(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2009 년 8 월 6 일 (06.08.2009)

PCT

(10) 국제공개번호
WO 2009/096738 A2

(51) 국제특허분류:
H04L 9/08 (2006.01) *H04L 12/28* (2006.01)

(21) 국제출원번호: PCT/KR2009/000468

(22) 국제출원일: 2009 년 1 월 30 일 (30.01.2009)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
61/024,967 2008 년 1 월 31 일 (31.01.2008) US
10-2008-0069749 2008 년 7 월 17 일 (17.07.2008) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **삼성전자 주식회사 (SAMSUNG ELECTRONICS CO., LTD.)** [KR/KR]; 경기도 수원시 영통구 매탄동 416, 442-742 Gyeonggi do (KR).

(72) 발명자: **김형식 (KIM, Hyoung-Shick)**; 경기도 용인시 기흥구 농서동 산 14-1 삼성종합기술원, 446-712 Gyeonggi-do (KR). **이주열 (LEE, Joo-Yeol)**; 경기도 용인시 기흥구 농서동 산 14-1 삼성종합기술원, 446-712 Gyeonggi-do (KR).

(74) 대리인: **리앤목 특허법인 (Y.P.LEE, MOCK & PARTNERS)**; 서울특별시 서초구 서초동 1575-1 고려빌딩, 137-875 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

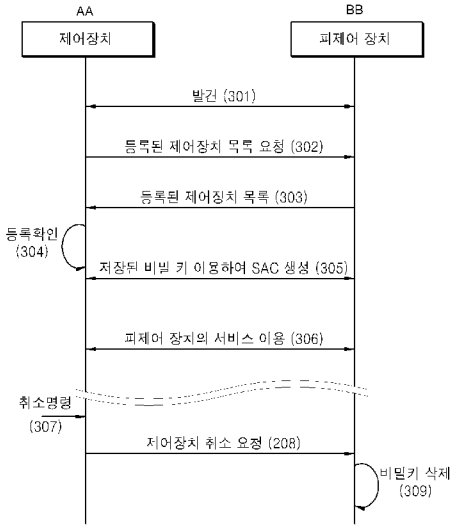
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) **Title**: METHOD FOR ENSURING COMMUNICATION SECURITY IN HOME NETWORK AND APPARATUS FOR SAME

(54) **발명의 명칭**: 홈 네트워크에서의 통신 보안성을 보장하는 방법 및 이를 위한 장치

도 3



AA ... Controller
BB ... Controlled device
301 ... Discover
302 ... Request registered controller list
303 ... Registered controller list
304 ... Confirm registration
305 ... Create SAC by using stored secret key
306 ... Use services of controlled device
307 ... Cancel command
208 ... Request controller cancel
309 ... Delete secret key

(57) **Abstract**: Since a home network is dynamically set up independently of an infrastructure by a central administration, there exists a need for implementing a key distribution scheme without assumption for a trusted third party. In a home network, a controller creates a registration SAC (Secure Authenticated Channel) through a controlled device and a TLS-PSK protocol by using a PIN of the controlled device input from a user, shares a secret key through said channel, and uses services of the controlled device through a service SAC created through a TLS-PSK protocol by using the shared secret key.

(57) **요약서**: 홈 네트워크는 중앙 통제(central administration)에 의한 인프라스트럭처에 의존하지 않고 동적으로 셋업되므로, 신뢰성 있는 제 3 자에 대한 가정 없이 키 분배 스킴을 구현할 필요가 있다. 홈 네트워크에서 제어 장치는 사용자로부터 입력받은 피제어 장치의 PIN 을 이용하여 피제어 장치와 TLS-PSK 프로토콜을 통해 등록 SAC(Secure Authenticated Channel) 을 생성하고, 이러한 채널을 통해 비밀 키를 공유하며, 공유된 비밀 키를 이용하여 TLS-PSK 프로토콜을 통해 생성된 서비스 SAC 을 통해 피제어 장치의 서비스를 이용한다

WO 2009/096738 A2

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

명세서
홈 네트워크에서의 통신 보안성을 보장하는 방법 및 이를 위한 장치

[1]

기술분야

[2] 본 발명은 홈 네트워크에 관한 것으로, 더욱 상세하게는 홈 네트워크에서 제어 장치와 피제어 장치 간의 통신에 있어서 보안성을 보장하기 위한 방법에 관한 것이다.

배경기술

[3] 홈 네트워크 기술이 발달함에 따라 다양한 종류의 홈 디바이스들이 디지털 정보에 액세스할 수 있게 되었고, 사용자는 다양한 디바이스들을 이용하여 홈 네트워크에서 제공되는 서비스를 이용할 수 있게 되었다.

[4] 그러나, 보안성 있는 프레임 워크가 없다면, 사용자의 개인 데이터를 포함한 디지털 정보가 악의의 공격자에게 노출될 수 있다. 공개 키 암호화 시스템은 일반적으로 기밀성(confidentiality) 및 완전성(integrity)를 제공하지만, 키들의 분배는 신뢰성 있는 제3자(trusted third party) 없이는 중간자 공격(man-in-the-middle attack)에 의해 깨지기 쉽다.

[5] 일반적으로 홈 네트워크는 중앙 통제(central administration)에 의한 인프라스트럭처에 의존하지 않고 동적으로 셋업되므로, 신뢰성 있는 제3자에 대한 가정 없이 키 분배 스킴을 구현할 필요가 있다.

[6] 예를 들면, UPnP(Universal Plug and Play)를 기반으로 하는 홈 네트워크에서, 홈 네트워크 외부로부터 진입한 CP(Control Point)가 모든 홈 디바이스들이 제공하는 서비스를 아무런 제약 없이 이용할 수 있게 해서는 안된다.

도면의 간단한 설명

[7] 도 1은 일 실시예에 따라 제어 장치가 피제어 장치를 제어하는 과정을 나타낸 순서도 ,

[8] 도 2는 일 실시예에 따라 제어 장치를 피제어 장치에 등록하는 방법을 설명하기 위한 흐름도 ,

[9] 도 3은 일 실시예에 따라 피제어 장치에 등록된 제어 장치가 피제어 장치를 제어하는 방법을 설명하기 위한 흐름도 ,

[10] 도 4는 일 실시예에 따라 TLS 세션 재개 프로토콜을 이용하여 TLS-PKS 프로토콜을 구현하는 방법을 설명하기 위한 흐름도 ,

[11] 도 5는 일 실시예에 따라 PIN을 관리하는 방법을 설명하기 위한 도면 ,

[12] 도 6은 일 실시예에 따라 PIN을 관리하는 제어 장치의 동작 과정을 나타낸 순서도 ,

[13] 도 7은 일 실시예에 따른 제어 장치의 구조를 나타낸 도면이다.

발명의 상세한 설명

기술적 과제

[14]

기술적 해결방법

[15] 본 실시예들은 홈 네트워크에서 제어 장치와 피제어 장치 간의 통신 보안성을 보장하는 장치 및 방법을 제공한다.

유리한 효과

[16] 본 발명에 따르면, 홈 네트워크에서 통신 보안성이 보장되는 프레임 워크를 쉽게 구현할 수 있다.

발명의 실시를 위한 최선의 형태

[17] 부가적인 관점들 및 /또는 효용들은 부분적으로 후술하는 발명의 상세한 설명에서 기술될 것이며 , 부분적으로는 , 발명의 상세한 설명에 의해 자명하거나 또는 발명의 실시에 의해 습득될 수 있을 것이다 .

[18] 앞서 말한 또는/및 다른 관점들은, 홈 네트워크에서 제어 장치가 피제어 장치와 안전하게 통신하는 방법에 있어서, 상기 피제어 장치에 제조시부터 부여된 식별자인 PIN을 이용하여 TLS-PSK(Transport Layer Security Pre-Shared Key ciphersuites) 프로토콜을 통해 상기 피제어 장치와 등록 SAC(Secure Authenticated Channel)을 생성하는 단계; 비밀 키를 생성하는 단계; 및 상기 등록 SAC을 통해 상기 생성된 비밀 키를 상기 피제어 장치와 공유함으로써 상기 제어 장치를 상기 피제어 장치에 등록하는 방법을 제공하는 것에 의해 성취된다.

[19] 상기 통신 방법은, 상기 등록 단계가 수행된 이후 상기 피제어 장치가 다시 발견되면, 상기 공유된 비밀 키를 이용하여 TLS-PSK 프로토콜을 통해 상기 피제어 장치와 서비스 SAC을 생성하는 단계를 더 포함하는 것이 바람직하다.

[20] 상기 SAC를 생성하는 단계는, 상기 제어 장치가 임의로 생성한 값을 세션 ID로 사용하는 TLS 세션 재개(session resumption) 프로토콜을 이용하여 상기 TLS-PSK 프로토콜을 구현하며, 상기 TLS 세션 재개(session resumption) 프로토콜의 ClientHello 메시지는 TLS 세션 재개 프로토콜을 이용한 TLS-PSK 프로토콜임을 나타내는 정보를 포함하는 것이 바람직하다.

[21] 상기 통신 방법은, 상기 비밀 키를 이용하여 생성된 서비스 SAC을 통해, 상기 제어 장치를 등록한 피제어 장치들의 PIN들을 상기 피제어 장치에게 송신하고, 상기 피제어 장치에 저장된 PIN들을 상기 피제어 장치로부터 수신함으로써 상기 피제어 장치와 PIN 목록을 동기화하는 단계를 더 포함하며, 상기 PIN을 이용하여 SAC을 생성하는 단계는, 상기 피제어 장치가 발견되면, 상기 피제어 장치의 PIN이 상기 제어 장치의 PIN 목록에 존재하는지 판단하는 단계; 및 상기 판단 결과 상기 피제어 장치의 PIN이 상기 제어 장치의 PIN 목록에 존재하지 않는 경우 사용자 인터페이스를 통해 상기 피제어 장치의 PIN을 요청하는 단계를 더 포함하는 것이 바람직하다.

[22] 상기 통신 방법은, 사용자 인터페이스를 통해 입력된 명령에 따라 상기 제어 장치에서 상기 비밀 키를 삭제하는 단계를 더 포함하는 것이 바람직하다.

[23] 상기 통신 방법은, 사용자 인터페이스를 통해 입력된 명령에 따라, 상기 피제어 장치에 저장된 비밀 키들 중 적어도 하나를 상기 비밀 키를 이용하여 생성된 서비스 SAC을 통해 삭제하는 단계를 더 포함하는 것이 바람직하다.

[24] 또한, 앞서 말한 및/또는 다른 관점들은 상기 통신 방법을 실행하는 컴퓨터 프로그램을 기록한 기록 매체를 제공함에 의해 성취된다.

[25] 또한, 앞서 말한 및/또는 다른 관점들은홈 네트워크에서 제어 장치가 피제어 장치와 안전하게 통신하도록 하는 장치에 있어서, 상기 피제어 장치에 제조시부터 부여된 식별자인 PIN을 이용하여 TLS-PSK 프로토콜을 통해 상기 피제어 장치와 안전한 인증 채널(SAC, Secure Authenticated Channel)을 생성하는 등록채널생성부; 및 비밀 키를 생성하고, 상기 생성된 비밀 키를 상기 생성된 SAC을 통해 상기 피제어 장치와 공유함으로써 상기 제어 장치를 상기 피제어 장치에 등록하는 등록수행부를 포함하는 장치를 제공하는 것에 의해 성취된다.

발명의 실시를 위한 형태

[26] 도 1은 일 실시예에 따라 제어 장치가 피제어 장치를 제어하는 과정을 나타낸 순서도이다 .

[27] 본 발명의 일 실시예에 따르면 , 피제어 장치는 자신에게 등록된 제어 장치에게만 안전한 인증 채널 (SAC, Secure Authenticated Channel), 즉 안전한 서비스 채널을 통해 서비스를 제공한다 . 따라서 , 피제어 장치는 인증된 제어 장치만을 등록해야 하며 , 이러한 등록 역시 SAC, 즉 안전한 등록 채널을 통해 수행되어야 한다 .

[28] 예를 들면 , 제어 장치는 UPnP 네트워크에서의 CP(Control Point)이고 , 피제어 장치는 UPnP 디바이스가 될 수 있으며 , UPnP 디바이스는 미리 정해진 특정 서비스들에 대하여는 등록된 CP에게만 SAC를 통해 제공하도록 설계될 수 있다 . 또한 , 본 발명의 구현을 위해 UPnP 디바이스에 새로운 액션들이 정의될 수 있을 것이다 .

[29] 단계 110에서 , 제어 장치는 PIN(Product Identification Number)을 이용하여 예를 들면 TLS-PSK(Transport Layer Security based on Pre-Shared Key, PSK ciphersuites for TLS) 프로토콜을 통해 SAC를 생성한다 . 여기서 , PIN은 상기 피제어 장치에 제조시부터 부여된 식별자를 의미할 수 있다. 이러한 PIN은 피제어 장치의 내부 또는 외부에 기록된 형태로, 또는 피제어 장치와는 별도로 피제어 장치를 구매한 사용자에게 제공될 수 있다.

[30] TLS(Transport Layer Security) 는 인터넷에서의 통신 보안을 위해 사용되는 프로토콜인데, TLS-PSK 은 공개 키 인증서 대신 미리 공유된 대칭 키(symmetric key)를 이용하여 TLS를 구현함으로써 공개 키를 이용한 인증 과정에 요구되는 복잡한 연산을 회피하도록 설계된 프로토콜이며, TLS-PSK 프로토콜에 의해 제어 장치와 피제어 장치 간에 SAC이 생성될 수 있다. TLS는 RFC 4346,

TLS-PSK는 RFC 4279에 정의되어 있으므로, 이에 대한 자세한 설명은 여기서는 생략한다.

[31] 단계 120에서, 제어 장치는 생성된 SAC, 즉 안전한 등록 채널을 통해 피제어 장치에 자신을 등록한다. 피제어 장치에 제어 장치가 등록된다는 것은 제어 장치가 자신이 생성한 비밀 키를 SAC를 통해 피제어 장치에게 송신함을 의미한다. 즉, 등록 과정이 완료되면, 제어 장치와 피제어 장치는 동일한 비밀 키를 공유한다.

[32] 단계 130에서, 제어 장치와 피제어 장치는 공유된 비밀 키를 이용하여 TLS-PSK 프로토콜을 통해 SAC를 생성한다. 단계 110에서 생성된 SAC는 제어 장치를 피제어 장치에 등록하기 위해 사용되는 등록 채널이며, 단계 130에서 생성된 SAC는 피제어 장치에 등록된 제어 장치가 피제어 장치를 제어함으로써 피제어 장치의 서비스를 제어 장치에게 제공하기 위해 사용되는 서비스 채널이다.

[33] 단계 140에서, 제어 장치는 단계 130에서 생성된 SAC를 통해 피제어 장치를 제어한다.

[34] 도 2는 일 실시예에 따라 제어 장치를 피제어 장치에 등록하는 방법을 설명하기 위한 흐름도이다 . 즉 , 본 실시예에서는 제어 장치가 피제어 장치에 등록되어 있지 않은 것으로 가정한다 .

[35] 단계 201에서 , 제어 장치는 피제어 장치를 발견 (discover)한다 . 예를 들면 , 이러한 과정은 UPnP 네트워크에서 SSDP(Simple Service Discovery Protocol)을 통한 디스커버리에 해당한다 .

[36] 단계 202에서 , 제어 장치는 피제어 장치에게 등록된 제어 장치의 목록을 요청한다 . 이러한 요청을 위해 UPnP 디바이스에 새로운 액션이 정의될 수 있다 .

[37] 단계 203에서 , 피제어 장치는 제어 장치에게 등록된 제어 장치의 목록을 송신한다 . 본 실시예에서는 제어 장치가 피제어 장치에 등록되어 있지 않은 것으로 가정하였으므로 , 제어 장치는 사용자 인터페이스를 통해 사용자에게 피제어 장치의 PIN을 요청한다 .

[38] 단계 204에서 , 제어 장치는 사용자 인터페이스를 통해 사용자로부터 피제어 장치의 PIN을 입력받는다 . 따라서 , PIN은 제어 장치와 피제어 장치에 의해 공유된다 .

[39] 단계 205에서 , 제어 장치와 피제어 장치는 공유된 PIN을 이용하여 TLS-PSK 프로토콜을 통해 SAC를 생성한다 . 이 때 생성된 SAC는 제어 장치를 피제어 장치에 등록하기 위한 등록 채널이다 .

[40] 단계 206에서 , 제어 장치는 임의로 비밀 키를 생성한다 .

[41] 단계 207에서 , 제어 장치는 생성된 비밀 키를 SAC를 통해 피제어 장치에게 송신한다 .

[42] 단계 208에서 , 피제어 장치는 수신된 비밀 키를 저장한다 . 이와 같은 과정을 통해 비밀 키는 제어 장치와 피제어 장치 간에 공유되며 , 공유된 비밀 키는 추후 서비스 채널을 TLS-PSK 프로토콜을 통해 생성하는 데 사용된다 .

[43] 한편 , 사용자는 제어 장치에서 더 이상 특정 피제어 장치를 제어하지 못하도록 하려는 경우가 생길 수 있다 . 단계 209 내지 단계 210에서 피제어 장치를 취소 (revoke)하는 절차를 설명한다 .

[44] 단계 209에서 , 사용자는 제어 장치의 사용자 인터페이스를 통해 특정 피제어장치에 대한 취소 명령을 입력한다 . 사용자가 피제어 장치를 식별할 수 있도록 사용자 인터페이스에는 피제어 장치의 friendly name이나 모델명 등이 표시될 수 있다 .

[45] 단계 210에서 , 제어 장치는 사용자가 지정한 피제어 장치에 대한 디바이스 ID, 비밀 키 등의 정보를 삭제한다 .

[46] 도 3은 일 실시예에 따라 피제어 장치에 등록된 제어 장치가 피제어 장치를 제어하는 방법을 설명하기 위한 흐름도이다 . 본 실시예에서는 제어 장치가 이미 피제어 장치에 등록되어 있는 것으로 가정한다 .

[47] 단계 301에서 , 제어 장치는 피제어 장치를 발견한다 .

[48] 단계 302에서 , 제어 장치는 피제어 장치에게 등록된 제어 장치의 목록을 요청한다 .

[49] 단계 304에서 , 제어 장치는 수신된 목록을 참조하여 피제어 장치에 자신이 등록되어 있음을 확인한다 . 등록된 제어 장치를 나타내기 위해 등록된 제어 장치의 목록에는 제어 장치의 디바이스 ID가 사용될 수 있으며 , 디바이스 ID로는 디바이스를 특정할 수 있는 것이면 어떠한 정보도 사용 가능하다 . 예를 들면 , 제어 장치의 MAC 어드레스를 사용할 수 있다 .

[50] 단계 305에서 , 제어 장치는 저장된 비밀 키를 이용하여 TLS-PSK 프로토콜을 통해 피제어 장치와 SAC를 생성한다 . 제어 장치가 피제어 장치에 등록이 되어 있다는 것은 제어 장치와 피제어 장치가 이미 비밀 키를 공유하고 있음을 의미한다 .

[51] 단계 306에서 , 제어 장치는 단계 305에서 생성한 SAC를 통해 피제어 장치의 서비스를 이용한다 .

[52] 한편 , 사용자는 피제어 장치에 등록된 제어 장치들 중 특정 제어 장치들을 취소 (revoke)하려는 경우가 있을 수 있다 . 이러한 과정은 단계 307 내지 단계 309에 도시하였다 .

[53] 단계 307에서 , 사용자는 제어 장치의 사용자 인터페이스를 통해 피제어 장치에 등록된 제어 장치들 중 특정 제어 장치에 대한 취소 명령을 입력한다 . 사용자가 등록된 제어 장치들을 식별할 수 있도록 사용자 인터페이스에는 제어 장치들의 friendly name이나 모델명 등이 표시될 수 있다 .

[54] 단계 308에서 , 제어 장치는 단계 305에서 생성된 SAC를 통해 피제어 장치에게 사용자가 지정한 제어 장치를 취소 (revoke)하도록 요청한다 . 이러한 취소는 피제어 장치가 제공하는 서비스에 포함될 수 있으며 , UPnP에서는 새로운 액션으로 정의될 수 있다 . 따라서 , 제어 장치의 취소 요청은 서비스 채널을 통해서만 이루어질 수 있다 .

[55] 단계 309에서 , 피제어 장치는 해당 제어 장치에 대한 정보 , 예를 들면 제어 장치 ID, 피제어 장치가 해당 제어 장치와 공유하는 비밀 키 등을 삭제한다 . 따라서 , 해당 제어 장치는 피제어 장치와 더 이상 비밀 키를 공유하지 못하므로 , 피제어 장치와 서비스 채널을 생성할 수 없으며 , 결국 피제어 장치의 서비스를 이용할 수 없다 .

[56] 도 4는 본 발명의 일 실시예에 따라 TLS 세션 재개 프로토콜을 이용하여 TLS-PKS 프로토콜을 구현하는 방법을 설명하기 위한 흐름도이다 .

[57] TLS-PKS는 RFC 4279에 기반하여 구현할 수 있다 . 그러나 , 현재 TLS 1.1을 구현한 대부분의 디바이스들이 RFC 4279를 지원하지 않는다 . 따라서 , TLS 프로토콜을 사용하는 기존 디바이스들의 프로토콜 스택의 변화를 최소화하기 위해 RFC 4279를 지원하지 않는 디바이스에서 TLS-PKS를 구현할 필요가 있다 . 본 실시예에서는 TLS 세션 재개 (session resumption) 프로토콜을 이용하여 TLS-PKS를 구현하는 방법을 설명한다 .

[58] 세션 재개 (session resumption) 프로토콜은 TLS를 통해 서버와 클라이언트가인증을 완료한 후 , 세션이 종료되었다가 다시 세션을 재개할 때 공개 키 연산들 (예를 들면 RSA)를 중복 수행하지 않도록 세션 ID를 이용하여 인증 과정을 생략하는 것이다 .

[59] 단계 401에서 , 제어 장치는 세션 ID, ciphers, 난수 R1을 피제어 장치에게 송신한다 . 이 때 , 세션 ID는 제어 장치가 임의로 선택한다 . 예를 들면 , 제어 장치 ID 및 /또는 피제어 장치 ID가 세션 ID로 사용될 수 있다 .

[60] 이러한 정보들은 세션 재개 프로토콜의 , 예를 들면 , ClientHello 메시지에 포함되어 피제어 장치에게 전달된다 . 따라서 , TLS 세션 재개 프로토콜을 이용한 TLS-PSK 프로토콜임을 나타내는 정보가 ClientHello 메시지에 포함되는 것이 바람직하다. 예를 들면, ciphers(cipher suites) 또는 세션 ID에 포함될 수 있다 .

[61] 단계 402에서 , 피제어 장치는 ClientHello 메시지에 포함된 정보를 통해 제어 장치가 TLS 세션 재개 프로토콜을 이용한 TLS-PSK 프로토콜을 요청하였음을 인지한다. 따라서, 세션 ID의 유효성을 판단하지 않고 수신된 세션 ID와 동일한 세션 ID, cipher, 난수 R2 및 Hash(S, 제어장치ID, 피제어장치ID, R1, R2)를 제어 장치에게 송신한다. 여기서, S는 TLS 세션 재개 프로토콜에서 PreMasterSecret으로 사용되는 값이며, 본 실시예에서는 사용자가 입력한 피제어 장치의 PIN이 S 값으로 할당된다. 단계 402에서 수신된 해쉬 값을 통해 제어 장치는 피제어 장치가 PreMasterSecret S를 가지고 있음을 확인할 수 있다.

[62] 단계 403에서 , 제어 장치는 자신도 PreMasterSecret S 를 가지고 있음을 피제어 장치에게 알리기 위해Hash(S, R1, R2)를 계산하고, 그 결과를 피제어 장치에게 송신한다.

[63] 단계 404에서, 피제어 장치는 제어 장치에게 프로토콜이 성공적으로 종료되었음을 알리는Finished 메시지를 송신한다.

[64] 도 5는 일 실시예에 따라 PIN을 관리하는 방법을 설명하기 위한 도면이다.

[65] 지금까지의 실시예에 따르면, 홈 네트워크에서 사용자는 제어 장치 또는 피제어 장치가 바뀔 때마다 등록 절차를 수행하기 위해 피제어 장치의 PIN을 알아내고, 제어 장치의 사용자 인터페이스를 통해 PIN을 입력해야 한다. 본 실시예에서는 이러한 번거로움을 줄이기 위한 방법을 제시한다.

[66] 본 실시예에서, 제어 장치와 피제어 장치는 모두 PIN 리스트를 관리하며, 제어 장치는 피제어 장치에 등록할 때마다 PIN 리스트를 동기화한다. PIN 리스트에는 피제어 장치 ID와 PIN이 매핑된 테이블 형태의 정보가 기록될 수 있다. 도 5를 참조하여 더욱 구체적으로 살펴보도록 한다.

[67] 사용자는 처음으로 제어 장치 1(510)을 피제어 장치 1(535)에 등록한다. 즉, 제어 장치 1(510)의 PIN 목록 (520)에 피제어 장치 1(530)의 PIN이 기록된다. 이 때, 피제어 장치 1(530)도 PIN 목록 (535)에 자신의 PIN을 기록한다.

[68] 다음으로, 사용자는 제어 장치 1(510)을 피제어 장치 2(540)에 등록한다. 따라서, 제어 장치 1(510)의 PIN 목록 (520)에 피제어 장치 2(540)의 PIN이 추가된다. 이 때, 제어 장치 1(510)은 자신의 PIN 목록 (520)을 피제어 장치 2(540)의 PIN 목록 (545)과 동기화한다. 따라서, 피제어 장치 2(545)의 PIN 목록 (545)에는 피제어 장치 1(530) 및 피제어 장치 2(540)의 PIN이 기록된다.

[69] 이와 같은 방식으로 제어 장치 1(510)이 피제어 장치 1(530), 피제어 장치 2(540), ..., 피제어 장치 N(550)에 등록 절차를 완료하게 되면, 도 5에 도시된 바와 같이 제어 장치 1(510)의 PIN 목록 (520)과 피제어 장치 N(550)의 PIN 목록 (555)에는 N개의 피제어 장치들의 PIN이 모두 기록된다.

[70] 이후, 사용자는 새로운 제어 장치인 제어 장치 2(570)를 이용하여 홈 네트워크에 접속한다. 사용자는 제어 장치 2(570)를 피제어 장치 N(550)에 등록하기 위해 제어 장치 2(570)의 사용자 인터페이스를 통해 피제어 장치 N(550)의 PIN을 입력한다.

[71] 제어 장치 2(570)가 피제어 장치 N(550)에 등록되면, 둘은 PIN 목록을 동기화하는데, 피제어 장치 N(550)의 PIN 목록 (555)에는 이미 모든 피제어 장치들의 PIN들이 기록되어 있으므로, 제어 장치 2(575)에도 역시 모든 피제어 장치들의 PIN들이 기록된다.

[72] 이후, 사용자가 제어 장치 2(570)를 다른 피제어 장치, 예를 들면 피제어 장치 1(530)에 등록하려고 할 때, 사용자는 피제어 장치 1(530)의 PIN을 제어 장치 2(570)에 입력하지 않아도 된다. 피제어 장치 1(530)의 PIN은 이미 제어 장치 2(570)의 PIN 목록 (575)에 기록되어 있기 때문이다.

[73] 도 6은 일 실시예에 따라 PIN을 관리하는 제어 장치의 동작 과정을 나타낸 순서도이다.

[74] 단계 610에서, 제어 장치는 등록된 제어 장치의 목록을 피제어 장치로부터 수신한다.

[75] 단계 620에서, 제어 장치는 목록에 기록된 디바이스 ID들 중 자신의 디바이스

ID가 포함되어 있는지를 검사하여 자신이 피제어 장치에 등록되어 있는지를 판단한다. 만약 등록되어 있다면, 단계 680으로 진행하고, 등록되어 있지 않다면 단계 630으로 진행한다.

[76] 단계 680에서, 제어 장치는 저장된 비밀 키를 추출한다. 제어 장치가 피제어 장치에 등록되어 있다는 것은 이미 비밀 키를 공유하고 있음을 의미하기 때문이다.

[77] 단계 690에서, 제어 장치와 피제어 장치는 비밀 키를 이용하여 TLS-PSK를 통해 SAC를 생성한다. 이 때 생성된 SAC는 피제어 장치의 서비스를 이용하기 위해 사용되는 채널이다.

[78] 단계 630 및 단계 640에서, 제어 장치는 PIN 목록을 검색하여 피제어 장치의 PIN을 찾는다. 만약 제어 장치의 PIN 목록에 피제어 장치의 PIN이 존재하면 단계 660으로, 그렇지 않으면 단계 650으로 진행한다.

[79] 단계 650에서, 제어 장치는 사용자 인터페이스를 통해 사용자로부터 피제어 장치의 PIN을 입력받는다.

[80] 단계 660에서, 제어 장치와 피제어 장치는 공유된 PIN을 이용하여 TLS-PSK 프로토콜을 통해 SAC을 생성한다. 이 때 생성된 SAC은 제어 장치를 제어 장치에 등록하기 위해 사용된다.

[81] 단계 670에서, 제어 장치는 단계 660에서 생성된 SAC을 통해 피제어 장치에게 비밀 키를 송신함으로써 등록 절차를 수행한다. 전술한 바와 같이, 비밀 키는 제어 장치가 임의로 생성할 수 있다.

[82] 단계 675에서, 제어 장치와 피제어 장치는 단계 660에서 생성된 SAC을 통해 PIN 목록을 동기화한다. 따라서, 제어 장치와 피제어 장치는 동일한 PIN 목록을 가지게 된다. 단계 690은 전술한 바와 같다.

[83] 도 7은 일 실시예에 따른 제어 장치의 구조를 나타낸 도면이다.

[84] 도 7에 도시된 바와 같이, 본 발명의 일 실시예에 따른 제어 장치 (700)는 사용자 인터페이스 (710), 제어장치 취소부 (720), 피제어장치 취소부 (730), 등록채널 생성부 (740), 저장부 (750), 등록 수행부 (760), 서비스채널 생성부 (770) 및 PIN 목록 동기화부 (780)를 포함하며, 등록채널 생성부 (740)는 PIN 검색부 (741) 및 PIN 입력부 (742)를 포함한다.

[85] 사용자 인터페이스 (710)는 사용자로부터 제어 장치 취소 명령, 피제어 장치취소 명령, 제어 장치의 PIN 등을 입력받고, 사용자에게 알리기 위한 다양한 정보를 표시한다.

[86] 등록 채널 생성부 (740)는 사용자가 입력한 피제어 장치 (도시하지 않음)의 PIN을 이용하여 TLS-PSK 프로토콜을 통해 피제어 장치와 SAC를 생성한다. 등록 채널 생성부 (740)는 TLS 세션 재개 프로토콜을 이용하여 TLS-PSK 프로토콜을 구현하기 위해 임의로 선택된 값을 TLS 세션 재개 프로토콜에서의 세션 ID로 사용하며, 이 때 ClientHello 메시지는 TLS 세션 재개 프로토콜을 이용한 TLS-PSK 프로토콜임을 나타내는 정보를 포함하는 것이 바람직하다.

[87] 피제어 장치가 발견되면 , PIN 검색부 (741)는 저장부 (750)에 저장된 PIN 목록에서 제어 장치 (700)의 PIN이 있는지 검색한다 . PIN 입력부 (742)는 만약 PIN 목록에 제어 장치 (700)의 PIN이 없으면 , 사용자 인터페이스 (710)를 통해 사용자로부터 PIN을 입력받는다 .

[88] 등록 수행부 (760)는 비밀 키를 생성하여 저장부 (750)에 저장하고 , 생성된 비밀 키를 등록 채널 생성부 (740)가 생성한 SAC를 통해 피제어 장치에게 안전하게 송신함으로써 제어 장치 (700)를 피제어 장치에 등록한다 .

[89] 서비스채널 생성부 (770)는 제어 장치 (700)와 피제어 장치가 공유하는 비밀 키를 이용하여 TLS-PSK 프로토콜을 통해 피제어 장치와 SAC를 생성한다 .

[90] PIN 목록 동기화부 (780)는 등록이 완료되면 PIN 목록을 피제어 장치와 동기화하여 저장부 (750)에 저장한다 .

[91] 제어장치 취소부 (720)는 사용자 인터페이스 (710)를 통해 사용자가 특정 피제어 장치에 대한 취소 명령을 입력하면 , 저장부 (750)에서 해당 피제어 장치에 관한 정보 , 예를 들면 디바이스 ID, 공유된 비밀 키 등을 삭제한다 .

[92] 피제어장치 취소부 (730)는 사용자 인터페이스 (710)를 통해 사용자가 피제어장치에 등록된 특정 제어 장치에 대한 취소 명령을 입력하면 , 서비스채널 생성부 (770)에 의해 생성된 SAC를 통해 피제어 장치에게 해당 제어 장치에 관한 취소를 요청한다 . 이러한 요청을 받은 피제어 장치는 해당 제어 장치에 관한 정보 , 예를 들면 디바이스 ID, 피제어 장치가 해당 제어 장치와 공유하는 비밀 키 등을 삭제한다 .

[93] 한편 , 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고 , 컴퓨터로 읽을 수 있는 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[94] 상기 컴퓨터로 읽을 수 있는 매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 매체를 포함한다.

[95] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

청구범위

[1] 【청구항 1】
홈 네트워크에서 제어 장치가 피제어 장치와 안전하게 통신하는 방법에 있어서,
상기 피제어 장치의 식별자를 이용하는 프로토콜을 통해 상기 피제어 장치와 등록 SAC(Secure Authenticated Channel)을 생성하는 단계;
비밀 키를 생성하는 단계; 및
상기 등록 SAC을 통해 상기 생성된 비밀 키를 상기 피제어 장치와 공유함으로써 상기 제어 장치를 상기 피제어 장치에 등록하는 단계를 포함하는 것을 특징으로 하는 방법.

[2] 【청구항 2】
제 1항에 있어서,
상기 프로토콜은 TLS-PSK(Transport Layer Security Pre-Shared Key ciphersuites)임을 특징으로 하는 방법.

[3] 【청구항 3】
제 2항에 있어서,
상기 식별자는 PIN(Product Identification Number)임을 특징으로 하는 방법.

[4] 【청구항 4】
제 3항에 있어서,
상기 등록 단계가 수행된 이후 상기 피제어 장치가 다시 발견되면, 상기 공유된 비밀 키를 이용하여 TLS-PSK 프로토콜을 통해 상기 피제어 장치와 서비스 SAC(Secure Authenticated Channel)을 생성하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[5] 【청구항 5】
제 2항에 있어서,
상기 SAC를 생성하는 단계는,
상기 제어 장치가 임의로 생성한 값을 세션 식별자로 사용하는 TLS 세션 재개(session resumption) 프로토콜을 이용하여 상기 TLS-PSK 프로토콜을 구현하며, 상기 TLS 세션 재개(session resumption) 프로토콜의 ClientHello 메시지는 TLS 세션 재개 프로토콜을 이용한 TLS-PSK 프로토콜임을 나타내는 정보를 포함하는 것을 특징으로 하는 방법.

[6] 【청구항 6】
제 4항에 있어서,
상기 비밀 키를 이용하여 생성된 등록 SAC을 통해, 상기 제어 장치를 등록한 피제어 장치들의 PIN들을 상기 피제어 장치에게 송신하고, 상기 피제어 장치에 저장된 PIN들을 상기 피제어 장치로부터 수신함으로써 상기 피제어 장치와 PIN 목록을 동기화하는 단계를 더 포함하며,

상기 PIN을 이용하여 등록 SAC을 생성하는 단계는,
상기 피제어 장치가 발견되면, 상기 피제어 장치의 PIN이 상기 제어 장치의 PIN 목록에 존재하는지 판단하는 단계; 및
상기 판단 결과 상기 피제어 장치의 PIN이 상기 제어 장치의 PIN 목록에 존재하지 않는 경우 사용자 인터페이스를 통해 상기 피제어 장치의 PIN을 요청하는 단계를 포함하는 것을 특징으로 하는 방법.

[7] 【청구항 7】
제 1항에 있어서,
사용자 인터페이스를 통해 입력된 명령에 따라 상기 제어 장치에서 상기 비밀 키를 삭제하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[8] 【청구항 8】
제 4항에 있어서,
사용자 인터페이스를 통해 입력된 명령에 따라, 상기 피제어 장치에 저장된 비밀 키들 중 적어도 하나를 상기 비밀 키를 이용하여 생성된 서비스 SAC을 통해 삭제하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[9] 【청구항 9】
제 1항에 있어서,
상기 피제어 장치의 식별자는 제조시에 부여되는 것을 특징으로 하는 방법.

[10] 【청구항 10】
제 1항에 의한 방법을 실행하는 컴퓨터 프로그램을 기록한 기록 매체.

[11] 【청구항 11】
홈 네트워크에서 제어 장치가 피제어 장치와 안전하게 통신하도록 하는 장치에 있어서,
상기 피제어 장치에 제조시부터 부여된 식별자인 PIN(Product Identification Number)을 이용하여 TLS-PSK 프로토콜을 통해 상기 피제어 장치와 등록 SAC(Secure Authenticated Channel)을 생성하는 등록채널생성부; 및
비밀 키를 생성하고, 상기 생성된 비밀 키를 상기 등록 SAC을 통해 상기 피제어 장치와 공유함으로써 상기 제어 장치를 상기 피제어 장치에 등록하는 등록수행부를 포함하는 것을 특징으로 하는 장치.

[12] 【청구항 12】
제 11항에 있어서,
상기 등록 단계가 수행된 이후 상기 피제어 장치가 다시 발견되면, 상기 공유된 비밀 키를 이용하여 TLS-PSK 프로토콜을 통해 상기 피제어 장치와 서비스 SAC(Secure Authenticated Channel)을 생성하는 서비스채널생성부를 더 포함하는 것을 특징으로 하는 장치.

[13] 【청구항 13】
제 11항에 있어서,
상기 등록채널생성부는,

상기 제어 장치가 임의로 생성한 값을 세션 식별자(ID)로 사용하는 TLS 세션 재개(session resumption) 프로토콜을 이용하여 상기 TLS-PSK 프로토콜을 구현하며, 상기 TLS 세션 재개(session resumption) 프로토콜의 ClientHello 메시지는 TLS 세션 재개 프로토콜을 이용한 TLS-PSK 프로토콜임을 나타내는 정보를 포함하는 것을 특징으로 하는 장치.

[14] 【청구항 14】

제 13항에 있어서,

상기 제어 장치의 식별자 및/또는 상기 피제어 장치의 식별자가 상기 세션 ID로 사용되는 것을 특징으로 하는 장치.

[15] 【청구항 15】

제 12항에 있어서,

상기 비밀 키를 이용하여 생성된 서비스 SAC을 통해, 상기 제어 장치를 등록한 피제어 장치들의 PIN들을 상기 피제어 장치에게 송신하고, 상기 피제어 장치에 저장된 PIN들을 상기 피제어 장치로부터 수신함으로써 상기 피제어 장치와 PIN 목록을 동기화하는 PIN목록동기화부를 더 포함하며,

상기 등록채널생성부는,

상기 피제어 장치가 발견되면, 상기 피제어 장치의 PIN이 상기 제어 장치의 PIN 목록에 존재하는지 판단하는 PIN검색부; 및

상기 판단 결과 상기 피제어 장치의 PIN이 상기 제어 장치의 PIN 목록에 존재하지 않는 경우 사용자 인터페이스를 통해 상기 피제어 장치의 PIN을 요청하는 PIN입력부를 포함하는 것을 특징으로 하는 장치.

[16] 【청구항 16】

제 11항에 있어서,

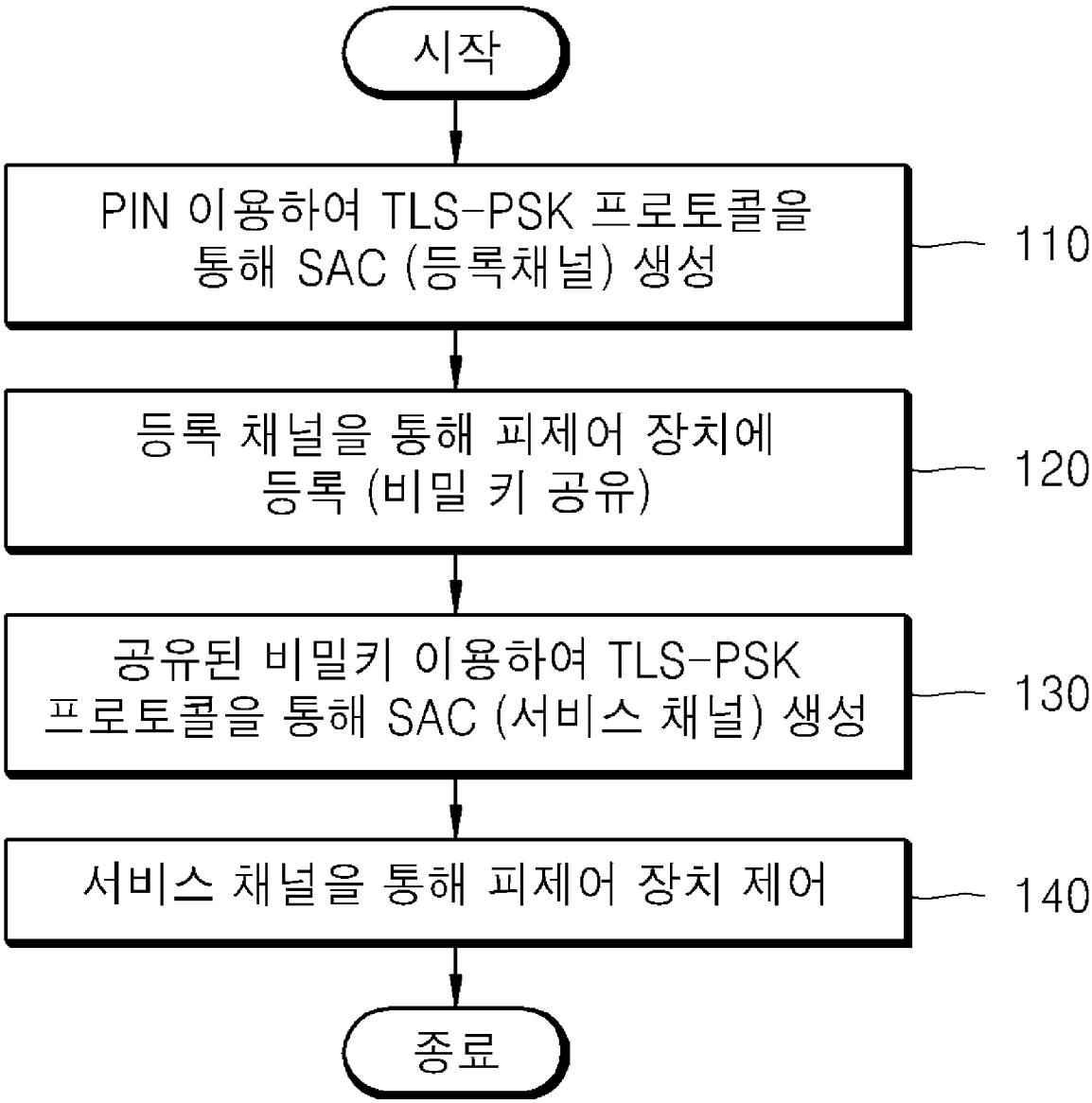
사용자 인터페이스를 통해 입력된 명령에 따라 상기 제어 장치에서 상기 비밀 키를 삭제하는 피제어장치취소부를 더 포함하는 것을 특징으로 하는 장치.

[17] 【청구항 17】

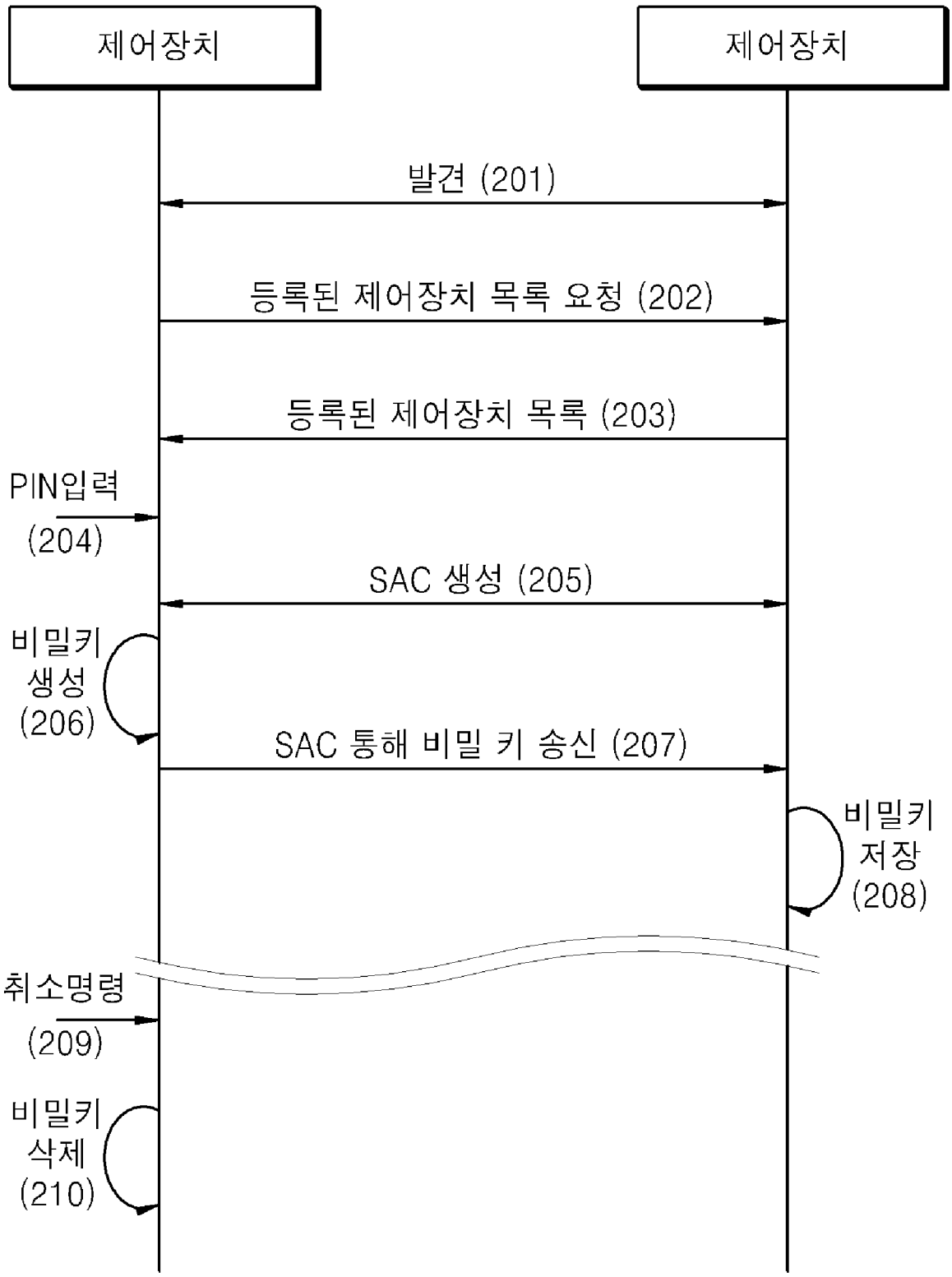
제 11항에 있어서,

사용자 인터페이스를 통해 입력된 명령에 따라, 상기 피제어 장치에 저장된 비밀 키들 중 적어도 하나를 상기 비밀 키를 이용하여 생성된 서비스 SAC을 통해 삭제하는 제어장치취소부를 더 포함하는 것을 특징으로 하는 장치.

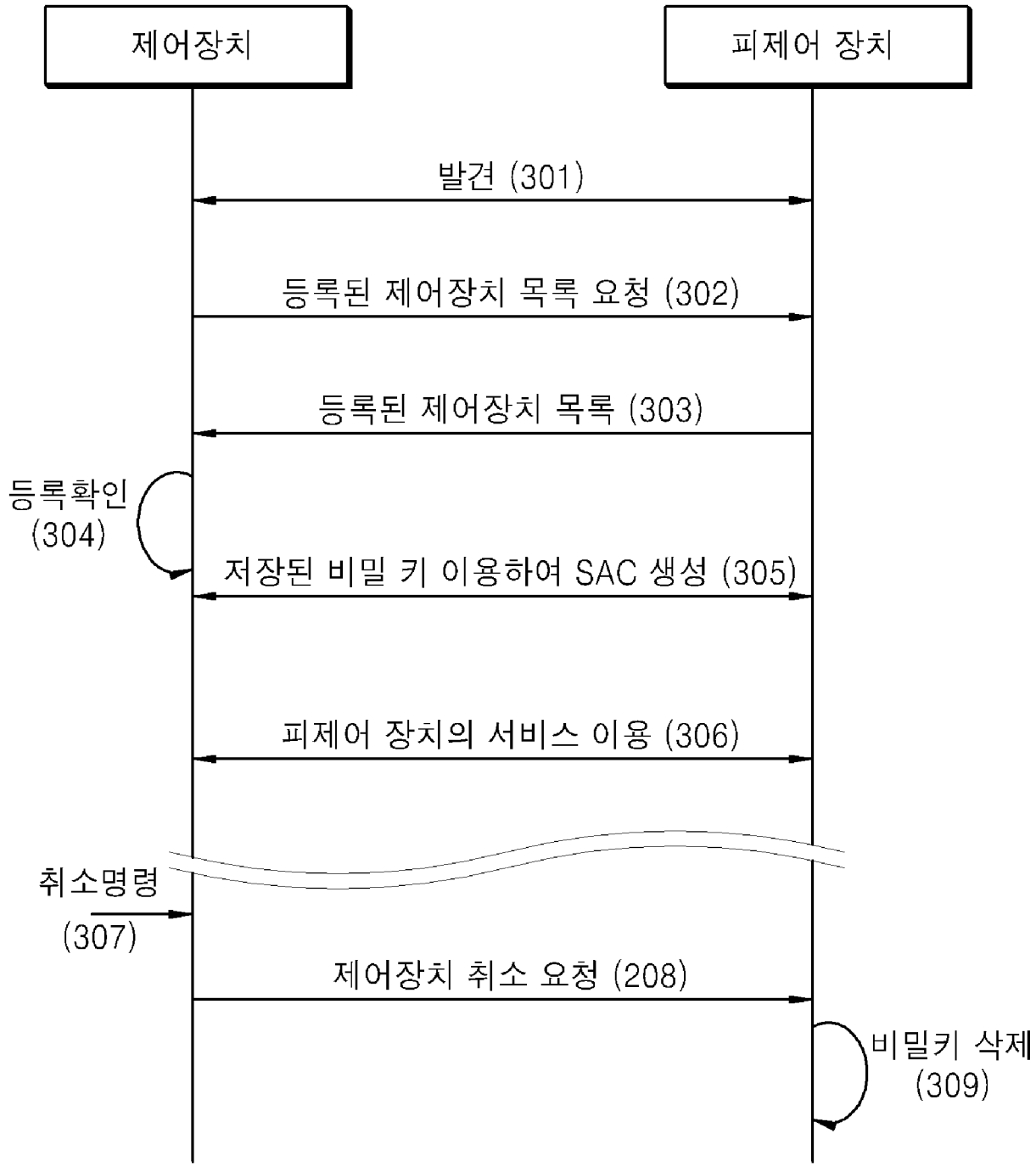
도 1


시작
PIN 이용하여 TLS-PSK 프로토콜을 통해 SAC (등록채널) 생성
110
등록 채널을 통해 피제어 장치에 등록 (비밀 키 공유)
120
공유된 비밀키 이용하여 TLS-PSK 프로토콜을 통해 SAC (서비스 채널) 생성
130
서비스 채널을 통해 피제어 장치 제어
140
종료

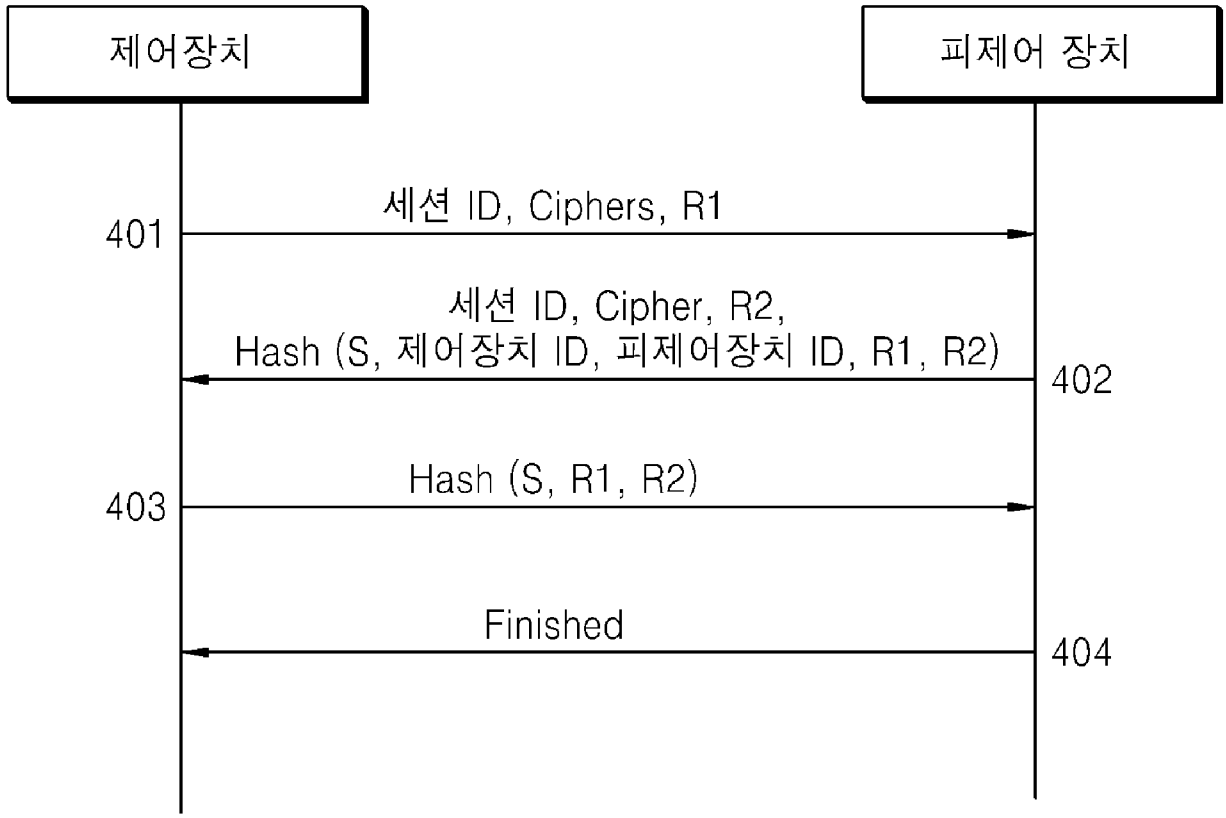
도 2


제어장치
제어장치
발견 (201)
등록된 제어장치 목록 요청 (202)
등록된 제어장치 목록 (203)
PIN입력
(204)
SAC 생성 (205)
비밀키
생성
(206)
SAC 통해 비밀 키 송신 (207)
비밀키
저장
(208)
취소명령
(209)
비밀키
삭제
(210)

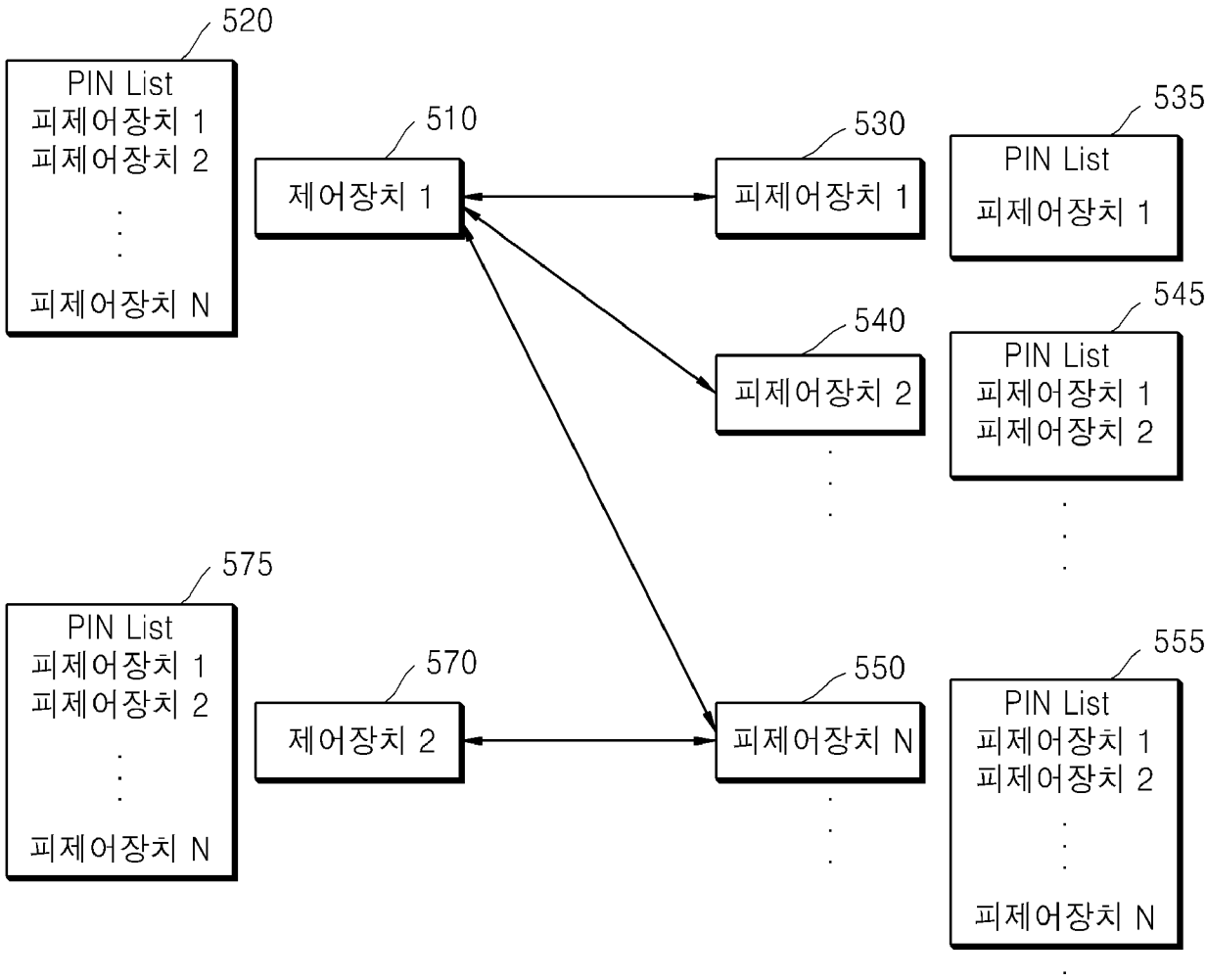
도 3


제어장치
피제어 장치
발견 (301)
등록된 제어장치 목록 요청 (302)
등록된 제어장치 목록 (303)
등록확인 (304)
저장된 비밀 키 이용하여 SAC 생성 (305)
피제어 장치의 서비스 이용 (306)
취소명령 (307)
제어장치 취소 요청 (208)
비밀키 삭제 (309)

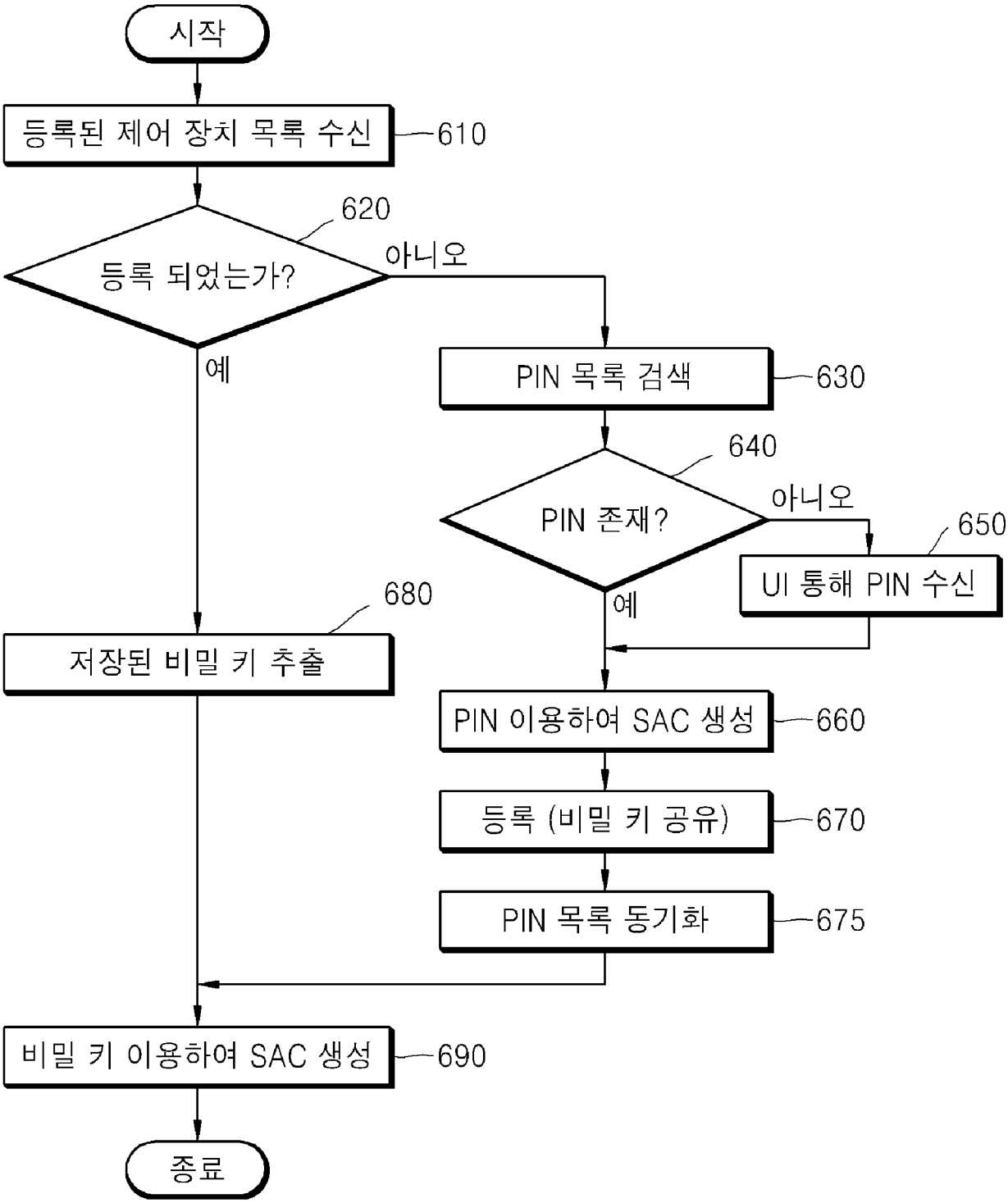
도 4


제어장치
피제어 장치
401
세션 ID, Ciphers, R1
세션 ID, Cipher, R2,
Hash (S, 제어장치 ID, 피제어장치 ID, R1, R2)
402
403
Hash (S, R1, R2)
Finished
404

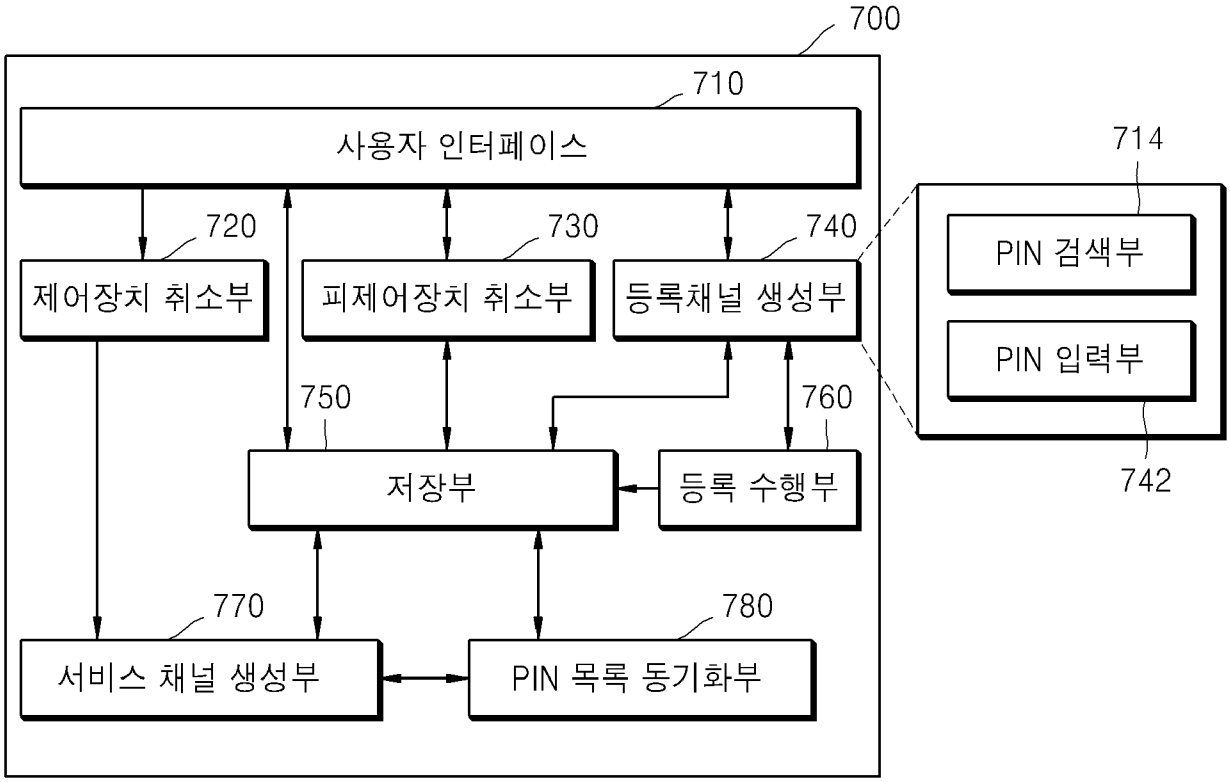
도 5


520
PIN List
피제어장치 1
피제어장치 2
피제어장치 N
510
제어장치 1
530
피제어장치 1
535
PIN List
피제어장치 1
540
피제어장치 2
545
PIN List
피제어장치 1
피제어장치 2
575
PIN List
피제어장치 1
피제어장치 2
피제어장치 N
570
제어장치 2
550
피제어장치 N
555
PIN List
피제어장치 1
피제어장치 2
피제어장치 N

도 6


시작
등록된 제어 장치 목록 수신
610
620
등록 되었는가?
아니오
예
PIN 목록 검색
630
640
PIN 존재?
아니오
650
UI 통해 PIN 수신
예
680
저장된 비밀 키 추출
PIN 이용하여 SAC 생성
660
등록 (비밀 키 공유)
670
PIN 목록 동기화
675
비밀 키 이용하여 SAC 생성
690
종료

도 7


700
710
사용자 인터페이스
714
720
730
740
제어장치 취소부
피제어장치 취소부
등록채널 생성부
PIN 검색부
PIN 입력부
750
760
742
저장부
등록 수행부
770
780
서비스 채널 생성부
PIN 목록 동기화부