

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2013-0053923 (43) 공개일자 2013년05월24일
(51) 국제특허분류(Int. Cl.) H04L 9/08 (2006.01) H04W 12/04 (2009.01)		(71) 출원인 경희대학교 산학협력단 경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스 내 (서천동, 경희대학교)
(21) 출원번호 10-2011-0119636 (22) 출원일자 2011년11월16일 심사청구일자 2011년11월16일		(72) 발명자 홍충선 경기도 용인시 수지구 상현동 성원상떼빌아파트 233동 101호 송태일 서울특별시 강서구 금남화로23길 8, 105동 1304호 (방화동, 동성아파트) (뒷면에 계속)
		(74) 대리인 서재승

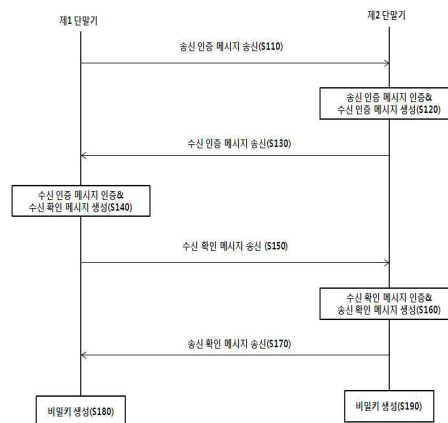
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 무선 단말기와 유선 단말기 사이의 비밀키 교환 방법

(57) 요약

본 발명은 단말기 사이의 비밀키 교환 방법에 관한 것으로, 보다 구체적으로 에너지원이 한정된 무선 단말기와 유선 단말기 사이에서 무선 단말기의 다수 프로세서가 공유하는 공통 보안 통신 세션을 통해 무선 단말기와 유선 단말기 사이의 비밀키를 교환하고, 교환한 비밀키로 데이터를 암호화하여 공통 보안 통신 세션을 통해 보안 통신을 수행하는 비밀키 교환 방법에 관한 것이다.

대표도 - 도4



(72) 발명자

조웅준

경기도 수원시 영통구 청명로59번길 54, 103호 (영통동)

강형규

제주특별자치도 서귀포시 하효중앙로 148 (하효동)

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

단말기 사이의 비밀키 교환 방법에 있어서

- (a) 제1 단말기에서 송신 시드값과 송신 랜덤값을 구비하는 송신 인증 메시지를 생성하고, 생성한 상기 송신 인증 메시지를 제2 단말기로 송신하는 단계;
 - (b) 상기 제2 단말기에서 상기 송신 인증 메시지의 무결성을 판단하고, 수신 시드값과 수신 랜덤값 및 암호화된 상기 수신 시드값, 상기 수신 랜덤값, 상기 송신 랜덤값을 구비하는 수신 인증 메시지를 상기 제1 단말기로 송신하는 단계;
 - (c) 상기 제1 단말기에서 상기 수신 인증 메시지의 무결성과 상기 송신 랜덤값에 기초하여 상기 송신 인증 메시지의 재전송 공격을 판단하고, 암호화된 상기 송신 시드값 및 수신 시드값의 조합으로 생성되는 키, 상기 무선 단말기의 식별자, 관리 서버의 식별자 및 상기 수신 랜덤값을 구비하는 수신 확인 메시지를 상기 제2 단말기로 송신하는 단계; 및
 - (d) 상기 제2 단말기에서 상기 수신 확인 메시지의 무결성과 상기 수신 랜덤값에 기초하여 상기 수신 인증 메시지의 재전송 공격 여부를 판단하고, 암호화된 상기 제1 단말기의 식별자, 상기 제2 단말기의 식별자 및 상기 제2 단말기가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 구비하는 송신 확인 메시지를 상기 제1 단말기로 송신하는 단계를 포함하며,
- 상기 제1 단말기와 상기 제2 단말기는 상기 송수신된 키 및 상기 제1 단말기의 식별자를 이용하여 상기 제1 단말기와 상기 제2 단말기 사이의 비밀키를 생성하는 것을 특징으로 하는 비밀키 교환 방법.

청구항 2

제 1 항에 있어서,

상기 제1 단말기는 무선 통신 네트워크의 무선 단말기이며, 상기 제2 단말기는 유선 통신 네트워크의 유선 단말기인 것을 특징으로 하는 비밀키 교환 방법.

청구항 3

제 1 항에 있어서, 상기 송신 인증 메시지는

상기 제1 단말기에서 상기 제1 단말기 식별자, 생성된 송신 시드값, 송신 랜덤값, 상기 송신 인증 메시지의 수명값 및 상기 제1 단말기 식별자, 생성된 송신 시드값, 송신 랜덤값, 상기 송신 인증 메시지의 수명값을 암호화한 제1 암호화값을 구비하며,

상기 송신 시드값은 송신 시드 랜덤값(SC), 상기 제1 단말기와 상기 제2 단말기가 공유하는 설정값(M), 상기 제1 단말기의 패스워드(PW) 및 시드 함수(g)의 조합으로부터 생성되는 것을 특징으로 하는 비밀키 교환 방법.

청구항 4

제 3 항에 있어서, 상기 (b) 단계는

상기 제2 단말기에서 상기 제1 단말기로부터 상기 송신 인증 메시지를 수신하는 단계;

상기 수신한 상기 제1 단말기 식별자, 상기 송신 시드값, 상기 송신 랜덤값 및 상기 송신 인증 메시지의 수명값을 암호화한 제2 암호화값과 상기 제1 암호화 값의 동일 여부로 상기 송신 인증 메시지의 무결성을 판단하는 단계; 및

상기 송신 인증 메시지의 무결성 판단이 완료된 후, 상기 제2 단말기에서 상기 제2 단말기의 식별자, 생성된 수신 시드값, 수신 랜덤값, 상기 수신 인증 메시지의 수명값과 상기 제2 단말기의 식별자, 생성된 수신 시드값, 수신 랜덤값, 상기 수신 인증 메시지의 수명값을 암호화한 제3 암호화값, 상기 송신 랜덤값을 암호화한 제4 암호화값을 구비하는 수신 인증 메시지를 생성하고 상기 수신 인증 메시지를 상기 제1 단말기로 송신하는 단계를

포함하는 것을 포함하며,

상기 수신 시드값은 수신 시드 랜덤값(SS), 상기 설정값(M), 상기 패스워드(PW) 및 시드 함수(g)의 조합으로부터 생성되는 것을 특징으로 하는 비밀키 교환 방법.

청구항 5

제 4 항에 있어서, 상기 (c) 단계는

상기 제1 단말기에서 상기 수신 인증 메시지를 수신하는 단계;

상기 수신한 제2 단말기 식별자, 상기 수신 시드값, 상기 수신 랜덤값 및 상기 수신 인증 메시지의 수명값을 암호화한 제5 암호화값과 상기 제3 암호화 값의 동일 여부로 상기 수신 인증 메시지의 무결성을 판단하는 단계;

상기 제1 단말기가 보유하고 있는 상기 송신 랜덤값을 암호화한 제6 암호화값과 상기 제4 암호화값의 동일 여부로 상기 송신 인증 메시지의 재전송 공격 여부를 판단하는 단계;

상기 수신 인증 메시지의 무결성 및 상기 송신 인증 메시지의 재전송 공격 여부의 판단이 완료된 후, 상기 제1 단말기의 식별자, 제2 단말기의 식별자, 상기 제1 단말기에서 상기 송신 시드값 및 수신 시드값의 조합으로 생성되는 키를 암호화한 제7 암호화값과 상기 수신 랜덤값을 암호화한 제8 암호화값을 구비하는 수신 확인 메시지를 생성하는 단계; 및

상기 생성한 수신 확인 메시지를 상기 제2 단말기로 송신하는 단계를 포함하는 것을 특징으로 하는 비밀키 교환 방법.

청구항 6

제 5 항에 있어서, 상기 (d) 단계는

상기 제2 단말기에서 상기 수신 확인 메시지를 수신하는 단계;

상기 제2 단말기에서 상기 제1 단말기의 식별자, 상기 제2 단말기의 식별자 및 상기 제2 단말기가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 암호화한 제9 암호화값과 상기 제7 암호화값의 동일 여부로 상기 수신 확인 메시지의 무결성을 확인하는 단계;

상기 제2 단말기가 보유하고 있는 상기 수신 랜덤값을 암호화한 제10 암호화값과 상기 제8 암호화값의 동일 여부로 상기 수신 인증 메시지의 재전송 공격 여부를 판단하는 단계;

상기 수신 인증 메시지의 무결성 및 재전송 공격 여부의 판단이 완료된 후, 상기 제2 단말기에서 상기 제2 단말기의 식별자, 상기 제1 단말기의 식별자 및 상기 제2 단말기가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 암호화한 제11 암호화값을 구비하는 송신 확인 메시지를 생성하는 단계; 및

상기 송신 확인 메시지를 상기 제1 단말기로 송신하는 단계를 포함하는 것을 특징으로 하는 비밀키 교환 방법.

청구항 7

무선 통신 네트워크의 무선 단말기와 상기 무선 단말기가 접속하고 있는 유선 통신 네트워크 사이의 비밀키 교환 방법에 있어서,

상기 무선 단말기는 실행중인 다수의 프로세스 각각에 상기 유선 통신 네트워크와의 일반 통신 세션을 할당하여 상기 유선 네트워크와 일반 통신을 수행하며,

상기 다수의 프로세스는 상기 유선 통신 네트워크와 교환한 비밀키로 암호화된 송수신 데이터를 상기 다수의 프로세스의 공통 보안 통신 세션을 통해 상기 유선 네트워크와 보안 통신을 수행하는 것을 특징으로 하는 비밀키 교환 방법.

청구항 8

제 7 항에 있어서,

상기 무선 단말기는 상기 비밀키로 암호화된 송수신 데이터를 상기 공통 보안 통신 세션을 통해 상기 유선 네트워크의 관리 서버와 보안 통신을 수행하는 것을 특징으로 하는 비밀키 교환 방법.

청구항 9

제 8 항에 있어서, 상기 비밀키는

상기 공토 보안 통신 세션을 통해 상기 무선 단말기와 상기 관리 서버 사이에서 교환되는 것을 특징으로 하는 비밀키 교환 방법.

청구항 10

제 9 항에 있어서, 상기 무선 단말기와 상기 관리 서버 사이의 비밀키는

(a) 상기 무선 단말기에서 생성된 송신 시드값과 송신 랜덤값을 구비하는 송신 인증 메시지를 상기 관리 서버로 송신하는 단계;

(b) 상기 관리 서버에서 상기 송신 인증 메시지의 무결성을 판단하고, 수신 시드값과 수신 랜덤값 및 암호화된 상기 수신 시드값, 상기 수신 랜덤값, 상기 송신 랜덤값을 구비하는 수신 인증 메시지를 상기 무선 단말기로 송신하는 단계;

(c) 상기 무선 단말기에서 상기 수신 인증 메시지의 무결성과 상기 송신 랜덤값에 기초하여 상기 송신 인증 메시지의 재전송 공격을 판단하고, 암호화된 상기 송신 시드값 및 수신 시드값의 조합으로 생성되는 키, 상기 무선 단말기의 식별자, 관리 서버의 식별자 및 상기 수신 랜덤값을 구비하는 수신 확인 메시지를 상기 관리 서버로 송신하는 단계; 및

(d) 상기 관리 서버에서 상기 수신 확인 메시지의 무결성과 상기 수신 랜덤값에 기초하여 상기 수신 인증 메시지의 재전송 공격 여부를 판단하고, 암호화된 상기 무선 단말기의 식별자, 상기 관리 서버의 식별자 및 상기 관리 서버가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 구비하는 송신 확인 메시지를 상기 무선 단말기로 송신하는 단계를 통해 교환되며,

상기 무선 단말기와 상기 관리 서버는 상기 송수신된 키 및 상기 무선 단말기의 식별자를 이용하여 상기 무선 단말기와 상기 관리 서버 사이의 비밀키를 생성하는 것을 특징으로 하는 비밀키 교환 방법.

청구항 11

제 10 항에 있어서, 상기 송신 인증 메시지는

상기 무선 단말기에서 상기 무선 단말기 식별자, 생성된 송신 시드값, 송신 랜덤값, 상기 송신 인증 메시지의 수명값 및 상기 무선 단말기 식별자, 생성된 송신 시드값, 송신 랜덤값, 상기 송신 인증 메시지의 수명값을 암호화한 제1 암호화값을 구비하며,

상기 송신 시드값은 송신 시드 랜덤값(SC), 상기 무선 단말기와 상기 관리 서버가 공유하는 설정값(M), 상기 무선 단말기의 패스워드(PW) 및 시드 함수(g)의 조합으로부터 생성되는 것을 특징으로 하는 비밀키 교환 방법.

청구항 12

제 11 항에 있어서, 상기 (b) 단계는

상기 관리 서버에서 상기 무선 단말기로부터 상기 송신 인증 메시지를 수신하는 단계;

상기 수신한 상기 무선 단말기 식별자, 상기 송신 시드값, 상기 송신 랜덤값 및 상기 송신 인증 메시지의 수명값을 암호화한 제2 암호화값과 상기 제1 암호화 값의 동일 여부로 상기 송신 인증 메시지의 무결성을 판단하는 단계; 및

상기 송신 인증 메시지의 무결성 판단이 완료된 후, 상기 관리 서버에서 상기 관리 서버의 식별자, 생성된 수신 시드값, 수신 랜덤값, 상기 수신 인증 메시지의 수명값과 상기 관리 서버의 식별자, 생성된 수신 시드값, 수신 랜덤값, 상기 수신 인증 메시지의 수명값을 암호화한 제3 암호화값, 상기 송신 랜덤값을 암호화한 제4 암호화값을 구비하는 수신 인증 메시지를 생성하고 상기 수신 인증 메시지를 상기 무선 단말기로 송신하는 단계를 포함하는 것을 포함하며,

상기 수신 시드값은 수신 시드 랜덤값(SS), 상기 설정값(M), 상기 패스워드(PW) 및 시드 함수(g)의 조합으로부터 생성되는 것을 특징으로 하는 비밀키 교환 방법.

청구항 13

제 12 항에 있어서, 상기 (c) 단계는

상기 무선 단말기에서 상기 수신 인증 메시지를 수신하는 단계;

상기 수신한 관리 서버 식별자, 상기 수신 시드값, 상기 수신 랜덤값 및 상기 수신 인증 메시지의 수명값을 암호화한 제5 암호화값과 상기 제3 암호화 값의 동일 여부로 상기 수신 인증 메시지의 무결성을 판단하는 단계;

상기 무선 단말기가 보유하고 있는 상기 송신 랜덤값을 암호화한 제6 암호화값과 상기 제4 암호화값의 동일 여부로 상기 송신 인증 메시지의 재전송 공격 여부를 판단하는 단계;

상기 수신 인증 메시지의 무결성 및 상기 송신 인증 메시지의 재전송 공격 여부의 판단이 완료된 후, 상기 무선 단말기의 식별자, 관리 서버의 식별자, 상기 무선 단말기에서 상기 송신 시드값 및 수신 시드값의 조합으로 생성되는 키를 암호화한 제7 암호화값과 상기 수신 랜덤값을 암호화한 제8 암호화값을 구비하는 수신 확인 메시지를 생성하는 단계; 및

상기 생성한 수신 확인 메시지를 상기 관리 서버로 송신하는 단계를 포함하는 것을 특징으로 하는 비밀키 교환 방법.

청구항 14

제 13 항에 있어서, 상기 (d) 단계는

상기 관리 서버에서 상기 수신 확인 메시지를 수신하는 단계;

상기 관리 서버에서 상기 무선 단말기의 식별자, 상기 관리 서버의 식별자 및 상기 관리 서버가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 암호화한 제9 암호화값과 상기 제7 암호화값의 동일 여부로 상기 수신 확인 메시지의 무결성을 확인하는 단계;

상기 관리 서버가 보유하고 있는 상기 수신 랜덤값을 암호화한 제10 암호화값과 상기 제8 암호화값의 동일 여부로 상기 수신 인증 메시지의 재전송 공격 여부를 판단하는 단계;

상기 수신 인증 메시지의 무결성 및 재전송 공격 여부의 판단이 완료된 후, 상기 관리 서버에서 상기 관리 서버의 식별자, 상기 무선 단말기의 식별자 및 상기 관리 서버가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 암호화한 제11 암호화값을 구비하는 송신 확인 메시지를 생성하는 단계; 및

상기 송신 확인 메시지를 상기 무선 단말기로 송신하는 단계를 포함하는 것을 특징으로 하는 비밀키 교환 방법.

명세서

기술분야

[0001] 본 발명은 단말기 사이의 비밀키 교환 방법에 관한 것으로, 보다 구체적으로 에너지와 연산 능력이 한정된 무선 단말기와 유선 단말기 사이에서 무선 단말기의 다수 프로세서가 공유하는 공통 보안 통신 세션을 통해 무선 단말기와 유선 단말기 사이의 비밀키를 교환하고, 교환한 비밀키로 데이터를 암호화하여 공통 보안 통신 세션을 통해 보안 통신을 수행하는 비밀키 교환 방법에 관한 것이다.

배경기술

[0002] 종래의 유선 통신 네트워크 또는 무선 통신 네트워크에서 사용된 비밀키 교환 방법은 유선 통신 네트워크 또는 무선 통신 네트워크만을 각각 고려하여 개발되었기 때문에, 유선 통신 네트워크와 무선 통신 네트워크가 공존하는 복합적인 통신 네트워크에서는 종래의 유선 통신 네트워크를 위한 비밀키 교환 방법 또는 종래의 무선 통신 네트워크를 위한 비밀키 교환 방법을 그대로 적용하기 곤란하다.

[0003] 더욱이 에너지 제한이 있으며 연산량 처리 속도에 한계를 가지는 무선 단말기의 경우에는 유선 단말기와 접속하기 위하여 사용되는 에너지 소비율을 줄일 필요가 있으며, 적은 연산량으로 유선 단말기와 신뢰있는 비밀키를 교환하여야 한다.

[0004] H.Fereidooni와 2명이 2009년 무선 통신 네트워킹 및 모바일 컴퓨팅에 발표한 "A new authentication and key exchange protocol for insecure networks"에서는 안전하지 않은 통신 네트워크에서 비밀키를 공유하는 종래기

술1에 대해 기재하고 있다. 종래기술1에서 송신 단말기와 수신 단말기는 6차례 송수신되는 송신 단말기의 쿠키 또는 수신 단말기의 쿠키를 이용하여 비밀키를 교환하는데, 송신 단말기의 쿠키 또는 수신 단말기의 쿠키를 이용하여 송신 단말기 또는 수신 단말기의 무결성을 판단하여야 하므로 연산량이 늘어나며 이에 따라 소비되는 에너지도 커지며, 허락받지 않은 제3자에 송신 단말기와 수신 단말기의 쿠키가 유출될 가능성이 커져 높은 신뢰도로 비밀키를 교환하지 못한다는 문제점을 가진다.

[0005] 한편, 종래 무선 통신 네트워크의 무선 단말기에서 다수의 프로세스가 각각 유선 통신 네트워크의 서버와 통신을 수행하기 위해서는 도 1 또는 도2에 도시되어 있는 것과 같이 통신 세션을 형성해야 한다.

[0006] 도 1을 참고로 종래 통신 세션 형성 방법의 일 예를 보다 구체적으로 살펴보면, 무선 단말기(10)가 다수의 프로세스를 실행하여 유선 통신 네트워크의 관리 서버와 접속하는 경우 무선 단말기는 각 프로세스에 대해 관리 서버와의 통신 세션을 접속 제어하는 통신 모듈이 할당된다. 프로세스1(11)에 대해 통신 모듈1(21)이 할당되며, 프로세스2(13)에 대해 통신 모듈2(23)이 할당되며, 프로세스3(15)에 대해 통신 모듈3(25)이 할당된다. 여기서 프로세스란 무선 단말기에서 실행중인 프로그램 또는 애플리케이션을 의미한다.

[0007] 통신 모듈1(21)은 프로세스1(11)이 관리 서버와 통신을 수행하는 통신 세션(L1)을 설정하며, 통신 모듈2(23)은 프로세스2(13)이 관리 서버와 통신을 수행하는 통신 세션(L2)을 설정하며, 통신 모듈3(25)은 프로세스3(15)이 관리 서버와 통신을 수행하는 통신 세션(L3)을 설정한다. 통신 모듈1 내지 통신 모듈3(21, 23, 25)은 일반 통신을 수행하는 경우 통신 세션(L1, L2, L3)을 일반 통신 세션으로 설정하며, 보안 통신을 하는 경우 통신 세션(L1, L2, L3)을 보안 통신 세션으로 설정하고 보안 통신 세션을 통해 관리 서버와 비밀키를 교환하여 비밀키로 암호화된 데이터를 관리 서버와 송수신하는 보안 통신을 수행한다.

[0008] 도 2를 참고로 종래 통신 세션 형성 방법의 다른 예를 보다 구체적으로 살펴보면, 무선 단말기(20)가 다수의 프로세스를 실행하여 유선 통신 네트워크의 관리 서버와 접속하는 경우 무선 단말기는 각 프로세스에 대해 관리 서버와의 통신 세션을 접속 제어하는 통신 모듈이 할당된다. 프로세스1(11)에 대해 일반 통신 모듈1(31)과 보안 통신 모듈1(32)이 할당되며, 프로세스2(13)에 대해 일반 통신 모듈2(33)과 보안 통신 모듈2(34)이 할당되며, 프로세스3(15)에 대해 일반 통신 모듈3(35)과 보안 통신 모듈3(36)이 할당된다.

[0009] 일반 통신 모듈1(31)은 프로세스1(11)이 관리 서버와 일반 통신을 수행하는 일반 통신 세션(NL1)을 설정하고 보안 통신 모듈1(32)은 프로세스1(11)이 관리 서버와 보안 통신을 수행하는 보안 통신 세션(SL1)을 형성한다. 또한, 일반 통신 모듈2(33)은 프로세스2(13)이 관리 서버와 일반 통신을 수행하는 일반 통신 세션(NL2)을 설정하고 보안 통신 모듈2(34)은 프로세스2(13)이 관리 서버와 보안 통신을 수행하는 보안 통신 세션(SL2)을 형성한다. 일반 통신 모듈3(35)은 프로세스3(15)이 관리 서버와 일반 통신을 수행하는 일반 통신 세션(NL3)을 설정하고 보안 통신 모듈3(36)은 프로세스3(15)이 관리 서버와 보안 통신을 수행하는 보안 통신 세션(SL3)을 형성한다.

[0010] 일반 통신 모듈1 내지 일반 통신 모듈3(31, 33, 35)은 일반 통신 세션(NL1, NL2, NL3)을 통해 관리 서버와 일반 통신을 수행하며, 보안 통신 모듈1 내지 보안 통신 모듈3(32, 34, 36)은 보안 통신 세션(SL1, SL2, SL3)을 통해 관리 서버와 비밀 통신을 수행한다.

발명의 내용

해결하려는 과제

[0011] 종래기술1이 가지는 문제점을 해결하기 위하여 본 발명의 출원인이 2011년 1월 10일 출원한 한국특허출원 제10-2011-0002417호(이하 종래기술2)는 송신 단말기에서 수신 단말기에 접속 요청하기 위한 접속요청 메시지를 수신 단말기로 송신하는 단계(이하 a 단계)와, 수신 단말기에서 접속 요청 메시지에 응답하여 수신 단말기의 시드키를 구비하는 수신 인증 메시지를 생성하고 생성한 수신 인증 메시지를 송신 단말기로 송신하는 단계(이하 b 단계)와, 수신 인증 메시지에 응답하여 송신 단말기에서 수신 단말기의 시드키와 송신 단말기의 시드키를 이용하여 생성한 비밀키로 암호화된 송신 TLL(Time to Live)값과 송신 단말기의 시드키를 구비하는 송신 인증 메시지를 수신 단말기로 송신하는 단계(이하 c 단계)와, 수신 단말기에서 수신 단말기의 시드키와 송신 단말기의 시드키를 이용하여 생성한 비밀키로 송신 TLL 값을 복호화하고 수신 단말기와 송신 단말기 사이의 홉수 및 수신 단

말기에서 수신한 송신 인증 메시지의 수신 TTL값을 판단하는 단계(이하 d 단계)와, 수신 단말기에서 판단한 홉수와 수신 TTL 값을 각각 비밀키로 암호화하고 송신 TTL 값을 TTL값으로 설정한 인증 승인 메시지를 송신 단말기로 송신하는 단계(이하 e단계)와, 송신 단말기에서 홉수와 수신 TTL값을 비밀키로 복호화하고 복호화된 홉수와 수신 TTL값의 합을 송신 TTL값과 비교하여 송신 단말기와 수신 단말기 사이에서 교환된 비밀키의 신뢰성을 1차 인증하는 단계(이하 f단계)와, 복호화된 수신 TTL값과 송신 인증 메시지의 송신 TTL값을 비교하여 송신 단말기와 수신 단말기 사이에서 교환된 비밀키의 신뢰성을 2차 인증하는 단계(이하 g단계)를 포함하여 구성되어 있다.

[0012] 그러나 종래기술2에서 송신 단말기와 수신 단말기 사이에서 송수신되는 메시지의 수는 종래기술1과 비교하여 줄었으며 송신 TTL, 수신 TTL, 홉수에 기초하여 신뢰도 높은 비밀키의 교환이 가능하지만, 홉수에 기초하여 송신 단말기와 수신 단말기 사이에서 송수신되는 인증 메시지의 무결성을 판단하기 때문에 실시간으로 데이터 라우팅 경로가 변경되는 네트워크에서는 사용하기 곤란하다는 문제점을 가진다.

[0013] 한편, 종래 통신 세션 형성 방법1은 1개의 통신 세션을 일반 통신 세션과 보안 통신 세션으로 사용하기 때문에 보안 세션으로 설정된 후 다시 일반 세션으로 통신을 수행하고자 하는 경우, 관리 서버와 세션 모드 변경을 위한 메시지를 주기적으로 송수신하여야 한다는 문제점을 가진다. 또한 종래 통신 세션 형성 방법2는 각 프로세스마다 일반 통신 모듈과 보안 통신 모듈을 구비하여 통신 세션 모드를 변경하기 위해 관리 서버와 메시지를 송수신할 필요는 없지만 에너지 제한적이며 계산 능력이 작은 무선 단말기에서 다수의 통신 모듈을 제어하는데 많은 에너지와 계산량을 요구한다는 문제점을 가진다.

[0014] 본 발명은 위에서 언급한 종래 기술들이 가지는 문제점을 해결하기 위한 것으로, 본 발명이 이루고자 하는 목적은 에너지원과 계산량이 한정된 무선 단말기와 유선 단말기 사이의 비밀키 교환 방법을 제공하는 것이다.

[0015] 본 발명이 이루고자 하는 다른 목적은 라우팅 경로가 변경되는 통신 네트워크에서도 비밀키 교환을 위한 메시지의 무결성을 인증할 수 있는 비밀키 교환 방법을 제공하는 것이다.

[0016] 본 발명이 이루고자 하는 또 다른 목적은 단말기 사이에서 송수신되는 적은 메시지로 비밀키를 높은 신뢰도로 교환할 수 있으며 공격자 노드에 의한 메시지 재전송 공격을 방지할 수 있는 비밀키 교환 방법을 제공하는 것이다.

[0017] 본 발명이 이루고자 하는 또 다른 목적은 무선 단말기의 다수 프로세스가 공유하는 공통 보안 통신 세션을 통해 암호화된 데이터를 송수신할 수 있는 비밀키 교환 방법을 제공하는 것이다.

과제의 해결 수단

[0018] 본 발명에 따른 비밀키를 교환하고자 하는 제1 단말기와 제2 단말기 사이에서 비밀키 교환 방법은 제1 단말기에서 생성된 송신 시드값과 송신 랜덤값을 구비하는 송신 인증 메시지를 제2 단말기로 송신하는 단계(이하 a 단계)와, 제2 단말기에서 송신 인증 메시지의 무결성을 판단하고 수신 시드값과 수신 랜덤값 및 암호화된 수신 시드값, 수신 랜덤값, 송신 랜덤값을 구비하는 수신 인증 메시지를 제1 단말기로 송신하는 단계(이하 b 단계)와, 제1 단말기에서 수신 인증 메시지의 무결성과 송신 랜덤값에 기초하여 송신 인증 메시지의 재전송 공격을 판단하고, 암호화된 송신 시드값 및 수신 시드값의 조합으로 생성되는 키, 상기 무선 단말기의 식별자, 관리 서버의 식별자 및 수신 랜덤값을 구비하는 수신 확인 메시지를 제2 단말기로 송신하는 단계(이하 c 단계)와, 제2 단말기에서 수신 확인 메시지의 무결성과 수신 랜덤값에 기초하여 수신 인증 메시지의 재전송 공격 여부를 판단하고, 암호화된 제1 단말기의 식별자, 제2 단말기의 식별자 및 제2 단말기가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 구비하는 송신 확인 메시지를 제2 단말기로 송신하는 단계(이하 d 단계)를 포함하며, 제1 단말기와 제2 단말기는 송수신된 키 및 제1 단말기의 식별자를 이용하여 제1 단말기와 제2 단말기 사이의 비밀키를 생성하는 것을 특징으로 한다.

[0019] 여기서 제1 단말기는 무선 통신 네트워크의 무선 단말기이며 제2 단말기는 제1 단말기가 접속하고 있는 유선 통신 네트워크의 관리 서버이고, 무선 단말기는 실행중인 다수의 프로세스 각각에 관리 서버와의 일반 통신 세션을 할당하여 관리 서버와 일반 통신을 수행하며, 다수의 프로세스는 관리 서버와 교환한 비밀키로 암호화된 송수신 데이터를 다수의 프로세스의 공통 보안 통신 세션을 통해 관리 서버와 보안 통신을 수행한다.

[0020] 여기서 송신 인증 메시지는 제1 단말기에서 무선 단말기 식별자, 생성된 송신 시드값, 송신 랜덤값, 송신 인증 메시지의 수명값 및 제1 단말기 식별자, 생성된 송신 시드값, 송신 랜덤값, 송신 인증 메시지의 수명값을 암호화한 제1 암호화값을 구비하며, 송신 시드값은 송신 시드 랜덤값(SC), 제1 단말기와 제2 단말기가 공유하는 설

정값(M), 제1 단말기의 패스워드(PW) 및 시드 함수(g)의 조합으로부터 생성되는 것을 특징으로 한다.

[0021] 바람직하게 (b) 단계는 제2 단말기에서 제1 단말기로부터 송신 인증 메시지를 수신하는 단계와, 수신한 상기 제1 단말기 식별자, 송신 시드값, 송신 랜덤값 및 송신 인증 메시지의 수명값을 암호화한 제2 암호화값과 제1 암호화 값의 동일 여부로 송신 인증 메시지의 무결성을 판단하는 단계와, 송신 인증 메시지의 무결성 판단이 완료된 후 제2 단말기에서 제2 단말기의 식별자, 생성된 수신 시드값, 수신 랜덤값, 수신 인증 메시지의 수명값과 제2 단말기의 식별자, 생성된 수신 시드값, 수신 랜덤값, 수신 인증 메시지의 수명값을 암호화한 제3 암호화값, 송신 랜덤값을 암호화한 제4 암호화값을 구비하는 수신 인증 메시지를 생성하고 수신 인증 메시지를 제1 단말기로 송신하는 단계를 포함하는 것을 포함하며, 수신 시드값은 수신 시드 랜덤값(SS), 설정값(M), 패스워드(PW) 및 시드 함수(g)의 조합으로부터 생성되는 것을 특징으로 한다.

[0022] 바람직하게, (c) 단계는 제1 단말기에서 상기 수신 인증 메시지를 수신하는 단계와, 수신한 제2 단말기 식별자, 수신 시드값, 수신 랜덤값 및 수신 인증 메시지의 수명값을 암호화한 제5 암호화값과 제3 암호화 값의 동일 여부로 수신 인증 메시지의 무결성을 판단하는 단계와, 제1 단말기가 보유하고 있는 송신 랜덤값을 암호화한 제6 암호화값과 제4 암호화값의 동일 여부로 송신 인증 메시지의 재전송 공격 여부를 판단하는 단계와, 수신 인증 메시지의 무결성 및 송신 인증 메시지의 재전송 공격 여부의 판단이 완료된 후 제1 단말기의 식별자, 제2 단말기의 식별자, 제1 단말기에서 송신 시드값 및 수신 시드값의 조합으로 생성되는 키를 암호화한 제7 암호화값과 수신 랜덤값을 암호화한 제8 암호화값을 구비하는 수신 확인 메시지를 생성하는 단계와, 생성한 수신 확인 메시지를 제2 단말기로 송신하는 단계를 포함하는 것을 특징으로 한다.

[0023] 바람직하게 (d) 단계는 제2 단말기에서 상기 수신 확인 메시지를 수신하는 단계와, 제2 단말기에서 상기 제1 단말기의 식별자, 제2 단말기의 식별자 및 제2 단말기가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 암호화한 제9 암호화값과 제7 암호화값의 동일 여부로 수신 확인 메시지를 인증하는 단계와, 제2 단말기가 보유하고 있는 수신 랜덤값을 암호화한 제10 암호화값과 제8 암호화값의 동일 여부로 수신 인증 메시지의 재전송 공격 여부를 판단하는 단계와, 수신 인증 메시지의 인증 및 재전송 공격 여부의 판단이 완료된 후 제2 단말기에서 제2 단말기의 식별자, 제1 단말기의 식별자 및 제2 단말기가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 암호화한 제11 암호화값을 구비하는 송신 확인 메시지를 생성하는 단계와, 송신 확인 메시지를 제1 단말기로 송신하는 단계를 포함하는 것을 특징으로 한다.

발명의 효과

[0024] 본 발명에 따른 비밀키 교환 방법은 종래 비밀키 교환 방법과 비교하여 다음과 같은 다양한 효과를 가진다.

[0025] 첫째, 본 발명에 따른 비밀키 교환 방법은 비밀키 교환을 위해 단말기 사이에서 송수신되는 메시지의 수가 적어 에너지원과 계산량이 한정된 무선 단말기와 유선 단말기 사이에서 적은 에너지 소비와 적은 계산량으로 비밀키를 교환할 수 있다.

[0026] 둘째, 본 발명에 따른 비밀키 교환 방법은 인증 메시지에 기반하여 비밀키를 교환함으로써, 라우팅 경로가 변경되는 통신 네트워크에서도 홉수에 무관하게 비밀키 교환을 위한 메시지의 무결성을 인증할 수 있다.

[0027] 셋째, 본 발명에 따른 비밀키 교환 방법은 비밀키 교환을 수행하는 단말기에서 각각 비밀키 교환을 위한 메시지를 생성하는 경우 송신 랜덤값 또는 수신 랜덤값을 포함하여 송신함으로써, 공격자 노드에 의한 메시지 재전송 공격을 방지할 수 있다.

[0028] 넷째, 본 발명에 따른 비밀키 교환 방법은 무선 단말기의 다수 프로세스가 공유하는 공통 보안 통신 세션을 통해 다수 프로세스가 공통으로 사용하는 비밀키를 교환하고 교환된 공통의 비밀키로 공통 보안 통신 세션을 통해 보안 통신을 수행함으로써, 프로세스마다 각각 보안 통신 세션을 할당하거나 일반 통신 세션과 보안 통신 세션을 공통으로 사용하는 종래기술보다 적은 에너지를 사용하여 통신을 수행할 수 있다.

도면의 간단한 설명

[0029] 도 1은 종래 무선 단말기와 유선 단말기 사이의 통신 세션을 형성하는 방법의 일 예를 설명하기 위한 도면이다.

도 2는 종래 무선 단말기와 유선 단말기 사이의 통신 세션을 형성하는 방법의 다른 예를 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 비밀키 교환 방법이 적용되는 무선 단말기의 통신 모듈의 구성예를 설명하

는 기능블록도이다.

도 4는 본 발명의 일 실시예에 따른 비밀키 교환 방법에서 송수신되는 메시지 흐름을 설명하기 위한 흐름도이다.

도 5는 본 발명에 따라 송신 인증 메시지를 인증하고 수신 인증 메시지를 생성하는 단계(S120)를 보다 구체적으로 설명하기 위한 흐름도이다.

도 6은 본 발명에 따라 수신 인증 메시지를 인증하고 수신 확인 메시지를 생성하는 단계(S140)를 보다 구체적으로 설명하기 위한 흐름도이다.

도 7은 본 발명에 따라 수신 확인 메시지를 인증하고 송신 확인 메시지를 생성하는 단계(S160)를 보다 구체적으로 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0030] 이하 첨부한 도면을 참고로 본 발명에 따른 비밀키 교환 방법에 대해 보다 구체적으로 설명한다.

[0031] 도 3은 본 발명의 일 실시예에 따른 비밀키 교환 방법이 적용되는 무선 단말기의 통신 모듈의 구성예를 설명하는 기능블록도이다.

[0032] 도 3을 참고로 본 발명에 따른 무선 단말기의 통신 모듈의 구성예를 보다 구체적으로 살펴보면, 무선 통신 네트워크의 제1 무선 단말기(100)가 다수의 프로세스를 실행하여 유선 통신 네트워크의 제2 단말기와 접속하는 경우 제1 무선 단말기는 각 프로세스에 대해 제2 단말기와의 통신 세션을 접속 제어하는 일반 통신 모듈이 할당된다. 프로세스1(111)에 대해 일반 통신 모듈1(121)이 할당되며, 프로세스2(113)에 대해 일반 통신 모듈2(123)이 할당되며, 프로세스3(115)에 대해 일반 통신 모듈3(125)이 할당된다. 바람직하게, 유선 통신 네트워크의 제2 단말기는 유선 통신 네트워크에서 운행되는 단말기 단위 또는 애플리케이션 단위로 데이터 송수신을 관리하는 관리 서버인 것을 특징으로 한다.

[0033] 일반 통신 모듈1(121)은 프로세스1(111)이 제2 단말기와 일반 통신을 수행하는 일반 통신 세션(NL1)을 설정하고 일반 통신 모듈2(123)은 프로세스2(113)가 제2 단말기와 일반 통신을 수행하는 일반 통신 세션(NL2)을 설정하며 일반 통신 모듈3(125)은 프로세스3(115)이 제2 단말기와 일반 통신을 수행하는 일반 통신 세션(NL3)을 설정한다. 한편, 프로세스1 내지 프로세스3(111, 113, 115)에 대해 프로세스1 내지 프로세스3(111, 113, 115)가 공유하는 공통의 보안 통신 모듈(130)이 할당되며, 보안 통신 모듈(130)은 프로세스1 내지 프로세스3(111, 113, 115)가 제2 단말기와 보안 통신을 수행하는 보안 통신 세션(SL)을 설정한다.

[0034] 프로세스1 내지 프로세스3(111, 113, 115)는 프로세스1 내지 프로세스3(111, 113, 115)에 각각 할당된 일반 통신 세션(NL1, NL2, NL3)을 통해 제2 단말기와 일반 통신을 수행하며, 프로세스1 내지 프로세스3(111, 113, 115)가 공유하는 보안 통신 세션(SL)을 통해 제2 단말기와 보안 통신을 수행한다.

[0035] 일반 통신 모듈(121, 123, 125)은 보안 통신 모듈(130)과 프로세스 통신(IPC, Inter Process Communication)을 수행하는데, 프로세스1 내지 프로세스3(111, 113, 115)이 보안 통신을 수행하는 경우 프로세스1 내지 프로세스3(111, 113, 115)에 할당된 일반 통신 모듈(121, 123, 125)은 보안 통신 모듈(130)로 프로세스 통신을 통해 송신하고자 하는 데이터를 전달하며, 보안 통신 모듈(130)은 전달받은 데이터를 비밀키로 암호화하여 보안 통신 세션(SL)을 통해 제2 단말기로 송신한다.

[0036] 도 4는 본 발명의 일 실시예에 따른 비밀키 교환 방법에서 송수신되는 메시지 흐름을 설명하기 위한 흐름도이다.

[0037] 도 4를 참고로 보다 구체적으로 살펴보면, 무선 통신 네트워크의 제1 단말기는 유선 통신 네트워크의 제2 단말기, 예를 들어 관리 서버와 보안 통신을 수행하기 위해 송신 인증 메시지를 생성하고 생성한 송신 인증 메시지를 제2 단말기로 송신한다(S110). 송신 인증 메시지는 제1 단말기 식별자, 제1 단말기에서 생성된 송신 시드값, 송신 랜덤값, 송신 인증 메시지의 수명값 및 제1 단말기 식별자, 생성된 송신 시드값, 송신 랜덤값, 송신 인증 메시지의 수명값을 암호화한 제1 암호화값을 구비한다. 바람직하게, 제1 단말기 식별자, 제1 단말기에서 생성된 송신 시드값, 송신 랜덤값, 송신 인증 메시지의 수명값은 제1 해쉬함수로 암호화되는 것을 특징으로

한다.

[0038] 여기서 송신 시드값(SEED-D1)은 송신 시드 랜덤값(SC), 제1 단말기와 제2 단말기가 공유하는 설정값(M), 제1 단말기의 패스워드(PW) 및 시드 함수(g)의 조합으로부터 생성되는데, 예를 들어 아래의 수학적식(1)과 같이 생성된다.

[0039] [수학적식 1]

$$SEED-D1 = g^{D_1} SM^{pw1}$$

[0041] 제2 단말기는 제1 단말기로부터 송신 인증 메시지를 수신하는 경우, 제2 단말기는 송신 인증 메시지의 제1 단말기 식별자, 제1 단말기에서 생성된 송신 시드값, 송신 랜덤값, 송신 인증 메시지의 수명값을 제1 단말기와 동일한 암호화 방식으로 암호화한 제2 암호화 값과 송신 인증 메시지의 제1 암호화 값이 서로 동일한지 여부로 송신 인증 메시지의 무결성을 판단하여 송신 인증 메시지를 인증하고, 수신 시드값과 수신 랜덤값 및 암호화된 상기 수신 시드값, 상기 수신 랜덤값, 상기 송신 랜덤값을 구비하는 수신 인증 메시지를 생성한다(S120). 바람직하게, 제2 단말기는 제1 해쉬 함수로 제1 단말기 식별자, 송신 인증 메시지의 송신 시드값, 송신 랜덤값, 송신 인증 메시지의 수명값을 암호화하여 제2 암호화 값을 생성한다. 제2 단말기는 생성한 수신 인증 메시지를 제1 단말기로 송신한다(S130).

[0042] 제1 단말기는 제2 단말기로부터 수신 인증 메시지를 수신하는 경우, 수신 인증 메시지의 무결성을 판단하여 수신 인증 메시지를 인증하고 암호화된 송신 랜덤값에 기초하여 송신 인증 메시지의 재전송 공격이 존재하는지 판단하며, 수신 인증 메시지의 인증 및 재전송 공격이 판단된 경우 무선 단말기의 식별자, 관리 서버의 식별자, 암호화된 송신 시드값 및 수신 시드값의 조합으로 생성되는 키 및 암호화된 수신 랜덤값을 구비하는 수신 확인 메시지를 생성한다(S140). 제1 단말기는 제2 단말기로 생성한 수신 확인 메시지를 송신한다(S150).

[0043] 제2 단말기는 제1 단말기로부터 수신 확인 메시지를 수신하는 경우, 수신 확인 메시지의 무결성을 판단하여 수신 확인 메시지를 인증하고 수신 랜덤값에 기초하여 수신 인증 메시지의 재전송 공격 여부를 판단하며, 암호화된 제2 단말기의 식별자, 제1 단말기의 식별자 및 제2 단말기가 보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 구비하는 송신 확인 메시지를 생성한다(S160). 제2 단말기는 생성한 송신 확인 메시지를 제2 단말기로 송신한다(S170).

[0044] 제1 단말기와 제2 단말기는 서로 공유하는 송신 시드값, 수신 시드값, 제1 단말기 식별자에 기초하여 제1 단말기와 제2 단말기가 공유하는 비밀키를 생성하며, 생성한 비밀키로 데이터를 암호화하여 보안 통신을 수행한다(S180, S190).

[0045] 도 3에서 제1 단말기의 다수의 프로세스가 제2 단말기와 보안 통신을 수행하는 경우, 각 프로세스에 개별적인 보안 통신 모듈을 할당할 필요가 없으며, 다수 프로세스가 공유하는 공통 보안 통신 모듈에서 도 4에서 설명한 비밀키 교환 방식으로 제2 단말기와 비밀키를 교환하며, 다수의 프로세스는 교환한 1개의 비밀키를 통해 공통 보안 통신 모듈을 통해 제2 단말기와 보안 통신을 수행한다.

[0046] 제1 단말기와 제2 단말기는 송신 인증 메시지와 수신 인증 메시지에 기초하여 제1 단말기와 제2 단말기 사이에 필요한 송신 시드값과 수신 시드값을 서로 공유하며, 수신 인증 메시지의 송신 랜덤값, 수신 확인 메시지의 수신 랜덤값에 기초하여 송신 인증 메시지의 재전송 공격, 수신 인증 메시지의 재전송 공격 여부를 판단한다. 또한, 수신 확인 메시지와 송신 확인 메시지에 기초하여 제1 단말기와 제2 단말기가 공유하는 송신 랜덤값과 수신 랜덤값을 재확인하며, 송신 랜덤값, 수신 랜덤값 및 제1 단말기의 식별자에 기초하여 제1 단말기와 제2 단말기가 공유하는 비밀키를 교환한다.

[0047] 도 5는 본 발명에 따라 송신 인증 메시지를 인증하고 수신 인증 메시지를 생성하는 단계(S120)를 보다 구체적으로 설명하기 위한 흐름도이다.

[0048] 도 5를 참고로 보다 구체적으로 살펴보면, 제2 단말기는 제1 단말기로부터 송신 인증 메시지를 수신한다(S121). 제2 단말기는 수신한 송신 인증 메시지에 구비되어 있는 제1 단말기 식별자, 송신 시드값, 송신 랜덤값 및 송신

인증 메시지의 수명값을 암호화한 제2 암호화값을 계산하고(S123) 계산한 제2 암호화값과 송신 인증 메시지의 제1 암호화 값의 동일 여부로 송신 인증 메시지의 무결성을 판단한다(S125). 제2 단말기는 제1 단말기 식별자, 송신 시드값, 송신 랜덤값 및 송신 인증 메시지의 수명값을 제1 단말기에서 송신 인증 메시지의 제1 암호화값을 계산하는데 사용한 동일한 제1 해쉬 함수로 암호화하여 제2 암호화값을 계산한다.

[0049] 제2 단말기에서 송신 인증 메시지의 무결성 판단이 완료된 후, 제2 단말기의 식별자, 제2 단말기에서 생성된 수신 시드값, 수신 랜덤값, 수신 인증 메시지의 수명값과 제2 단말기의 식별자, 생성된 수신 시드값, 수신 랜덤값, 수신 인증 메시지의 수명값을 암호화한 제3 암호화값, 송신 랜덤값을 암호화한 제4 암호화값을 구비하는 수신 인증 메시지를 생성하고(S127), 생성한 수신 인증 메시지를 제1 단말기로 송신한다(S129). 바람직하게, 제3 암호화값은 제1 해쉬함수와 동일한 해쉬 함수를 사용하여 계산되거나 제1 해쉬 함수와 상이한 제2 해쉬 함수를 사용하여 계산된다. 한편, 제4 암호화값은 제1 해쉬함수와 동일한 해쉬 함수를 사용하여 계산되거나 제1 해쉬 함수와 상이한 제3 해쉬 함수를 사용하여 계산된다.

[0050] 여기서 수신 시드값(SEED-D2)은 수신 시드 랜덤값(SS), 설정값(M), 제1 단말기의 패스워드(PW) 및 시드 함수(g)의 조합으로부터 아래의 수학식(2)와 같이 생성된다.

[0051] [수학식 2]

$$SEED-D2 = g^{D_2} SM^{pw1}$$

[0052]

[0053] 도 6은 본 발명에 따라 수신 인증 메시지를 인증하고 수신 확인 메시지를 생성하는 단계(S140)를 보다 구체적으로 설명하기 위한 흐름도이다.

[0054] 도 6을 참고로 보다 구체적으로 살펴보면, 제1 단말기는 제2 단말기로부터 수신 인증 메시지를 수신한다(S141). 제1 단말기는 수신한 수신 인증 메시지에 구비되어 있는 제2 단말기 식별자, 수신 시드값, 수신 랜덤값 및 수신 인증 메시지의 수명값을 암호화한 제5 암호화값을 계산하고(S142) 계산한 제5 암호화값과 수신 인증 메시지의 제3 암호화 값의 동일 여부로 수신 인증 메시지의 무결성을 판단한다(S143). 여기서 제5 암호화값은 제2 단말기에서 제3 암호화값을 계산하는데 사용한 해쉬 함수와 동일한 해쉬 함수를 사용하여 계산된다.

[0055] 한편, 제1 단말기가 보유하고 있는 송신 랜덤값을 암호화한 제6 암호화값과 수신 인증 메시지의 제4 암호화값의 동일 여부로 송신 인증 메시지의 재전송 공격 여부를 판단한다(S144). 여기서 제6 암호화값은 제2 단말기에서 제4 암호화값을 계산하는데 사용한 해쉬 함수와 동일한 해쉬 함수를 사용하여 계산된다. 제1 단말기는 송신 인증 메시지를 송신할 때마다 송신 랜덤값을 무작위로 생성하며, 송신 랜덤값을 구비하여 송신 인증 메시지를 생성하여 제2 단말기로 송신한다. 제1 단말기와 제2 단말기 사이에 공격자 단말기가 존재하여 공격자 단말기는 제1 단말기로부터 수신한 송신 인증 메시지를 제2 단말기로 전송하며 동시에 제1 단말기로 재전송을 요구하는 경우, 제1 단말기는 서로 다른 송신 랜덤값을 구비하는 송신 인증 메시지를 생성하여 제2 단말기로 재전송을 반복하게 된다. 제2 단말기로부터 수신한 수신 인증 메시지에서 송신 랜덤값에 기초하여 재전송 공격을 판단함으로써, 제1 단말기는 재전송 공격이 존재하는 라우팅 경로를 제외하여 제2 단말기와 비밀키 교환 작업을 수행할 수 있다.

[0056] 수신 인증 메시지의 무결성 및 송신 인증 메시지의 재전송 공격 여부의 판단이 완료된 후, 제1 단말기는 제1 단말기 식별자, 제2 단말기 식별자, 송신 시드값 및 수신 시드값의 조합으로 생성되는 키를 암호화한 제7 암호화값과 수신 랜덤값을 암호화한 제8 암호화값을 구비하는 수신 확인 메시지를 생성하고, 생성한 수신 확인 메시지를 제2 단말기로 송신한다(S146). 바람직하게, 제7 암호화값은 제1 해쉬함수와 동일한 해쉬 함수를 사용하여 계산되거나 제1 해쉬 함수와 상이한 제4 해쉬 함수를 사용하여 계산된다. 한편, 제8 암호화값은 제1 해쉬함수와 동일한 해쉬 함수를 사용하여 계산되거나 제1 해쉬 함수와 상이한 제5 해쉬 함수를 사용하여 계산된다.

[0057] 도 7은 본 발명에 따라 수신 확인 메시지를 인증하고 송신 확인 메시지를 생성하는 단계(S160)를 보다 구체적으로 설명하기 위한 흐름도이다.

[0058] 도 7을 참고로 보다 구체적으로 살펴보면, 제2 단말기는 제1 단말기로부터 수신 확인 메시지를 수신한다(S161). 제2 단말기는 수신 확인 메시지에 구비되어 있는 제1 단말기의 식별자, 제2 단말기의 식별자 및 제2 단말기가

보유하는 송신 시드값과 수신 시드값의 조합으로 생성되는 키를 암호화한 제9 암호화값을 계산하고(S162), 계산한 제9 암호화값과 수신 확인 메시지의 제7 암호화값의 동일 여부를 수신 확인 메시지의 무결성을 판단한다(S163). 여기서 제9 암호화값은 제1 단말기에서 제7 암호화값을 계산하는데 사용한 해쉬 함수와 동일한 해쉬 함수를 사용하여 계산된다.

[0059] 한편, 제2 단말기가 보유하고 있는 수신 랜덤값을 암호화한 제10 암호화값과 수신 확인 메시지의 제8 암호화값의 동일 여부를 수신 인증 메시지의 재전송 공격 여부를 판단한다(S164). 여기서 제10 암호화값은 제1 단말기에서 제8 암호화값을 계산하는데 사용한 해쉬 함수와 동일한 해쉬 함수를 사용하여 계산된다. 제2 단말기는 수신 인증 메시지를 송신할 때마다 수신 랜덤값을 무작위로 생성하며, 수신 랜덤값을 구비하여 수신 인증 메시지를 생성하여 제1 단말기로 송신한다. 제1 단말기와 제2 단말기 사이에 공격자 단말기가 존재하여 공격자 단말기가 제2 단말기로부터 수신한 송신 인증 메시지를 제1 단말기로 전송하며 동시에 제2 단말기로 재전송을 요구하는 경우, 제2 단말기는 서로 다른 수신 랜덤값을 구비하는 수신 인증 메시지를 생성하여 제1 단말기로 재전송을 반복하게 된다. 제1 단말기로부터 수신한 수신 확인 메시지에서 수신 랜덤값에 기초하여 재전송 공격을 판단함으로써, 제2 단말기는 재전송 공격이 존재하는 라우팅 경로를 제외하여 제1 단말기와 비밀키 교환 작업을 수행할 수 있다.

[0060] 수신 확인 메시지의 무결성 및 수신 인증 메시지의 재전송 공격 여부를 판단이 완료된 후, 제2 단말기는 제2 단말기 식별자, 제1 단말기 식별자, 송신 시드값 및 수신 시드값의 조합으로 생성되는 키를 암호화한 제11 암호화값을 구비하는 송신 확인 메시지를 생성하고, 생성한 송신 확인 메시지를 제1 단말기로 송신한다(S166). 바람직하게, 제11 암호화값은 제1 단말기에서 제7 암호화값을 계산하는데 사용되는 해쉬 함수와 동일한 해쉬 함수로 계산된다.

[0061] 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.

[0062] 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.

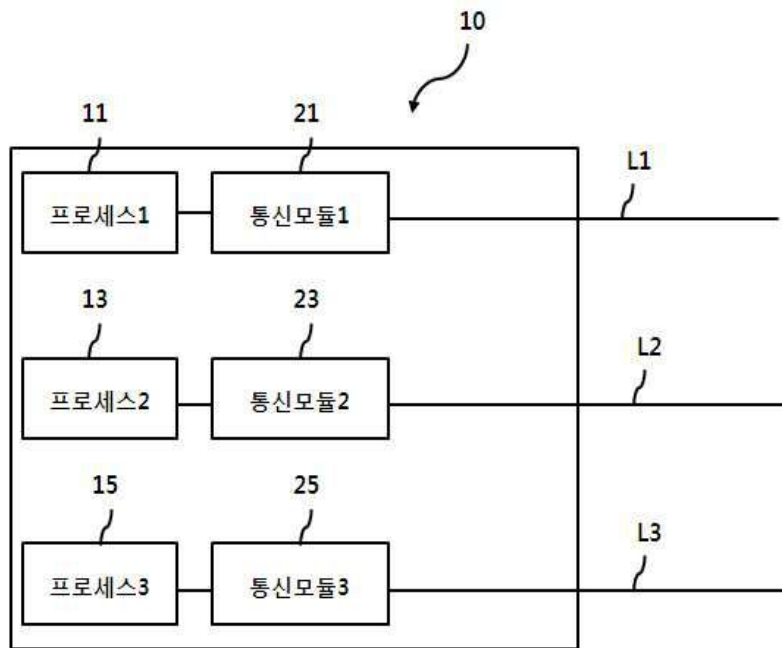
[0063] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

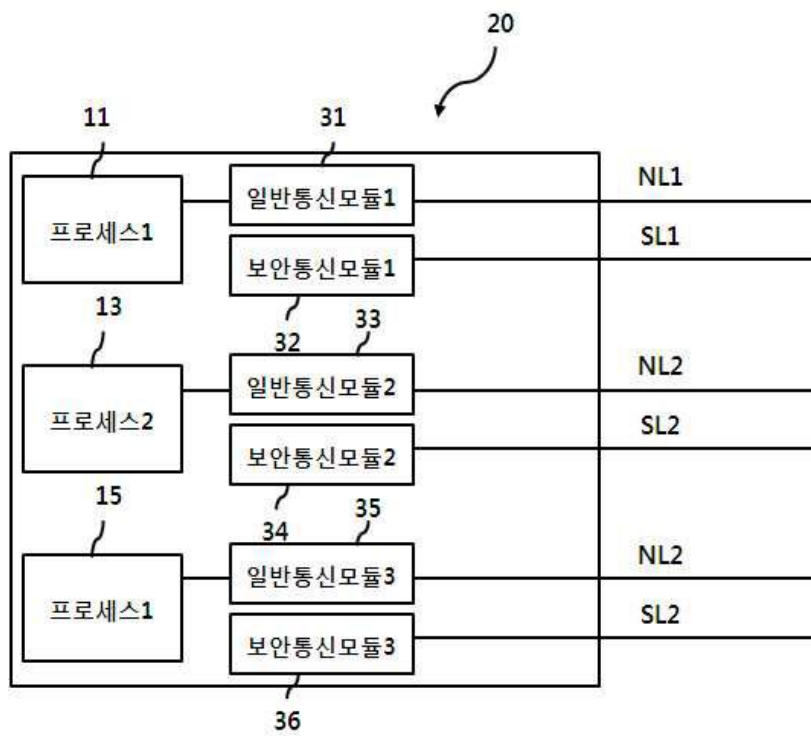
[0064]	10: 무선 단말기	20: 유선 단말기
	11, 13, 15: 프로세스	21, 23, 25: 통신 모듈
	31, 33, 35: 일반 통신 모듈	32, 34, 36: 보안 통신 모듈
	100: 무선 단말기	111, 113, 115: 프로세스
	121, 123, 125: 일반 통신 모듈	130: 보안 통신 모듈

도면

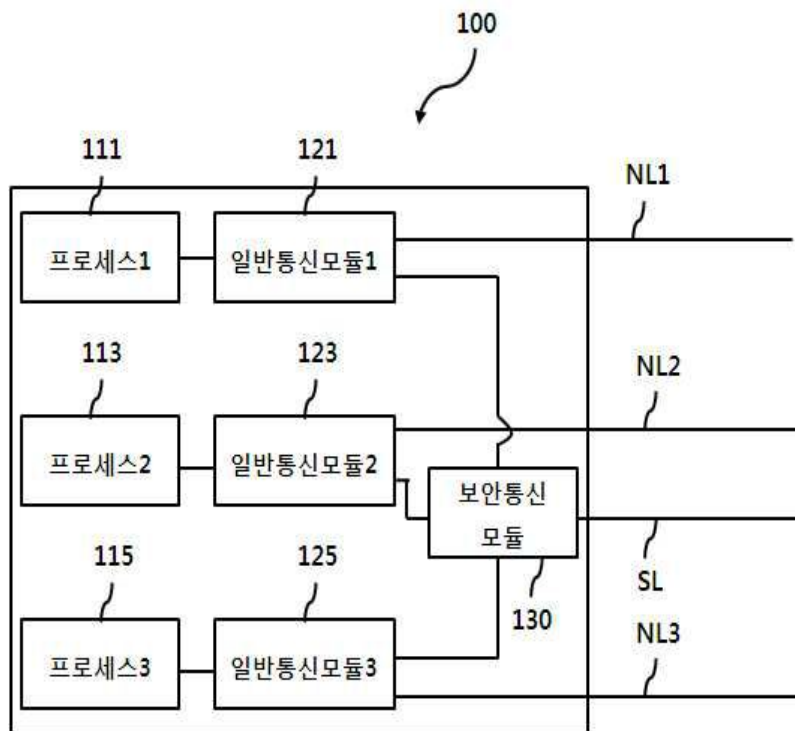
도면1



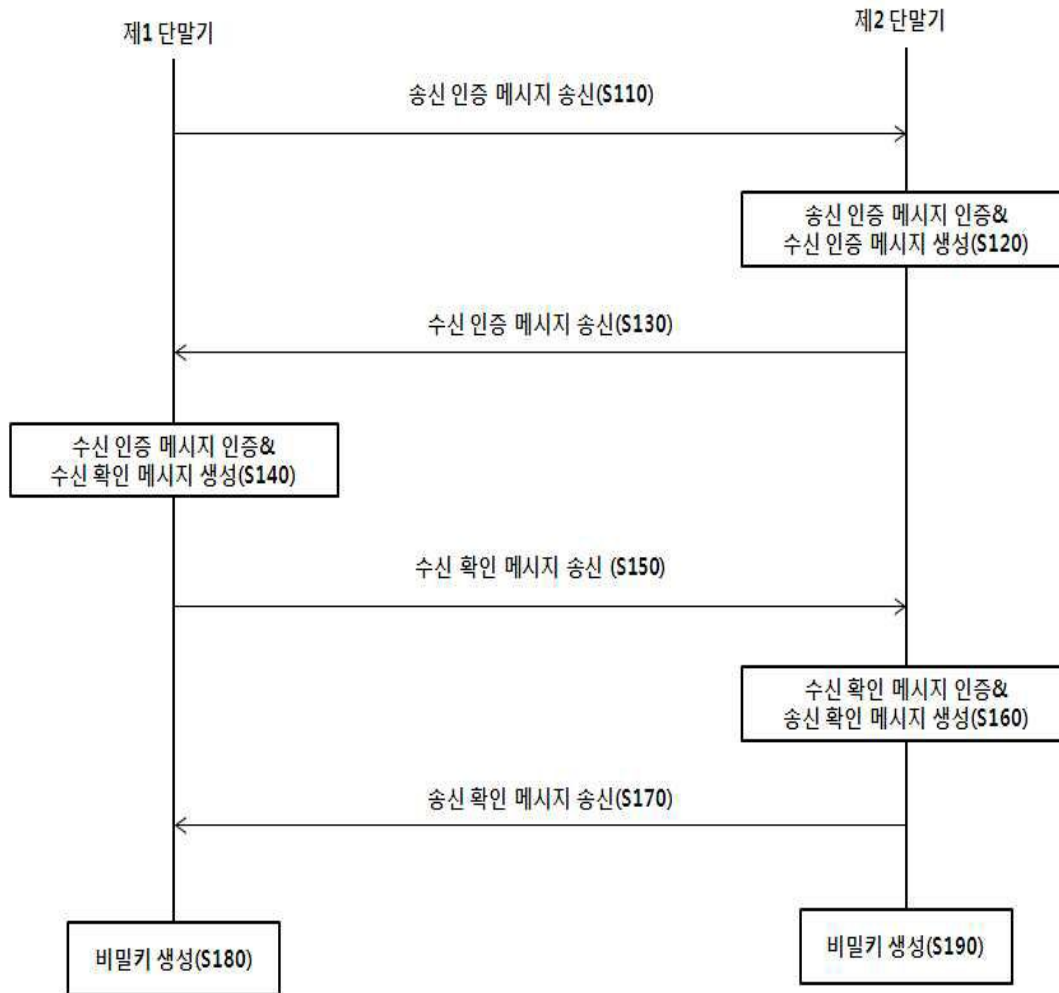
도면2



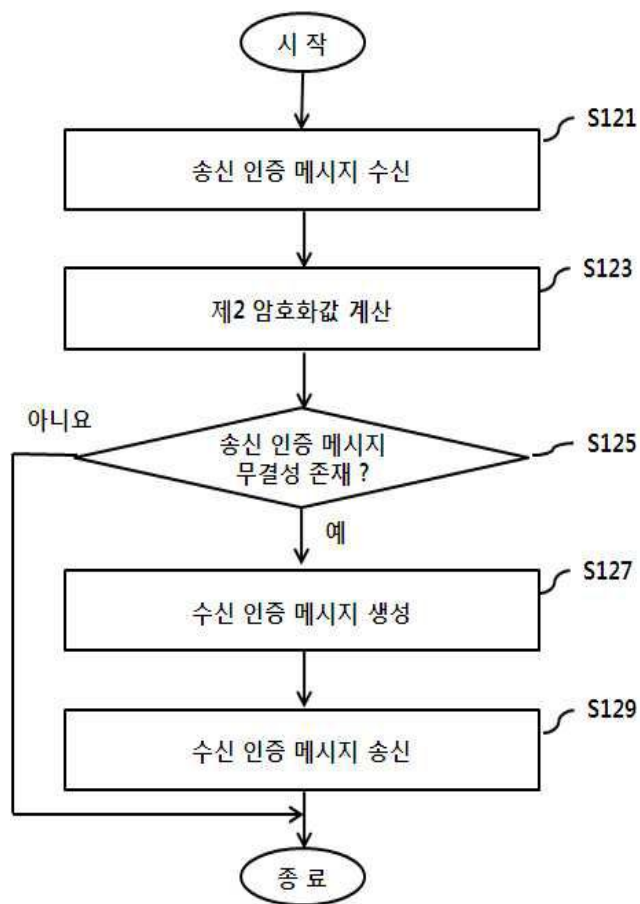
도면3



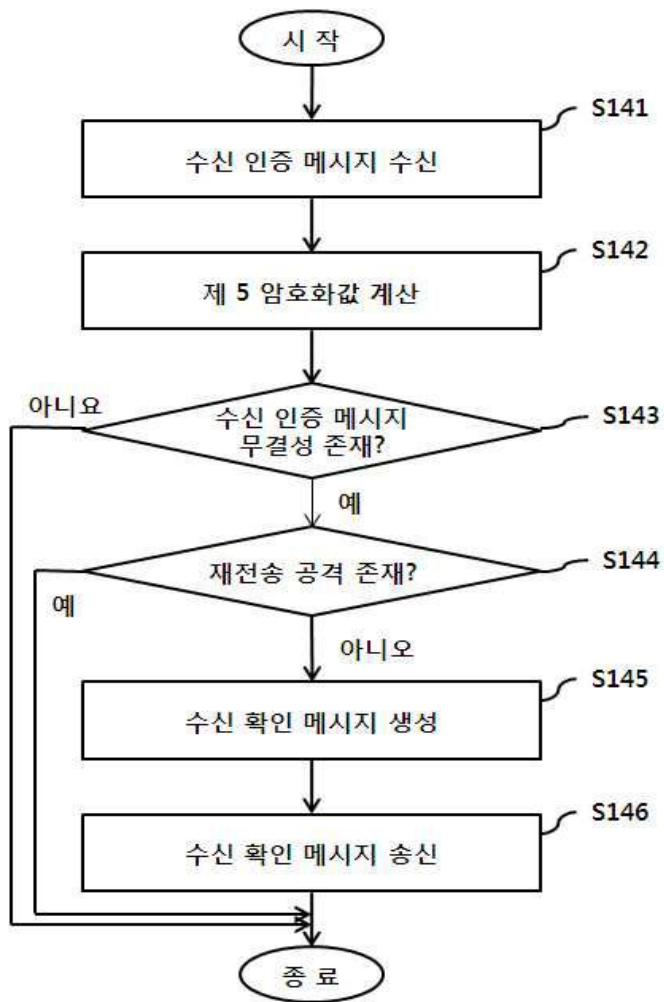
도면4



도면5



도면6



도면7

