(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0144027
(43) 공개일자 2016년12월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
H04L 9/0822 (2013.01)
H04L 63/062 (2013.01)
(21) 출원번호 10-2015-0071577
(22) 출원일자 2015년05월22일
심사청구일자 2015년05월22일

(71) 출원인
한발대학교 산학협력단
대전광역시 유성구 동서대로 125 (덕명동)
(72) 발명자
이창석
대전광역시 유성구 학하로 33 학의뜰 아파트 106-1601
(74) 대리인
특허법인 플러스

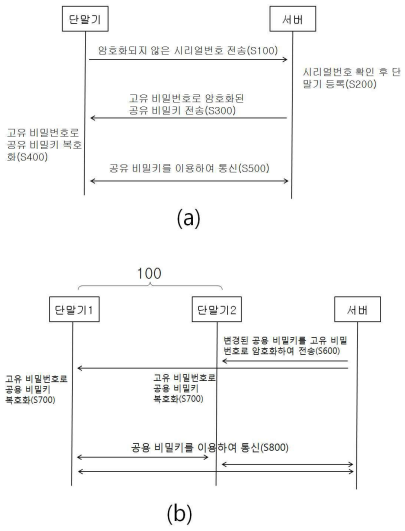
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 **보안키 공유 방법과 이를 위한 단말기 및 서버**

(57) 요 약

본 발명은 단말기와 서버 간의 보안키 공유 방법과 이를 위한 단말기 및 서버에 관한 것으로, 더욱 상세하게는 입력장치가 구비되지 않은 소형 가전기기와 같은 단말기와 서버가 통신하기 위해 보안키를 공유하는 방법에 있어서 간단한 방법으로도 보안 기능을 향상시킨 보안키 공유 방법과 이를 위한 단말기 및 서버에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0838 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 201401870001
부처명 중소기업청
연구관리전문기관 (사)한국산학연협회
연구사업명 산학연협력기술개발사업
연구과제명 보급형 스마트 전등 관리 시스템 기술 개발
기 여 율 1/1
주관기관 한밭대학교
연구기간 2014.06.01 ~ 2015.05.31

명 세 서

청구범위

청구항 1

단말기와 서버 간의 보안키를 공유 방법에 있어서,

a) 단말기가 자신의 시리얼번호를 서버로 송신하는 단계(S100);

b) 상기 서버가 상기 단말기로부터 수신된 상기 시리얼번호를 이용하여 서버의 데이터베이스에서 상기 단말기의 고유 비밀번호를 검색하여 찾는 단계(S200);

c) 상기 서버가 상기 단말기와의 통신을 위한 공유 비밀키를 해당 단말기의 고유 비밀번호로 암호화하여 상기 단말기로 전송하는 단계(S300);

d) 상기 단말기가 상기 서버로부터 수신된 암호화된 공유 비밀키를 상기 단말기에 저장되어 있는 상기 고유 비밀번호로 복호화하는 단계(S400); 및

e) 상기 서버 및 상기 단말기가 상기 공유 비밀키를 이용해 통신하는 단계(S500);

를 포함하여 이루어지는 보안키 공유 방법.

청구항 2

제 1항에 있어서, 상기 단말기는,

주변의 단말기들과 단말기 그룹을 이루며,

상기 공유 비밀키는 상기 단말기 그룹 내 단말기들에 공통으로 부여되는 공용 비밀키이거나, 상기 공유 비밀키와 별도로 부여되는 공용 비밀키인 것을 특징으로 하는 보안키 공유 방법.

청구항 3

제 2항에 있어서, 상기 e단계 이후,

f) 경우에 따라 상기 서버가 상기 공용 비밀키를 변경하고, 변경된 공용 비밀키를 상기 단말기 그룹 내 단말기들 각각의 고유 비밀번호로 암호화하여 전송하는 단계(S600);

g) 상기 단말기 그룹 내 단말기가 상기 서버로부터 상기 공용 비밀키를 수신하면 자신의 고유 비밀번호로 복호화하여 변경된 공용 비밀키를 저장하는 단계(S700); 및

h) 상기 단말기 그룹 내 통신 또는 상기 단말기 그룹과 상기 서버 간의 통신 시 상기 공용 비밀키를 이용해 통신하는 단계(S800);

를 더 포함하는 것을 특징으로 하는 보안키 공유 방법.

청구항 4

서버와의 통신 시 보안을 위해 보안키를 공유하기 위한 단말기에 있어서,

시리얼번호 및 고유 비밀번호가 영구 저장된 메모리를 포함하며,

서버에 상기 시리얼번호를 전송하며, 상기 서버로부터 암호화된 공유 비밀키를 수신하면 상기 고유 비밀번호로 복호화하고, 이후 상기 서버와 상기 공유 비밀키를 이용해 통신하는 것을 특징으로 하는 보안키 공유를 위한 단말기.

청구항 5

제 4항에 있어서, 상기 단말기는,

별도로 입력장치가 구비되지 않은 단말기이며, 처음으로 전원이 공급되고 인터넷이 연결되면 자동으로 서버에 상기 시리얼번호를 전송하는 것을 특징으로 하는 보안키 공유를 위한 단말기.

청구항 6

제 4항에 있어서, 상기 단말기는,

주변의 단말기들과 단말기 그룹을 이루며,

상기 단말기 그룹은 상기 서버로부터 공통으로 사용하는 공용 비밀키를 부여받아 상기 단말기 그룹 내 단말기 간의 통신 및 상기 서버와 상기 단말기 그룹 간의 통신을 하는 것을 특징으로 하는 보안키 공유를 위한 단말기.

청구항 7

단말기와의 통신 시 보안을 위해 보안키를 공유하기 위한 서버에 있어서,

상기 단말기에 저장되어 있는 고유 비밀번호와 동일한 비밀번호가 데이터베이스에 저장되어 있으며,

상기 단말기로부터 시리얼번호가 수신되면, 상기 시리얼번호를 이용하여 상기 데이터베이스에서 상기 단말기의 고유 비밀번호를 검색하여 찾고, 통신을 위한 공유 비밀키를 상기 고유 비밀번호로 암호화하여 상기 단말기로 전송하며, 이후 상기 단말기와 상기 공유 비밀키를 이용해 통신하는 것을 특징으로 하는 보안키 공유를 위한 서버.

청구항 8

제 7항에 있어서, 상기 서버는,

특정 단말기 그룹 내 단말기들에 공통으로 동일한 공용 비밀키를 전송하되, 상기 공용 비밀키는 각 단말기의 고유 비밀번호로 암호화하여 전송하며,

상기 단말기 그룹과는 상기 공용 비밀키를 이용해 통신하고, 개별 단말기와는 해당 단말기의 공유 비밀키를 이용해 통신하는 것을 특징으로 하는 보안키 공유를 위한 서버.

청구항 9

제 8항에 있어서, 상기 서버는,

보안 향상을 위해 주기적 또는 비주기적으로 상기 공용 비밀키를 변경하며,변경된 상기 공용 비밀키를 각 단말기의 고유 비밀번호로 암호화하여 전송하는 것을 특징으로 하는 보안키 공유를 위한 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 단말기와 서버 간의 보안키 공유 방법과 이를 위한 단말기 및 서버에 관한 것으로, 더욱 상세하게는 입력장치가 구비되지 않은 소형 가전기기와 같은 단말기와 서버가 통신하기 위해 보안키를 공유하는 방법에 있어서 간단한 방법으로도 보안 기능을 향상시킨 보안키 공유 방법과 이를 위한 단말기 및 서버에 관한 것이다.

배 경 기 술

[0002] 최근 뜨겁게 떠오르고 있는 IT 서비스 중 하나가 바로 사물 인터넷(IoT; Internet of Things)이다.

[0003] 사물 인터넷이란 지능화된 사물들이 연결되어 형성되는 네트워크상에서 사람과 사물, 사물과 사물 간에 상호 소통하고 상황인식 기반의 지식이 결합되어 지능적인 서비스를 제공하는 인프라로 정의할 수 있다. 최근에는 IoT 중 사물을 뜻하는 'T'hings를 넘어서 인간까지 포함하는 Io'E'everything으로까지 그 개념이 확장되어 가고 있다. 사물 인터넷의 가장 큰 특징은 단순히 인터넷으로 사물들이 연결된 것이 아니라 사물 스스로 주고받은 데이터를 가지고 '사고'를 한다는 것이다.

[0004] 구체적인 예로, 냉장고가 스스로 부족한 식재료를 마트에 주문하고 세탁기는 스스로 고장을 체크하고 사용자의 스케줄을 확인하여 AS기사와의 약속까지 잡아 사용자에게 알려주는 등 영화에서만 볼 수 있었던 일이 점점 실현 가능해지고 있다.

[0005] 만약, 가전제품과 같은 단말기가 인터넷과 연결되어 서버 또는 다른 단말기와 통신하여 데이터를 주고받는 과정에 있어서, 데이터가 암호화 되어있지 않다면 외부에서 데이터의 내용을 쉽게 파악할 수 있고 무단으로 변조할 수도 있는 등의 문제가 있다. 따라서, 통신 과정에서 데이터의 보안이 필수적이라고 할 수 있다.

[0006] 종래에 흔히 사용되고 있는 보안 방법은 단말과 서버 간의 비밀키로 통신하는 것이다. 그러나 이 방법은 처음 비밀키를 생성하고 이를 상대방에 전송하는 과정에서 비밀키가 노출될 위험이 크다. 또 다른 방법으로는 비대칭 암호화 방법으로, 단말과 서버가 각각 공개키와 비밀키 한 쌍을 가지고 통신하는 방법이다. 공개키를 이용해 암호화하면 비밀키로 해석할 수 있어, 보안성이 향상되는 장점이 있으나, 데이터를 해석하는데 많은 조작이 필요하기 때문에 간단한 소형 기기에는 적합하지 않은 문제가 있다.

[0007] 즉, 사물 인터넷 환경에서 단말과 서버 간 데이터 통신에 적용할 수 있는 단순하면서도 보안성이 우수한 보안 방법이 요구되고 있는 실정이다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국공개특허 제 10-2008-0078555호("보안 데이터 송수신 시스템 및 방법")

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기한 문제점을 해결하기 위하여 안출된 것으로, 본 발명의 목적은 사물인터넷 환경 하에서 안전한 통신을 위해 소형 가전기기와 같은 단말기와 서버 간의 보안키를 공유하는 방법과 이를 위한 단말기 및 서버를 제공하는 것이다.

[0010] 특히, 미리 지정된 단말기들의 그룹을 설정하고, 해당 단말기 그룹에 공통으로 공유 비밀키를 부여함으로써, 보다 효율적인 통신이 가능하도록 한 보안키 공유 방법과 이를 위한 단말기 및 서버를 제공하는 것이다.

과제의 해결 수단

[0011] 본 발명은 단말기와 서버 간의 보안키를 공유 방법에 있어서, a) 단말기가 자신의 시리얼번호를 서버로 송신하는 단계; b) 상기 서버가 상기 단말기로부터 수신된 상기 시리얼번호를 이용하여 서버의 데이터베이스에서 상기 단말기의 고유 비밀번호를 검색하여 찾는 단계; c) 상기 서버가 상기 단말기와의 통신을 위한 공유 비밀키를 해당 단말기의 상기 고유 비밀번호로 암호화하여 상기 단말기로 전송하는 단계; d) 상기 단말기가 상기 서버로부터 수신된 암호화된 상기 공유 비밀키를 상기 단말기에 저장되어 있는 상기 고유 비밀번호로 복호화하는 단계; 및 e) 상기 서버 및 상기 단말기가 상기 공유 비밀키를 이용해 통신하는 단계;를 포함하여 이루어질 수 있다.

[0012] 이때, 상기 단말기는 주변의 단말기들과 단말기 그룹을 이루며, 상기 공유 비밀키는 상기 단말기 그룹 내 단말기들에 공통으로 부여되는 공용 비밀키이거나, 상기 공유 비밀키와 별도로 부여되는 공용 비밀키일 수 있다.

[0013] 또한, 상기 e단계 이후, f) 경우에 따라 상기 서버가 상기 공용 비밀키를 변경하고, 변경된 공용 비밀키를 상기 단말기 그룹 내 단말기들 각각의 고유 비밀번호로 암호화하여 전송하는 단계; g) 상기 단말기 그룹 내 단말기가 상기 서버로부터 상기 공용 비밀키를 수신하면 자신의 고유 비밀번호로 복호화하여 변경된 공용 비밀키를 저장하는 단계; h) 상기 단말기 그룹 내 통신 또는 상기 단말기 그룹과 상기 서버 간의 통신 시 상기 공용 비밀키를 이용해 통신하는 단계;를 더 포함할 수 있다.

[0014] 한편, 본 발명은 서버와의 통신 시 보안을 위해 보안키를 공유하기 위한 단말기에 있어서, 시리얼번호 및 고유 비밀번호가 영구 저장된 메모리를 포함하며, 서버에 상기 시리얼번호를 전송하며, 상기 서버로부터 암호화된 공유 비밀키를 수신하면 상기 고유 비밀번호로 복호화하고, 이후 상기 서버와 상기 공유 비밀키를 이용해 통신할 수 있다.

[0015] 이때, 상기 단말기는 별도로 입력장치가 구비되지 않은 단말기이며, 처음으로 전원이 공급되고 인터넷이 연결되면 자동으로 서버에 상기 시리얼번호를 전송할 수 있다.

[0016] 또한, 상기 단말기는 주변의 단말기들과 단말기 그룹을 이루며, 상기 단말기 그룹은 상기 서버로부터 공통으로 사용하는 공용 비밀키를 부여받아 상기 단말기 그룹 내 단말기 간의 통신 및 상기 서버와 상기 단말기 그룹 간의 통신을 할 수 있다.

[0017] 또한, 본 발명은 단말기와의 통신 시 보안을 위해 보안키를 공유하기 위한 서버에 있어서, 상기 단말기에 저장되어 있는 고유 비밀번호와 동일한 비밀번호가 저장되어 있으며, 상기 단말기로부터 시리얼번호가 수신되면, 상기 시리얼번호를 이용하여 서버의 데이터베이스에서 상기 단말기의 고유 비밀번호를 검색하여 찾고, 통신을 위한 공유 비밀키를 상기 고유 비밀번호로 암호화하여 상기 단말기로 전송하며, 이후 상기 단말기와 상기 공유 비밀키를 이용해 통신할 수 있다.

[0018] 이때, 상기 서버는 특정 단말기 그룹 내 단말기들에 공통으로 동일한 공용 비밀키를 전송하되, 상기 공용 비밀키는 각 단말기의 고유 비밀번호로 암호화하여 전송하며, 상기 단말기 그룹과는 상기 공용 비밀키를 이용해 통신하고, 개별 단말기와는 해당 단말기의 공유 비밀키를 이용해 통신할 수 있다.

[0019] 아울러, 상기 서버는 보안 향상을 위해 주기적 또는 비주기적으로 상기 공용 비밀키를 변경하며, 변경된 상기 공용 비밀키를 각 단말기의 고유 비밀번호로 암호화하여 전송할 수 있다.

발명의 효과

[0020] 종래의 대칭 비밀키 방법은 처음에 암호화 없이 비밀키를 전달받기 때문에 이 과정에서 비밀키가 노출될 위험이 큰 문제가 있었으며, 비대칭 공개키/비밀키 방법은 보안성은 뛰어나나 암호화/복호화 과정이 복잡하기 때문에 단순 기능을 하는 단말기들에 적용하기에는 적절하지 못한 문제가 있었다.

[0021] 본 발명은 이러한 문제들을 모두 해결할 수 있는 보안키 공유 방법으로, 단말기가 제작될 때부터 서버와 통신할 수 있도록 하기 위해 시리얼번호 및 고유 비밀번호를 영구적으로 저장하며, 처음으로 전원이 연결되면 자동으로 서버에 접속하여 공유 비밀키를 수신하고, 공유 비밀키를 이용해 서버와 통신하는 것으로, 매우 간단한 방법이지만 보안성이 굉장히 우수한 장점이 있다. 즉, 단말기가 서버로 전송하는 시리얼번호는 외부로 노출될 가능성이 있지만, 고유 비밀번호는 서버와 단말기만 알고 있기 때문에 공유 비밀키 전송 시 고유 비밀번호로 암호화되는 공유 비밀키가 노출될 위험이 매우 낮다.

[0022] 아울러, 서버가 공용 비밀키를 필요에 따라 변경함으로써 보안을 더욱 향상시킬 수 있으며 변경 방법도 고유 비밀번호를 이용함으로써 간단하면서도 안전한 효과가 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 일실시예에 따른 보안키 공유 과정을 나타낸 도면.

도 2는 도 1의 보안키 공유 방법에 따른 전체 시스템을 나타낸 개략구성도.

발명을 실시하기 위한 구체적인 내용

[0024] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명한다. 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 게시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 게시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0025] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0026] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.

[0027] 본 발명은 단말기와 서버 간의 보안키를 공유 방법에 관한 것이다.

[0028] 먼저, 본 발명에서 의미하는 단말기는 유무선 네트워크를 통해 통신이 가능하도록 구비된 가전기기이다. 유무선 네트워크는 유선통신 외에 와이파이(Wireless Fidelity), 지그비(Zigbee), 블루투스(Bluetooth), NFC(Near Field Communication) 등 다양한 방식의 무선통신일 수 있다.

[0029] 이때, 통신이 가능한 가전기기는 구체적으로 냉장고, 오븐, 세탁기, 청소기, 프린터, 팩스, 복합기, 웹캠, 텔레비전, 비디오, 디브이디 플레이어, 오디오, 인터폰, 에어컨, 히터, 제습기 등 모든 가전기기일 수 있다.

[0030] 최근 통신, 반도체 기술의 발전으로 인하여 통신 칩이 매우 소형화 되고 있고, 이들 가전기기는 특히 전원을 꾸준하게 인가받을 수 있는 환경 하에 있는 경우가 많고, 기기 자체의 크기가 일반적인 모바일디바이스에 비해서 큰 경우가 많으므로, 가전기기에 통신기능을 탑재하는 것이 최근 전 세계 모든 전자회사들의 주요 관심사가 되고 있다.

[0031] 특히, 사물인터넷 개념이 대두됨에 따라 모든 가전기기에 통신기능이 탑재되어 서버와 통신하거나 가전기기들간 통신을 하며, 이때 가전기기 스스로 주변 환경을 감지(sensing)하여 데이터를 송수신하고 서버로부터 제어신호를 받는 등의 기능이 수행되고 있다.

[0032] 현재, 이러한 데이터 송수신 시 보안이 취약하여 외부에서 데이터 내용을 쉽게 파악할 수 있으며 무단 변조가 가능한 경우가 많고, 반대로 암호화 기술이 복잡하여 단순 기능을 하는 소형 단말기에는 적용되지 못하는 문제가 있다.

[0033] 더 나아가, 점차 기술이 발전할수록 통신 데이터량이 급증하기 때문에, 비교적 단순한 방법으로도 보안성을 높일 수 있는 보안 방법에 대한 필요성이 커지고 있다.

[0034] 본 발명은 이와 같은 사물인터넷 환경 하에서 이루어지는 데이터 송수신 과정에 적용할 수 있는 간단하면서도 안전성이 뛰어난 보안 방법을 제공하려는 것이다.

[0035] 도 1은 본 발명의 일실시예에 따른 보안키 공유 과정을 나타낸 도면이며, 도 2는 도 1의 보안키 공유 방법에 따른 전체 시스템을 나타낸 개략구성도이다. 이하, 본 발명의 기술적 사상을 첨부된 도면을 사용하여 더욱 구체적으로 설명한다.

[0036] 첨부된 도면은 본 발명의 기술적 사상을 더욱 구체적으로 설명하기 위하여 도시한 일예에 불과하므로 본 발명의 기술적 사상이 첨부된 도면의 형태에 한정되는 것은 아니다.

[0037] 도 1에 도시된 바와 같이, 본 발명의 일실시예에 따른 보안키 공유 방법은 하기의 a ~ e단계를 포함하여 구성될 수 있다.

[0038] a단계는 단말기(10)가 자신의 시리얼번호를 서버(20)로 송신하는 단계(S100)이다. 이때, 단말기(10)에는 자신의 시리얼번호와 함께 고유 비밀번호가 메모리상에 영구 저장되어 있다. 또한, 처음으로 전원이 공급되고 네트워크를 통해 서버(20)와 연결되면 자동으로 서버(20)에 자신의 시리얼번호를 전송하도록 설정되어 있을 수 있다.

[0039] 이후, b단계에서 서버(20)가 단말기(10)로부터 시리얼번호를 수신하면, 수신된 시리얼번호를 이용하여 서버의 데이터베이스에서 해당 단말기(10)의 고유 비밀번호를 검색하여 찾는다.(S200).

[0040] 다음으로 c단계에서 서버(20)가 단말기(10)와의 통신을 위한 공유 비밀키를 생성하고, 생성된 공유 비밀키를 해당 단말기(10)의 고유 비밀번호를 이용하여 암호화하여 단말기(10)로 전송한다(S300).

[0041] 여기서, 고유 비밀번호는 앞서 언급한 바와 같이 단말기(10)에 영구 저장된 번호로, 서버(20)의 데이터베이스에도 동일한 고유 비밀번호가 단말기(10)의 시리얼번호와 연계되어 저장되어 있다. 따라서 서버(20)는 공유 비밀키를 해당 단말기(10)의 고유 비밀번호로 암호화하여 단말기(10)로 전송한다.

[0042] 이어지는 d단계에서 단말기(10)가 서버(20)로부터 수신된 암호화된 공유 비밀키를 단말기(10)에 저장되어 있는 고유 비밀번호로 복호화한다(S400).

[0043] 상기한 과정을 통해 서버(20)와 단말기(10) 간의 공유 비밀키(보안키) 공유가 이루어지면 이후 e단계에서 단말기(10)와 서버(20)가 공유 비밀키를 이용하여 상호 간 통신하게 된다(S500). 즉, 단말기(10)는 서버(20)로부터 암호화된 공유 비밀키를 수신하면 고유 비밀번호로 복호화하고, 이후 서버(20)와 공유 비밀키를 이용해 통신하게 되는 것이다.

[0044] 종래의 대칭 비밀키 방법은 처음에 암호화없이 비밀키를 전달받기 때문에 이 과정에서 비밀키가 노출될 위험이 큰 문제가 있었으며, 비대칭 공개키/비밀키 방법은 보안성은 뛰어나나 암호화/복호화 과정이 복잡하기 때문에 단순 기능을 하는 단말기들에 적용하기에는 적절하지 못한 문제가 있었다. 그러나, 본 발명은 이러한 문제들을 모두 해결할 수 있는 보안키 공유 방법으로, 단말기가 제작될 때부터 서버와 통신할 수 있도록 하기 위해 시리얼번호 및 고유 비밀번호를 영구적으로 저장하며, 처음으로 전원이 공급되고 네트워크에 연결되면 자동으로 서버에 접속하여 공유 비밀키를 수신하고, 공유 비밀키를 이용해 서버와 통신하는 것으로, 매우 간단한 방법이지만 보안성이 굉장히 우수한 방법이다. 즉, 단말기가 a단계에서 전송하는 시리얼번호는 외부로 노출될 가능성이 있지만, 고유 비밀번호는 서버와 단말기만 알고 있기 때문에 공유 비밀키 전송 시 고유 비밀번호로 암호화되는 공유 비밀키가 노출될 위험이 매우 낮은 장점이 있다.

[0045] 특히, 본 발명은 별도로 키보드나 마우스와 같은 입력장치가 구비되지 않은 단말기에 적용되는 것이 가장 적합하다. 예를 들어, 단말기가 콘센트라고 하면, 콘센트는 주기적으로 또는 서버의 요청에 따라 서버에 자신의 현재 상태(사용중/비사용중)를 전송하고, 서버가 일정 시간 이상 콘센트가 사용되고 있지 않다고 판단하면 콘센트의 전원을 차단할 수 있다. 또한, 외부의 사용자가 통신기기를 사용하여 서버에 접속하고, 서버에 특정한 신호를 보낼 수 있으며, 해당 신호에 따라 단말기에 동작명령 및 정보요청명령 등을 요청할 수 있다.

[0046] 즉, 콘센트나 전등과 같은 단순 On/Off 동작을 하는 단말기의 경우 입력장치가 구비되지 않았음에도 서버와 연결되어 데이터를 안전하게 송수신할 수 있는 장점이 있다.

[0047] 한편, 본 발명은 도 1 및 도 2에 도시된 것처럼, 주변의 단말기들과 단말기 그룹(100)을 이룰 수 있다. 이때, 단말기 그룹(100)은 동일/유사한 기능을 갖는 단말기를 모아놓은 그룹이거나, 서로 연계되어 동작할 수 있는 단말기를 모아놓은 그룹일 수 있다.

[0048] 이와 같이 단말기들이 어느 단말기 그룹(100)에 속하게 되는 경우, 단말기가 서버로부터 수신하는 공유 비밀키는 단말기 그룹(100)에 공통으로 부여되는 공용 비밀키일 수 있다. 또한 공유 비밀키와 별도로 단말기 그룹(100) 별로 사용하는 공용 비밀키를 추가적으로 부여할 수도 있다.

[0049] 즉, 단말기 그룹(100)은 서버로부터 공통으로 사용하는 공용 비밀키를 부여받아 단말기 그룹 내 단말기 간의 통신과 서버와 단말기 그룹 간의 통신을 함에 있어서, 공용 비밀키로 암호화/복호화하는 것이다.

[0050] 서버는 특정 단말기 그룹(100) 내 단말기들에 공통으로 동일한 공용 비밀키를 전송하되, 이때 공용 비밀키는 각 단말기의 고유 비밀번호로 암호화하여 전송한다. 서버는 단말기 그룹(100)과 공용 비밀키를 이용해 통신하고, 개별 단말기와는 해당 단말기의 공유 비밀키를 이용해 통신할 수 있다.

[0051] 예를 들어, 단말기 그룹(100)이 조명들을 모아놓은 그룹이라면, 각 조명(단말기)은 서버로부터 각 고유 비밀번호로 암호화된 공용 비밀키를 수신하게 된다. 따라서 서버는 조명을 On/Off하는 명령을 공용 비밀키로 암호화하여 전송하면, 그룹 내 조명 전체를 동시 제어할 수 있다.

[0052] 또한, 공용 비밀키를 통해 그룹 내 조명들 간의 통신이 이루어질 수 있다. 예를들어, 각 조명은 다른 조명들이 어디에 위치하고 있는지 현재 작동하고 있는지 알고 있으며, 다른 조명들과 연계하여 외부의 조도에 따라서 각 조명들 간의 밝기를 자동 조절하도록 제어될 수도 있다.

[0053] 한편, 서버는 보안 향상을 위해 주기적 또는 비주기적으로 공용 비밀키를 변경하며, 변경된 공용 비밀키는 각 단말기의 고유 비밀번호로 암호화하여 전송한다. 단말기가 이를 복호화하여 변경된 공용 비밀키를 적용하여 이후 통신이 이루어지게 된다.

[0054] 즉, 도 1에 도시된 것처럼, 본 발명의 일실시예에 따른 방법에서 e단계 이후 공용 비밀키를 변경하는 f ~ h단계를 더 포함할 수 있다.

[0055] f단계는 경우에 따라 서버가 공용 비밀키를 변경하고, 변경된 공용 비밀키를 단말기 그룹 내 단말기들 각각의 고유 비밀번호로 암호화하여 전송하는 단계이다(S600). 이때, 공용 비밀키 변경은 주기적으로 수행될 수도 있으며, 사용자의 요청 등에 의해 비주기적으로 수행될 수도 있다.

[0056] 다음으로 g단계에서 단말기 그룹 내 단말기가 서버로부터 공용 비밀키를 수신하면 자신의 고유 비밀번호로 복호화하여 변경된 공용 비밀키를 저장하고(S700), 마지막 h단계에서 단말기 그룹 내 통신 또는 단말기 그룹과 서버 간의 통신 시 공용 비밀키를 이용해 통신한다(S800).

[0057] 즉, 상술한 것처럼, 공용 비밀키를 필요에 따라 변경함으로써 보안을 더욱 향상시킬 수 있으며 변경 방법도 고유 비밀번호를 이용함으로써 간단하면서도 안전한 효과가 있다.

[0058] 본 발명은 상기한 실시예에 한정되지 아니하며, 적용범위가 다양함은 물론이고, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 다양한 변형 실시가 가능한 것은 물론이다.

부호의 설명

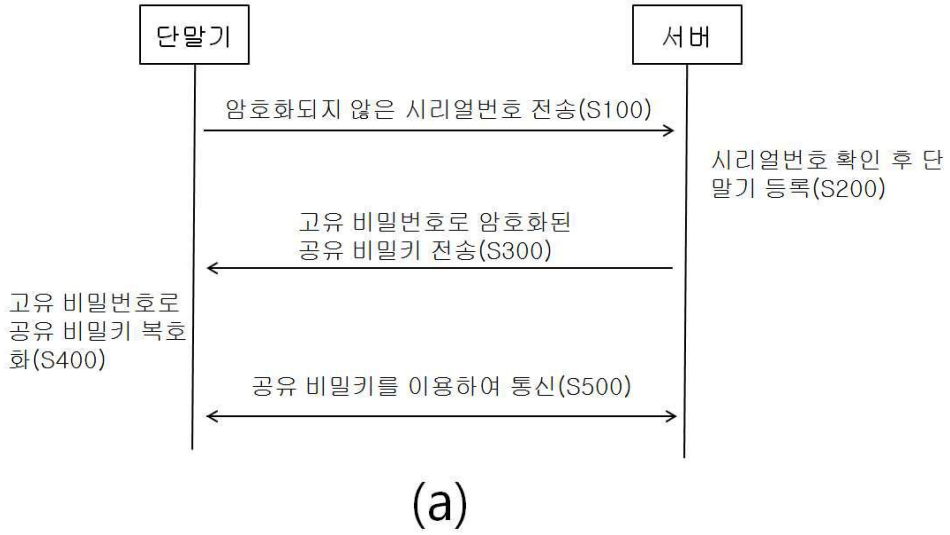
[0059] 10 : 단말기

20 : 서버

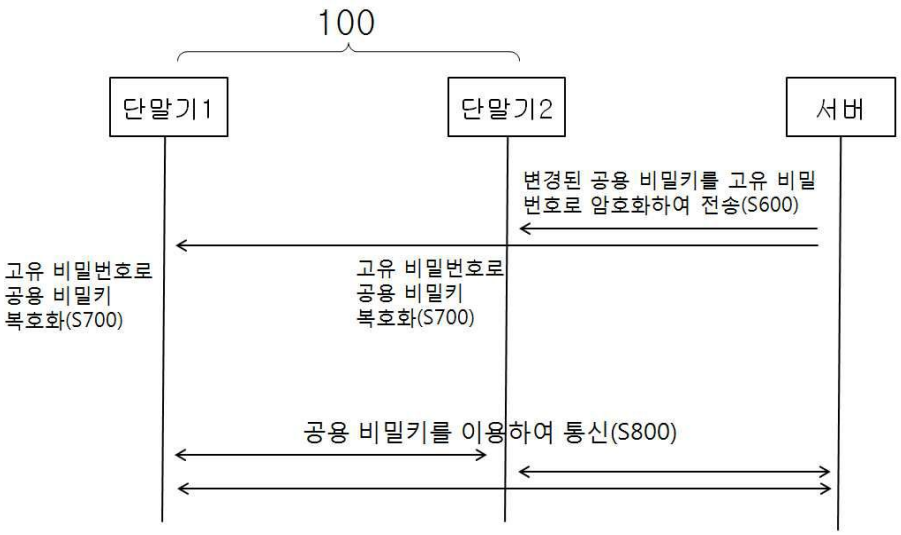
100 : 단말기 그룹

도면

도면1


단말기
서버
암호화되지 않은 시리얼번호 전송(S100)
시리얼번호 확인 후 단말기 등록(S200)
고유 비밀번호로 암호화된 공유 비밀키 전송(S300)
고유 비밀번호로 공유 비밀키 복호화(S400)
공유 비밀키를 이용하여 통신(S500)

(a)


100
단말기1
단말기2
서버
변경된 공용 비밀키를 고유 비밀번호로 암호화하여 전송(S600)
고유 비밀번호로 공용 비밀키 복호화(S700)
고유 비밀번호로 공용 비밀키 복호화(S700)
공용 비밀키를 이용하여 통신(S800)

(b)

도면2