(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0091566
(43) 공개일자 2013년08월19일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01)
(21) 출원번호 10-2012-0012949
(22) 출원일자 2012년02월08일
심사청구일자 2012년02월08일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스 내 (서천동, 경희대학교)
(72) 발명자
홍충선
경기도 용인시 수지구 상현동 성원상떼빌아파트 233동 101호
송태일
서울특별시 강서구 방화3동 동성아파트 105동 1304호
(뒷면에 계속)
(74) 대리인
서재승

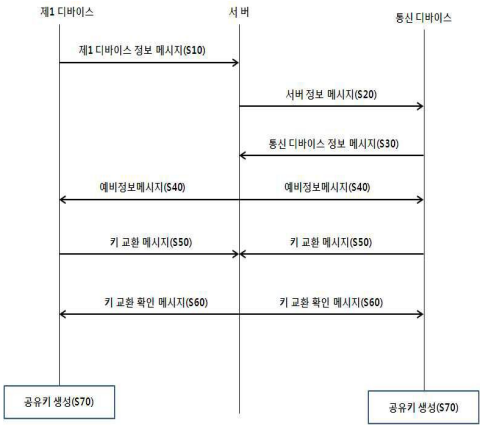
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 **통신 네트워크에서 신뢰성 있는 서버를 이용한 통신 그룹의 공유 키 교환 방법**

(57) 요 약

본 발명은 무선 통신 네트워크에서 서버를 통해 디바이스의 공유 키를 교환하는 방법에 관한 것으로, 보다 구체적으로 다수의 디바이스 중 그룹 통신을 요청하는 제1 디바이스로부터 그룹 통신 요청 메시지를 수신하는 경우 서버를 통해 그룹 통신 디바이스와 제1 디바이스 사이에 시드키를 송수신하여 제1 디바이스와 그룹 통신 디바이스 사이의 공유키를 교환하며, 공유키를 주기적으로 갱신하여 허가받지 않은 제3자가 공유키를 해킹하는 것을 방지하며 통신 그룹에서 탈퇴하는 디바이스가 존재하는 경우 통신 그룹을 구성하는 디바이스 사이에서 시드키를 서버로 송수신하여 통신 그룹을 구성하는 디바이스 사이의 공유키를 갱신하여 통신 그룹을 구성하는 디바이스 사이에서 공유키를 교환하는 방법에 관한 것이다.

대 표 도 - 도3



(72) 발명자

조응준

경기도 수원시 영통구 영통동 1029-12번지 103호

강형규

제주특별자치도 서귀포시 하효동 212번지

이준

전라북도 전주시 완산구 삼천동 오성아파트 101동 302호

이 발명을 지원한 국가연구개발사업

과제고유번호	KI002164
부처명	지식경제부
연구사업명	산업원천기술개발사업
연구과제명	센싱기반 감성 서비스 모바일 단말 기술개발
주관기관	한국산업기술대학교 산학협력단
연구기간	2011.03.01 ~ 2012.02.28

특허청구의 범위

청구항 1

안전한 채널로 접속되어 있는 서버와 다수의 디바이스를 구비하는 통신 시스템에서 상기 서버를 통한 상기 디바이스 사이의 공유 키 교환 방법에 있어서,

(a) 상기 다수의 디바이스 중 제1 디바이스에서 생성된 제1 시드값과 상기 제1 디바이스가 통신 요청하는 통신 디바이스의 정보를 수신하는 단계;

(b) 상기 서버로부터 상기 통신 디바이스로 상기 서버의 시드값과 상기 서버 정보를 송신하는 단계;

(c) 상기 통신 디바이스에서 각각 생성된 시드값과 상기 통신 디바이스의 정보를 상기 서버에서 수신하는 경우, 상기 제1 디바이스 또는 상기 통신 디바이스의 시드값으로부터 생성한 예비 그룹 시드값 및 상기 제1 디바이스 또는 상기 통신 디바이스의 예비 통신 그룹 정보를 상기 제1 디바이스와 상기 통신 디바이스에 각각 송신하는 단계;

(d) 상기 서버에서 상기 제1 디바이스 또는 상기 통신 디바이스에서 생성한 그룹 시드값, 통신 그룹 정보 및 서버 정보를 구비하는 키 교환 메시지를 수신하는 경우, 상기 키 교환 메시지에 기초하여 상기 제1 디바이스와 상기 통신 디바이스 사이에서 교환된 키의 동일성을 판단하고 키 교환 확인 메시지를 상기 제1 디바이스와 상기 통신 디바이스에 각각 송신하는 단계를 포함하며,

상기 제1 디바이스와 상기 통신 디바이스는 상기 키 교환 확인 메시지에 기초하여 상기 제1 디바이스와 상기 통신 디바이스 사이에서 서로 공유하는 공유 키를 생성하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 2

제 1 항에 있어서, 상기 키 교환 방법은

상기 다수의 디바이스 중 제1 디바이스와 상기 서버 사이에서 공유하는 비밀키(XY)로 암호화된 상기 제1 디바이스의 패스워드를 상기 제1 디바이스로부터 수신하여 상기 제1 디바이스의 패스워드를 상기 서버에 등록하는 단계를 더 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 3

제 2 항에 있어서, 상기 제1 디바이스의 패스워드를 상기 서버에 등록하는 단계는

상기 제1 디바이스에서 생성한 제1 행렬(X)과 제1 행렬의 의사역행렬(X')의 곱을 상기 제1 디바이스로부터 수신하는 단계;

상기 서버에서 생성한 제2 행렬(Y)과 제2 행렬의 의사역행렬(Y')과 상기 제1 행렬(X) 및 제1 행렬의 의사역행렬(X')의 곱으로부터 행렬 조합(XX'Y, XX'YY')를 생성하고 제1 디바이스로 송신하여 상기 제1 디바이스에게 상기 서버의 공유 비밀키(Y)를 제공하는 단계;

상기 제1 디바이스로부터 수신한 행렬 조합(XYY')으로부터 상기 제1 디바이스의 공유 비밀키(X)를 획득하고, 상기 제1 디바이스와 상기 서버의 공유 비밀키(XY)로 상기 제1 디바이스의 시드 생성값(M)을 암호화하여 상기 제1 디바이스로 송신하는 단계; 및

상기 공유 비밀키(XY)로 암호화된 상기 제1 디바이스의 패스워드를 상기 제1 디바이스로부터 수신하여 상기 제1 디바이스를 상기 서버에 등록하는 단계를 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 4

제 3 항에 있어서, 상기 제1 디바이스는 시드 생성값(M)과 상기 시드 생성값(M)의 해쉬값을 구비하는 등록 메시지를 상기 공유 비밀키(XY)로 암호화하여 상기 서버로 송신하며,

상기 서버는 공유 비밀키(XY)로 상기 등록 메시지를 복호화하며, 상기 복호화된 시드 생성값과 상기 시드 생성값의 해쉬값을 비교하여 상기 등록 메시지의 무결성을 판단하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 5

제 1 항에 있어서, 상기 (a) 단계는

상기 서버에서 상기 제1 디바이스로부터 그룹통신 요청 메시지를 수신하는 단계;

상기 서버에서 상기 그룹통신 요청 메시지에 구비되어 있는 상기 제1 디바이스 식별자에 기초하여 상기 제1 디바이스가 상기 서버에 등록된 디바이스인지 검증하는 단계;

상기 서버에서 검증 결과에 따라 상기 제1 디바이스로 상기 서버에 등록된 디바이스 중 통신 가능한 통신 가능 디바이스 정보를 송신하는 단계; 및

상기 제1 디바이스로부터 상기 제1 디바이스에서 생성된 제1 시드값를 구비하는 상기 제1 디바이스의 시드 조합값(A_1)과 상기 통신 가능 디바이스 중 상기 제1 디바이스가 통신 요청하는 통신 디바이스 정보를 수신하는 단계를 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 6

제 5 항에 있어서, 상기 제1 디바이스의 시드 조합값(A_1)은 아래의 수학식(1)에 의해 생성되며,

[수학식 1]

$$A_1 = g^{x_1} \cdot M_1 \cdot pw_1$$

여기서 g^{x_1} 은 상기 제1 디바이스에서 생성한 제1 시드값이며, M_1은 상기 서버에서 생성하여 상기 제1 디바이스로 제공된 제1 시드 생성값이며, pw_1은 제1 디바이스의 패스워드인 것을 특징으로 하는 공유 키 교환 방법.

청구항 7

제 1 항에 있어서, 상기 (b) 단계는

상기 통신 디바이스 정보에 기초하여 상기 서버에 등록된 통신 가능 디바이스 중 상기 제1 디바이스가 통신 요청한 통신 디바이스와 상기 제1 디바이스로 통신 그룹을 생성하는 단계;

상기 서버에서 서버 시드값을 생성하고 상기 통신 디바이스에 해당하는, 상기 서버 시드값을 구비하는 서버 시드 조합값(B_i)을 생성하는 단계;

상기 통신 디바이스로 서버 시드 조합값과 상기 서버 정보 및 상기 서버 시드값과 상기 서버 정보의 해쉬값을 송신하는 단계를 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 8

제 7 항에 있어서,

상기 서버 시드 조합값(B_i)은 아래의 수학식(2)에 의해 생성되며,

[수학식 2]

$$B_i = g^{G} \cdot M_i \cdot pw_i$$

여기서 g^{G} 은 상기 서버 시드값이며, M_i은 상기 서버에서 생성하여 상기 통신 디바이스에 각각 제공된 시드 생성값이며, pw_i은 통신 디바이스 각각의 패스워드인 것을 특징으로 하는 공유 키 교환 방법.

청구항 9

제 1 항에 있어서, 상기 (c) 단계는

상기 통신 디바이스로부터 수신한 상기 통신 디바이스의 시드 조합값에서 상기 통신 디바이스의 시드값을 획득하는 단계;

상기 제1 디바이스 또는 상기 통신 디바이스가 보유하고 있는 시드값을 제외한 상기 제1 디바이스 및 상기 통신 디바이스의 시드값으로부터 상기 제1 디바이스 및 상기 통신 디바이스 각각에 대한 예비 그룹 시드값(G_i)을 계산하는 단계;

상기 제1 디바이스 및 상기 통신 디바이스에서 자신을 제외한 디바이스 정보로 상기 제1 디바이스 및 상기 통신 디바이스 각각에 대한 예비 통신 그룹 정보(K_i)를 생성하는 단계;

상기 제1 디바이스로 상기 제1 디바이스에 해당하는 상기 예비 그룹 시드값을 구비하는 예비 그룹 시드 조합값, 상기 예비 통신 그룹 정보 및 상기 서버의 시드 조합값을 송신하는 단계;

상기 통신 디바이스로 상기 통신 디바이스 각각에 해당하는 상기 예비 그룹 시드값을 구비하는 예비 그룹 시드 조합값과 상기 예비 통신 그룹 정보를 상기 통신 디바이스로 각각 송신하는 단계를 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 10

제 1 항에 있어서, 상기 (d) 단계는

상기 서버에서 상기 제1 디바이스 및 상기 통신 디바이스에서 각각 생성한, 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G) 순서의 해쉬 함수값의 키 교환 메시지를 수신하는 단계;

상기 키 교환 메시지의 해쉬 함수값과 상기 서버가 보유하고 있는 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)의 해쉬 함수값을 비교하여 상기 제1 디바이스와 상기 통신 디바이스 사이에서 교환된 키의 동일성을 판단하는 단계; 및

상기 동일성 판단 결과에 따라 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G) 순서의 해쉬 함수값의 키 교환 확인 메시지를 상기 제1 디바이스와 상기 통신 디바이스로 각각 송신하는 단계를 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 11

제 1 항에 있어서, 상기 공유 키 교환 방법은

(e) 상기 통신 그룹의 각 디바이스로부터 수신한 갱신 키 교환 메시지에 기초하여 상기 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하고 판단 결과에 따라 갱신 키 교환 확인 메시지를 상기 통신 그룹의 디바이스로 송신하여 상기 통신 그룹의 디바이스 사이의 공유 키를 갱신하는 단계를 더 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 12

제 11 항에 있어서, 상기 공유 키를 갱신하는 단계는

상기 서버에서 상기 통신 그룹의 디바이스에게 공유 키 갱신 메시지를 송신하고 상기 공유 키 갱신 메시지에 응답하여 상기 통신 그룹의 디바이스 각각으로부터 각 디바이스의 시드키를 수신하는 단계;

상기 수신한 각 디바이스의 시드키로부터 상기 통신 그룹의 각 디바이스가 보유하고 있는 시드값을 제외한 시드값으로부터 상기 통신 그룹 디바이스 각각에 대한 갱신 예비 그룹 시드값과, 상기 통신 그룹의 디바이스에서 자신을 제외한 디바이스 정보로 상기 통신 그룹 디바이스 각각에 대한 갱신 예비 통신 그룹 정보(K_i)를 생성하는 단계;

상기 통신 그룹 디바이스 각각에 해당하는 갱신 예비 그룹 시드값과 상기 갱신 예비 통신 그룹 정보를 상기 통신 그룹 디바이스 각각에 송신하는 단계;

상기 갱신 예비 그룹 시드값과 상기 갱신 예비 통신 그룹 정보에 기초하여 상기 통신 그룹 디바이스 각각에서 생성한 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 메시지를 수신

하는 단계;

상기 갱신 키 교환 메시지의 해쉬 함수값과 상기 서버가 보유하고 있는 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)의 해쉬 함수값을 비교하여 상기 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하는 단계;

상기 동일성 판단 결과에 따라 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 확인 메시지를 상기 통신 그룹의 디바이스로 송신하는 단계를 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 13

제 11 항에 있어서, 상기 공유 키 교환 방법은

(f)상기 통신 그룹의 디바이스 중 탈퇴 디바이스로부터 탈퇴 요청 메시지를 수신하는 경우, 상기 서버에 등록되어 있는 통신 그룹 정보를 갱신하고 상기 탈퇴 디바이스로 탈퇴 완료 메시지를 송신하는 단계를 더 포함하며,

상기 탈퇴 완료 메시지의 송신 후, 상기 (e) 단계를 수행하여 상기 통신 그룹 디바이스 사이의 공유 키를 갱신하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 14

제 13 항에 있어서, 상기 (f) 단계는

상기 통신 그룹의 디바이스 중 탈퇴 디바이스로부터 탈퇴 디바이스의 식별자를 구비하는 탈퇴 요청 메시지를 수신하는 단계;

상기 탈퇴 요청 메시지에 응답하여 상기 탈퇴 디바이스를 삭제하여 상기 서버에 등록되어 있는 통신 그룹 정보를 갱신하는 단계; 및

상기 통신 그룹 정보의 갱신이 완료된 후, 상기 탈퇴 디바이스에게 탈퇴 완료 메시지를 송신하는 단계를 더 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 15

안전한 채널로 접속되어 있는 서버와 다수의 디바이스를 구비하는 통신 시스템에서 상기 서버를 통한 상기 디바이스 사이의 공유 키 교환 방법에 있어서,

상기 서버에서 상기 다수의 디바이스 중 통신 그룹의 디바이스에게 공유 키 갱신 메시지를 송신하고 상기 공유 키 갱신 메시지에 응답하여 상기 통신 그룹의 디바이스 각각으로부터 각 디바이스의 시드키를 수신하는 단계;

상기 수신한 각 디바이스의 시드키로부터 상기 통신 그룹의 각 디바이스가 보유하고 있는 시드값을 제외한 시드값으로부터 상기 통신 그룹 디바이스 각각에 대한 갱신 예비 그룹 시드값과, 상기 통신 그룹의 디바이스에서 자신을 제외한 디바이스 정보로 상기 통신 그룹 디바이스 각각에 대한 갱신 예비 통신 그룹 정보(K_i)를 생성하는 단계;

상기 통신 그룹 디바이스 각각에 해당하는 갱신 예비 그룹 시드값과 상기 갱신 예비 통신 그룹 정보를 상기 통신 그룹 디바이스 각각에 송신하는 단계;

상기 갱신 예비 그룹 시드값과 상기 갱신 예비 통신 그룹 정보에 기초하여 상기 통신 그룹 디바이스 각각에서 생성한 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 메시지를 수신하는 단계;

상기 갱신 키 교환 메시지의 해쉬 함수값과 상기 서버가 보유하고 있는 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)의 해쉬 함수값을 비교하여 상기 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하는 단계;

상기 동일성 판단 결과에 따라 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 확인 메시지를 상기 통신 그룹의 디바이스로 송신하는 단계를 포함하며,

상기 통신 그룹의 디바이스는 상기 갱신 키 교환 확인 메시지에 기초하여 상기 통신 그룹의 디바이스 사이에서

서로 공유하는 공유 키를 갱신하여 생성하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 16

안전한 채널로 접속되어 있는 서버와 다수의 디바이스를 구비하는 통신 시스템에서 상기 서버를 통한 상기 디바이스 사이의 공유 키 교환 방법에 있어서,

상기 다수의 디바이스 중 통신 그룹에서 탈퇴하는 탈퇴 디바이스로부터 탈퇴 요청 메시지를 수신하는 경우, 상기 서버에 등록되어 있는 통신 그룹 정보를 갱신하고 상기 탈퇴 디바이스로 탈퇴 완료 메시지를 송신하는 단계;

상기 탈퇴 디바이스를 제외한 갱신 통신 그룹의 디바이스로 키 갱신 요청 메시지를 송신하는 단계; 및

상기 키 갱신 요청 메시지에 응답하여 상기 갱신 통신 그룹의 각 디바이스로부터 수신한 갱신 키 교환 메시지에 기초하여 상기 갱신 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하고 판단 결과에 따라 갱신 키 교환 확인 메시지를 상기 갱신 통신 그룹의 디바이스로 송신하여 상기 갱신 통신 그룹의 디바이스 사이의 공유 키를 갱신하는 단계를 포함하는 것을 특징으로 하는 공유 키 교환 방법.

청구항 17

제 16 항에 있어서, 상기 공유 키를 갱신하는 단계는

상기 서버에서 상기 갱신 통신 그룹의 디바이스에게 공유 키 갱신 메시지를 송신하고 상기 공유 키 갱신 메시지에 응답하여 상기 갱신 통신 그룹의 디바이스 각각으로부터 각 디바이스의 시드키를 수신하는 단계;

상기 수신한 각 디바이스의 시드키로부터 상기 갱신 통신 그룹의 각 디바이스가 보유하고 있는 시드값을 제외한 시드값으로부터 상기 갱신 통신 그룹의 디바이스 각각에 대한 갱신 예비 그룹 시드값과, 상기 갱신 통신 그룹의 디바이스에서 자신을 제외한 디바이스 정보로 상기 갱신 통신 그룹 디바이스 각각에 대한 갱신 예비 통신 그룹 정보(K_i)를 생성하는 단계;

상기 갱신 통신 그룹의 디바이스 각각에 해당하는 갱신 예비 그룹 시드값과 상기 갱신 예비 통신 그룹 정보를 상기 갱신 통신 그룹 디바이스 각각에 송신하는 단계;

상기 갱신 예비 그룹 시드값과 상기 갱신 예비 통신 그룹 정보에 기초하여 상기 갱신 통신 그룹 디바이스 각각에서 생성한 갱신 통신 그룹 정보(K), 서버 정보(S) 및 갱신 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 메시지를 수신하는 단계;

상기 갱신 키 교환 메시지의 해쉬 함수값과 상기 서버가 보유하고 있는 갱신 통신 그룹 정보(K), 서버 정보(S) 및 갱신 그룹 시드값(G)의 해쉬 함수값을 비교하여 상기 갱신 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하는 단계;

상기 동일성 판단 결과에 따라 서버 정보(S), 갱신 통신 그룹 정보(K) 및 갱신 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 확인 메시지를 상기 갱신 통신 그룹의 디바이스로 송신하는 단계를 포함하며,

상기 갱신 통신 그룹의 디바이스는 상기 갱신 키 교환 확인 메시지에 기초하여 상기 갱신 통신 그룹의 디바이스 사이에서 서로 공유하는 공유 키를 갱신하여 생성하는 것을 특징으로 하는 공유 키 교환 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 무선 통신 네트워크에서 서버를 통해 디바이스의 공유 키를 교환하는 방법에 관한 것으로, 보다 구체적으로 다수의 디바이스 중 그룹 통신을 요청하는 제1 디바이스로부터 그룹 통신 요청 메시지를 수신하는 경우 서버를 통해 그룹 통신 디바이스와 제1 디바이스 사이에 시드키를 송수신하여 제1 디바이스와 그룹 통신 디바이스 사이의 공유키를 교환하며, 공유키를 주기적으로 갱신하여 허가받지 않은 제3자가 공유키를 해킹하는 것을 방지하며 통신 그룹에서 탈퇴하는 디바이스가 존재하는 경우 통신 그룹을 구성하는 디바이스 사이에서 시드키를 서버로 송수신하여 통신 그룹을 구성하는 디바이스 사이의 공유키를 갱신하여 통신 그룹을 구성하는 디바이스 사이에서 공유키를 교환하는 방법에 관한 것이다.

배 경 기 술

[0002] 이동 디바이스는 유선/무선 복합 환경에서 통신이 이루어지는데, 서버와 이동 디바이스 사이의 보안 통신이 최근 중요한 이슈로 떠오르고 있다. 신뢰성 있는 서버를 이용하는 3자 인증 키 교환 프로토콜(3-Party Authentication Key Exchange, 이하 3PAKE 프로토콜로 언급)은 서버에 미리 저장된 이동 디바이스의 암호키를 이용하여 서버에 등록된 다른 이동 디바이스와의 보안 통신을 가능하게 해주는 프로토콜이다. 이러한 3PAKE 프로토콜은 스마트 카드, 휴대폰 인증 및 통신, 센서 네트워크 등 다양한 분야에서 보안 통신을 위해 널리 사용하고 있다.

[0003] 현재 이동 디바이스 사이의 일대일 통신뿐만 아니라 일대다 통신, 즉 그룹 통신도 중요한 이슈로 다루어지고 있다. 신뢰성 있는 서버를 이용하여 사용자의 패스워드를 이용한 3PAKE와 같은 키 교환 프로토콜은 이동 디바이스 사이의 일대일 통신을 넘어 일대다 통신에서 이동 디바이스에게 쉽고 안전하게 키 교환을 해 줄 수 있는 장점이 있다.

[0004] 종래 이동 디바이스 사이의 일대다 보안 통신을 위해 사용되는 키 교환 프로토콜로 왕 밍후이(Wang Minghui), 판 준후아즈(Pan Junhuaz), 왕 지안동(Wang Jiandong)이 제안한 경량화된 S-3PAKE(이하 '종래기술'이라 언급)가 있다. 종래기술은 서버와 디바이스에서 각각 서버와 다른 모든 디바이스의 패스워드 및 식별자 등의 서버 및 디바이스 정보를 보유하고 있으며, 보유하고 있는 서버 및 디바이스 정보를 이용하여 그룹 통신을 수행하고자 하는 디바이스 사이에서 공유 키를 교환한다.

발명의 내용

해결하려는 과제

[0005] 그러나 종래기술은 서버와 모든 디바이스가 각각 서버와 다른 모든 디바이스의 정보를 공유하고 있어 디바이스에 저장 부하가 발생하며 서버와 다른 모든 디바이스의 정보를 공유하기 위한 통신 부하를 주게 된다. 또한 통신 네트워크를 구성하는 디바이스 중 1개라도 허가받지 못한 제3자에게 노출되는 경우 통신 네트워크 전체의 보안이 붕괴될 수 있다는 문제점을 가진다. 또한 종래기술은 서버와 모든 디바이스에 각각 서버와 다른 모든 디바이스의 정보를 저장한다는 전제에 동작하는 것이므로, 네트워크를 유연하게 구성하지 못하며 따라서 통신 네트워크에서 추가되거나 탈퇴하는 디바이스가 존재하는 경우 실시간으로 통신 네트워크 및 통신 네트워크를 구성하는 디바이스의 공유 키를 갱신하지 못한다는 문제점을 가진다.

[0006] 본 발명은 위에서 언급한 종래기술이 가지는 문제점을 해결하기 위한 것으로, 본 발명이 이루고자 하는 목적은 통신 네트워크에서 신뢰성있는 서버를 통해 통신 그룹을 구성하는 디바이스 사이에 공유 키를 교환하는 방법을 제공하는 것이다.

[0007] 본 발명이 이루고자 하는 다른 목적은 서버에만 통신 네트워크를 구성하는 모든 디바이스의 정보를 저장하며 통신 그룹을 구성하는 경우에만 통신 그룹을 구성하는 디바이스로 통신 그룹의 디바이스 정보를 제공하여, 공유 키 교환을 위해 디바이스의 저장 부하와 통신 부하를 줄일 수 있는 공유 키 교환 방법을 제공하는 것이다.

[0008] 본 발명이 이루고자 하는 또 다른 목적은 통신 네트워크에 가입하고자 하는 디바이스가 존재하는 경우, 서버에 가입 디바이스의 패스워드를 안전하게 송수신하여 통신 네트워크에 가입하며 가입 후 공유 키를 교환하는 방법을 제공하는 것이다.

[0009] 본 발명이 이루고자 하는 또 다른 목적은 다수 디바이스 중 통신 그룹을 구성하는 디바이스 사이의 공유 키를 주기적으로 갱신하여 제3자의 공유 키 해킹을 방지할 수 있는 공유 키 교환 방법을 제공하는 것이다.

[0010] 본 발명이 이루고자 하는 또 다른 목적은 통신 그룹을 구성하는 디바이스 중 탈퇴 디바이스가 존재하는 경우, 탈퇴 디바이스를 실시간으로 반영하여 탈퇴 디바이스를 제외한 통신 그룹의 공유키를 갱신하며 갱신된 공유 키를 교환하는 방법을 제공하는 것이다.

과제의 해결 수단

[0011] 본 발명의 목적을 달성하기 위하여 본 발명의 일 실시예에 따른 공유 키 교환 방법은 다수의 디바이스 중 제1 디바이스에서 생성된 제1 시드값과 제1 디바이스가 통신 요청하는 통신 디바이스의 정보를 수신하는 단계와(이하 a 단계), 서버로부터 통신 디바이스로 서버의 시드값과 서버 정보를 송신하는 단계와(이하 b 단계), 통신 디바이스에서 각각 생성된 시드값과 통신 디바이스의 정보를 서버에서 수신하는 경우 제1 디바이스 및 통신 디바이스의 시드값으로부터 생성한 예비 그룹 시드값 및 통신 디바이스의 예비 통신 그룹 정보를 제1 디바이스와 통신 디바이스에 각각 송신하는 단계와(이하 c 단계), 서버에서 제1 디바이스 또는 통신 디바이스에서 생성한 그

룹 시드값, 통신 그룹 정보 및 서버 정보를 구비하는 키 교환 메시지를 수신하는 경우 키 교환 메시지에 기초하여 제1 디바이스와 통신 디바이스 사이에서 교환된 키의 동일성을 판단하고 키 교환 확인 메시지를 제1 디바이스와 통신 디바이스에 각각 송신하는 단계(이하 d 단계)를 포함하며, 제1 디바이스와 통신 디바이스는 키 교환 확인 메시지에 기초하여 제1 디바이스와 통신 디바이스 사이에서 서로 공유하는 공유 키를 생성하는 것을 특징한다.

[0012] 본 발명에 따른 공유 키 교환 방법은 다수의 디바이스 중 제1 디바이스와 서버 사이에서 공유하는 비밀키(XY)로 암호화된 제1 디바이스의 패스워드를 제1 디바이스로부터 수신하여 제1 디바이스의 패스워드를 서버에 등록하는 단계를 더 포함한다.

[0013] 제1 디바이스의 패스워드를 상기 서버에 등록하는 단계를 보다 구체적으로 살펴보면, 제1 디바이스에서 생성한 제1 행렬(X)과 제1 행렬의 의사역행렬(X')의 곱을 제1 디바이스로부터 수신하는 단계와, 서버에서 생성한 제2 행렬(Y)과 제2 행렬의 의사역행렬(Y')과 제1 행렬(X) 및 제1 행렬의 의사역행렬(X')의 곱으로부터 행렬 조합(XX'Y, XX'YY')를 생성하고 제1 디바이스로 송신하여 제1 디바이스에게 서버의 공유 비밀키(Y)를 제공하는 단계와, 제1 디바이스로부터 수신한 행렬 조합(XYY')으로부터 제1 디바이스의 공유 비밀키(X)를 획득하고 제1 디바이스와 서버의 공유 비밀키(XY)로 제1 디바이스의 시드 생성값(M)을 암호화하여 제1 디바이스로 송신하는 단계와, 공유 비밀키(XY)로 암호화된 제1 디바이스의 패스워드를 제1 디바이스로부터 수신하여 제1 디바이스를 서버에 등록하는 단계를 포함한다.

[0014] 여기서 제1 디바이스는 시드 생성값(M)과 시드 생성값(M)의 해쉬값을 구비하는 등록 메시지를 공유 비밀키(XY)로 암호화하여 상기 서버로 송신하며, 서버는 공유 비밀키(XY)로 등록 메시지를 복호화하며 복호화된 시드 생성값과 시드 생성값의 해쉬값을 비교하여 등록 메시지의 무결성을 판단한다.

[0015] 제1 디바이스에서 생성된 제1 시드값과 제1 디바이스가 통신 요청하는 통신 디바이스의 정보를 수신하는 (a)단계를 보다 구체적으로 살펴보면, 서버에서 제1 디바이스로부터 그룹통신 요청 메시지를 수신하는 단계와, 서버에서 그룹통신 요청 메시지에 구비되어 있는 제1 디바이스 식별자에 기초하여 제1 디바이스가 서버에 등록된 디바이스인지 검증하는 단계와, 서버에서 검증 결과에 따라 제1 디바이스로 서버에 등록된 디바이스 중 통신 가능한 통신 가능 디바이스 정보를 송신하는 단계와, 제1 디바이스로부터 제1 디바이스에서 생성된 제1 시드값를 구비하는 제1 디바이스의 시드 조합값(A_1)과 통신 가능 디바이스 중 제1 디바이스가 통신 요청하는 통신 디바이스 정보를 수신하는 단계를 포함하는 것을 특징으로 한다.

[0016] 제1 디바이스의 시드 조합값(A_1)은 아래의 수학식(1)에 의해 생성되며,

[0017] [수학식 1]

[0018] $$A_1 = g^{x_1} \cdot M_1 \cdot pw_1$$

[0019] 여기서 g^{x_1} 은 제1 디바이스에서 생성한 제1 시드값이며, M_1은 서버에서 생성하여 제1 디바이스로 제공된 제1 시드 생성값이며, pw_1은 제1 디바이스의 패스워드이다.

[0020] 서버로부터 통신 디바이스로 서버의 시드값과 서버 정보를 송신하는 (b) 단계를 보다 구체적으로 살펴보면, 통신 디바이스 정보에 기초하여 서버에 등록된 통신 가능 디바이스 중 제1 디바이스가 통신 요청한 통신 디바이스와 제1 디바이스로 통신 그룹을 생성하는 단계와, 서버에서 서버 시드값을 생성하고 통신 디바이스에 해당하는, 서버 시드값을 구비하는 서버 시드 조합값(B_i)을 생성하는 단계와, 통신 디바이스로 서버 시드 조합값과 서버 정보 및 서버 시드값과 서버 정보의 해쉬값을 송신하는 단계를 포함하는 것을 특징으로 한다.

[0021] 여기서 서버 시드 조합값(B_i)은 아래의 수학식(2)에 의해 생성되며,

[0022] [수학식 2]

[0023] $$B_i = g^{G} \cdot M_i \cdot pw_i$$

[0024] 여기서 g^G 은 서버 시드값이며, M_i은 서버에서 생성하여 통신 디바이스에 각각 제공된 시드 생성값이며, pw_i은 통신 디바이스 각각의 패스워드인 것을 특징으로 한다.

[0025] 예비 그룹 시드값 및 통신 디바이스의 예비 통신 그룹 정보를 제1 디바이스와 통신 디바이스에 각각 송신하는 (c) 단계를 보다 구체적으로 살펴보면, 통신 디바이스로부터 수신한 통신 디바이스의 시드 조합값에서 통신 디바이스의 시드값을 획득하는 단계와, 제1 디바이스 또는 통신 디바이스가 보유하고 있는 시드값을 제외한 제1 디바이스 및 통신 디바이스의 시드값으로부터 제1 디바이스 및 통신 디바이스 각각에 대한 예비 그룹 시드값(G_i)을 계산하는 단계와, 제1 디바이스 및 통신 디바이스에서 자신을 제외한 디바이스 정보로 제1 디바이스 및 통신 디바이스 각각에 대한 예비 통신 그룹 정보(K_i)를 생성하는 단계와, 제1 디바이스로 제1 디바이스에 해당하는 예비 그룹 시드값을 구비하는 예비 그룹 시드 조합값, 예비 그룹 정보 및 서버의 시드 조합값을 송신하는 단계와, 통신 디바이스로 통신 디바이스 각각에 해당하는 예비 그룹 시드값을 구비하는 예비 그룹 시드 조합값과 예비 그룹 정보를 통신 디바이스로 각각 송신하는 단계를 포함하는 것을 특징으로 한다.

[0026] 키 교환 확인 메시지를 제1 디바이스와 통신 디바이스에 각각 송신하는 (d) 단계를 보다 구체적으로 살펴보면, 서버에서 제1 디바이스 및 통신 디바이스에서 각각 생성한, 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G) 순서의 해쉬 함수값의 키 교환 메시지를 수신하는 단계와, 키 교환 메시지의 해쉬 함수값과 서버가 보유하고 있는 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)의 해쉬 함수값을 비교하여 제1 디바이스와 통신 디바이스 사이에서 교환된 키의 동일성을 판단하는 단계와, 동일성 판단 결과에 따라 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G) 순서의 해쉬 함수값의 키 교환 확인 메시지를 제1 디바이스와 통신 디바이스로 각각 송신하는 단계를 포함하는 것을 특징으로 한다.

[0027] 본 발명의 일 실시예에 따른 공유 키 교환 방법은 통신 그룹의 각 디바이스로부터 수신한 갱신 키 교환 메시지에 기초하여 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하고 판단 결과에 따라 갱신 키 교환 확인 메시지를 통신 그룹의 디바이스로 송신하여 통신 그룹의 디바이스 사이의 공유 키를 갱신하는 단계(이하 e 단계)를 더 포함한다.

[0028] 본 발명의 일 실시예에 따른 공유 키 교환 방법은 통신 그룹의 디바이스 중 탈퇴 디바이스로부터 탈퇴 요청 메시지를 수신하는 경우, 서버에 등록되어 있는 통신 그룹 정보를 갱신하고 탈퇴 디바이스로 탈퇴 완료 메시지를 송신하는 단계를 더 포함하며, 탈퇴 완료 메시지의 송신 후, (e) 단계를 수행하여 통신 그룹 디바이스 사이의 공유 키를 갱신하는 것을 특징으로 한다.

[0029] 본 발명의 다른 실시예에 따른 공유 키 교환 방법은 서버에서 다수의 디바이스 중 통신 그룹의 디바이스에게 공유 키 갱신 메시지를 송신하고 공유 키 갱신 메시지에 응답하여 통신 그룹의 디바이스 각각으로부터 각 디바이스의 시드키를 수신하는 단계와, 수신한 각 디바이스의 시드키로부터 통신 그룹의 각 디바이스가 보유하고 있는 시드값을 제외한 시드값으로부터 통신 그룹 디바이스 각각에 대한 갱신 예비 그룹 시드값과, 통신 그룹의 디바이스에서 자신을 제외한 디바이스 정보로 통신 그룹 디바이스 각각에 대한 갱신 예비 통신 그룹 정보(K_i)를 생성하는 단계와, 통신 그룹 디바이스 각각에 해당하는 갱신 예비 그룹 시드값과 갱신 예비 통신 그룹 정보를 통신 그룹 디바이스 각각에 송신하는 단계와, 갱신 예비 그룹 시드값과 갱신 예비 통신 그룹 정보에 기초하여 통신 그룹 디바이스 각각에서 생성한 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 메시지를 수신하는 단계와, 갱신 키 교환 메시지의 해쉬 함수값과 서버가 보유하고 있는 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)의 해쉬 함수값을 비교하여 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하는 단계와, 동일성 판단 결과에 따라 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 확인 메시지를 통신 그룹의 디바이스로 송신하는 단계를 포함하며, 통신 그룹의 디바이스는 갱신 키 교환 확인 메시지에 기초하여 통신 그룹의 디바이스 사이에서 서로 공유하는 공유 키를 갱신하여 생성하는 것을 특징으로 한다.

[0030] 본 발명의 또 다른 실시예에 따른 공유 키 교환 방법은 다수의 디바이스 중 통신 그룹에서 탈퇴하는 탈퇴 디바이스로부터 탈퇴 요청 메시지를 수신하는 경우, 서버에 등록되어 있는 통신 그룹 정보를 갱신하고 탈퇴 디바이스로 탈퇴 완료 메시지를 송신하는 단계와, 디바이스를 제외한 갱신 통신 그룹의 디바이스로 키 갱신 요청 메시지를 송신하는 단계와, 키 갱신 요청 메시지에 응답하여 갱신 통신 그룹의 각 디바이스로부터 수신한 갱신 키 교환 메시지에 기초하여 갱신 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하고 판단 결과에 따라 갱신 키 교환 확인 메시지를 갱신 통신 그룹의 디바이스로 송신하여 갱신 통신 그룹의 디바이스 사이의 공

유 키를 갱신하는 단계를 포함한다.

[0031] 여기서 공유 키를 갱신하는 단계는 서버에서 갱신 통신 그룹의 디바이스에게 공유 키 갱신 메시지를 송신하고 공유 키 갱신 메시지에 응답하여 갱신 통신 그룹의 디바이스 각각으로부터 각 디바이스의 시드키를 수신하는 단계와, 수신한 각 디바이스의 시드키로부터 갱신 통신 그룹의 각 디바이스가 보유하고 있는 시드값을 제외한 시드값으로부터 갱신 통신 그룹의 디바이스 각각에 대한 갱신 예비 그룹 시드값과, 갱신 통신 그룹의 디바이스에서 자신을 제외한 디바이스 정보로 갱신 통신 그룹 디바이스 각각에 대한 갱신 예비 통신 그룹 정보(K_i)를 생성하는 단계와, 갱신 통신 그룹의 디바이스 각각에 해당하는 갱신 예비 그룹 시드값과 갱신 예비 통신 그룹 정보를 갱신 통신 그룹 디바이스 각각에 송신하는 단계와, 갱신 예비 그룹 시드값과 갱신 예비 통신 그룹 정보에 기초하여 갱신 통신 그룹 디바이스 각각에서 생성한 갱신 통신 그룹 정보(K), 서버 정보(S) 및 갱신 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 메시지를 수신하는 단계와, 갱신 키 교환 메시지의 해쉬 함수값과 서버가 보유하고 있는 갱신 통신 그룹 정보(K), 서버 정보(S) 및 갱신 그룹 시드값(G)의 해쉬 함수값을 비교하여 갱신 통신 그룹의 디바이스 사이에서 교환된 갱신 키의 동일성을 판단하는 단계와, 동일성 판단 결과에 따라 서버 정보(S), 갱신 통신 그룹 정보(K) 및 갱신 그룹 시드값(G) 순서의 해쉬 함수값의 갱신 키 교환 확인 메시지를 갱신 통신 그룹의 디바이스로 송신하는 단계를 포함하며, 갱신 통신 그룹의 디바이스는 갱신 키 교환 확인 메시지에 기초하여 갱신 통신 그룹의 디바이스 사이에서 서로 공유하는 공유 키를 갱신하여 생성하는 것을 특징으로 한다.

발명의 효과

[0032] 본 발명에 따른 공유 키 교환 방법은 종래 기술과 비교하여 다음과 같은 다양한 효과를 가진다.

[0033] 첫째, 본 발명에 따른 공유 키 교환 방법은 통신 네트워크에서 신뢰성있는 서버를 통해 통신 그룹을 구성하는 디바이스 사이에서 안전하게 공유 키를 교환할 수 있다.

[0034] 둘째, 본 발명에 따른 공유 키 교환 방법은 서버에만 통신 네트워크를 구성하는 모든 디바이스의 정보를 저장하며 통신 그룹을 구성하는 경우에만 통신 그룹을 구성하는 디바이스로 통신 그룹의 디바이스 정보를 제공함으로써, 공유 키 교환을 위해 디바이스의 저장 부하와 통신 부하를 줄일 수 있다.

[0035] 셋째, 본 발명에 따른 공유 키 교환 방법은 통신 네트워크에 가입하고자 하는 디바이스가 존재하는 경우, 서버에 가입 디바이스의 패스워드를 안전하게 송수신하여 통신 네트워크에 자유롭게 가입하며 가입 후 공유 키를 교환할 수 있다.

[0036] 넷째, 본 발명에 따른 공유 키 교환 방법은 다수 디바이스 중 통신 그룹을 구성하는 디바이스 사이의 공유 키를 주기적으로 갱신함으로써, 제3자의 공유 키 해킹을 방지할 수 있다.

[0037] 다섯째, 본 발명에 따른 공유 키 교환 방법은 통신 그룹을 구성하는 디바이스 중 탈퇴 디바이스가 존재하는 경우 탈퇴 디바이스를 실시간으로 반영함으로써, 탈퇴 디바이스를 제외한 통신 그룹의 공유키를 갱신하여 갱신한 공유 키를 교환할 수 있다.

도면의 간단한 설명

[0038] 도 1은 본 발명에 따른 통신 네트워크를 설명하기 위한 기능 블록도이다.

도 2는 본 발명에 따른 통신 네트워크에서 그룹 통신을 설명하기 위한 기능 블록도이다.

도 3은 본 발명에 따른 통신 네트워크에서 공유 키 교환을 위해 제1 디바이스, 서버, 통신 디바이스에서 송수신되는 메시지를 설명하기 위한 흐름도이다.

도 4는 본 발명에 따라 신규 디바이스를 서버에 등록하는 방법을 설명하기 위한 흐름도이다.

도 5는 서버에서 수행되는 본 발명에 따른 공유 키 교환 방법을 설명하기 위한 흐름도이다.

도 6은 제1 디바이스 정보 메시지를 수신하는 단계를 보다 구체적으로 설명하는 흐름도이다.

도 7은 서버에서 통신 디바이스로 서버 정보 메시지를 송신하는 단계를 보다 구체적으로 설명하는 흐름도이다.

도 8은 예비 정보 메시지를 제1 디바이스와 통신 디바이스로 송신하는 단계를 보다 구체적으로 설명하는 흐름도이다.

도 9는 키 교환 확인 메시지를 제1 디바이스와 통신 디바이스로 송신하는 단계를 보다 구체적으로 설명하는 흐름도이다.

도 10은 본 발명에 따른 공유 키 교환 방법에서 공유 키를 갱신하는 단계를 보다 구체적으로 설명하는 흐름도이다.

도 11은 통신 그룹에서 탈퇴하는 탈퇴 디바이스를 서버에 등록하는 단계를 보다 구체적으로 설명하는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0039] 이하 첨부한 도면을 참고로 본 발명에 따른 공유 키 교환 방법에 대해 보다 구체적으로 살펴본다.

[0040] 도 1은 본 발명에 따른 통신 네트워크를 설명하기 위한 기능 블록도이다.

[0041] 도 1을 참고로 보다 구체적으로 살펴보면, 유선/무선 네트워크(20)에 서버(10)와 다수의 디바이스가 존재하는 디바이스 네트워크(30)가 접속되어 있다. 서버(10)는 외부 물리적 공격이나 해킹으로부터 보안상 안전하며 신뢰성있게 네트워크(20)에 접속되어 있음을 가정한다. 외부 물리적 공격이나 해킹으로부터 보안상 안전하기 위해 서버(10)는 유선으로 네트워크(20)에 접속될 수 있다. 디바이스 네트워크(30)에 존재하는 디바이스(MT)는 자신의 패드워드를 서버(10)로 제공하여 디바이스(MT)를 서버(10)에 등록하며 서버(10)는 디바이스를 등록시 각 디바이스에 고유한 시드 생성값을 제공한다.

[0042] 디바이스 네트워크(30)에는 다수의 디바이스(MT)가 존재하는데, 디바이스 네트워크(30)에 존재하는 디바이스(MT)는 선택적으로 다른 디바이스와 일대일 통신을 수행하거나 일대다 그룹 통신을 수행한다. 일대일 통신 또는 일대다 그룹 통신을 수행하기 위해, 디바이스는 서버(10)의 중계에 의해 다른 디바이스와 공유 키를 교환하며 교환한 공유 키를 통해 송수신되는 메시지를 암호화한다.

[0043] 도 2는 본 발명에 따른 통신 네트워크에서 그룹 통신을 설명하기 위한 기능 블록도이다.

[0044] 디바이스 네트워크(30)에 존재하는 다수 디바이스들 중 제1 디바이스(RMT)가 디바이스 네트워크(30)에 존재하는 다수 디바이스 중 일부의 디바이스와 그룹 통신을 요청하는 경우, 서버(10)는 디바이스 네트워크(30) 중 그룹 통신이 가능한 가능 통신 디바이스에 대한 정보를 제1 디바이스(RMT)로 제공하며, 가능 통신 디바이스 중 제1 디바이스(RMT)가 그룹 통신을 요청한 통신 디바이스와 제1 디바이스(RMT)를 통신 그룹(CG)로 생성한다.

[0045] 서버(10)는 통신 그룹(CG)을 구성하는 제1 디바이스(RMT)와 통신 디바이스로 이루어진 통신 그룹의 통신 그룹 정보, 제1 디바이스(RMT)와 통신 디바이스부터 수신한 시드값으로부터 그룹 시드값, 서버 정보로 공유 키를 생성하며, 생성한 공유 키를 제1 디바이스(RMT)와 통신 디바이스로 제공하여 제1 디바이스(RMT)와 통신 디바이스 사이의 공유 키를 교환토록 한다.

[0046] 한편, 서버(10)는 통신 그룹(CG)에 새로운 디바이스가 가입하거나 통신 그룹(CG)에서 탈퇴하는 디바이스가 존재하는 경우, 가입 디바이스 또는 탈퇴 디바이스를 그룹 시드값과 통신 그룹 정보에서 제외하여 새로운 공유 키를 갱신 생성하며, 갱신한 공유 키를 통신 그룹에 존재하는 디바이스로 제공하여 디바이스 사이에서 갱신 공유 키를 교환토록 한다.

[0047] 도 3은 본 발명에 따른 통신 네트워크에서 공유 키 교환을 위해 제1 디바이스, 서버, 통신 디바이스에서 송수신되는 메시지를 설명하기 위한 흐름도이다.

[0048] 도 3을 참고로 보다 구체적으로 살펴보면, 그룹 통신을 요청하는 제1 디바이스(RMT)는 서버(10)로 제1 디바이스 정보 메시지를 송신한다(S10). 제1 디바이스 정보 메시지는 제1 디바이스(RMT)에서 생성한 제1 시드값을 구비하는 제1 시드 조합값과 디바이스 네트워크(30) 중 제1 디바이스(RMT)에서 그룹 통신을 요청한 통신 디바이스 정보가 포함되어 있다.

[0049] 서버(10)는 제1 디바이스(RMT)로부터 제1 디바이스 정보 메시지를 수신하는 경우, 통신 그룹의 통신 디바이스로 서버 정보 메시지를 송신한다(S20). 서버 정보 메시지는 서버(10)에서 생성한 서버 시드값을 구비하는 서버 시드 조합값과 서버 정보 및, 서버 시드 조합값과 서버 정보의 해쉬값을 포함하고 있다. 서버 시드 조합값과 서버 정보의 해쉬값을 계산하는데 사용되는 해쉬 함수는 서버(10)와 디바이스 네트워크(30)를 구성하는 디바이스

가 서로 공유한다.

[0050] 통신 그룹의 통신 디바이스는 서버(10)로부터 서버 정보 메시지를 수신하는 경우 서버 정보 메시지의 무결성을 판단하며, 서버 정보 메시지의 무결성이 판단되는 경우 통신 디바이스 정보 메시지를 서버(10)로 송신한다(S30). 통신 디바이스 정보 메시지는 통신 그룹의 각 통신 디바이스에서 생성한 자신에 고유한 시드값을 구비하는 시드 조합값과 통신 디바이스 정보가 포함되어 있다. 바람직하게, 통신 디바이스의 시드 조합값은 각 통신 디바이스에서 아래의 수학식(0)과 같이 계산되는데,

[0051] [수학식 0]

[0052] $$A_i = g^{x_i} \cdot M_i \cdot pw_i$$

[0053] 여기서 g^{x_i} 은 통신 그룹의 통신 디바이스(i) 생성한 시드값이며, M_i는 서버에서 생성하여 통신 디바이스(i)로 제공된 시드 생성값이며, pw_i은 통신 디바이스(i)가 보유하고 있는 패스워드인 것을 특징으로 한다. 통신 디바이스(i)의 패스워드는 서버에 등록되어 있다.

[0054] 서버(10)는 제1 디바이스 정보 메시지와 통신 디바이스 정보 메시지를 수신하는 경우, 예비 정보 메시지를 생성하여 제1 디바이스(RMT)와 통신 디바이스로 각각 송신한다(S40). 제1 디바이스(RMT)와 통신 디바이스로 송신되는 예비 정보 메시지는 제1 디바이스의 시드값 또는 통신 디바이스의 시드값으로부터 생성되는 예비 그룹 시드값과 제1 디바이스 정보 또는 통신 디바이스 정보로부터 생성되는 예비 통신 그룹 정보를 포함한다.

[0055] 제1 디바이스(RMT)와 통신 디바이스는 서버(10)로부터 각각 예비 정보 메시지를 수신하는 경우, 제1 디바이스와 통신 디바이스 사이에 동일한 키가 교환되었는지 확인하기 위해 키 교환 메시지를 생성하여 서버(10)로 송신한다(S50). 서버(10)로 송신되는 키 교환 메시지는 제1 디바이스(RMT)와 통신 디바이스에서 각각 생성한 통신 그룹 정보, 서버 정보 및 그룹 시드값을 포함한다. 여기서 통신 그룹 정보는 수신한 예비 통신 그룹 정보와 자신의 디바이스 정보로부터 생성되며, 그룹 시드값은 수신한 예비 그룹 시드값과 자신의 시드값으로부터 생성된다. 예를 들어 통신 디바이스(i)의 통신 그룹 정보는 통신 디바이스(i)의 예비 통신 그룹 정보와 통신 디바이스(i)의 디바이스 정보의 리스트로부터 생성되며, 통신 디바이스(i)의 그룹 시드값은 통신 디바이스(i)의 예비 그룹 시드값과 통신 디바이스(i)의 시드값의 곱으로부터 생성된다. 바람직하게, 키 교환 메시지는 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)의 순서로 해쉬 함수에 적용한 해쉬값을 더 포함한다.

[0056] 서버(10)는 제1 디바이스(RMT)와 통신 디바이스로부터 키 교환 메시지를 수신하는 경우, 키 교환 메시지에 포함되어 있는 통신 그룹 정보, 서버 정보 및 그룹 시드값이 서버(10)에 저장되어 있는 통신 그룹 정보, 서버 정보 및 그룹 시드값과 동일한지 판단하고, 판단 결과 키 교환 메시지와 서버(10)에 저장되어 있는 통신 그룹 정보, 서버 정보 및 그룹 시드값이 동일한 경우 제1 디바이스(RMT)와 통신 디바이스로 동일한 키가 교환되었음을 확인하는 키 교환 확인 메시지를 생성하여 제1 디바이스(RMT)와 통신 디바이스로 송신한다(S60). 키 교환 확인 메시지는 서버에 저장되어 있는 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G)을 포함한다. 바람직하게, 키 교환 확인 메시지는 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G)의 순서로 해쉬함수에 적용한 해쉬값을 더 포함한다.

[0057] 제1 디바이스(RMT)와 통신 디바이스는 키 교환 확인 메시지를 수신하는 경우, 제1 디바이스(RMT)와 통신 디바이스가 각각 공유하는 공유 키, 예를 들어 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G)의 조합으로부터 이루어진 공유 키를 생성한다(S70). 제1 디바이스(RMT)와 통신 디바이스는 각각 생성한 공유 키를 이용하여 제1 디바이스(RMT)와 통신 디바이스로 이루어진 통신 그룹에서 송수신되는 메시지를 암호화 및 복호화한다.

[0058] 바람직하게, 서버(10)는 제1 디바이스(RMT) 또는 통신 디바이스로부터 키 교환 메시지를 수신하는 경우, 서버(10)에 저장되어 있는 통신 그룹 정보, 서버 정보 및 그룹 시드값의 해쉬값과 키 교환 메시지의 해쉬값을 비교하여 키 교환 메시지의 무결성을 판단하며, 제1 디바이스(RMT) 또는 통신 디바이스는 키 교환 확인 메시지를 수신하는 경우, 제1 디바이스(RMT) 또는 통신 디바이스에 저장되어 있는 서버 정보, 통신 그룹 정보 및 그룹 시드값의 해쉬값과 키 교환 확인 메시지의 해쉬값을 비교하여 키 교환 확인 메시지의 무결성을 판단한다.

[0059] 도 4는 본 발명에 따라 신규 디바이스를 서버에 등록하는 방법을 설명하기 위한 흐름도이다.

[0060] 도 4를 참고로 보다 구체적으로 살펴보면, 서버는 신규 디바이스로부터 제1 행렬(X)과 제1 행렬의 의사역행렬(X')의 곱을 수신한다(S1). 신규 디바이스가 서버(10)에 등록하고자 하는 경우 신규 디바이스는 제1 행렬(X)과 제1 행렬의 의사역행렬(X')을 생성하고, 제1 행렬(X)과 제1 행렬의 의사역행렬(X')의 곱을 계산하여 서버(10)로 송신한다.

[0061] 제1 행렬(X)과 제1 행렬의 의사역행렬(X')의 곱을 수신한 서버는 제2 행렬(Y)과 제2 행렬의 의사역행렬(Y')을 생성하며, 생성한 제2 행렬(Y)과 제2 행렬의 의사역행렬(Y'), 수신한 1 행렬(X) 및 제1 행렬의 의사역행렬(X')의 곱으로부터 행렬 조합(XX'Y, XX'YY')를 생성하여 신규 디바이스로 송신한다(S2).

[0062] 신규 디바이스는 서버(10)로부터 수신한 행렬 조합(XX'Y, XX'YY')과 신규 디바이스가 보유하고 있는 제1 행렬(X)과 제1 행렬의 의사역행렬(X')로부터 서버의 공유 비밀키(Y)를 획득하며, 행렬 조합(XYY')를 생성하여 서버(10)로 송신한다(S3).

[0063] 서버(10) 신규 디바이스로부터 행렬 조합(XYY')을 수신하는 경우, 서버(10)가 보유하고 있는 제2 행렬(Y)과 제2 행렬의 의사역행렬(Y')의 곱과 수신한 행렬 조합(XYY')으로부터 신규 디바이스의 공유 비밀키(X)를 획득하고, 신규 디바이스와 서버의 공유 비밀키(XY)로 신규 디바이스의 시드 생성값(M)을 암호화한 등록 메시지를 신규 디바이스로 송신한다(S4).

[0064] 한편, 서버(10)는 신규 디바이스로부터 신규 디바이스와 서버의 공유 비밀키(XY)로 암호화된 제1 디바이스의 패스워드를 수신하여 신규 디바이스를 서버(10)에 신규 등록한다(S5). 바람직하게, 서버(10)는 시드 생성값(M)과 시드 생성값(M)의 해쉬값을 구비하는 등록 메시지를 공유 비밀키(XY)로 암호화하여 신규 디바이스로 송신하며, 신규 디바이스는 공유 비밀키(XY)로 등록 메시지를 복호화하며, 복호화된 시드 생성값과 시드 생성값의 해쉬값을 비교하여 등록 메시지의 무결성을 판단한다.

[0065]

[0066] 도 5는 서버에서 수행되는 본 발명에 따른 공유 키 교환 방법을 설명하기 위한 흐름도이다.

[0067] 도 5를 참고로 보다 구체적으로 살펴보면, 서버(10)는 서버(10)에 등록되어 있는 디바이스 중 제1 디바이스로부터 그룹 통신을 요청받는 경우, 제1 디바이스(RMT)로부터 제1 디바이스(RMT)에서 생성한 제1 시드값을 구비하는 제1 시드 조합값과 디바이스 네트워크(30) 중 제1 디바이스(RMT)에서 그룹 통신을 요청한 통신 디바이스 정보가 구비하고 있는 제1 디바이스 정보 메시지를 수신한다(S10).

[0068] 제1 디바이스 정보 메시지를 수신하는 단계를 보다 구체적으로 설명하고 있는 도 6을 참고로 살펴보면, 서버(10)는 제1 디바이스로부터 그룹통신 요청 메시지를 수신한다(S11). 그룹통신 요청 메시지에는 제1 디바이스의 식별자가 구비되어 있으며, 서버(10)는 그룹통신 요청 메시지에 구비되어 있는 제1 디바이스 식별자에 기초하여 제1 디바이스가 서버에 등록된 디바이스인지 검증한다(S13).

[0069] 서버는 검증 결과에 따라 제1 디바이스로 서버에 등록된 디바이스 중 통신 가능한 통신 가능 디바이스 정보를 송신한다(S15). 여기서 통신 가능 디바이스 정보는 서버에 등록된 디바이스 중 통신 가능한 디바이스의 식별자인 것을 특징으로 한다.

[0070] 서버(10)는 제1 디바이스로부터 제1 디바이스에서 생성된 제1 시드값를 구비하는 제1 디바이스의 시드 조합값(A_1)과 통신 가능 디바이스 중 제1 디바이스가 통신 요청하는 통신 디바이스 정보를 수신한다(S17). 여기서 통신 디바이스 정보는 통신 가능 디바이스 중 제1 디바이스가 통신 그룹으로 통신하고자 하는 디바이스의 식별자인 것을 특징으로 한다.

[0071] 바람직하게, 제1 디바이스의 시드 조합값(A_1)은 아래의 수학식(1)에 의해 생성되며,

[0072] [수학식 1]

[0073] $$A_1 = g^{x_1} \cdot M_1 \cdot pw_1$$

[0074] 여기서 g^{x_1} 은 제1 디바이스에서 생성한 제1 시드값이며, M_1은 서버에서 생성하여 제1 디바이스로 제공된 제

1 시드 생성값이며, pw_i은 제1 디바이스의 패스워드인 것을 특징으로 한다.

[0075] 다시 도 5를 참고로 살펴보면, 서버(10)는 제1 디바이스로부터 제1 디바이스 정보 메시지를 수신하는 경우, 그룹 통신의 통신 디바이스로 서버 정보 메시지를 송신한다(S20).

[0076] 서버에서 통신 디바이스로 서버 정보 메시지를 송신하는 단계를 보다 구체적으로 설명하고 있는 도 7을 참고로 살펴보면, 서버(10)는 통신 디바이스 정보에 기초하여 서버(10)에 등록된 통신 가능 디바이스 중 제1 디바이스가 통신 요청한 통신 디바이스와 제1 디바이스로 통신 그룹을 생성한다(S21). 서버는 서버 시드값(g^G)을 생성하고(S23), 생성한 서버 시드값에 기초하여 통신 그룹의 각 통신 디바이스에 해당하는, 서버 시드값을 구비하는 서버 시드 조합값(B_i)을 생성한다(S25). 서버 시드 조합값(B_i)은 아래의 수학식(2)에 의해 생성되며,

[0077] [수학식 2]

[0078] $$B_i = g^G \cdot M_i \cdot pw_i$$

[0079] 여기서 g^G 은 서버 시드값이며, M_i은 서버에서 생성하여 통신 디바이스에 각각 제공된 시드 생성값이며, pw_i은 통신 디바이스 각각의 패스워드인 것을 특징으로 한다. 여기서 각 통신 디바이스에 제공된 통신 디바이스의 시드 생성값(M_i)와 각 통신 디바이스의 패스워드(pw_i)는 서버에 등록되어 있다.

[0080] 서버(10)는 각 통신 디바이스로 각 통신 디바이스의 서버 시드 조합값과 서버 정보를 구비하는 서버 정보 메시지를 송신한다(S27). 바람직하게, 서버 정보 메시지는 서버 시드 조합값과 서버 정보를 서버(10)와 각 통신 디바이스가 공유하는 해쉬 함수에 적용한 해쉬값을 더 포함한다.

[0081] 다시 도 5를 참고로 살펴보면, 서버(10)는 제1 디바이스 정보 메시지와 통신 디바이스 정보 메시지를 수신하는 경우, 예비 정보 메시지를 생성하여 제1 디바이스(RMT)와 통신 디바이스로 각각 송신한다(S40).

[0082] 예비 정보 메시지를 제1 디바이스와 통신 디바이스로 송신하는 단계를 보다 구체적으로 설명하는 도 8을 참고로 살펴보면, 서버는 제1 디바이스와 통신 디바이스로부터 수신한 시드 조합값으로부터 제1 디바이스와 각 통신 디바이스의 시드값을 획득한다(S41). 제1 디바이스 또는 통신 디바이스가 보유하고 있는 시드값을 제외한 제1 디바이스 및 통신 디바이스의 시드값으로부터 제1 디바이스 및 통신 디바이스 각각에 대한 예비 그룹 시드값(G_i)을 계산한다(S43). 여기서 예비 그룹 시드값은 제1 디바이스 또는 통신 디바이스가 보유하고 있는 시드값을 제외한 제1 디바이스 및 통신 디바이스의 시드값의 조합으로부터 생성되는데, 예를 들어 제1 디바이스의 예비 그룹 시드값은 제1 디바이스의 시드값을 제외한 모든 통신 디바이스의 시드값의 곱으로 계산되며, 통신 디바이스(i)의 예비 그룹 시드값은 통신 디바이스(i)의 시드값을 제외한 모든 통신 디바이스와 제1 디바이스의 시드값의 곱으로 계산된다.

[0083] 한편, 서버는 제1 디바이스 및 통신 디바이스에서 자신을 제외한 디바이스 정보의 조합으로 제1 디바이스 및 통신 디바이스 각각에 대한 예비 통신 그룹 정보(K_i)를 생성한다(S45). 예를 들어, 제1 디바이스의 예비 통신 그룹 정보는 제1 디바이스 정보(식별자)를 제외한 모든 통신 디바이스의 정보 리스트로 생성되며, 통신 디바이스(i)의 예비 통신 그룹 정보는 통신 디바이스(i) 정보를 제외한 모든 디바이스의 정보와 제1 디바이스 정보 리스트로 생성된다.

[0084] 서버는 제1 디바이스 또는 통신 디바이스에 해당하는 예비 그룹 시드값과 예비 통신 그룹 정보를 구비하는 예비 정보 메시지를 생성하며(S47), 제1 디바이스와 통신 디바이스로 제1 디바이스 또는 통신 디바이스 각각에 해당하는 예비 정보 메시지를 각각 송신한다(S49). 예를 들어 서버는 제1 디바이스에 해당하는 예비 그룹 시드 조합값, 예비 통신 그룹 정보, 서버 정보, 서버 시드값을 구비하는 예비 정보 메시지를 생성하여 제1 디바이스로 송신하며, 통신 디바이스(i)에 해당하는 예비 그룹 시드 조합값, 예비 통신 그룹 정보, 서버 정보를 구비하는 예비 정보 메시지를 생성하여 통신 디바이스(i)로 송신한다. 바람직하게, 예비 정보 메시지는 서버 시드값, 예비 그룹 시드값을 구비하는 예비 그룹 시드 조합값, 예비 통신 그룹 정보를 해쉬함수에 적용한 해쉬값을 더

포함한다.

[0085] 다시 도 5를 참고로 살펴보면, 서버는 제1 디바이스와 통신 디바이스로부터 키 교환 메시지를 수신하는 경우, 키 교환 메시지에 기초하여 제1 디바이스와 통신 디바이스 사이에 동일한 키가 교환되었는지 확인 후 키 교환 확인 메시지를 생성하여 제1 디바이스와 통신 디바이스로 각각 송신한다(S60).

[0086] 키 교환 확인 메시지를 제1 디바이스와 통신 디바이스로 송신하는 단계를 보다 구체적으로 도시하고 있는 도 9를 참고로 살펴보면, 서버는 키 교환 메시지의 해쉬값과 키 교환 메시지에 저장되어 있는 정보를 서버가 가지는 해쉬함수에 적용하여 생성된 해쉬값과 비교하여 키 교환 메시지의 무결성을 판단한 후(S61), 키 교환 메시지의 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)을 서버가 보유하고 있는 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)에 비교하여 제1 디바이스와 통신 디바이스 사이에서 교환된 키가 서로 동일한지 판단한다(S63). 바람직하게, 키 교환 메시지의 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)의 해쉬값과 서버가 보유하고 있는 통신 그룹 정보(K), 서버 정보(S) 및 그룹 시드값(G)의 해쉬값을 비교하여 제1 디바이스와 통신 디바이스 사이에서 교환된 키가 서로 동일한지 판단할 수 있다. 동일성 판단 결과에 따라 서버 정보(S), 통신 그룹 정보(K) 및 그룹 시드값(G) 순서의 해쉬값의 키 교환 확인 메시지를 생성하여 제1 디바이스와 통신 디바이스로 각각 송신한다(S65).

[0087] 다시 도 5를 참고로 살펴보면, 서버는 통신 그룹을 구성하는 디바이스 사이에서 공유 키를 교환하여 통신하는 중에도 주기적으로 통신 그룹을 구성하는 디바이스 사이에서 공유하는 공유 키를 갱신한다(S80). 한편, 통신 그룹을 구성하는 디바이스 중 통신 그룹을 탈퇴하는 탈퇴 디바이스가 존재하는 경우 서버의 통신 그룹 정보에서 탈퇴 디바이스를 삭제하고 탈퇴 디바이스의 시드값을 삭제한 새로운 공유 키로 갱신한다(S90).

[0088] 도 10은 본 발명에 따른 공유 키 교환 방법에서 공유 키를 갱신하는 단계를 보다 구체적으로 설명하는 흐름도이다.

[0089] 도 10을 참고로 보다 구체적으로 살펴보면, 서버는 그룹 통신의 공유 키를 갱신하고자 하는 경우 공유 키 갱신 메시지를 생성하여 통신 그룹의 디바이스로 송신한다(S81). 공유 키 갱신 메시지를 수신한 통신 그룹의 디바이스는 각각 자신의 디바이스 시드키를 생성하고, 생성한 디바이스 시드키를 구비하는 시드 조합값, 디바이스 정보를 포함하는 갱신 디바이스 정보 메시지를 서버로 송신한다(S82). 통신 그룹의 디바이스로부터 각각 갱신 디바이스 정보 메시지를 수신한 서버는 통신 그룹의 각 디바이스 시드값으로부터 갱신 예비 그룹 시드값을 생성하고(S83), 통신 그룹의 각 디바이스 정보로부터 갱신 예비 통신 그룹 정보를 생성한다(S84). 여기서 갱신 예비 그룹 시드값은 앞서 설명한 예비 그룹 시드값과 같이 자신을 제외한 통신 그룹의 다른 디바이스 시드값의 조합으로 생성되며, 갱신 예비 통신 그룹 정보는 앞서 설명한 예비 통신 그룹 정보와 같이 자신을 제외한 통신 그룹의 다른 디바이스 정보 조합으로 생성된다.

[0090] 서버는 갱신 예비 그룹 시드값, 갱신 예비 통신 그룹 정보 및 서버 정보를 구비하는 갱신 예비 정보 메시지를 생성하여 통신 그룹의 각 디바이스로 송신한다(S85). 갱신 예비 정보 메시지를 수신한 통신 그룹의 각 디바이스는 수신한 갱신 예비 그룹 시드값과 자신이 보유하고 있는 디바이스 시드값으로부터 갱신 그룹 시드값을 생성하며, 수신한 갱신 예비 통신 그룹 정보와 자신이 보유하고 있는 디바이스 정보로부터 갱신 통신 그룹 정보를 생성한다. 통신 그룹의 각 디바이스는 갱신 통신 그룹 정보, 서버 정보 및 갱신 그룹 시드값을 구비하는 갱신 키 교환 메시지를 생성하여 서버로 송신한다(S86). 여기서 갱신 키 교환 메시지는 각 디바이스의 갱신 통신 그룹 정보, 서버 정보 및 갱신 그룹 시드값 순서의 해쉬값을 더 구비하고 있다.

[0091] 서버는 통신 그룹 각 디바이스로부터 수신한 갱신 키 교환 메시지의 갱신 통신 그룹 정보, 서버 정보 및 갱신 그룹 시드값을 서버가 보유하고 있는 해쉬 함수에 적용한 해쉬값과 갱신 키 교환 메시지의 해쉬값과 비교하여 갱신 키 교환 메시지의 무결성을 판단하며, 통신 그룹 각 디바이스로부터 수신한 갱신 키 교환 메시지의 갱신 키가 서로 동일한지 판단한다(S87). 판단 결과 통신 그룹 각 디바이스의 갱신 키가 서로 동일한 경우, 서버 정보, 각 디바이스의 갱신 통신 그룹 정보와 갱신 그룹 시드값를 구비하는 갱신 키 교환 확인 메시지를 생성하여 통신 그룹의 각 디바이스로 송신한다(S88). 갱신 키 교환 확인 메시지를 수신한 통신 그룹의 각 디바이스는 서버 정보, 갱신 통신 그룹 정보 및 갱신 그룹 시드값의 조합으로 이루어진 공통의 갱신 키를 생성하여 통신 그룹의 각 디바이스에서 송수신되는 메시지를 암호화하는데 사용되는 공유 키로 사용한다. 여기서 갱신 키 교환 확

인 메시지는 각 디바이스의 서버 정보, 갱신 통신 그룹 정보 및 갱신 그룹 시드값 순서의 해쉬값을 더 구비하고 있다. 바람직하게, 통신 그룹 각 디바이스는 수신한 갱신 키 교환 확인 메시지의 서버 정보, 갱신 통신 그룹 정보 및 갱신 그룹 시드값을 서버가 보유하고 있는 해쉬 함수에 적용한 해쉬값과 갱신 키 교환 확인 메시지의 해쉬값과 비교하여 갱신 키 교환 확인 메시지의 무결성을 판단한다.

[0092] 도 11은 통신 그룹에서 탈퇴하는 탈퇴 디바이스를 서버에 등록하는 단계를 보다 구체적으로 설명하는 흐름도이다.

[0093] 도 11을 참고로 보다 구체적으로 살펴보면, 통신 그룹의 디바이스 중 통신 그룹에서 탈퇴하고자 하는 탈퇴 디바이스가 존재하는 경우 탈퇴 디바이스는 탈퇴 디바이스의 식별자를 구비하는 탈퇴 요청 메시지를 생성하고, 생성한 탈퇴 요청 메시지를 서버로 송신한다(S91). 탈퇴 요청 메시지를 수신하는 경우, 서버는 탈퇴 요청 메시지에 응답하여 서버에 등록되어 있는 통신 그룹에서 탈퇴 디바이스의 식별자를 삭제하여 서버에 등록되어 있는 통신 그룹 정보를 갱신한다(S93). 서버에서 통신 그룹 정보의 갱신이 완료된 후, 서버는 탈퇴 디바이스에게 탈퇴 완료 메시지를 송신하며, 탈퇴 디바이스를 제외한 통신 그룹을 구성하는 디바이스 사이의 공유 키를 앞서 도 10을 참고로 설명한 갱신 방법으로 갱신한다(S95).

[0094] 한편, 상술한 본 발명의 실시 예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0095] 상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장 매체(예를 들어, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

[0096] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

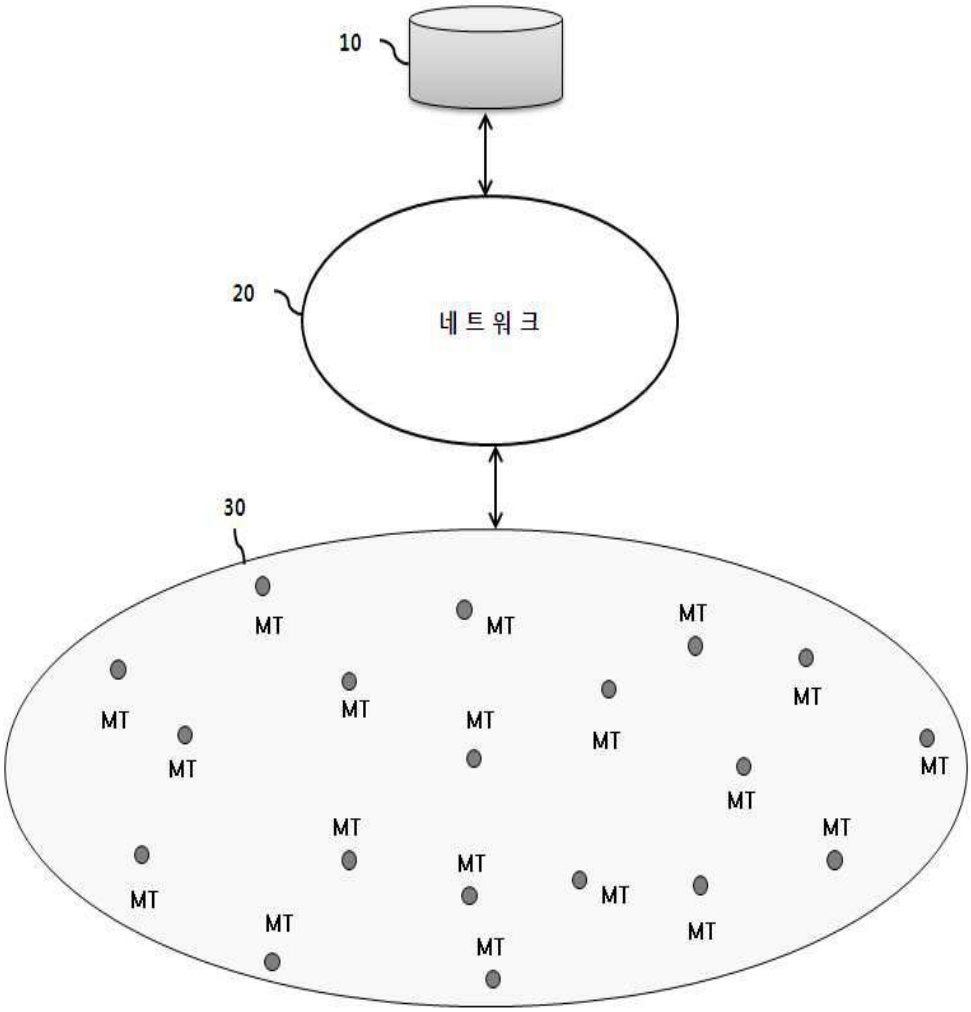
부호의 설명

[0097] 10: 서버 20: 네트워크

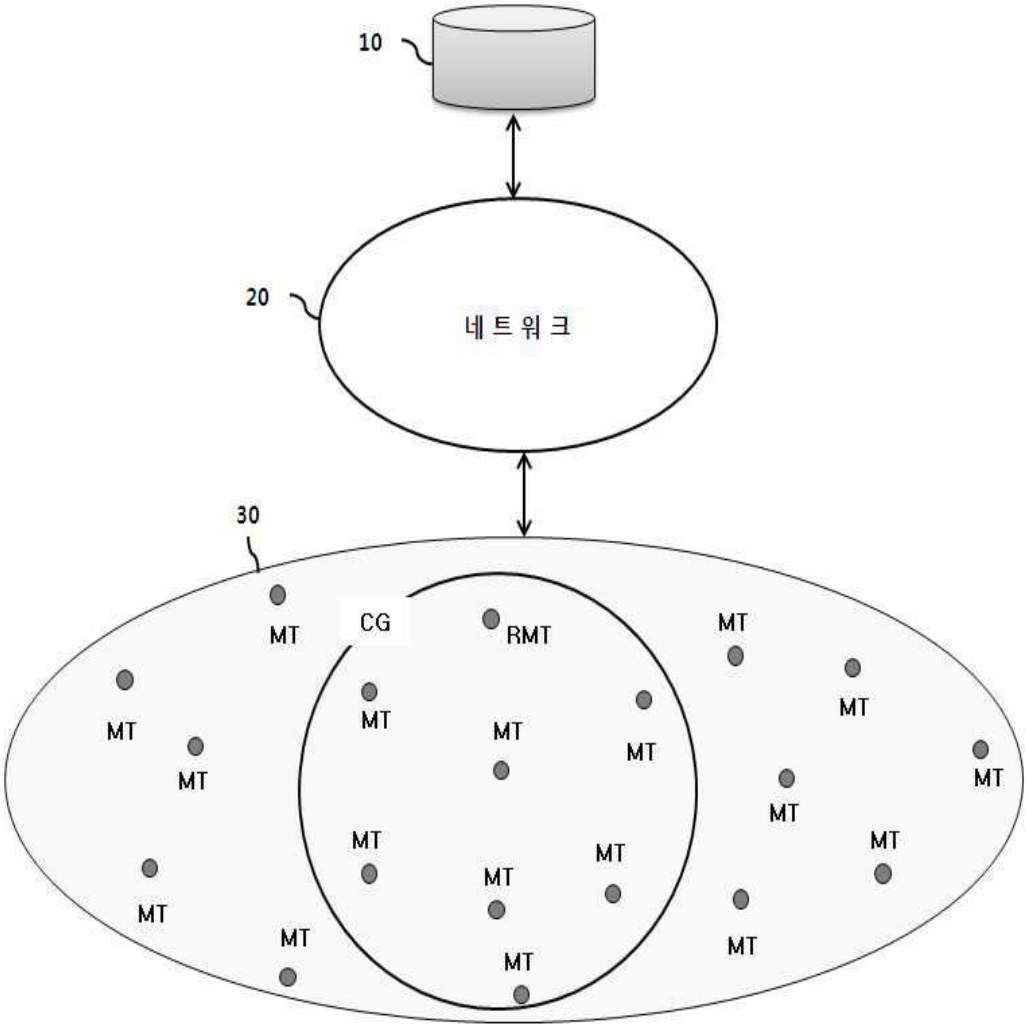
30: 디바이스 네트워크

도면

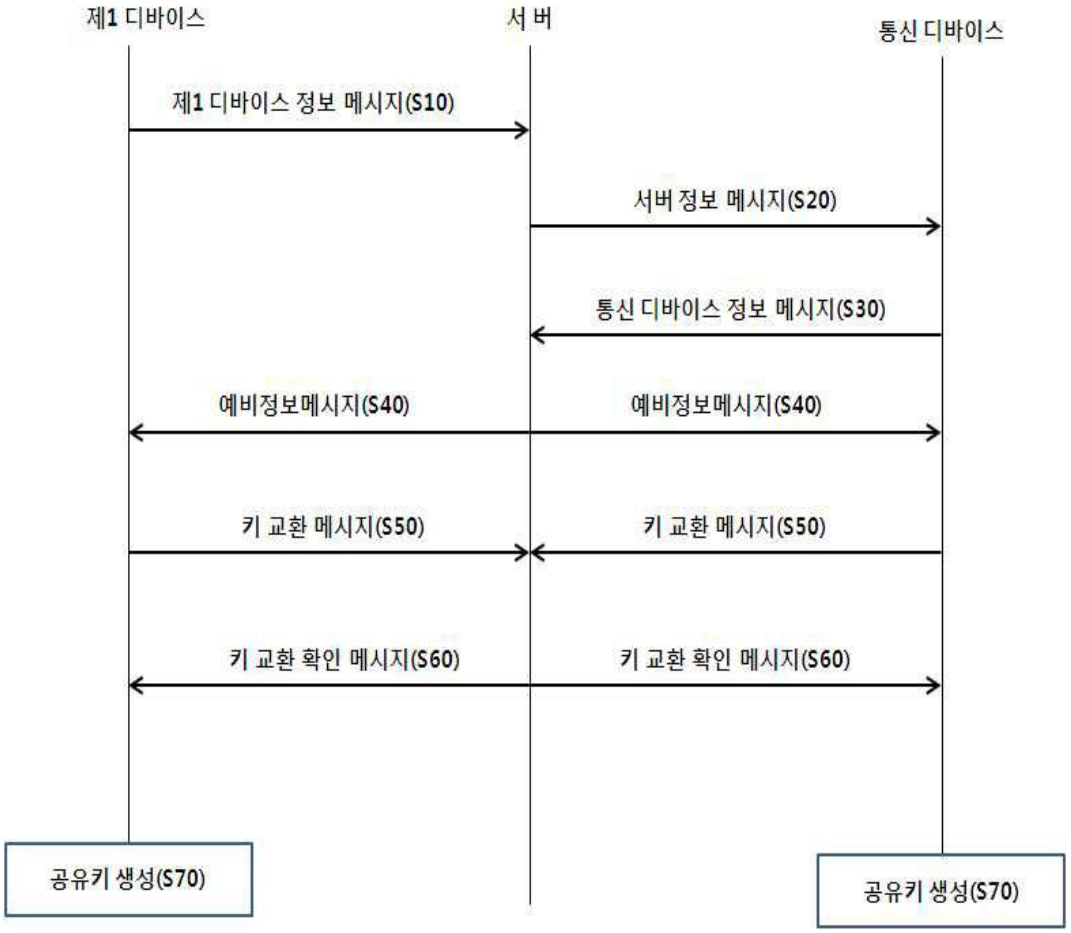
도면1



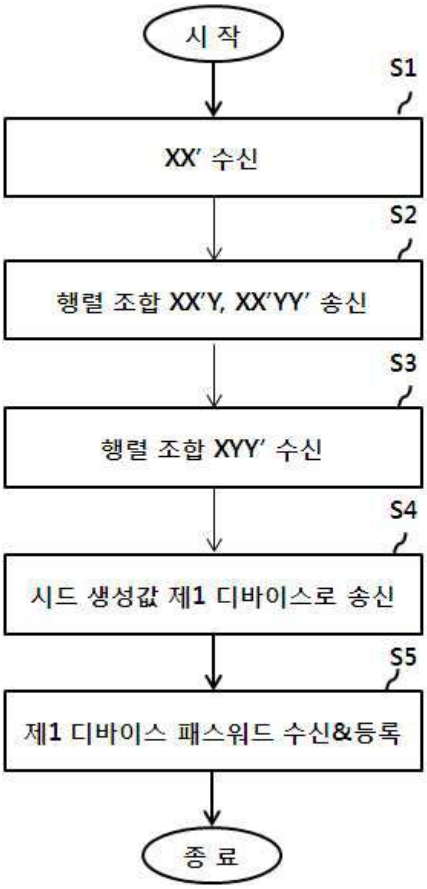
도면2


10
20
네트워크
30
MT
CG
RMT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT
MT

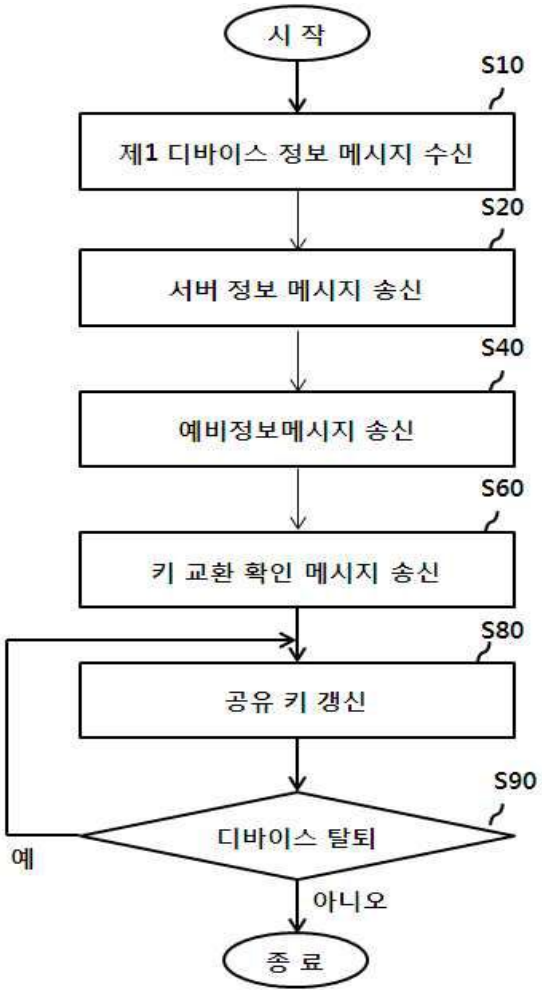
도면3


제1 디바이스
서 버
통신 디바이스
제1 디바이스 정보 메시지(S10)
서버 정보 메시지(S20)
통신 디바이스 정보 메시지(S30)
예비정보메시지(S40)
예비정보메시지(S40)
키 교환 메시지(S50)
키 교환 메시지(S50)
키 교환 확인 메시지(S60)
키 교환 확인 메시지(S60)
공유키 생성(S70)
공유키 생성(S70)

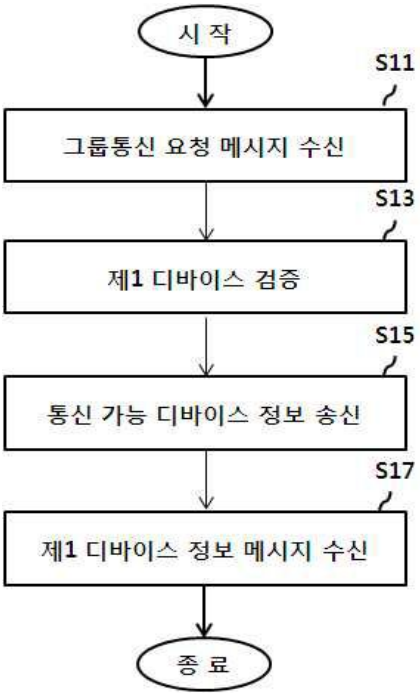
도면4


시 작
S1
XX′ 수신
S2
행렬 조합 XX′Y, XX′YY′ 송신
S3
행렬 조합 XYY′ 수신
S4
시드 생성값 제1 디바이스로 송신
S5
제1 디바이스 패스워드 수신&등록
종 료

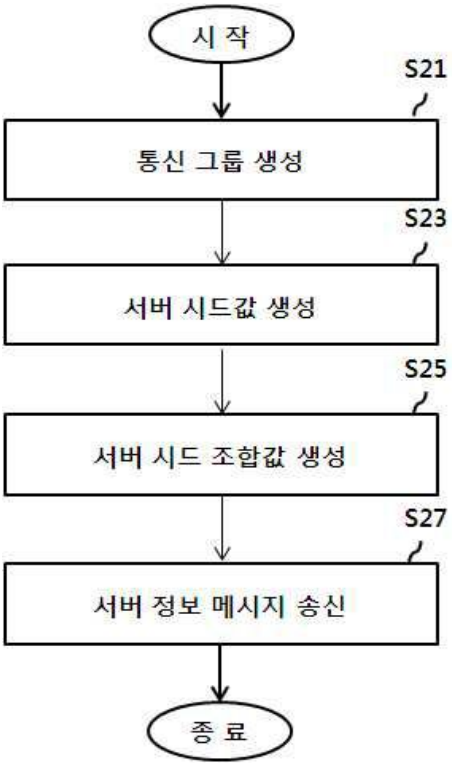
도면5


시 작
S10
제1 디바이스 정보 메시지 수신
S20
서버 정보 메시지 송신
S40
예비정보메시지 송신
S60
키 교환 확인 메시지 송신
S80
공유 키 갱신
S90
디바이스 탈퇴
예
아니오
종 료

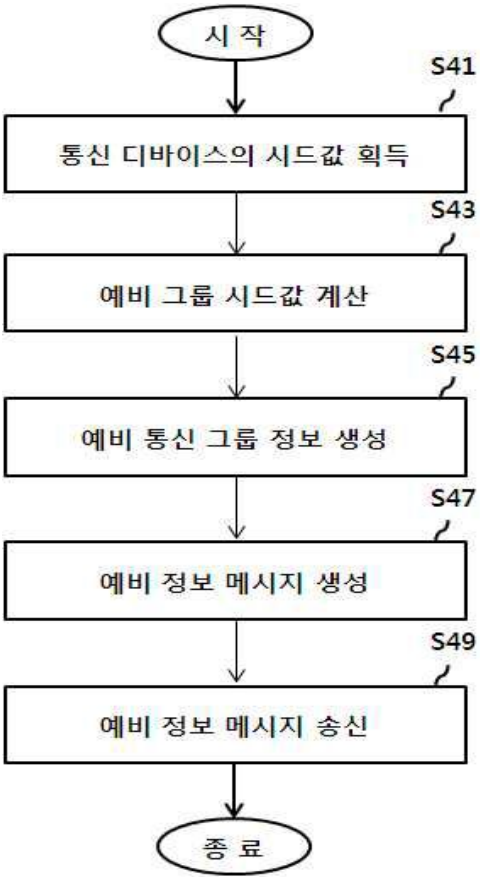
도면6


시 작
S11
그룹통신 요청 메시지 수신
S13
제1 디바이스 검증
S15
통신 가능 디바이스 정보 송신
S17
제1 디바이스 정보 메시지 수신
종 료

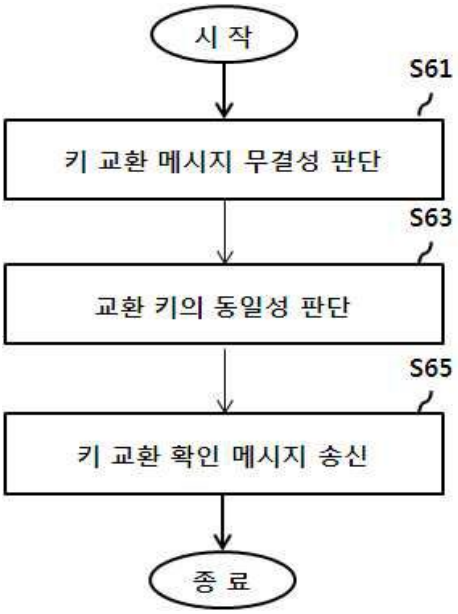
도면7


시 작
S21
통신 그룹 생성
S23
서버 시드값 생성
S25
서버 시드 조합값 생성
S27
서버 정보 메시지 송신
종 료

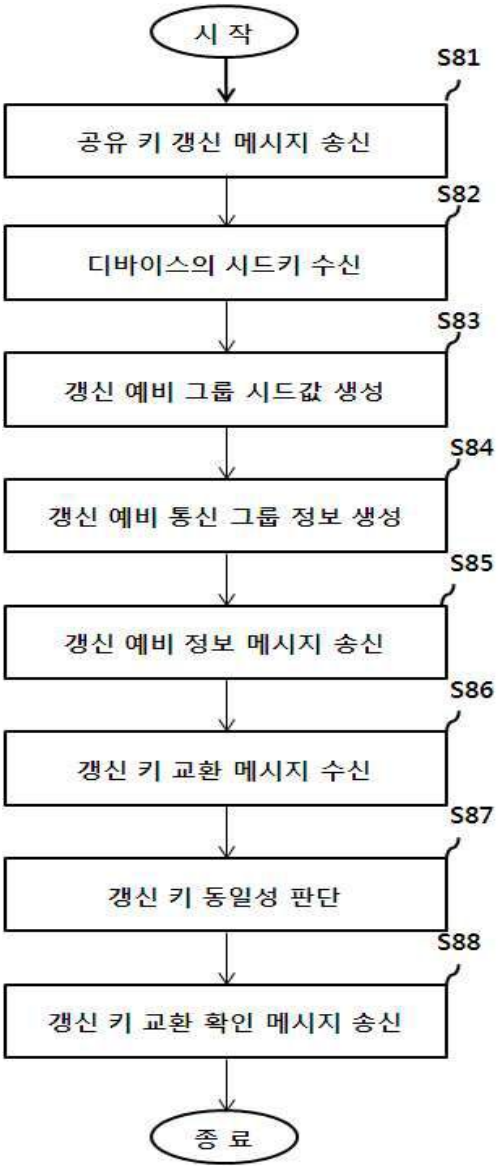
도면8


시 작
S41
통신 디바이스의 시드값 획득
S43
예비 그룹 시드값 계산
S45
예비 통신 그룹 정보 생성
S47
예비 정보 메시지 생성
S49
예비 정보 메시지 송신
종 료

도면9



도면10


시 작
S81
공유 키 갱신 메시지 송신
S82
디바이스의 시드키 수신
S83
갱신 예비 그룹 시드값 생성
S84
갱신 예비 통신 그룹 정보 생성
S85
갱신 예비 정보 메시지 송신
S86
갱신 키 교환 메시지 수신
S87
갱신 키 동일성 판단
S88
갱신 키 교환 확인 메시지 송신
종 료

도면11

