 허용되지 않는 어떠한 문자들도 포함하고 있지 않으면, DMPP 로부터 디바이스 패스워드를 발생시킬 때 DMPP 의 임의의 문자들을 대체시키기 위해 기술-특정 패스워드를 발생시

키도록 채용된 변환이 필요하지 않을 수도 있다.

[0052] DMPP 가 타깃 네트워크 기술에 의해 허용된 최소 개수의 패스워드 문자들보다 더 적은 문자들을 포함하면 (예를 들어, DMPP 가 너무 짧으면), DMPP 는 (예를 들어, 타깃 네트워크 기술에 의해 허용된 "x" 와 같은 하나 이상의 문자들 또는 심볼들을 이용한) 결정론적인 방식으로 패딩될 수도 있다. 패딩 문자들은, DMPP 내의 문자들을 복제하는 것 및 또 다른 변환 동작을 이용한 단순한 문자 대체를 포함하여, DMPP 내의 문자들로부터 결정론적으로 유도된 문자들을 포함할 수도 있어서, DMPP 로부터 발생된 디바이스 패스워드가 타깃 네트워크 기술을 준수하도록 한다 (예를 들어, 결과적인 기술-특정 디바이스 패스워드가 타깃 네트워크 기술에 의해 허용된 가장 짧은 길이로 되도록 한다).

[0053] DMPP 가 타깃 네트워크 기술에 의해 허용된 최대 개수의 패스워드 문자들보다 더 많은 문자들을 포함하면 (예를 들어, DMPP 가 너무 길면), 또 다른 변환 동작을 이용하여 DMPP 가 절단될 수도 있어서, DMPP 로부터 발생된 디바이스 패스워드가 타깃 네트워크 기술을 준수하도록 한다 (예를 들어, 결과적인 기술-특정 디바이스 패스워드가 타깃 네트워크 기술에 의해 허용된 가장 긴 길이로 되도록 한다). 다른 실시형태들에 대해, 타깃 네트워크 기술에 의해 허용된 가장 긴 길이를 초과하는 다수의 DMPP 문자들이, 다르게는 절단되지 않은 DMPP 문자들과 조합되어, DMPP 의 모든 문자들로부터 (예를 들어, 타깃 네트워크 기술에 의해 허용된 가장 긴 길이를 갖는) 새로운 패스워드를 유도하도록 할 수도 있다. 따라서, 이러한 다른 실시형태들에 대해, DMPP 의 부분을 절단하기보다는, 적합한 문자 조합 또는 인코딩 알고리즘을 이용하여 DMPP 의 문자들의 하나 이상의 그룹들이 조합되어, 타깃 네트워크 기술에 의해 허용된 대응하는 개수의 단일 문자들 또는 심볼들을 생성하도록 한다.

[0054] 디바이스 패스워드들을 발생시키기 위해 DMPP 에 대해 수행된 변환 동작(들) 과 관계없이, 결과적인 기술-특정 디바이스 패스워드들이 대응하는 타깃 네트워크 기술들과 연관된 패스워드 요건들에 따르는 것, 및 디바이스 패스워드들이 결정론적인 방식으로 발생되어, 비교적 단순한 변환 동작들 (예를 들어, 문자 대체, 패딩, 절단, 및 인코딩) 중 특정한 것을 이용하여 주어진 DMPP 를 변환하는 것이, 디바이스가 DMPP 로부터 디바이스 패스워드(들) 를 유도하는 것에 상관없이, 동일한 패스워드를 생성하도록 하는 것은 중요하다.

[0055] 대안적인 실시형태들에 대해, 주어진 네트워크 기술에 대한 (예를 들어, 404 에서 비교적 단순한 변환 동작들을 이용한) 관련 DMPP 로부터의 디바이스 패스워드의 유도는, 주어진 네트워크 기술을 이용하는 제 2 디바이스를 대신하여, 주어진 네트워크 기술을 이용할 수도 있거나 이용하지 않을 수도 있는 제 1 디바이스에 의해 수행될 수도 있다. 이들 대안적인 실시형태들은, 제 2 디바이스가 본 발명에 따라 DMPP 로부터 디바이스 패스워드의 유도를 구현하지 않는다는 상황들에 대해서 채용될 수도 있다. 이러한 대안적인 실시형태에서, 디바이스 패스워드는 제 1 디바이스의 UI 에 디스플레이될 수도 있어서, 사용자가 그 패스워드를 판독하게 하고 그 패스워드를 제 2 디바이스 상의 UI 에 입력하게 한다.

[0056] 본 실시형태들에 따라 비교적 단순한 변환 동작들을 이용하여 다양한 기술-특정 디바이스 패스워드들이 DMPP 로부터 유도되었다면, 네트워크 기술 타입에 응답하여, 디바이스 패스워드들에 대해 하나 이상의 비교적 복잡한 변환 동작들이 수행되어 (408) 하나 이상의 디바이스 보안 키들을 발생시킬 수도 있다 (410). 일부 실시형태에 대해, 비교적 복잡한 변환 동작들이 선택적으로 디바이스 패스워드들을 해싱 또는 연결하여 디바이스 보안 키들을 유도할 수도 있고, 이 디바이스 보안 키들은 이어서 디바이스들을 인증하고 및/또는 이 디바이스들을 하이브리드 네트워크에 합류시키기 위해 이용될 수도 있다. 예를 들어, PLC 서브-네트워크들에 대해, 합류 디바이스에 송신하기 위한 네트워크 멤버십 키 (NMK) 를 암호화하기 위해 네트워크의 멤버 디바이스에 의해 합류 디바이스의 DAK 가 이용될 수도 있고, 이 합류 디바이스는 이어서 DAK 를 이용하여 NMK 를 암호해독한 후에 NMK 를 이용하여 네트워크에 합류할 수도 있다.

[0057] 더욱 상세하게는, HPAV 디바이스 패스워드 (DPW) 는 제 1 해싱 함수에 따라 해싱되어 HPAV 디바이스 액세스 키 (DAK) 를 발생시킬 수도 있고 (410A), WLAN 디바이스 패스워드 (WLDP) 는 제 2 해싱 함수에 따라 해싱되어 WLAN 디바이스 키 (WLDK) 를 발생시킬 수도 있으며 (410C), 다른 디바이스 패스워드 (NTDP) 는 제 3 해싱 함수에 따라 해싱되어 다른 네트워크 기술에 대한 디바이스 키 (NTDK) 를 발생시킬 수도 있다 (410D). 일부 실시형태에 대해, 제 1, 제 2, 및 제 3 해싱 함수들이 상이할 수도 있지만, 다른 실시형태들에 대해서는, 제 1, 제 2, 및 제 3 해싱 함수들 중 하나 이상이 동일할 수도 있다.

[0058] 또한, 대안적인 실시형태들에 대해, 주어진 네트워크 기술에 대한 (예를 들어, 408 에서 비교적 복잡한 변환 동작을 이용한) 관련 디바이스 패스워드로부터의 디바이스 보안 키의 유도는, 주어진 네트워크 기술을 이용하는 또 다른 디바이스를 대신하여, 주어진 네트워크 기술을 이용하지 않는 디바이스에 의해 수행될 수도 있다. 이들 대안적인 실시형태들은, 다른 디바이스가, 사용자가 마스터 패스프레이즈들 또는 디바이스 패스워드들을

입력하게 하는 UI 를 갖고 있지 않은 상황들에 대해서 채용될 수도 있다.

[0059] 또한, 네트워크 기술 타입에 응답하여, 하나 이상의 복잡한 변환 및/또는 보안 메시지 교환 동작들을 이용하여 결과적인 기술-특정 디바이스 키들이 변환되어 (412) 일시적인 디바이스 키들을 발생시킬 수도 있다 (414). 예를 들어, HPAV DAK 가 변환 (예를 들어, 해싱) 되어 HPAV 일시적 디바이스 액세스 키 (temporary device access key; TDAK) 를 유도할 수도 있고 (414A), WLAN 디바이스 키가 변환 (예를 들어, 해싱) 되어 WLAN 일시적 디바이스 액세스 키 (WLAN temporary device key; WTDK) 를 유도할 수도 있다 (414B). 더욱 상세하게는, 일부 실시형태에 대해, 키들의 유도는, 적합한 변환 동작들과 함께 2개의 디바이스들 간의 메시지 교환들을 수반할 수도 있다. 예를 들어, 더 많은 보안을 달성하기 위해, 일시적인 키들의 유도는 2개의 디바이스들 간에서 기능적으로 분리될 수도 있고, (예를 들어, 802.11 RSNA 데이터 신뢰성 프로토콜들에 기재된 "4-웨이 핸드셰이크 (4-Way Handshake)" 에 따라) 인증 메시지 교환들의 부산물로서 수행된다.

[0060] 도 5 내지 도 8 과 관련하여 아래의 본 실시형태들의 특정 예들을 설명하기 전에, 사용자가 마스터 패스프레이즈 (예를 들어, NMPP 또는 DMPP 중 어느 하나) 를 생성하고 마스터 패스프레이즈를 UI 를 갖는 디바이스들에 입력할 때, 디바이스들은 마스터 패스프레이즈로부터 기술-특정 패스워드들을 유도하는 변환 동작들을 수행하기 위해 미리 결정된 합의 및/또는 표준을 가질 수도 있다는 것에 주목한다. 예를 들어, 사용자가 랩톱을 이용하여 네트워크를 생성하면, 사용자는 DAK 기법들을 이용함으로써 UI 를 갖지 않는 선택된 디바이스에 합류할 수도 있다. 더욱 상세하게는, 이 예에 대해, 사용자는 선택된 디바이스의 DAK 를 랩톱에 입력할 수도 있어서, 랩톱 및 선택된 디바이스가, 그들 사이에 보안 링크를 확립하는데 이용될 수도 있는 공통 비밀 키를 갖도록 한다. 그 후에, 랩톱은 마스터 패스프레이즈를 암호화하고 그 암호화된 마스터 패스프레이즈를 보안 링크를 통해 선택된 디바이스와 공유할 수도 있다. 그 후에, 선택된 디바이스는 그의 DAK 를 이용하여 암호화된 마스터 패스프레이즈를 암호해독한 후에, 마스터 패스프레이즈에 대한 변환 동작들을 수행하여 선택된 디바이스를 네트워크에 합류하기 위한 패스워드들 및 키들을 발생시킬 수도 있다.

[0061] 또한, 사용자가, Wi-Fi 디바이스를, 이미 HPAV 패스워드들 및 키들을 갖고 있는 기존의 HPAV 네트워크에 합류하기를 원하는 상황들에 대해 (예를 들어, 그에 의해 HPAV 네트워크를 변경하여 하이브리드 네트워크를 생성), PLC 디바이스들 중 선택된 PLC 디바이스가 HPAV 네트워크 패스워드 (NPW) 에 대한 역변환 동작을 수행하여, (예를 들어, 또 다른 변환 동작을 이용하여) 후속하여 변환되어 WLAN 패스워드 요건들을 준수하는 WLAN 패스워드 (WLNP) 를 생성할 수도 있는 적합한 NMPP 를 유도할 수도 있다. 이러한 실시형태들에 대해, 선택된 PLC 디바이스는 역변환된 NMPP 를 사용자에게 디스플레이할 수도 있고, 또한 (예를 들어, 사용자가 결과적인 WLAN 패스워드를 Wi-Fi 디바이스에 입력하여 네트워크에의 자신의 인증을 용이하게 할 수도 있도록) 결과적인 WLAN 패스워드를 사용자에게 디스플레이할 수도 있다.

[0062] 본 실시형태들에 따른 마스터 패스프레이즈들을 이용한 다양한 예시적인 셋업 동작들은 도 5 내지 도 8 과 관련하여 후술되고, 여기서 거리는 수평 방향으로 나타내고 시간은 수직 방향으로 나타낸다 (하측 방향으로 시간이 증가함).

[0063] 도 5 는 PLC 네트워크 인터페이스를 각각 갖는 2개의 PLC 디바이스들 (PL2 및 PL3), Wi-Fi 네트워크 인터페이스를 갖는 Wi-Fi 디바이스 (WL2), 및 PLC 및 Wi-Fi 네트워크 인터페이스들 양쪽을 갖는 하이브리드 PLC/Wi-Fi 디바이스 (PL1/WL1) 를 포함하여 하이브리드 네트워크 (500) 를 형성하는 것과 연관된 메시지 교환들을 예시한 순서도이다. 네트워크 (500) 의 형성 이후에, PLC 디바이스 인터페이스들 (PL1 내지 PL3) 이 PLC 서브-네트워크 (501) 를 통해 서로 통신할 수도 있고 Wi-Fi 디바이스들 (WL1 및 WL2) 이 Wi-Fi 서브-네트워크 (단순화를 위해 미도시) 를 통해 서로 통신할 수도 있다는 것에 주목한다. 네트워크 (500) 의 형성 이후에, 하이브리드 PLC/Wi-Fi 디바이스 (PL1/WL1) 가 PLC 서브-네트워크와 Wi-Fi 서브-네트워크 사이의 프레임들을 포워딩하는 것이 가능하면, 네트워크 (500) 내의 모든 디바이스들이 서로 통신할 수 있다. 도 5 의 예에 대해, PLC 디바이스들 (PL2 및 PL3) 이 우선, 사용자-입력된 네트워크 마스터 패스프레이즈 (NMPP) 를 이용한 상호 인증, 그에 후속하여 PLC 디바이스 (PL3) 에 입력된 디바이스 마스터 패스워드를 이용한 하이브리드 디바이스 (PL1/WL1) 의 인증을 통해 네트워크를 형성한다. 인증 동작 동안, 하이브리드 디바이스 (PL1/WL1) 는 PLC 디바이스 (PL3) 디바이스로부터 NMPP 를 획득한 후에, NMPP 를 이용하여 Wi-Fi 디바이스 (WL2) 를 인증한다.

[0064] 더욱 상세하게는, 사용자는 우선, NMPP 를 PLC 디바이스들 (PL2 및 PL3) 에 입력하고, 이 PLC 디바이스들 (PL2 및 PL3) 은 이어서 NMPP 를 변환하여 NMK 를 유도한다. PLC 디바이스들 (PL2 및 PL3) 양쪽이 NMPP 로부터 NMK 를 유도하였다면, 디바이스들 (PL2 및 PL3) 은 PLC 서브-네트워크를 형성하고 서로의 인증을 인가할 수 있다. 디바이스들 (PL2 및 PL3) 이 PLC 서브-네트워크를 형성한 후에, 사용자는 하이브리드 디바이스

(PL1/WL1) 의 디바이스 마스터 패스프레이즈 (DMPP) 를 디바이스 (PL3) 에 입력한다. 이에 응답하여, 디바이스 (PL3) 는 (예를 들어, 적합한 해싱 기법들을 이용하여) DMPP 로부터 하이브리드 디바이스 (PL1/WL1) 의 인터페이스 (PL1) 의 DAK 를 유도한다. 그 후에, 하이브리드 디바이스 (PL1/WL1) 의 인터페이스 (PL1) 에 대한 유도된 DAK 가 이용되어 하이브리드 디바이스 (PL1/WL1) 의 PLC 인터페이스 (PL1) 를 인가 및 인증하도록 할 수도 있다.

[0065] 예를 들어, 디바이스 (PL3) 는 하이브리드 디바이스 (PL1/WL1) 의 인터페이스 (PL1) 의 DAK 를 이용하여 NMK 를 암호화하고 그 NMK 를 하이브리드 디바이스 (PL1/WL1) 에 송신하도록 할 수 있다. 그 후에, 하이브리드 디바이스 (PL1/WL1) 의 인터페이스 (PL1) 는 그의 미리 저장된 DAK 를 이용하여 NMK 를 암호해독한 후에, 그 암호해독된 NMK 를 이용하여 PLC 서브-네트워크 (501) 에 합류한다.

[0066] 하이브리드 디바이스 (PL1/WL1) 의 인터페이스 (PL1) 가 PLC 서브-네트워크에 합류하였으면, 디바이스 (PL3) 는 지금 확립된 PLC 서브-네트워크 (501) 를 통해 NMPP 를 하이브리드 디바이스 (PL1/WL1) 에 전달하고, 하이브리드 디바이스 (PL1/WL1) 의 인터페이스 (PL1) 의 상위 소프트웨어 계층 (upper software layer; USL) 은 NMPP 를 하이브리드 디바이스 (PL1/WL1) 의 WLAN 인터페이스 (WL1) 에 전달한다. 그 후에, 하이브리드 디바이스 (PL1/WL1) 의 인터페이스 (WL1) 는 NMPP 를 이용하여 WLAN PSK 를 유도할 수 있다. PLC 디바이스 (PL3) 로부터 하이브리드 디바이스 (PL1/WL1) 로의 NMPP 의 전달은, 사용자가 NMPP 를 하이브리드 디바이스 (PL1/WL1) 의 Wi-Fi 인터페이스 (WL1) 에 직접 입력한 경우와 동일한 목적을 만족시키지만, 유리하게는 사용자가 NMPP 를 하이브리드 디바이스 (PL1/WL1) 에 수동으로 입력할 필요는 없다는 것에 주목한다. 다른 실시형태들에 대해, 2개의 디바이스들 간의 보안 링크가 확립된 후에, NMPP 가 암호화된 메시지로 하이브리드 디바이스 (PL1/WL1) (또는 또 다른 디바이스) 에 전달될 수도 있다.

[0067] 다음에, 사용자는 NMPP 를 Wi-Fi 디바이스 (WL2) 에 입력하고, 이 Wi-Fi 디바이스 (WL2) 는 이어서 NMPP 로부터 WLAN PSK 를 유도한다. 동일한 NMPP 가 Wi-Fi 디바이스들 (WL1 및 WL2) 양쪽에 제공 또는 입력되었기 때문에, 이들 양쪽은 동일한 PSK 를 유도하여서, 예를 들어, RSNA (Robust Security Network Association) 인증 기법들에 따라 PSK 를 이용하여 WLAN 서브-네트워크를 확립할 수 있다.

[0068] 도 6 은 PLC 네트워크 인터페이스를 갖는 PLC 디바이스 (PL2), Wi-Fi 네트워크 인터페이스를 각각 갖는 2개의 Wi-Fi 디바이스들 (WL2 및 WL3), 및 PLC 및 Wi-Fi 네트워크 인터페이스들 양쪽을 갖는 하이브리드 PLC/Wi-Fi 디바이스 (PL1/WL1) 를 포함하여 하이브리드 네트워크 (600) 를 형성하는 것과 연관된 메시지 교환들을 예시한 순서도이다. 네트워크 (600) 의 형성 이후에, PLC 디바이스 인터페이스들 (PL1 및 PL2) 이 PLC 서브-네트워크 (601) 를 통해 서로 통신할 수도 있고 Wi-Fi 디바이스들 (WL1 내지 WL3) 이 Wi-Fi 서브-네트워크 (단순화를 위해 미도시) 를 통해 서로 통신할 수도 있다는 것에 주목한다. 네트워크 (600) 의 형성 이후에, 하이브리드 PLC/Wi-Fi 디바이스 (PL1/WL1) 가 PLC 서브-네트워크와 Wi-Fi 서브-네트워크 사이의 프레임들을 포워딩하는 것이 가능하면, 네트워크 (600) 내의 모든 디바이스들이 서로 통신할 수 있다. 도 6 의 예에 대해, 네트워크 마스터 패스프레이즈 (NMPP) 및 "단순한 접속" 푸시버튼 셋업 동작들의 조합이 이용되어 하이브리드 네트워크에 대한 디바이스들을 인증함으로써, Wi-Fi 디바이스들 (WL2 및 WL3) 이 NMPP 을 이용하여 서로 인증하고, 단순한 접속 셋업 동작이 이용되어 Wi-Fi 디바이스 (WL3) 를 하이브리드 디바이스 (PL1/WL1) 의 Wi-Fi 인터페이스 (WL1) 에 접속한 후에 NMPP 를 하이브리드 디바이스 (PL1/WL1) 에 전달한다. 그 후에, 하이브리드 디바이스 (PL1/WL1) 는 본 실시형태들에 따라 NMPP 로부터 유도된 공통 NMK 를 이용하여 PLC 디바이스 (PL2) 에 의한 PLC 서브-네트워크를 형성한다.

[0069] 더욱 상세하게는, 사용자는 우선, NMPP 를 Wi-Fi 디바이스들 (WL2 및 WL3) 에 입력하고, 이 Wi-Fi 디바이스들 (WL2 및 WL3) 은 이어서 NMPP 를 변환하여 WLAN 네트워크 패스워드 및 그 후에 PSK 를 유도한다. Wi-Fi 디바이스들 (WL2 및 WL3) 양쪽이 NMPP 로부터 PSK 를 유도하였다면, 디바이스들 (WL2 및 WL3) 은 RSNA 기법들을 이용하여 서로 인증하여 WLAN 서브-네트워크를 형성한다. 그 후에, 사용자는 Wi-Fi 디바이스 (WL3) 및 하이브리드 디바이스 (PL1/WL1) 에 대한 푸시버튼들을 활성화하는데, 이는 Wi-Fi 디바이스 (WL3) 가 부가 상태에 진입하게 하고 하이브리드 디바이스 (PL1/WL1) 의 Wi-Fi 인터페이스가 합류 상태에 진입하게 한다. Wi-Fi 디바이스들 (WL3 및 WL1) 은 Wi-Fi 버튼 프레스 단순 접속 프로토콜을 완료하여 하이브리드 디바이스 (PL1/WL1) 의 Wi-Fi 인터페이스 (WL1) 를 Wi-Fi 서브-네트워크에 합류한 후에, Wi-Fi 디바이스 (WL3) 의 USL 이 NMPP 를 하이브리드 디바이스 (PL1/WL1) 의 Wi-Fi 인터페이스 (WL1) 에 송신한다. 하이브리드 디바이스 (PL1/WL1) 는 NMPP 를 그의 Wi-Fi 인터페이스 (WL1) 로부터 그의 PLC 인터페이스 (PL1) 로 전달하고, 이 PLC 인터페이스 (PL1) 는 그 후에 NMPP 를 변환하여 HPAV NMK 를 유도한다. 사용자는 그 후에 NMPP 를 PLC 디바이스 (PL2) 에 입력하고, 이 PLC 디바이스 (PL2) 는 이에 응답하여 본 실시형태들에 따른 변환 동작들을 이용하여 HPAV NMK

를 유도한다. 하이브리드 디바이스 (PL1/WL1) 의 PLC 인터페이스 (PL1) 및 PLC 디바이스 (PL2) 양쪽은 지금 동일한 NMK 를 갖고 있기 때문에, 이들은 서로 인증하고 PLC 서브-네트워크 (601) 를 형성하는 것이 가능하다.

[0070] 도 7 은 PLC 네트워크 인터페이스를 각각 갖는 2개의 PLC 디바이스들 (PL2 및 PL3) 을 하이브리드 네트워크 (700) 에 부가하는 것과 연관된 메시지 교환들을 예시한 순서도이다. 여기에 사용되는 바와 같이, 디바이스들을 네트워크에 "부가" 하는 것은 또한 디바이스들을 새로운 네트워크에 부가하는 (예를 들어, 그에 의해 새로운 네트워크를 "형성" 하는) 것을 지칭할 수도 있다는 것에 주목한다. 도 7 의 예에 대해, 하이브리드 디바이스 (PL1/WL1) 의 Wi-Fi 인터페이스 (WL1) 및 Wi-Fi 디바이스들 (WL2 및 WL3) 는 이미 WLAN 서브-네트워크의 멤버들이다. 네트워크 (700) 의 형성 이후에, PLC 디바이스 인터페이스들 (PL1 내지 PL3) 은 PLC 서브-네트워크 (701) 를 통해 서로 통신할 수도 있다는 것에 주목한다. 네트워크 (700) 의 형성 이후에, 하이브리드 PLC/Wi-Fi 디바이스 (PL1/WL1) 는 PLC 서브-네트워크와 Wi-Fi 서브-네트워크 사이의 프레임들을 포워딩하는 것이 가능하면, 네트워크 (700) 내의 모든 디바이스들은 서로 통신할 수 있다. PLC 디바이스 (PL2) 는 인증하는 디바이스로서 Wi-Fi 디바이스 (WL3) 를 이용하여 디바이스 마스터 패스프레이즈 (DMPP) 로 네트워크에 대해 인증된다. 하이브리드 디바이스 (PL1/WL1) 은 인증된 PL2 디바이스와 인증하는 WL3 디바이스 사이의 인증 메시지들을 릴레이한다. 도 7 의 예시적인 도면에 대해, Wi-Fi 디바이스 (WL3) 는 제 1 HPAV DAK 기반 프로토콜 (DAK-Based Protocol; DBP) 메시지 (DBP-M1) 를 하이브리드 디바이스 (PL1/WL1) 에 전달하고, 이 하이브리드 디바이스 (PL1/WL1) 는 이어서 DBP-M1 및 DAK2 를 PLC 디바이스들 (PL2 및 PL3) 에 전송한다는 것에 주목한다. 따라서, 여기에 사용되는 바와 같이, DBP-Mn 은 DAK 기반 프로토콜 메시지 (Mn) 를 지칭하고, 여기서 n 은 정수이다.

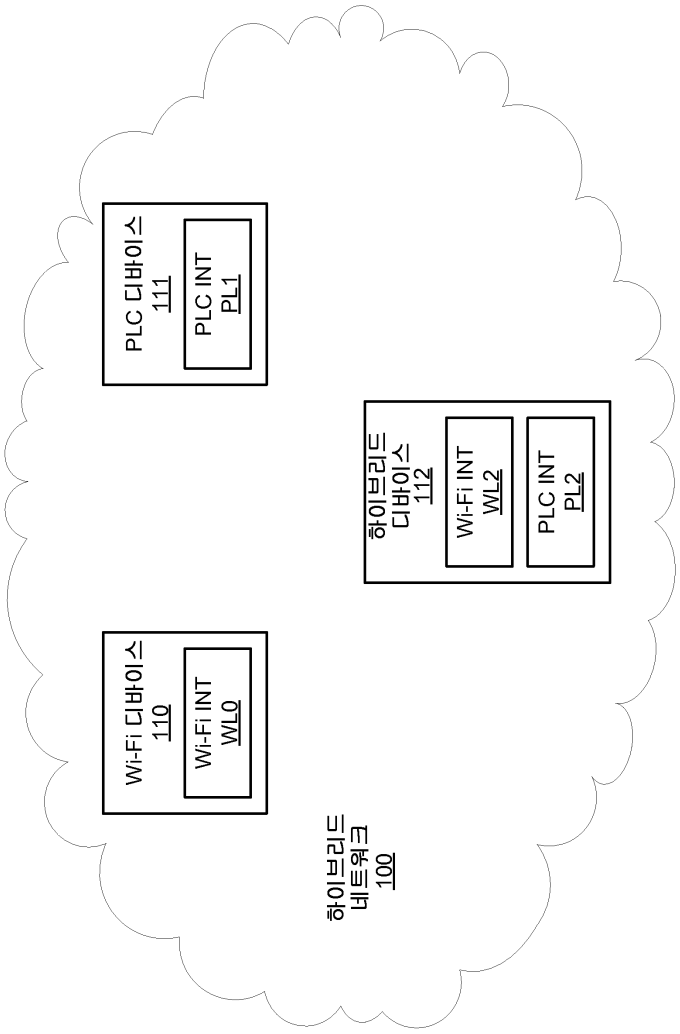
[0071] 도 8 은 또 다른 예시적인 실시형태 하에서 디바이스들을 부가하기 위한 인터페이스 디바이스들 간의 메시지 교환들을 예시한 순서도 (800) 이다. 이 실시형태에 대한 상황은 도 7 에 도시된 상황과 유사하고; PLC 디바이스 (PL2) 는, 하이브리드 디바이스 (PL1/WL1) 의 보조로, 인증하는 디바이스로서 Wi-Fi 디바이스 (WL3) 를 이용하여 디바이스 마스터 패스프레이즈로 네트워크에 대해 인증된다. 그러나, 인증 메커니즘의 상세들은 도 7 과 관련하여 상술된 것과는 상이하다. 더욱 상세하게는, 도 8 의 예에 대해, 일시적인 키들이 유도되고 디바이스 (PL1/WL1) 가 PLC 서브-네트워크 상의 디바이스 (WL3) 에 대한 프록시로서 기능하여 인증 프로토콜의 실행을 용이하게 한다.

[0072] 전술한 명세서에서, 본 실시형태들은 특정 예들을 참조하여 설명되었다. 그러나, 첨부된 특허청구범위에 제시된 본 개시물의 더 넓은 사상 및 범위로부터 벗어나는 일 없이 다양한 변경들 및 변화들이 이루어질 수도 있다는 것이 명백하다. 본 명세서 및 도면들은 이에 따라 제한된 의미보다는 예시적인 의미로 간주되어야 한다.

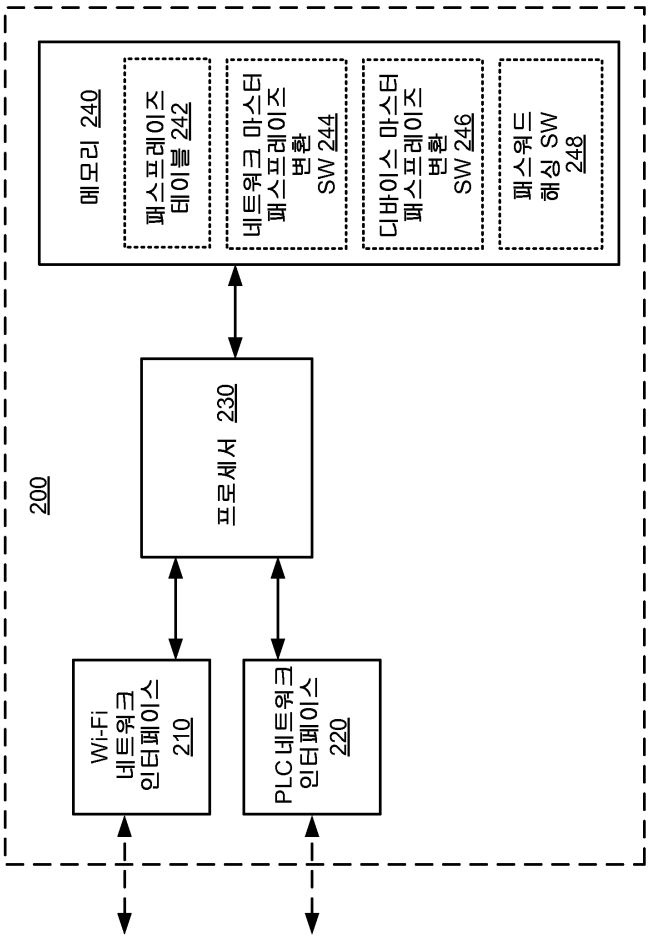
[0073] 본 실시형태들은, 명령들을 저장하고 있는 비일시적 머신 판독가능 매체를 포함할 수도 있는 컴퓨터 프로그램 제품 또는 소프트웨어로서 제공될 수 있다. 머신 판독가능 매체는 컴퓨터 시스템 (또는 다른 전자 디바이스들) 을 프로그래밍하여 본 실시형태들을 구현하는데 이용될 수도 있다. 머신 판독가능 매체는 플로피 디스켓들, 광 디스크들, CD-ROM들 및 광자기 디스크들, ROM들, RAM들, EPROM들, EEPROM들, 자석 또는 광 카드들, 플래시 메모리, 또는 전자 명령들을 저장하기에 적합한 다른 타입의 미디어/머신 판독가능 매체를 포함하지만, 이에 제한되지 않는다.

도면

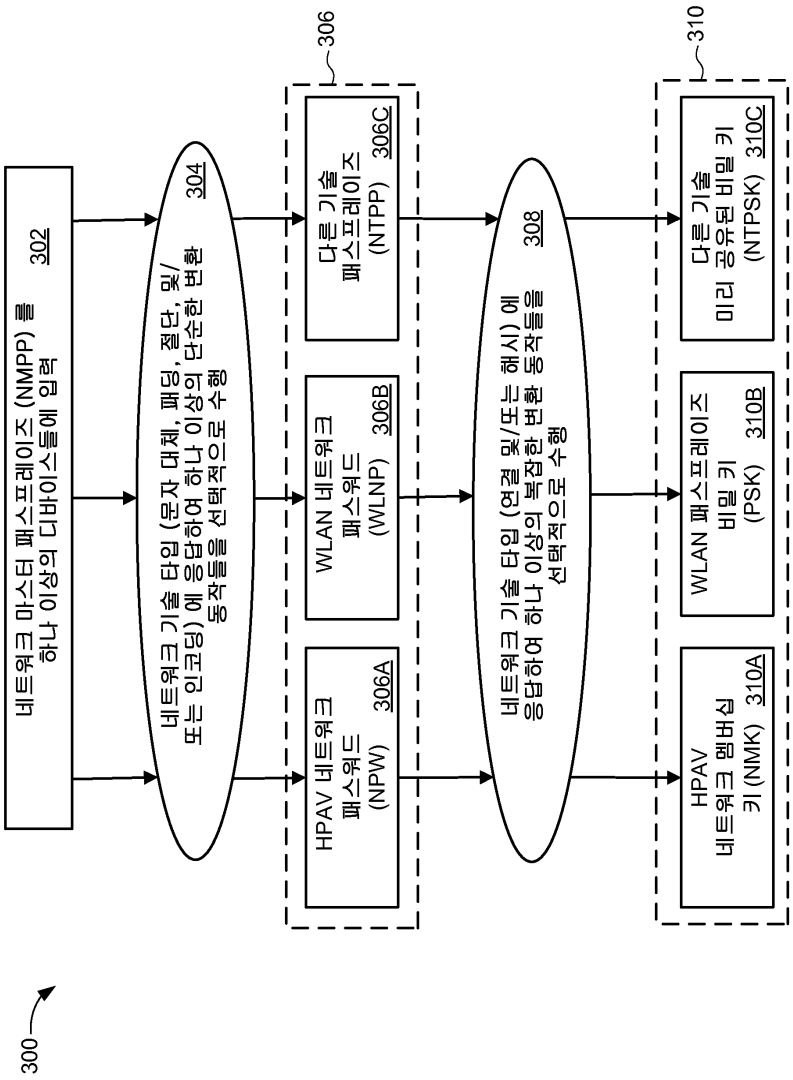
도면1


하이브리드
네트워크
100
Wi-Fi 디바이스
110
Wi-Fi INT
WL0
PLC 디바이스
111
PLC INT
PL1
하이브리드
디바이스
112
Wi-Fi INT
WL2
PLC INT
PL2

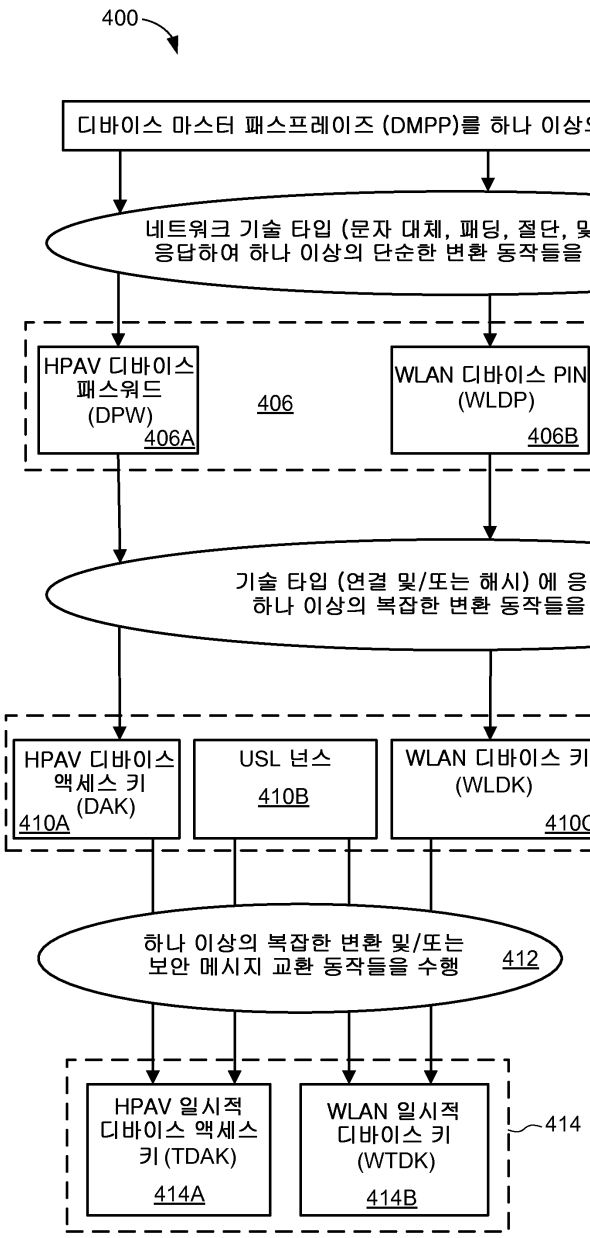
도면2


200
메모리 240
패스프레이즈 테이블 242
네트워크 마스터 패스프레이즈 변환 SW 244
디바이스 마스터 패스프레이즈 변환 SW 246
패스워드 해싱 SW 248
프로세서 230
Wi-Fi 네트워크 인터페이스 210
PLC 네트워크 인터페이스 220

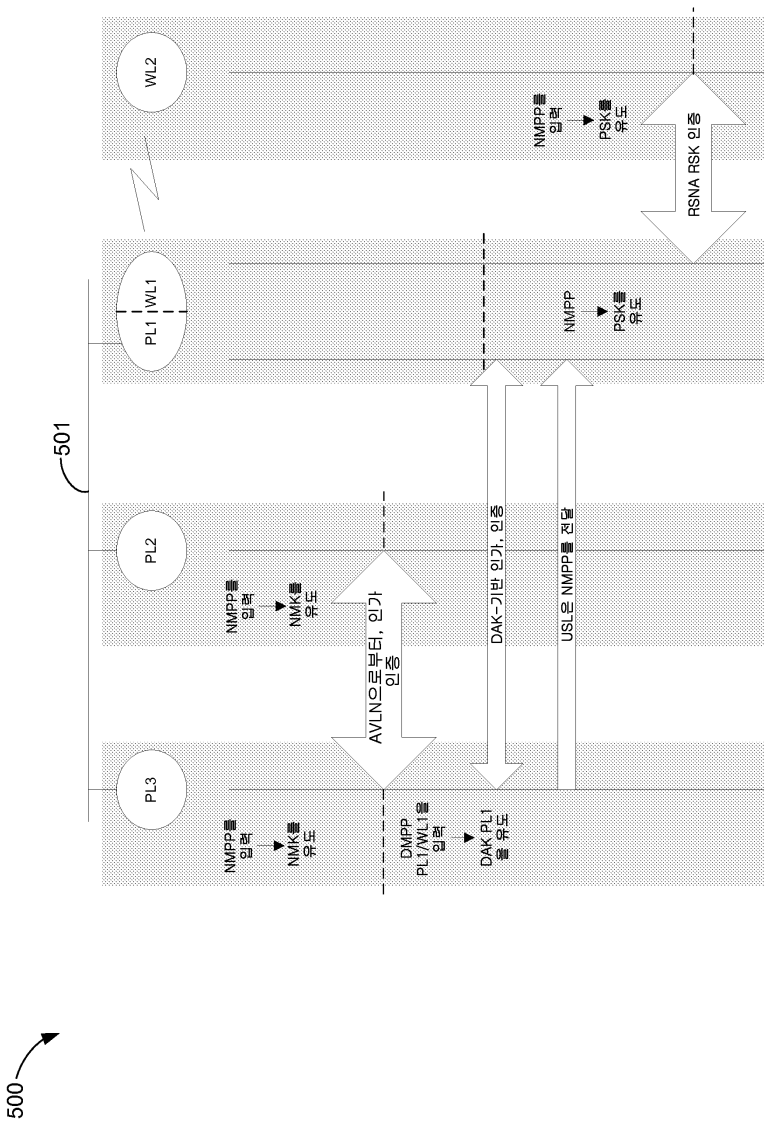
도면3


300
네트워크 마스터 패스프레이즈 (NMPP) 를 하나 이상의 디바이스들에 입력 302
네트워크 기술 타입 (문자 대체, 패딩, 절단, 및/또는 인코딩) 에 응답하여 하나 이상의 단순한 변환 동작들을 선택적으로 수행 304
306
HPAV 네트워크 패스워드 (NPW) 306A
WLAN 네트워크 패스워드 (WLNP) 306B
다른 기술 패스프레이즈 (NTPP) 306C
네트워크 기술 타입 (연결 및/또는 해시) 에 응답하여 하나 이상의 복잡한 변환 동작들을 선택적으로 수행 308
310
HPAV 네트워크 멤버십 키 (NMK) 310A
WLAN 패스프레이즈 비밀 키 (PSK) 310B
다른 기술 미리 공유된 비밀 키 (NTPSK) 310C

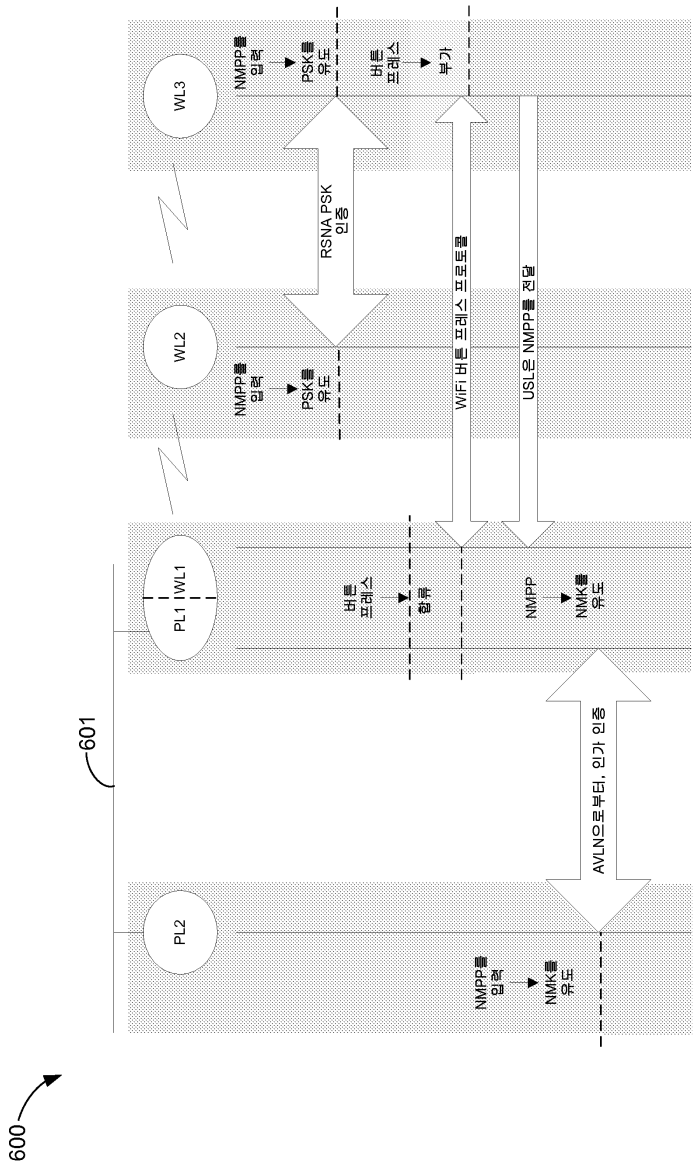
도면4


400
디바이스 마스터 패스프레이즈 (DMPP)를 하나 이상의 디바이스들에 입력 402
네트워크 기술 타입 (문자 대체, 패딩, 절단, 및/또는 인코딩) 에 응답하여 하나 이상의 단순한 변환 동작들을 선택적으로 수행 404
HPAV 디바이스 패스워드 (DPW) 406A
406
WLAN 디바이스 PIN (WLDP) 406B
다른 기술 디바이스 패스워드 (NTDP) 406C
기술 타입 (연결 및/또는 해시) 에 응답하여 하나 이상의 복잡한 변환 동작들을 수행 408
410
HPAV 디바이스 액세스 키 (DAK) 410A
USL 넌스 410B
WLAN 디바이스 키 (WLDK) 410C
다른 기술 디바이스 키 (NTDK) 410D
하나 이상의 복잡한 변환 및/또는 보안 메시지 교환 동작들을 수행 412
HPAV 일시적 디바이스 액세스 키 (TDAK) 414A
WLAN 일시적 디바이스 키 (WTDK) 414B
414

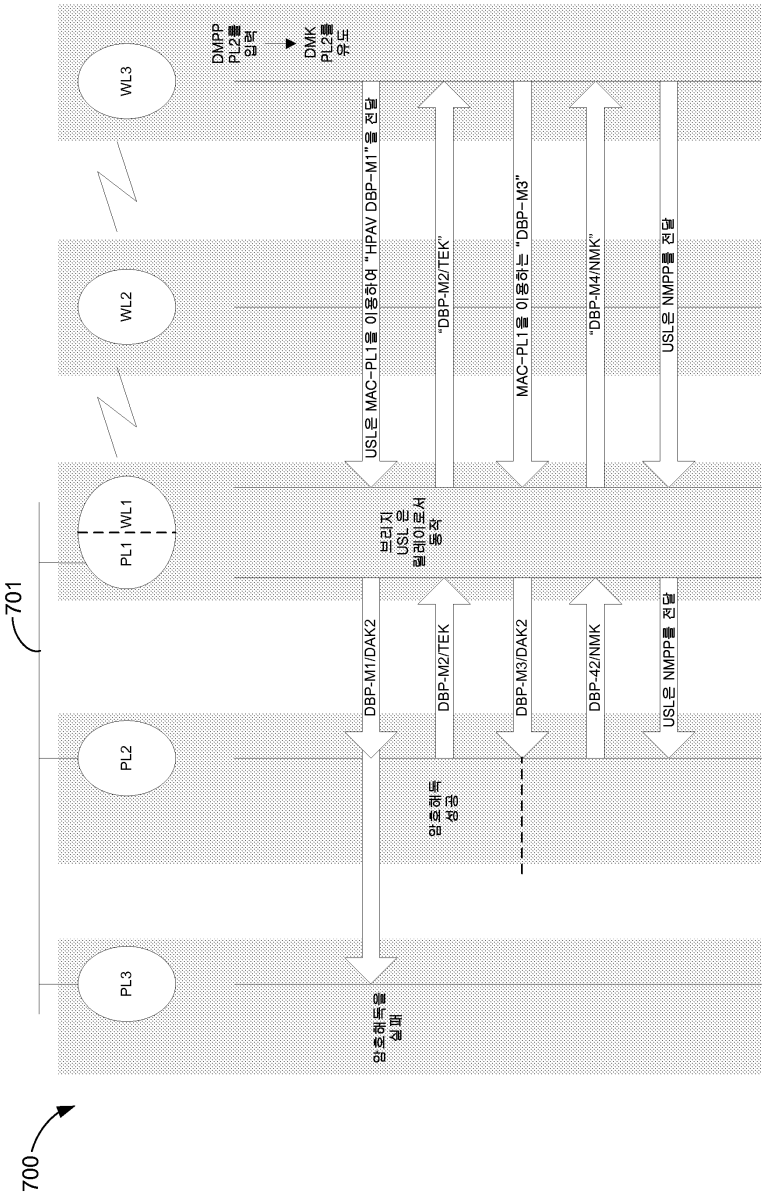
도면5


500
501
WL2
PL1 / WL1
PL2
PL3
NMPP를 입력
PSK를 유도
RSNA PSK 인증
NMPP
PSK를 유도
NMPP를 입력
NMK를 유도
AVLN으로부터, 인가
인증
DAK-기반 인가, 인증
USL은 NMPP를 전달
NMPP를 입력
NMK를 유도
DMPP PL1/WL1을 입력
DAK PL1을 유도

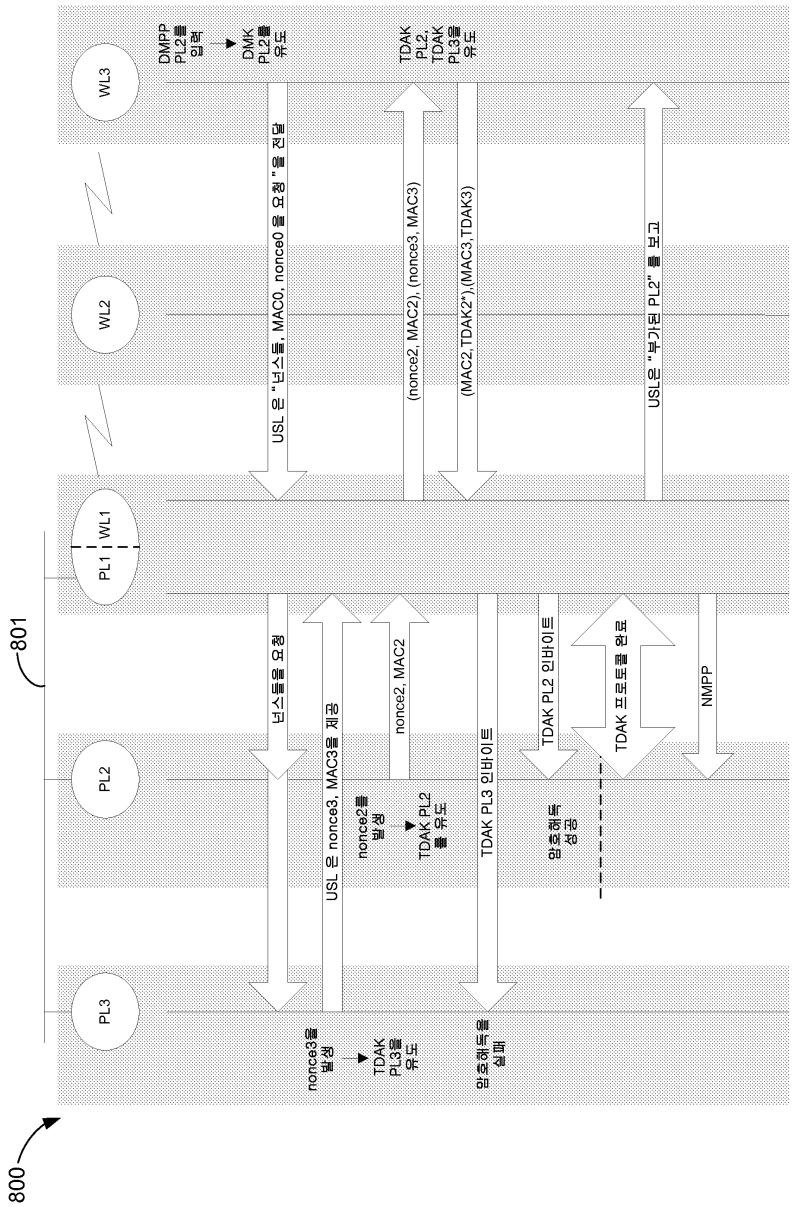
도면6


600
601
WL3
WL2
PL1 IWL1
PL2
NMPP를 입찰
PSK를 유도
버튼 프레스
부가
RSNA PSK 인증
WiFi 버튼 프레스 프로토콜
USL은 NMPP를 전달
버튼 프레스
협류
NMPP
NMK를 유도
AVLN으로부터, 인가 인증
NMPP를 입찰
NMK를 유도

도면7


700
701
WL3
WL2
WL1
PL3
PL2
PL1
DMPP PL2를 입력
DMK PL2를 유도
USL은 MAC-PL1을 이용하여 "HPAV DBP-M1"을 전달
"DBP-M2/TEK"
MAC-PL1을 이용하는 "DBP-M3"
"DBP-M4/NMK"
USL은 NMPP를 전달
브리지 USL을 릴레이로서 동작
DBP-M1/DAK2
DBP-M2/TEK
DBP-M3/DAK2
DBP-42/NMK
USL은 NMPP를 전달
암호해독 성공
암호해독을 실패

도면8


800
801
WL3
WL2
WL1
PL3
PL2
PL1
DMPP
PL2를
입력
DMK
PL2를
유도
USL 은 "넌스들, MAC0, nonce0 을 요청" 을 전달
TDAK
PL2,
TDAK
PL3을
유도
(nonce2, MAC2), (nonce3, MAC3)
(MAC2,TDAK2"),(MAC3,TDAK3)
USL은 "구축된 PL2" 를 통고
넌스들을 요청
USL 은 nonce3, MAC3을 제공
nonce2를
발생
TDAK PL2
를 유도
nonce2, MAC2
TDAK PL3 인바이트
TDAK PL2 인바이트
TDAK 프로토콜 완료
NMPP
암호해독
성공
nonce3를
발생
TDAK
PL3을
유도
암호해독을
실패