(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년12월11일
(11) 등록번호 10-1210938
(24) 등록일자 2012년12월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2011-0008817
(22) 출원일자 2011년01월28일
심사청구일자 2011년01월28일
(65) 공개번호 10-2012-0087550
(43) 공개일자 2012년08월07일
(56) 선행기술조사문헌
KR1020100082184 A
US20030217165 A1
KR1020040106098 A
장유정외 5명, "SIP P2P 스팸 방지를 위한 인증 및 SDP 암호화 키 교환 기법", 한국통신학회논문지 제32권 제12호(네트워크 및 서비스), page(s): 719-831, 2007. 12.
전체 청구항 수 : 총 10 항

(73) 특허권자
오픈스택 주식회사
경기도 성남시 분당구 새나리로 25, 첨단기술연구센터 411호 (야탑동)
(72) 발명자
남재권
경기도 성남시 분당구 새나리로 25, 첨단기술연구센터 411호 (야탑동)
이형우
경기도 성남시 분당구 새나리로 25, 첨단기술연구센터 411호 (야탑동)
(뒷면에 계속)
(74) 대리인
남승희

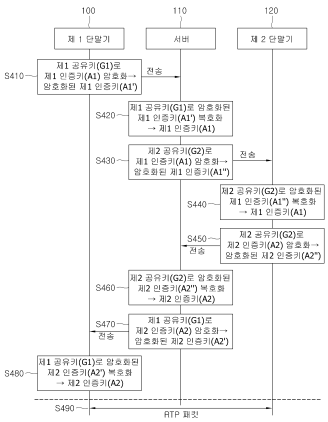
심사관 : 이형일

(54) 발명의 명칭 **암호 통신 방법 및 이를 이용한 암호 통신 시스템**

(57) 요 약

본 발명은 암호 통신 방법 및 이를 이용한 암호 통신 시스템에 관한 것으로, 특히 간편하고 안전하게 인증키를 교환하여 암호 통신을 할 수 있는 암호 통신 방법 및 이를 이용한 암호 통신 시스템에 관한 것으로, 두 단말기 사이에서 데이터를 교환하는 암호 통신 방법에 있어서, 제1 단말기가 데이터 패킷의 암호화/복호화를 위한 제1 인증키(A1)를 생성하고, 상기 제1 인증키(A1)를 제1 공유키(G1)로 암호화하고, 암호화된 제1 인증키(A1')를 서버에 전송하는 과정; 상기 서버가 암호화된 제1 인증키(A1')를 수신하여 제1 공유키(G1)로 복호화하고, 복호화된 제1 인증키(A1)를 제2 공유키(G2)로 암호화하고, 암호화된 제2 인증키(A'')를 제2 단말기에 전송하는 과정; 및 상기 제2 단말기가 암호화된 제1 인증키(A1'')를 수신하여 제2 공유키(G2)로 복호화하고, 복호화된 제1 인증키(A1)를 획득하는 과정을 포함한다.

대 표 도 - 도4



(72) 발명자

이선민

경기도 성남시 분당구 새나리로 25, 첨단기술연구센터 411호 (야탑동)

안효원

경기도 성남시 분당구 새나리로 25, 첨단기술연구센터 411호 (야탑동)

특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

두 단말기 사이에서 데이터를 교환하는 암호 통신 방법에 있어서,

제1 단말기가 데이터 패킷의 암호화/복호화를 위한 제1 인증키(A1)를 생성하고, 상기 제1 인증키(A1)를 제1 공유키(G1)로 암호화하여 생성한 암호화된 제1 인증키(A1')를 서버에 전송하는 과정;

상기 서버가 제1 공유키(G1)를 제2 공유키(G2)로 암호화하여 생성한 암호화된 제1 공유키(G1'')와, 상기 제1 단말기로부터 수신된 암호화된 제1 인증키(A1')를 제2 단말기에 전송하는 과정; 및

상기 제2 단말기가 암호화된 제1 공유키(G1'')를 제2 공유키(G2)로 복호화하여 복호화된 제1 공유키(G1)를 생성하고, 상기 복호화된 제1 공유키(G1)를 이용하여 상기 서버로부터 수신한 암호화된 제1 인증키(A1')를 복호화하여 제1 인증키(A1)를 획득하는 과정을 포함하는 암호 통신 방법.

청구항 4

청구항 3에 있어서,

상기 제2 단말기가 제2 인증키(A2)를 생성하고, 상기 제2 인증키(A2)를 제2 공유키(G2)로 암호화하고, 암호화된 제2 인증키(A2'')를 서버에 전송하는 과정;

상기 서버가 제2 공유키(G2)를 제1 공유키(G1)로 암호화하고, 암호화된 제2 공유키(G2') 및 상기 제2 단말기로부터 수신된 암호화된 제2 인증키(A2'')를 제1 단말기에 전송하는 과정; 및

상기 제1 단말기가 암호화된 제2 공유키(G2')를 수신하여 제1 공유키(G1)로 복호화하고, 복호화된 제2 공유키(G2)로 상기 서버로부터 수신된 암호화된 제2 인증키(A2'')를 복호화하고, 복호화된 제2 인증키(A2)를 획득하는 과정을 더 포함하는 암호 통신 방법.

청구항 5

청구항 3 또는 청구항 4에 있어서,

상기 제1 단말기 및 제2 단말기는 VoIP 단말기이며,

상기 인증키는 상기 제1 단말기와 제2 단말기 사이에서 교환되는 SIP 메시지에 포함되어 전송되며,

상기 데이터 패킷은 RTP 패킷인 것을 특징으로 하는 암호 통신 방법.

청구항 6

청구항 3 또는 청구항 4에 있어서,

상기 제1 공유키는 제1 단말기와 서버가 공유하는 정보로부터 생성되며, 상기 제2 공유키는 제2 단말기와 서버가 공유하는 정보로부터 생성되는 것을 특징으로 하는 암호 통신 방법.

청구항 7

청구항 6에 있어서,

상기 공유키는, 두 단말기의 1회의 암호 통신시마다 생성하는 것을 특징으로 하는 암호 통신 방법.

청구항 8

청구항 3 또는 청구항 4에 있어서,

상기 제1 공유키는 제1 단말기가 서버에 접속하기 위한 세션키이며, 상기 제2 공유키는 제2 단말기가 서버에 접속하기 위한 세션키인 것을 특징으로 하는 암호 통신 방법.

청구항 9

청구항 3 또는 청구항 4에 있어서,

상기 제1 단말기와 제2 단말기의 데이터 패킷 교환 방법은, 상기 인증키를 이용하여 데이터 패킷을 암호화/복호화하는 SRTP 기술을 이용하는 방법인 것을 특징으로 하는 암호 통신 방법.

청구항 10

청구항 3 또는 청구항 4에 있어서,

상기 인증키는, 두 단말기의 1회의 암호 통신시마다 생성하는 것을 특징으로 하는 암호 통신 방법.

청구항 11

청구항 3 또는 청구항 4에 있어서,

상기 공유키를 이용한 인증키의 암호화/복호화는, ARIA 암호화 알고리듬 방식, AES 암호화 알고리듬 방식, SEED 암호화 알고리듬 방식, 및 Camellia 암호화 알고리듬 방식 중 어느 하나인 것을 특징으로 하는 것을 특징으로 하는 암호 통신 방법.

청구항 12

청구항 3 또는 청구항 4에 있어서,

상기 제1 단말기와 제2 단말기 사이에서 인증키의 전송을 중계하는 서버는 복수이며, 상기 복수의 서버 사이에서의 인증키 교환은 소정의 보안 상태에서 이루어지는 것을 특징으로 하는 암호 통신 방법.

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 암호 통신 방법 및 이를 이용한 암호 통신 시스템에 관한 것으로, 특히 간편하고 안전하게 인증키를 교환하여 암호 통신을 할 수 있는 암호 통신 방법 및 이를 이용한 암호 통신 시스템에 관한 것이다.

배 경 기 술

[0002] 통신 수단으로 과거에 많이 이용되었던 PSTN(public switched telephone network)은 이제 점점 수요가 줄어들고 있으며, 최근에는 휴대폰, 인터넷 전화가 주요 통신 수단이 되고 있다.

[0003] 이 중에서 인터넷 전화는 공개된 통신망인 인터넷을 이용하여 음성, 영상 등의 미디어 데이터를 주고받는다. 이러한 인터넷 전화는 VoIP(Voice over Internet Protocol) 전화라고도 불리며, 일반적으로 두 인터넷 전화의 통신은 세션 설정을 위하여 SIP(Session Initiation Protocol) 메시지를 이용하며, 음성, 영상 등의 미디어 교환을 위하여 RTP(Real Time Protocol) 패킷을 이용한다.

[0004] SIP 기반의 VoIP 환경에서 ID기반의 암호화시스템(ID-based cryptosystem)을 이용하여 사용자 인증 및 RTP 패킷의 비밀키 교환에 관한 연구가 많이 이루어지고 있다.

[0005] ID기반의 암호화시스템은 사용자의 ID(예, IP 주소, 전화번호, 이메일 주소 등)를 공개키로 사용하여 공개키 기반 구조(PKI; Public Key Infrastructure)의 환경을 구축하지 않고 공개키 암호 알고리즘을 사용할 수 있는 암호 기술이다.

[0006] ID기반의 암호화시스템에서는 키생성센터(KGC; Key Generation Center)라는 제3의 기관이 사용자들의 ID를 사용하여 각 사용자의 비밀키를 생성 및 분배하고, 각 사용자들은 자신의 ID를 자신의 비밀키와 쌍을 이루는 공개키로 사용한다. 이와 같은 ID기반의 암호화시스템은 상대방의 ID를 상대방의 공개키로 사용하기 때문에 PKI에서와 같이 인증기관(CA; Certificate Authority)의 서명을 통해 상대방의 공개키를 검증할 필요 없이 상대방의 ID만 유효하다면 공개키 기반 구조(PKI)의 환경 구축 없이 공개키 암호 알고리즘을 사용할 수 있다.

[0007] 그러나, ID기반의 암호화시스템은 키생성센터에서 사용자들의 비밀키를 생성하기 때문에, 암호화 및 전자서명 등에 사용되는 키들을 제3의 기관이 백업 또는 보관하고, 이 키를 사용하는 당사자의 협조 없이도 제3의 기관이 당사자가 비밀 통신에 사용하였던 비밀키를 복원할 수 있다는 문제, 즉, 키 에스크로 문제를 유발한다. 나아가, 이러한 키 에스크로 문제는 개인 사용자들의 비밀 통신을 보장할 수 없다는 심각한 문제를 발생시킬 수 있다.

[0008] 또한, 사용자의 비밀키가 공격자에게 노출되었을 때, 노출된 비밀키와 쌍을 이루는 사용자 ID에 대한 유효성 검증 방법이 없다. 즉 ID기반의 암호화시스템 환경에서 사용자의 비밀키가 노출될 경우, 사용자의 ID와 그에 대응하는 비밀키가 유일하게 하나의 쌍을 이루는 값이므로, 비밀키가 노출되었다면 사용자 ID는 더 이상 신뢰할 수 없게 된다. 따라서, 사용자의 ID를 변경하고 새로운 비밀키를 KGC로부터 할당받아야 하는 문제, 즉 ID폐지(ID revocation) 문제를 유발한다.

[0009] 전술한 바와 같이, 종래 기술은 VoIP 망에서 전송 계층 보안 프로토콜, 즉 TLS(Transport Layer Security Protocol) 및 S/MIME(Secure Multi-Purpose Internet Mail Extensions)과 같은 공개키 기반 구조(PKI)의 보안 기술이 표준으로 정의되어 있지만, 공개키 기반 구조(PKI)의 구축 미비와 공개키 기반 구조(PKI)의 관리 오버헤드로 인해 실제 VoIP 네트워크에 적용되기 어렵다.

[0010] 따라서, 이러한 문제로 인해 기존에 제안된 ID기반의 암호화시스템의 보안 기술 또한 VoIP 망에 적용되는 것이 제한적이며, 새로운 암호 통신 방안이 요구된다.

발명의 내용

해결하려는 과제

[0011] 본 발명의 기술적 과제는 SIP 기반의 VoIP 환경에서, 간단하고 안전하게 인증키를 전달할 수 있는 암호 통신 방법 및 암호 통신 시스템을 제공하는 것에 있다.

[0012] 또한, 본 발명의 다른 기술적 과제는 SIP 기반의 VoIP 환경에서, RTP 패킷을 보호하기 위한 비밀키의 키 에스크로(key escrow) 문제를 해결할 수 있는 암호 통신 방법 및 암호 통신 시스템을 제공하는 것에 있다.

[0013] 또한, 본 발명의 다른 기술적 과제는 SIP 기반의 VoIP 환경에서, 비밀키 노출시 또는 사용자의 VoIP 단말 분실시 발생하는 ID 폐지(ID revocation) 문제를 해결할 수 있는 암호화 인증 방법을 제시하는데 또 다른 목적이 있다.

과제의 해결 수단

[0014] 본 발명의 일 실시예에 따른 암호 통신 방법은, 두 단말기 사이에서 데이터를 교환하는 암호 통신 방법에 있어서, 제1 단말기가 데이터 패킷의 암호화/복호화를 위한 제1 인증키(A1)를 생성하고, 상기 제1 인증키(A1)를 제1 공유키(G1)로 암호화하고, 암호화된 제1 인증키(A1')를 서버에 전송하는 과정; 상기 서버가 암호화된 제1 인증키(A1')를 수신하여 제1 공유키(G1)로 복호화하고, 복호화된 제1 인증키(A1)를 제2 공유키(G2)로 암호화하고, 암호화된 제2 인증키(A'')를 제2 단말기에 전송하는 과정; 및 상기 제2 단말기가 암호화된 제1 인증키(A1'')를 수신하여 제2 공유키(G2)로 복호화하고, 복호화된 제1 인증키(A1)를 획득하는 과정을 포함한다.

[0015] 상기 제2 단말기가 제2 인증키(A2)를 생성하고, 상기 제2 인증키(A2)를 제2 공유키(G2)로 암호화하고, 암호화된 제2 인증키(A2'')를 서버에 전송하는 과정; 상기 서버가 암호화된 제2 인증키(A2'')를 수신하여 제2 공유키(G2)로 복호화하고, 복호화된 제2 인증키(A2)를 제1 공유키(G1)로 암호화하고, 암호화된 상기 제2 인증키(A2')를 상기 제1 단말기에 전송하는 과정; 및 상기 제1 단말기가 암호화된 제2 인증키(A2')를 수신하여 제1 공유키(G1)로 복호화하고, 복호화된 제2 인증키(A2)를 획득하는 과정을 더 포함할 수 있다.

[0016] 본 발명의 다른 일 실시예에 따른 암호 통신 방법은, 두 단말기 사이에서 데이터를 교환하는 암호 통신 방법에 있어서, 제1 단말기가 데이터 패킷의 암호화/복호화를 위한 제1 인증키(A1)를 생성하고, 상기 제1 인증키(A1)를 제1 공유키(G1)로 암호화하고, 암호화된 제1 인증키(A1')를 서버에 전송하는 과정; 상기 서버가 제1 공유키(G1)를 제2 공유키(G2)로 암호화하고, 암호화된 제1 공유키(G1'') 및 상기 제1 단말기로부터 수신된 암호화된 제1 인증키(A1')를 제2 단말기에 전송하는 과정; 및 상기 제2 단말기가 암호화된 제1 공유키(G1'')를 수신하여 제2 공유키(G2)로 복호화하고, 복호화된 제1 공유키(G1)로 상기 서버로부터 수신된 암호화된 제1 인증키(A1')를 복호화하고, 복호화된 제1 인증키(A1)를 획득하는 과정을 포함한다.

[0017] 상기 제2 단말기가 제2 인증키(A2)를 생성하고, 상기 제2 인증키(A2)를 제2 공유키(G2)로 암호화하고, 암호화된 제2 인증키(A2'')를 서버에 전송하는 과정; 상기 서버가 제2 공유키(G2)를 제1 공유키(G1)로 암호화하고, 암호화된 제2 공유키(G2') 및 상기 제2 단말기로부터 수신된 암호화된 제2 인증키(A2'')를 제1 단말기에 전송하는 과정; 및 상기 제1 단말기가 암호화된 제2 공유키(G2')를 수신하여 제1 공유키(G1)로 복호화하고, 복호화된 제2 공유키(G2)로 상기 서버로부터 수신된 암호화된 제2 인증키(A2'')를 복호화하고, 복호화된 제2 인증키(A2)를 획득하는 과정을 더 포함할 수 있다.

[0018] 상기 제1 단말기 및 제2 단말기는 VoIP 단말기이며, 상기 인증키는 상기 제1 단말기와 제2 단말기 사이에서 교환되는 SIP 메시지에 포함되어 전송되며, 상기 데이터 패킷은 RTP 패킷일 수 있다.

[0019] 상기 제1 공유키는 제1 단말기와 서버가 공유하는 정보로부터 생성되며, 상기 제2 공유키는 제2 단말기와 서버가 공유하는 정보로부터 생성될 수 있다.

[0020] 상기 공유키는, 두 단말기의 1회의 암호 통신시마다 생성할 수 있다.

[0021] 상기 제1 공유키는 제1 단말기가 서버에 접속하기 위한 세션키이며, 상기 제2 공유키는 제2 단말기가 서버에 접속하기 위한 세션키일 수 있다.

[0022] 상기 제1 단말기와 제2 단말기의 데이터 패킷 교환 방법은, 상기 인증키를 이용하여 데이터 패킷을 암호화/복호화하는 SRTP 기술을 이용하는 방법일 수 있다.

[0023] 상기 인증키는, 두 단말기의 1회의 암호 통신시마다 생성할 수 있다.

[0024] 상기 공유키를 이용한 인증키의 암호화/복호화는, ARIA 암호화 알고리듬 방식, AES 암호화 알고리듬 방식, SEED 암호화 알고리듬 방식, 및 Camellia 암호화 알고리듬 방식 중 어느 하나일 수 있다.

[0025] 상기 제1 단말기와 제2 단말기 사이에서 인증키의 전송을 중계하는 서버는 복수이며, 상기 복수의 서버 사이에서의 인증키 교환은 소정의 보안 상태에서 이루어질 수 있다.

[0026] 본 발명의 다른 일 실시예에 따른 암호 통신 시스템은, 두 단말기 사이에서 SIP 메시지를 교환하여 세션 설정을 하고, RTP 패킷을 교환하는 암호 통신 시스템에 있어서, 제2 단말기와의 통신시 RTP 패킷의 암호화/복호화를 위

한 제1 인증키(A1) 및 상기 제1 인증키(A1)의 암호화/복호화를 위한 제1 공유키(G1)를 생성하고, 상기 제1 공유키(G1)로 제1 인증키(A1)를 암호화하고, 암호화된 제1 인증키(A1')를 서버를 경유하여 제2 단말기에 전송하는 제1 단말기; 제1 단말기와의 통신시 RTP 패킷의 암호화/복호화를 위한 제2 인증키(A2) 및 상기 제2 인증키(A2)의 암호화/복호화를 위한 제2 공유키(G2)를 생성하고, 상기 제2 공유키(G2)로 제2 인증키(A2'')를 암호화하고, 암호화된 제2 인증키(A2'')를 서버를 경유하여 제1 단말기에 전송하는 제2 단말기; 및 상기 제1 단말기와 제2 단말기 간의 인증키 교환을 중계하며, 상기 제1 단말기와의 공유 정보를 이용하여 제1 공유키(G1)를 생성하고, 제2 단말기와의 공유 정보를 이용하여 제2 공유키(G2)를 생성하고, 일방의 단말기로부터 수신한 암호화된 인증키를 일방의 단말기의 공유키를 이용하여 복호화하고, 복호화된 인증키를 타방의 단말기의 공유키를 이용하여 다시 암호화하여 서버를 포함한다.

[0027] 상기 제1 단말기와 제2 단말기는, 상기 인증키를 1회의 암호 통신시마다 생성할 수 있다.

[0028] 상기 제1 단말기, 제2 단말기 및 서버는, 상기 공유키를 1회의 암호 통신시마다 생성할 수 있다.

발명의 효과

[0029] 본 발명의 실시 형태에 따르면, 단말기와 서버가 공유하고 있는 정보를 이용하여 인증키를 암호화/복호화하므로, 안전하고 간편하게 암호 통신을 실현할 수 있다.

[0030] 또한, 상기 인증키는 SIP 메시지에 포함되어 교환하므로, 별도의 데이터 교환 과정 없이도 인증키를 교환할 수 있으므로, 부가적인 장치 없이 간단하게 암호 통신을 실현할 수 있다.

[0031] 또한, 인증키를 단말기에서 1회의 통신마다 생성하고, 단말기와 서버가 공유하고 있는 정보를 이용하여 인증키를 암호화/복호화하므로, RTP 패킷을 보호하기 위한 인증키의 키 에스크로(key escrow) 문제를 해결하고, 인증키 노출시 또는 사용자의 VoIP 단말 분실시 발생하는 ID 폐지(ID revocation) 문제를 해결할 수 있다.

도면의 간단한 설명

[0032] 도 1은 본 발명의 제1 실시예에 따른 암호 통신 시스템의 개략도이다.

도 2는 본 발명의 제1 실시예에 따른 암호 통신에서 사용되는 SIP 메시지에 포함되는 SDP 메세지의 일부를 나타낸 도면이다.

도 3은 본 발명의 제1 실시예에 따른 SIP 메시지의 흐름도이다.

도 4는 본 발명의 제1 실시예에 따른 암호 통신의 흐름도이다.

도 5는 본 발명의 제2 실시예에 따른 암호 통신의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0033] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 더욱 상세히 설명하기로 한다. 그러나 본 발명은 이하에서 개시되는 실시예에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이다. 도면상에서 동일 부호는 동일한 요소를 지칭한다.

[0034] 도 1은 본 발명의 제1 실시예에 따른 암호 통신 시스템의 개략도이며, 도 2는 본 발명의 제1 실시예에 따른 암호 통신에서 사용되는 SIP 메시지에 포함되는 SDP 메세지의 일부를 나타낸 도면이다.

[0035] 본 발명의 제1 실시예에 따른 암호 통신 시스템은, SIP(Session Initiation Protocol)와 RTP(Real-time Transport Protocol)를 이용한 VoIP 전화 통신 시스템이다.

[0036] SIP는 회의나 전화통화에 상대방을 쉽게 초대할 수 있게 하기 위해 만들어진 프로토콜이다. SIP는 어떠한 프로토콜 스택에 메여 있지 않고, HTTP와 같은 텍스트 기반으로 정의되어 있어 확장이 용이하며 쉽게 사용할 수 있는 프로토콜이다. SIP는 기존에 사용하고 있는 E-MAIL 주소를 사용하고, 위치 지정 메시지를 통해 이동성을 제공하므로, 전화를 지정한 장소에서 받는 것이 가능한 단순한 프로토콜이다.

[0037] 도 1에 도시된 두 단말기(100, 120)는 서버(110)를 경유하여 SIP 메시지를 주고받으며, 이러한 SIP 메시지에는 SDP(Session Description Protocol, SIP에서 음성이나 영상 등의 멀티미디어 세션 파라미터를 설정하는 프로토

콜) 메시지가 포함된다.

[0038] SDP는 멀티미디어 회의 , VoIP 전화, 스트리밍 비디오 등, 여러 미디어 데이터를 초기화 할 때, 교환 미디어 데이터의 설정, 전송할 주소, 그 외의 파라미터를 설정하기 위한 프로토콜이다. 상기 두 단말기(100, 120)는 SIP 메시지 교환을 통하여 두 단말기 사이에 세션이 형성되면, RTP 패킷을 교환하여 음성이나 영상 데이터를 주고받는다.

[0039] 도 1을 참조하면, 본 발명의 제1 실시예에 따른 암호 통신 시스템은 SIP 메시지를 교환하여 세션 설정을 하고, RTP 패킷을 교환하여 미디어 데이터를 주고받는 제1 단말기(100) 및 제2 단말기(120)와, 상기 제1 단말기(100)와 제2 단말기(120) 사이의 SIP 메시지 교환을 중계하는 서버(110)를 포함한다.

[0040] 상기 제1 단말기(100)와 제2 단말기(120)는 서버 접속 모듈(101, 121), 공유키 관리 모듈(103, 123), 인증키 관리 모듈(105, 125), SIP 모듈(107, 127), 및 RTP 모듈(109, 129)을 포함한다.

[0041] 또한, 서버(110)는 단말기 접속 모듈(111), 공유키 관리 모듈(113), 및 SIP 중계 모듈(114)을 포함한다.

[0042] 제1 단말기(100)와 제2 단말기(120)는, 예를 들면 VoIP를 통하여 음성이나 영상 통화, 또는 데이터의 송수신이 가능한 VoIP 전용 단말기로 구현될 수 있고, 인터넷과 연결된 컴퓨터, 모바일기기, 스마트폰, 네비게이션 등으로도 구현될 수 있다.

[0043] 서버(110)에는 외부의 일반 전화망(미도시)이나 이동통신 전화망(미도시)이 연결될 수 있으며, 상기 서버(110)는 상기 단말기(100, 120)와 외부의 PSTN 전화망 또는 이동통신 전화망과의 통신을 중계할 수도 한다. 상기 서버(110)는 VoIP 전화 통신 시스템에서 사용하는 SIP 프록시 서버이며, 상기 서버(110)와 제1 단말기(100) 또는 제2 단말기(120) 사이에는 라우터, 방화벽 등의 다양한 네트워크 장비가 있을 수 있다.

[0044] 또한, 도 1에서, 제1 단말기(100)와 제2 단말기(120) 사이에 하나의 서버만이 존재하지만, 이와는 달리 복수의 서버가 존재할 수도 있다. 즉, 제1 단말기(100)가 접속하는 서버와, 제2 단말기(120)가 접속하는 서버가 서로 다를 수 있다. 이때, 서버(SIP 프록시 서버)끼리는 서로만이 알 수 있는 정보로 인증과정을 거쳐서 연결되어 있거나, 혹은, 공개된 인터넷 망이 아닌 내부 네트워크로 연결되어 있을 수 있다. 이때, 인증과정을 거쳐서 연결된 서버사이에서는, 서로만이 알 수 있는 정보에 의하여 인증키가 암호화/복호화 과정을 거쳐서 전송될 수 있으며, 내부 네트워크로 연결된 서버사이에서는, 인증키가 그대로 전송될 수 있다.

[0045] 단말기(100, 120)의 서버 접속 모듈(101, 121)은 서버(110)의 단말기 접속 모듈(111)과 대응한다. 상기 단말기(100, 120)의 서버 접속 모듈(101, 121)과, 서버(110)의 단말기 접속 모듈(111)에는, 상기 단말기(110, 120)가 서버(110)에 접속할 수 있도록 각각 고유의 ID(예: IP 주소, 전화번호, 이메일 주소 등)와 패스워드 등의 정보가 입력된다. 여기서, 상기 제1 단말기(100)와 서버(110)가 공유하는 ID와 패스워드 등의 정보는 제1 공유 정보, 상기 제2 단말기(120)와 서버(110)가 공유하는 ID와 패스워드 등의 정보는 제2 공유 정보라 칭한다.

[0046] 상기 서버(110)의 단말기 접속 모듈(111)은 상기 공유 정보를 이용하여 하나의 단말기의 접속만을 허용한다. 즉, 하나의 단말기가 VoIP 전화 통신 가입시에 입력된 공유 정보로 서버에 접속하면, 상기 공유 정보를 이용한 다른 단말기의 접속은 차단되거나, 또는, 새로운 단말기의 접속이 연결되고 이전 단말기의 접속은 끊어지는 등의 예외 처리가 이루어진다.

[0047] 제1 단말기(100)의 공유키 관리 모듈(103)은, 상기 제1 공유 정보로부터 제1 공유키(G1)를 생성하고, 제2 단말기(120)의 공유키 관리 모듈(123)은, 제2 공유 정보로부터 제2 공유키(G2)를 생성한다. 또한, 서버(110)의 공유키 관리 모듈(113)은, 제1 공유 정보로부터 제1 공유키(G1), 제2 공유 정보로부터 제2 공유키(G2)를 각각 생성한다. 상기 공유키는 SIP 메시지 교환시에, 상기 SIP 메시지에 포함되는 인증키(A)를 암호화하거나 복호화하는데 사용한다. SIP 메시지 교환과 인증키(A)에 관하여는 후술한다.

[0048] 상기 제1 공유키(G1)와 제2 공유키(G2)는 상기 공유 정보의 일부를 그대로 취하여 사용할 수 있고, 또한, 상기 ID와 패스워드 중 일부를 취합하거나, 상기 ID와 패스워드를 현재 시간과 취합, 연산하여 1회의 통화시마다 생성할 수도 있다. 예를 들어, 1회의 통화시마다 공유키를 생성하는 방법으로는, 패스워드와 시간을 조합한 데이터를 해싱테이블로 연산하여 생성하는 방법이 있을 수도 있다. 또한, 상기 제1 공유키(G1)와 제2 공유키(G2)는 상기 단말기(100, 120)가 서버(110)에 접속하기 위한 세션키를 그대로 사용할 수도 있다.

[0049] 단말기(100, 120)의 인증키 관리 모듈(105, 125)은 상기 단말기(100, 120)의 SIP 모듈(107, 127)이 SIP INVITE 메시지 또는 SIP 200 OK 메시지를 송신하기 전에 인증키(A)를 생성하고, 상기 SIP 모듈(107, 127)에 상기 인증

키(A)를 전송한다.

[0050] 상기 두 단말기(100, 120)는 SIP 모듈(107, 127)에서 SIP 메시지를 교환하여 세션을 설정한 후에, RTP 모듈(109, 129)에서 RTP 패킷을 교환하여 통신을 시작할 때에, 두 단말기(100, 120)는 RTP 패킷을 전송하기 전에 상기 RTP 패킷을 인증키(A)를 사용하여 암호화하고, 수신한 후에 암호화된 RTP 패킷을 상기 인증키(A)를 사용하여 복호화함으로써 암호 통신을 실현한다.

[0051] 상기 인증키(A)는 SIP 메시지를 교환하여 세션을 설정할 때에, 상기 SIP 메시지에 포함되는 SDP 메시지에 포함되어 전송되며, 이 과정을 통하여 암호 통신을 하는 두 단말기(100, 120)는 상기 인증키(A)를 공유한다.

[0052] 상기 인증키(A)의 생성은 공유키의 생성과 비슷하게, ID와 패스워드 중 일부를 취합하거나, 상기 ID와 패스워드를 현재 시간과 취합, 연산하여 1회의 통화시마다 생성할 수도 있다. 예를 들어, 1회의 통화시마다 인증키(A)를 생성하는 방법으로는, 패스워드와 시간을 조합한 데이터를 제2의 해싱테이블로 연산하여 생성하는 방법이 있을 수 있다.

[0053] 상기 두 단말기(100, 120)는 암호 통신을 위하여 하나의 인증키(A)를 사용하여 RTP 패킷을 암호화/복호화 할 수 있으며, 본 발명의 실시예에서는 상기 제1 단말기(100)가 제1 인증키(A1)를, 제2 단말기(120)가 제2 인증키(A2)를 생성하고 서로 교환한 후에, 제1 단말기(100)가 전송하는 RTP 패킷은 제1 인증키(A1)로 암호화하고, 제2 단말기(120)가 전송하는 RTP 패킷은 제2 인증키(A2)로 암호화하여 암호 통신을 실현한다. 이와 같은 경우에는 제2 단말기(120)가 수신하는 RTP 패킷은 제1 인증키(A1)로 복호화하고, 제1 단말기(100)가 수신하는 RTP 패킷은 제2 인증키(A2)로 복호화해야 한다. 상기 RTP 패킷의 암호화 및 복호화는 상기 인증키(A)를 이용한 일반적인 SRTP(Secure Real-time Transport Protocol) 방법인, AES 알고리즘을 사용하는 것이 바람직하다.

[0054] 단말기(100, 120)의 SIP 모듈(107, 127)은 사용자의 요청에 따라 서버의 SIP 중계 모듈(115)을 경유하여 SIP 메시지를 교환한다. 즉, 제1 단말기(100)에서 제2 단말기(120)로의 세션 설정(호 연결, 호 설정)을 요청할 때에는, 제1 단말기(100)의 SIP 모듈(107)이 서버(110)의 SIP 중계 모듈(115)을 경유하여 제2 단말기(120)의 SIP 모듈(127)에 세션 설정을 요청하는 SIP INVITE 메시지를 송신한다.

[0055] 먼저, 제1 단말기(100)의 SIP 모듈(107)은, 공유키 관리 모듈(103)에 제1 공유키(G1), 인증키 관리 모듈(105)에 제1 인증키(A1)의 전송을 요청한다. 그리고, 상기 SIP 모듈(107)은 상기 제1 인증키(A1)를 상기 제1 공유키(G1)로 암호화한 후, 암호화된 제1 인증키(A1')를 SIP INVITE 메시지에 포함시켜서 서버(110)에 전송한다.

[0056] 상기 암호화된 제1 인증키(A1')는 도 2에 도시된 바와 같이 SIP 메시지에 포함되는 SDP 메시지에 포함되는 것이 바람직하다. 도 2에 도시된 인증키는 밑줄이 그어져 있는 색칠한 부분 두 줄이며, 첫째 줄은 마스터 키, 둘째 줄은 마스터 솔트이다. 도 2에서는 인증키로서 마스터 키와 마스터 솔트가 두 줄로서 제시되어 있지만, 이와는 달리 한 줄로 표현되는 인증키를 사용할 수도 있다. 또한, 도 2에 도시된 인증키는 암호화되어 있지 않지만, 본 발명의 실시예에서는 상기 인증키는 공유키에 의하여 암호화된다. 이러한 인증키를 암호화하는 방법으로는, ARIA 암호화 알고리듬 방식이나 AES 암호화 알고리듬 방식, SEED 암호화 알고리듬 방식, 또는 Camellia 암호화 알고리듬 방식 등 다양한 암호화 알고리듬 방식을 이용할 수 있다.

[0057] 서버(110)의 SIP 중계 모듈(115)은 상기 암호화된 제1 인증키(A1')가 포함된 SIP INVITE 메시지를 수신하고, 공유키 관리 모듈(113)에 제1 단말기에 대응하는 제1 공유키(G1)와 제2 단말기에 대응하는 제2 공유키(G2)의 전송을 요청한다. 그리고 상기 SIP 중계 모듈(115)은 상기 제1 단말기(100)로부터 수신한 암호화된 제1 인증키(A1')를 제1 공유키(G1)로 복호화하여 제1 인증키(A1)를 추출한다. 계속하여 상기 SIP 중계 모듈(115)은 상기 제1 인증키(A1)를 제2 공유키(G2)로 암호화한 후, 암호화된 제1 인증키(A1'')를 상기 SIP INVITE 메시지에 포함시켜서 제2 단말기(120)에 전송한다.

[0058] 제2 단말기(120)의 SIP 모듈(127)은, 공유키 관리 모듈(123)에 제2 공유키(G2)의 전송을 요청한다. 그리고, 상기 SIP 모듈(107)은 상기 서버(110)로부터 수신한 암호화된 제1 인증키(A1'')를 상기 제2 공유키(G2)로 복호화하여 제1 인증키(A1)를 추출한다. 이로써 제1 단말기(100)에서 생성된 제1 인증키(A1)가 제2 단말기(120)에 전달된다.

[0059] 상기 제2 단말기(120)의 SIP 모듈(127)은 상기 제1 단말기(100)에서 서버(110)를 경유하여 수신된 SIP INVITE 메시지에 대하여, 세션 설정을 허락하지 않으면 그에 해당하는 SIP 메시지를 제1 단말기(100)에 전송하며, 세션 설정을 허락하면 그에 해당하는 SIP 200 OK 메시지를 서버(110)를 경유하여 제1 단말기(100)에 전송한다.

[0060] 제2 단말기(120)의 SIP 모듈(127)이 세션 설정을 수락하는 SIP 200 OK 메시지를 송신하는 경우에는, 공유키 관

리 모듈(123)에 제2 공유키(G2), 인증키 관리 모듈(125)에 제2 인증키(A2)의 전송을 요청한다. 그리고, 상기 SIP 모듈(127)은 상기 제2 인증키(A2)를 상기 제2 공유키(G2)로 암호화한 후, 암호화된 제2 인증키(A2'')를 SIP 200 OK 메시지에 포함시켜서 서버(110)에 전송한다.

[0061] 서버(110)의 SIP 중계 모듈(115)은 상기 암호화된 제2 인증키(A2'')가 포함된 SIP 200 OK 메시지를 수신한다. 그리고 상기 SIP 중계 모듈(115)은 상기 제2 단말기(120)로부터 수신한 암호화된 제2 인증키(A2'')를 제2 공유키(G2)로 복호화하여 제2 인증키(A2)를 추출한다. 계속하여 상기 SIP 중계 모듈(115)은 상기 제2 인증키(A2)를 제1 공유키(G1)로 암호화한 후, 암호화된 제2 인증키(A2')를 상기 SIP 200 OK 메시지에 포함시켜서 제1 단말기(100)에 전송한다.

[0062] 제1 단말기(100)의 SIP 모듈(107)은, 상기 서버(110)로부터 수신한 암호화된 제2 인증키(A2')를 상기 제1 공유키(G1)로 복호화하여 제2 인증키(A2)를 추출한다. 이로써 제2 단말기(120)에서 생성된 제2 인증키(A2)가 제2 단말기(100)에 전달된다.

[0063] 다음으로 제1 단말기(100)에서 제2 단말기(120)로 SIP 200 OK 메시지를 잘 받았다는 SIP ACK 확인 메시지를 송신한다. 제2 단말기(120)에서 이 SIP ACK 확인 메시지를 수신하면 세션이 설정된다.

[0064] 이 과정을 통하여 두 단말기(100, 120) 사이에 세션 설정이 이루어지면, 제1 단말기(100)와 제2 단말기(120)의 RTP 모듈(106, 126)을 이용하여 음성이나 영상 등의 멀티미디어 데이터 교환이 가능해진다.

[0065] 제1 단말기(100)의 RTP 모듈(109)과 제2 단말기(120)의 RTP 모듈(129)은, 상기 제1 인증키(A1)와 제2 인증키(A2)를 보유하게 되며, 제1 단말기(100)가 전송하는 RTP 패킷은 제1 인증키(A1)로 암호화하고, 제2 단말기(120)가 전송하는 RTP 패킷은 제2 인증키(A2)로 암호화하여 암호 통신을 실현할 수 있다. 이와 같은 경우에는 제2 단말기(120)가 수신하는 RTP 패킷은 제1 인증키(A1)로 복호화하고, 제1 단말기(100)가 수신하는 RTP 패킷은 제2 인증키(A2)로 복호화해야 한다.

[0066] 또한, 이와는 달리 상기 두 단말기(100, 120)는 암호 통신을 위하여 하나의 인증키(A)를 사용하여 RTP 패킷을 암호화/복호화 할 수 있다. 즉, 제1 단말기(100)의 RTP 모듈(109)과 제2 단말기(120)의 RTP 모듈(129)은, 단말기(100, 120)에서 RTP 패킷을 전송하기 전에 상기 RTP 패킷을 제1 인증키(A1)로 암호화하고, RTP 패킷을 수신한 후에 상기 RTP 패킷을 제1 인증키(A2)로 복호화하여 암호 통신을 실현할 수 있다.

[0067] 그리고 제1 단말기(100)와 제2 단말기(120) 중 어느 하나의 단말기에서 세션의 종료를 위한 SIP BYE 메시지를 송신하고 다른 하나의 단말기에서 이를 수신하면 세션은 종료된다.

[0068] 이와 같이 본 발명의 제1 실시예에 따른 암호 통신 시스템은, 상기 RTP 패킷을 인증키(A)를 이용하여 암호화(인코딩)하여 송신하고, 수신한 후에 복호화(디코딩)하므로, 중간에서 송수신되는 RTP 패킷을 아무나 읽을 수 없게 된다.

[0069] 본 발명의 제1 실시예에 따르면, 단말기와 서버가 공유하고 있는 정보로부터 공유키를 생성하고 상기 공유키를 이용하여 인증키를 암호화/복호화하므로, 안전하고 간편하게 암호 통신을 실현할 수 있다.

[0070] 또한, 상기 인증키는 SIP 메시지에 포함되어 교환하므로, 별도의 데이터 교환 과정 없이도 인증키를 교환할 수 있으므로, 부가적인 장치 없이 간단하게 암호 통신을 실현할 수 있다.

[0071] 또한, 인증키를 단말기에서 1회의 통신마다 생성하고, 단말기와 서버가 공유하고 있는 정보로부터 공유키를 생성하고, 상기 공유키를 이용하여 인증키를 암호화/복호화하므로, RTP 패킷을 보호하기 위한 인증키의 키 에스크로(key escrow) 문제를 해결하고, 인증키 노출시 또는 사용자의 VoIP 단말 분실시 발생하는 ID 폐지(ID revocation) 문제를 해결할 수 있다.

[0072] 이때, 상기 단말기는 음성 통화를 위한 전화기의 기본 구성(미도시)과, 사용자의 영상 통화를 위한 카메라(미도시)와, 통화 연결된 다른 단말기로부터의 영상 데이터를 표시하기 위한 표시부(미도시)와, 카메라가 찍은 영상과 표시부에서 처리할 영상을 처리하기 위한 영상처리부(미도시)를 더 구비한다.

[0073] 전화기의 기본 구성은 착신 신호 수신 시 사용자에게 알리는 벨, 전화를 받고 끊음을 위한 후크, 전화 번호 또는 사용자의 조작 명령의 입력을 위한 다수의 숫자키와 기능키를 포함하는 입력 버튼과, 음성 입력부, 음성 출력부, 음성 처리부 등이 포함된다.

[0074] 음성 입력부와 음성 출력부는 일반 전화의 송수화기와 유사하게 형성될 수 있으며, 단말기가 가령 컴퓨터 등으로 구현될 경우 컴퓨터에 연결된 마이크, 스피커와 같은 음성 입출력 수단이 될 수 있다.

[0075] 음성 처리부는 음성 입력부로부터 입력되는 가청음을 전기적인 신호인 음성 데이터로 변환하여 RTP 모듈로 송출하거나, RTP 모듈로부터 수신된 음성 데이터를 가청음으로 변환하여 음성 출력부에 전달한다.

[0076] 카메라는 예를 들면, 퍼스널 컴퓨터 또는 랩톱에 사용될 수 있는 웹 캠으로 구현될 수 있으며, 추가로 구매하여 단말기에 탈부착 될 수도 있고, 더욱 바람직하게는 단말기에 일체로 구비될 수 있다. 카메라는 단말기 사용자의 영상을 촬영하여 영상처리부로 송출한다.

[0077] 표시부는 예를 들면, LCD와 같은 액정표시장치로 구현될 수 있으며, 단말기가 컴퓨터로 구현될 경우 해당 컴퓨터와 연결된 모니터가 될 수 있다. 표시부는 영상처리부로부터 수신되는 정지영상 또는 동영상와 같은 영상 데이터를 표시하며, 단말기의 사용 상태를 표시하게 된다.

[0078] 영상처리부는 예를 들면, 디지털 신호 처리를 위한 DSP(Digital Signal Processor)로 구현될 수 있으며, 상기 카메라에서 수신되는 영상을 영상데이터로 변환하여 RTP 모듈로 송출하거나, RTP 모듈로부터 수신된 영상 데이터를 표시부로 송출한다.

[0079] 다음으로, 도 3 및 도 4를 참조하여 본 발명의 제1 실시예에 따른 인증키를 이용한 암호 통신 과정에 대하여 보다 상세히 설명한다.

[0080] 도 3은 본 발명의 제1 실시예에 따른 SIP 메시지의 흐름도이며, 도 4는 본 발명의 제1 실시예에 따른 암호 통신의 흐름도이다.

[0081] 본 발명의 제1 실시예에 따른 암호 통신 방법은 도 3에 도시한 바와 같이 서버(110)에 접속되어 있는 제1 단말기(100) 및 제2 단말기(120)가 SIP 메시지를 주교환하여 세션 설정을 하고(S210 ~ S240), RTP 패킷을 교환하여 음성이나 영상 등의 미디어 데이터를 교환하는(S250) 과정에 부가되는 방법이다.

[0082] 도 3 및 도 4를 참조하여 본 발명의 제1 실시예에 따른 암호 통신 방법을 살펴보면, 먼저, 제1 단말기(100)와 제2 단말기(120)가 각각 고유의 ID와 패스워드 등의 정보를 이용해서 서버(110)에 접속한다.

[0083] 상세하게는 제1 단말기(100)는 서버(110)가 공유하는 고유의 ID와 패스워드 등의 제1 공유 정보를 이용하여 소정의 세션키를 생성하고, 상기 세션키를 이용하여 제1 단말기(100)가 서버(110)에 접속하며, 상기 서버(110)는 상기 세션키를 확인하여 제1 단말기(100)의 접속을 허가한다. 또한, 제2 단말기(120)도 서버(110)가 공유하는 고유의 ID와 패스워드 등의 제2 공유 정보를 이용하여 소정의 세션키를 생성하고, 상기 세션키를 이용하여 제2 단말기(120)가 서버(110)에 접속하며, 상기 서버(110)는 상기 세션키를 확인하여 제2 단말기(120)의 접속을 허가한다.

[0084] 또한, 이와는 다른 방법으로, 단말기(100, 120)가 서버(110)에 접속할 수 있으며, 예를 들어 상기 ID와 패스워드를 이용하여 단말기(100, 120)가 서버(110)에 접속하는 방법을 이용할 수도 있다.

[0085] 다음으로 제1 단말기(100)가 제2 단말기(120)에 통화 연결을 요청하는 경우에, 먼저 제1 단말기(100)가 제1 공유 정보를 이용하여 제1 공유키(G1) 및 제1 인증키(A1)를 생성한다.

[0086] 공유 정보는 제1 단말기(100)와 서버(110)가 공유하는 정보로써, ID, 패스워드, 이용자의 주민등록번호 등의 정보를 말한다.

[0087] 공유키(G)는 SIP 메시지 교환시에, 상기 SIP 메시지에 포함되는 인증키(A)를 암호화하거나 복호화하는데 사용한다. 상기 공유키(G)는 상기 공유 정보의 일부를 그대로 취하여 사용할 수 있고, 또한, 상기 ID와 패스워드 중 일부를 취합하거나, 상기 ID와 패스워드를 현재 시간과 취합, 연산하여 1회의 통화시마다 생성할 수도 있다. 예를 들어, 1회의 통화시마다 공유키를 생성하는 방법으로는, 패스워드와 시간을 조합한 데이터를 제2 해싱테이블로 연산하여 생성하는 방법이 있을 수도 있다.

[0088] 또한, 상기 제1 공유키(G1)와 제2 공유키(G2)는 상기 단말기(100, 120)가 서버(110)에 접속하기 위한 세션키를 그대로 사용할 수도 있다.

[0089] 인증키(A)는 통화 연결 이후에 음성이나 영상 등의 미디어 데이터를 포함하는 RTP 패킷을 암호화/복호화 하기 위한 암호키이며, 보다 안전한 미디어 데이터 보안을 위해서는 1회의 통화시마다 생성하는 것이 바람직하다. 예를 들어, 1회의 통화시마다 패스워드와 시간을 조합한 데이터를 제1 해싱테이블로 연산하여 생성하는 방법이 있다.

[0090] 인증키(A) = 제1 해싱테이블(패스워드*시간)

[0091] 다음으로, 제1 단말기(100)는 제1 공유키(G1)를 이용하여 제1 인증키(A1)를 암호화하고, 암호화된 제1 인증키(A1')를 서버(110)에 전송한다(S410).

[0092] 상기 제1 인증키(A1)의 암호화 방법으로는 상기 제1 공유키(G1)를 이용한 ARIA 암호화 알고리듬 방식이나 AES 암호화 알고리듬 방식, SEED 암호화 알고리듬 방식, 또는 Camellia 암호화 알고리듬 방식 등 다양한 암호화 알고리듬 방식을 이용할 수 있다.

[0093] 상기 제1 인증키(A1')의 전송은 제1 단말기(100)가 제2 단말기(120)에 통화 연결을 위한 세션 설정을 요청하는 SIP INVITE 메시지에 포함되는, 음성이나 영상 등의 멀티미디어 세션 파라미터를 설정하는 SDP 메시지 안에 포함시켜서 전송한다.

[0094] 서버(110)는 제1 공유키(G1) 및 제2 공유키(G2)를 생성하고, 상기 제1 단말기(100)로부터 수신된 암호화된 제1 인증키(A1')를 제1 공유키(G1)로 복호화하여 제1 인증키(A1)를 생성한다(S420).

[0095] 즉, 상기 서버(110)는 상기 제1 인증키(A1')를 제1 단말기(100)가 암호화했던 동일한 방식으로 복호화하여 제1 인증키(A1)를 생성시킨다.

[0096] 상기 제1 인증키(A1')는 SIP INVITE 메시지에 포함되는 SDP 메시지 안에 포함되므로, SIP INVITE 메시지에서 상기 제1 인증키(A1')를 추출하여 제1 인증키(A1)를 생성한다.

[0097] 서버(110)가 제2 공유키(G2)를 이용하여 제1 인증키(A1)를 암호화하여 암호화된 제1 인증키(A1'')를 생성하고, 제2 단말기(120)에 전송한다(S430).

[0098] 제2 단말기(120)가 제2 공유키(G2)를 생성하고, 상기 제2 공유키(G2)를 이용하여 암호화된 제1 인증키(A1'')를 복호화하여 제1 인증키(A1)를 생성한다(S440).

[0099] 이로써, 제1 단말기(100)의 제1 인증키(A1)가 제2 단말기(120)로 전송된다.

[0100] 다음으로, 상기 제2 단말기(120)가 제1 단말기(100)의 통화 연결 요청에 연결에 응하는 경우, 제2 단말기(120)는 제2 인증키(A2)를 생성하고, 상기 제2 공유키(G2)를 이용하여 제2 인증키(A2)를 암호화하고, 암호화된 제2 인증키(A2'')를 서버(110)에 전송한다(S450).

[0101] 이때, 상기 제2 단말기(120)는 상기 SIP INVITE 메시지에 대응하여 연결에 응한다는 SIP 200 OK 메시지를 서버(110)를 통하여 제1 단말기(100)에 전송하며, 상기 제2 인증키(A2'')는 상기 SIP 200 OK 메시지에 포함되어 전송된다.

[0102] 서버(110)가 제2 공유키(G2)를 이용하여 암호화된 제2 인증키(A2'')를 복호화하여 제2 인증키(A2)를 생성한다(S460).

[0103] 서버(110)가 제1 공유키(G1)를 이용하여 제2 인증키(A2)를 암호화하고, 암호화된 제2 인증키(A2')를 제1 단말기(100)에 전송한다(S470).

[0104] 제1 단말기(100)가 제1 공유키(G1)를 이용하여 암호화된 제2 인증키(A2')를 복호화하여 제2 인증키(A2)를 생성한다(S480).

[0105] 이로써, 제2 단말기(120)의 제2 인증키(A2)가 제1 단말기(100)로 전송된다.

[0106] 이와 같이 제1 단말기(100)와 제2 단말기(120)가 인증키(A1, A2)를 안전하게 서로 교환하게 되면, 제1 단말기(100)와 제2 단말기(120)는 제1 인증키(A1)와 제2 인증키(A2)를 모두 보유하게 된다.

[0107] 또한, 상기 제1 인증키(A1)와 제2 인증키(A2)의 교환이 SIP INVITE 메시지와 SIP 200 OK 메시지를 통하여 이루어진 후에는, 제1 단말기(100)가 제2 단말기(120)에 SIP ACK 메시지를 전송한다. 상기 제2 단말기(120)에서 SIP ACK 메시지를 수신하면 세션 설정이 이루어진다.

[0108] 이와 같이 제1 단말기(100)와 제2 단말기(120)의 세션 설정이 이루어지면, 상기 인증키(A1, A2)를 이용하여 통화 등의 멀티미디어 데이터 교환을 시작하게 된다.

[0109] 즉, 제1 단말기(100)에서 사용자에 의해 생성되는 미디어 데이터는 제1 인증키(A1)로 암호화되어 제2 단말기(120)에 전송되고, 제2 단말기(100)에서 수신되는 미디어 데이터는 제1 인증키(A1)로 복호화되어 사용자에게 음

성이나 영상으로 전달된다.

[0110] 마찬가지로, 제2 단말기(200)에서 사용자에 의해 생성되는 미디어 데이터는 제2 인증키(A2)로 암호화되어 제1 단말기(100)에 전송되고, 제2 단말기(120)에서 수신되는 미디어 데이터는 제2 인증키(A2)로 복호화되어 사용자에게 음성이나 영상으로 전달된다.

[0111] 본 발명의 제1 실시예에서는 두 개의 인증키를 이용하여 미디어 데이터를 교환하는 방법에 대하여 설명했지만, 이와는 달리, 제1 단말기(100)와 제2 단말기(200)의 미디어 데이터의 교환을 하나의 인증키를 이용할 수도 있다.

[0112] 즉, 제1 단말기(100)의 제1 인증키(A1)를 제2 단말기(120)에 전달하고, 제2 단말기(200)에서 사용자에 의해 생성되는 미디어 데이터도 제1 인증키(A1)로 암호화하여 제1 단말기(100)에 전송하고, 제2 단말기(120)에서 수신되는 미디어 데이터도 제1 인증키(A1)로 복호화하여 사용자에게 음성이나 영상으로 전달하게 할 수도 있다.

[0113] 또한, 본 발명의 제1 실시예에서는, 제1 단말기(100)와 제2 단말기(120) 사이에 하나의 서버만이 존재하지만, 이와는 달리 복수의 서버가 존재할 수도 있다.

[0114] 즉, 제1 단말기(100)가 접속하는 서버와, 제2 단말기(120)가 접속하는 서버가 서로 다를 수 있다. 이때, 서버(일반적으로는 SIP 프록시 서버)끼리는 서로만이 알 수 있는 정보로 인증과정을 거쳐서 연결되어 있거나, 혹은, 공개된 인터넷 망이 아닌 내부 네트워크로 연결되어 있을 수 있다.

[0115] 이때, 인증과정을 거쳐서 연결된 서버사이에서는, 서로만이 알 수 있는 정보에 의하여 인증키가 암호화/복호화 과정을 거쳐서 전송될 수 있으며, 내부 네트워크로 연결된 서버사이에서는, 인증키가 그대로 전송될 수 있다.

[0116] 다음으로 도 5를 참조하여, 본 발명의 제2 실시예에 따른 암호 통신 방법에 대하여 상세하게 설명한다.

[0117] 먼저, 제1 단말기(300)와 제2 단말기(320)가 각각 고유의 ID와 패스워드 등의 정보를 이용해서 서버(310)에 접속한다.

[0118] 상세하게는 제1 단말기(300)는 서버(310)가 공유하는 고유의 ID와 패스워드 등의 제1 공유 정보를 이용하여 소정의 세션키를 생성하고, 상기 세션키를 이용하여 제1 단말기(300)가 서버(310)에 접속하며, 상기 서버(310)는 상기 세션키를 확인하여 제1 단말기(300)의 접속을 허가한다. 또한, 제2 단말기(320)도 서버(310)가 공유하는 고유의 ID와 패스워드 등의 제2 공유 정보를 이용하여 소정의 세션키를 생성하고, 상기 세션키를 이용하여 제2 단말기(320)가 서버(310)에 접속하며, 상기 서버(310)는 상기 세션키를 확인하여 제2 단말기(320)의 접속을 허가한다.

[0119] 또한, 이와는 다른 방법으로, 예를 들어 상기 ID와 패스워드를 이용하여 단말기(300, 320)가 서버(310)에 접속할 수도 있다.

[0120] 다음으로 제1 단말기(300)가 제2 단말기(320)에 통화 연결을 요청하는 경우에, 먼저 제1 단말기(300)가 제1 공유 정보를 이용하여 제1 공유키(G1) 및 제1 인증키(A1)를 생성한다.

[0121] 공유 정보는 제1 단말기(300)와 서버(310)가 공유하는 정보로써, ID, 패스워드, 이용자의 주민등록번호 등의 정보를 말한다.

[0122] 공유키(G)는 SIP 메시지 교환시에, 상기 SIP 메시지에 포함되는 인증키(A)를 암호화하거나 복호화하는데 사용한다. 상기 공유키(G)는 상기 공유 정보의 일부를 그대로 취하여 사용할 수 있고, 또한, 상기 ID와 패스워드 중 일부를 취합하거나, 상기 ID와 패스워드를 현재 시간과 취합, 연산하여 1회의 통화시마다 생성할 수도 있다. 예를 들어, 1회의 통화시마다 공유키를 생성하는 방법으로는, 패스워드와 시간을 조합한 데이터를 제2 해싱테이블로 연산하여 생성하는 방법이 있을 수도 있다. 또한, 상기 제1 공유키(G1)와 제2 공유키(G2)는 상기 단말기(300, 320)가 서버(310)에 접속하기 위한 세션키를 그대로 사용할 수도 있다.

[0123] 인증키(A)는 통화 연결 이후에 음성이나 영상 등의 미디어 데이터를 포함하는 RTP 패킷을 암호화/복호화 하기 위한 암호키이며, 보다 안전한 미디어 데이터 보안을 위해서는 1회의 통화시마다 생성하는 것이 바람직하다. 예를 들어, 1회의 통화시마다 패스워드와 시간을 조합한 데이터를 제1 해싱테이블로 연산하여 생성하는 방법이 있다.

[0124] 인증키(A) = 제1 해싱테이블(패스워드*시간)

[0125] 다음으로, 제1 단말기(300)는 제1 공유키(G1)를 이용하여 제1 인증키(A1)를 암호화하고, 암호화된 제1 인증키(A1')를 서버(310)에 전송한다(S510).

[0126] 상기 제1 인증키(A1)의 암호화 방법으로는 상기 제1 공유키(G1)를 이용한 ARIA 암호화 알고리듬 방식이나 AES 암호화 알고리듬 방식, SEED 암호화 알고리듬 방식, 또는 Camellia 암호화 알고리듬 방식 등 다양한 암호화 알고리듬 방식을 이용할 수 있다.

[0127] 이때, 상기 제1 인증키(A1')의 전송은 제1 단말기(300)가 제2 단말기(320)에 통화 연결을 위한 세션 설정을 요청하는 SIP INVITE 메시지에 포함되는, 음성이나 영상 등의 멀티미디어 세션 파라미터를 설정하는 SDP 메시지 안에 포함시켜서 전송한다.

[0128] 서버(310)는 제1 공유키(G1) 및 제2 공유키(G2)를 생성하고, 상기 제1 공유키(G1)를 제2 공유키(G2)로 암호한다. 그리고, 상기 암호화된 제1 공유키(G1'')와, 상기 제1 단말기(300)로부터 수신된 암호화된 제1 인증키(A1')를 제2 단말기(320)에 전송한다(S520).

[0129] 이때, 상기 제1 인증키(A1')가 포함된 SIP INVITE 메시지에 제1 공유키(G1'')를 더 포함시켜서 제2 단말기(320)에 전송한다.

[0130] 제2 단말기(320)는 암호화된 제1 공유키(G1'')와 암호화된 제1 인증키(A1')를 수신하고, 제2 공유키(G2)를 생성하고, 상기 제2 공유키(G2)를 이용하여 암호화된 제1 공유키(G1'')를 복호화하여 제1 공유키(A1)를 생성한다(S530).

[0131] 제2 단말기(320)는 상기 제1 공유키(A1)를 이용하여 암호화된 제1 인증키(A1')를 복호화하여 제1 인증키(A1)를 생성한다(S540).

[0132] 이로써, 제1 단말기(300)의 제1 인증키(A1)가 제2 단말기(320)로 전송된다.

[0133] 다음으로, 상기 제2 단말기(320)가 제1 단말기(300)의 통화 연결 요청에 연결에 응하는 경우, 제2 단말기(320)는 제2 인증키(A2)를 생성하고, 상기 제2 공유키(G2)를 이용하여 제2 인증키(A2)를 암호화하고, 암호화된 제2 인증키(A2'')를 서버(310)에 전송한다(S550).

[0134] 이때, 상기 제2 단말기(320)는 상기 SIP INVITE 메시지에 대응하여 연결에 응한다는 SIP 200 OK 메시지를 서버(310)를 통하여 제1 단말기(300)에 전송하며, 상기 제2 인증키(A2'')는 상기 SIP 200 OK 메시지에 포함되어 전송된다.

[0135] 서버(310)는 제1 공유키(G1) 및 제2 공유키(G2)를 생성하고, 상기 제2 공유키(G2)를 제1 공유키(G1)로 암호한다. 그리고, 상기 암호화된 제1 공유키(G1')와, 상기 제2 단말기(320)로부터 수신된 암호화된 제2 인증키(A2'')를 제1 단말기(300)에 전송한다(S560).

[0136] 제1 단말기(300)는 암호화된 제2 공유키(G2')와 암호화된 제2 인증키(A2'')를 수신하고, 제1 공유키(G1)를 생성하고, 상기 제1 공유키(G1)를 이용하여 암호화된 제2 공유키(G2')를 복호화하여 제2 공유키(A2)를 생성한다(S570).

[0137] 제1 단말기(300)는 상기 제2 공유키(A2)를 이용하여 암호화된 제2 인증키(A2'')를 복호화하여 제2 인증키(A2)를 생성한다(S580).

[0138] 이로써, 제2 단말기(320)의 제2 인증키(A2)가 제1 단말기(300)로 전송된다.

[0139] 이와 같이 제1 단말기(300)와 제2 단말기(320)가 인증키(A1, A2)를 안전하게 서로 교환하게 되면, 제1 단말기(300)와 제2 단말기(320)는 제1 인증키(A1)와 제2 인증키(A2)를 모두 보유하게 된다.

[0140] 또한, 상기 제1 인증키(A1)와 제2 인증키(A2)의 교환이 SIP INVITE 메시지와 SIP 200 OK 메시지를 통하여 이루어진 후에는, 제1 단말기(300)가 제2 단말기(320)에 SIP ACK 메시지를 전송한다. 상기 제2 단말기(320)에서 SIP ACK 메시지를 수신하면 세션 설정이 이루어진다.

[0141] 이와 같이 제1 단말기(300)와 제2 단말기(320)의 세션 설정이 이루어지면, 상기 인증키(A1, A2)를 이용하여 통화 등의 멀티미디어 데이터 교환을 시작하게 된다.

[0142] 즉, 제1 단말기(300)에서 사용자에 의해 생성되는 미디어 데이터는 제1 인증키(A1)로 암호화되어 제2 단말기(320)에 전송되고, 제2 단말기(300)에서 수신되는 미디어 데이터는 제1 인증키(A1)로 복호화되어 사용자에게 음

성이나 영상으로 전달된다.

[0143] 마찬가지로, 제2 단말기(200)에서 사용자에 의해 생성되는 미디어 데이터는 제2 인증키(A2)로 암호화되어 제1 단말기(300)에 전송되고, 제2 단말기(320)에서 수신되는 미디어 데이터는 제2 인증키(A2)로 복호화되어 사용자에게 음성이나 영상으로 전달된다.

[0144] 본 발명의 제2 실시예에서는 두 개의 인증키를 이용하여 미디어 데이터를 교환하는 방법에 대하여 설명했지만, 이와는 달리, 제1 단말기(300)와 제2 단말기(200)의 미디어 데이터의 교환을 하나의 인증키를 이용할 수도 있다.

[0145] 즉, 제1 단말기(300)의 제1 인증키(A1)를 제2 단말기(320)에 전달하고, 제2 단말기(200)에서 사용자에 의해 생성되는 미디어 데이터도 제1 인증키(A1)로 암호화하여 제1 단말기(300)에 전송하고, 제2 단말기(320)에서 수신되는 미디어 데이터도 제1 인증키(A1)로 복호화하여 사용자에게 음성이나 영상으로 전달하게 할 수도 있다.

[0146] 또한, 본 발명의 제2 실시예에서는, 제1 단말기(300)와 제2 단말기(320) 사이에 하나의 서버만이 존재하지만, 이와는 달리 복수의 서버가 존재할 수도 있다.

[0147] 즉, 제1 단말기(300)가 접속하는 서버와, 제2 단말기(320)가 접속하는 서버가 서로 다를 수 있다. 이때, 서버(일반적으로는 SIP 프록시 서버)끼리는 서로만이 알 수 있는 정보로 인증과정을 거쳐서 연결되어 있거나, 혹은, 공개된 인터넷 망이 아닌 내부 네트워크로 연결되어 있을 수 있다.

[0148] 이때, 인증과정을 거쳐서 연결된 서버사이에서는, 서로만이 알 수 있는 정보에 의하여 인증키와 공유키가 암호화/복호화 과정을 거쳐서 전송될 수 있으며, 내부 네트워크로 연결된 서버사이에서는, 인증키와 공유키가 그대로 전송될 수 있다.

[0149] 본 발명을 첨부 도면과 전술된 바람직한 실시예를 참조하여 설명하였으나, 본 발명은 이에 한정되지 않으며, 후술되는 특허청구범위에 의해 한정된다. 따라서, 본 기술분야의 통상의 지식을 가진 자라면 후술되는 특허청구범위의 기술적 사상에서 벗어나지 않는 범위 내에서 본 발명을 다양하게 변형 및 수정할 수 있다.

부호의 설명

[0150] 100, 300: 제1 단말기

120, 320: 제2 단말기

101, 121: 서버 접속 모듈

103, 123: 공유키 관리 모듈

105, 125: 인증키 관리 모듈

107, 127: SIP 모듈

109, 129: RTP 모듈

110, 310: 서버

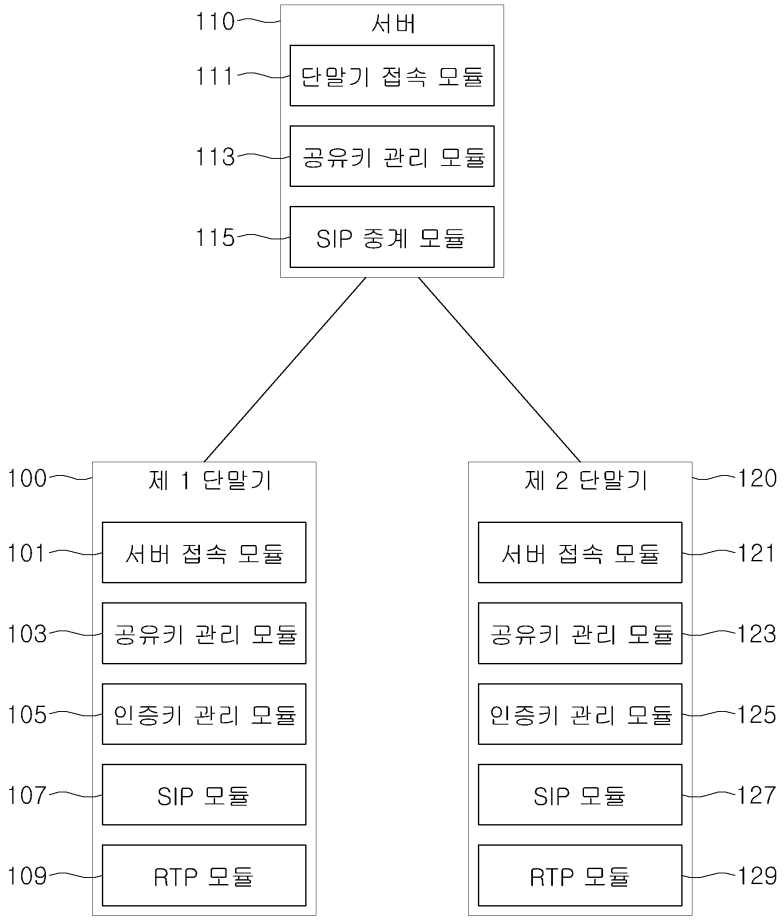
111: 단말기 접속 모듈

113: 공유키 관리 모듈

115: SIP 중계 모듈

도면

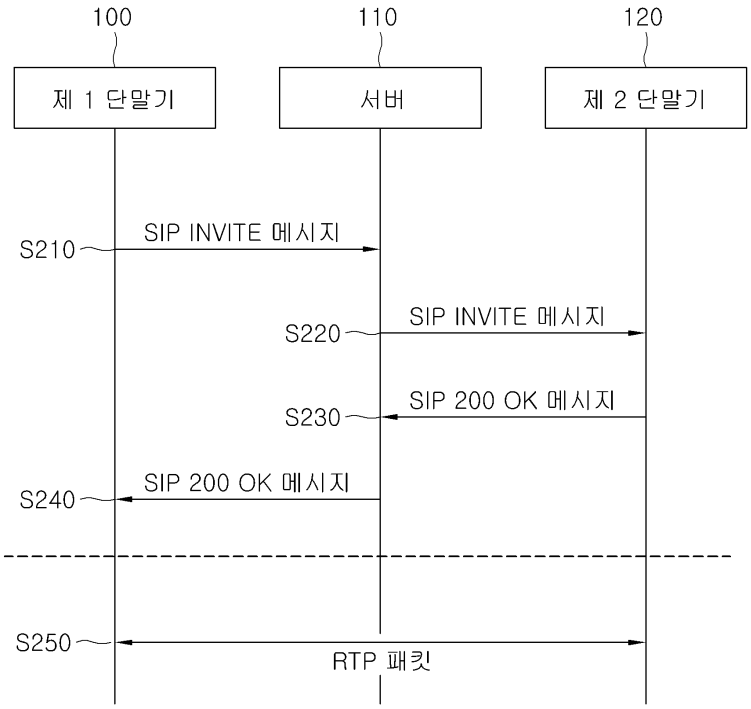
도면1



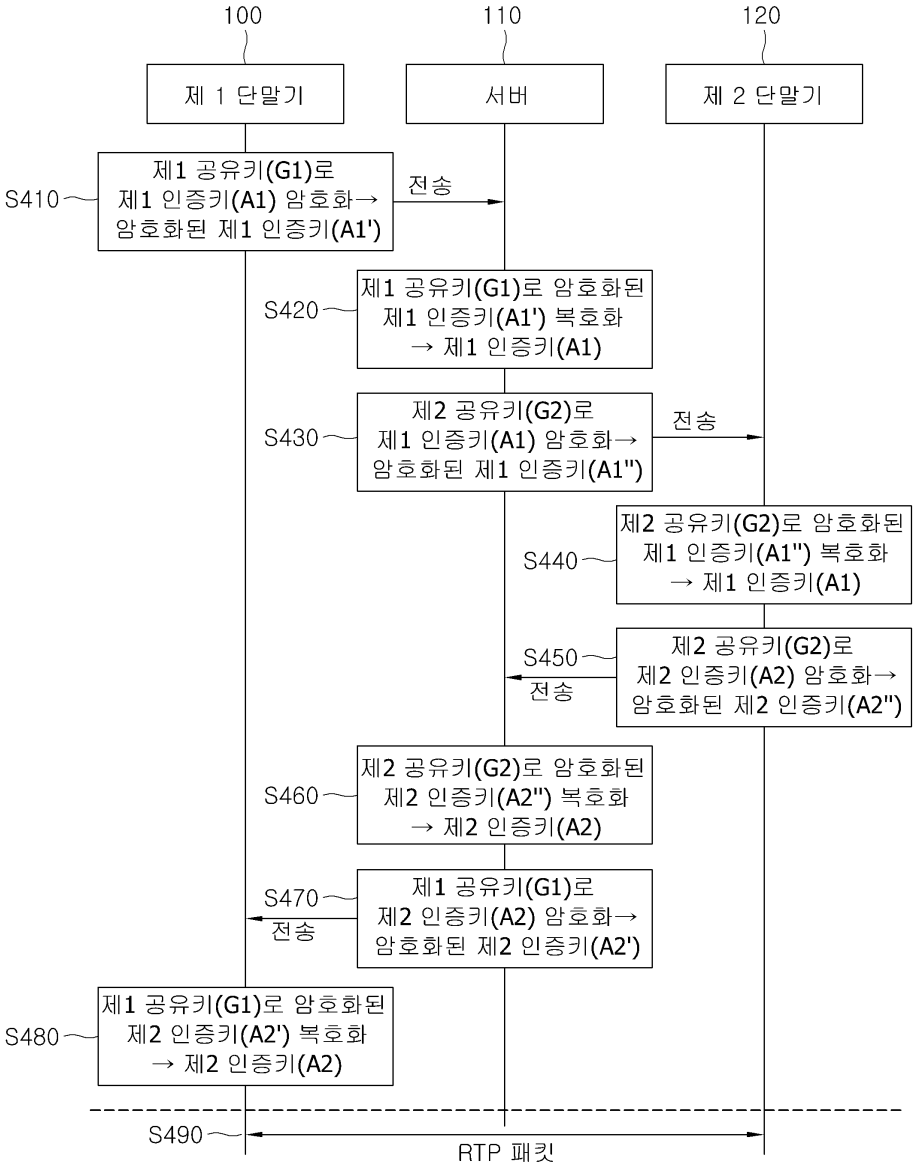
도면2

```
v=0
o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.example.com/seminars/sdp.pdf
e=j.doe@example.com (Jane Doe)
c=IN IP4 161.44.17.12/127
t=2873397496 2873404696
m=video 51372 RTP/SAVP 31
a=crypto:1 ARIA_CM_128_HMAC_SHA1_80 inline:dORmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
m=audio 49170 RTP/SAVP 0
a=crypto:1 ARIA_CM_128_HMAC_SHA1_32 inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32
m=application 32416 udp wb
a=orient:portrait
```

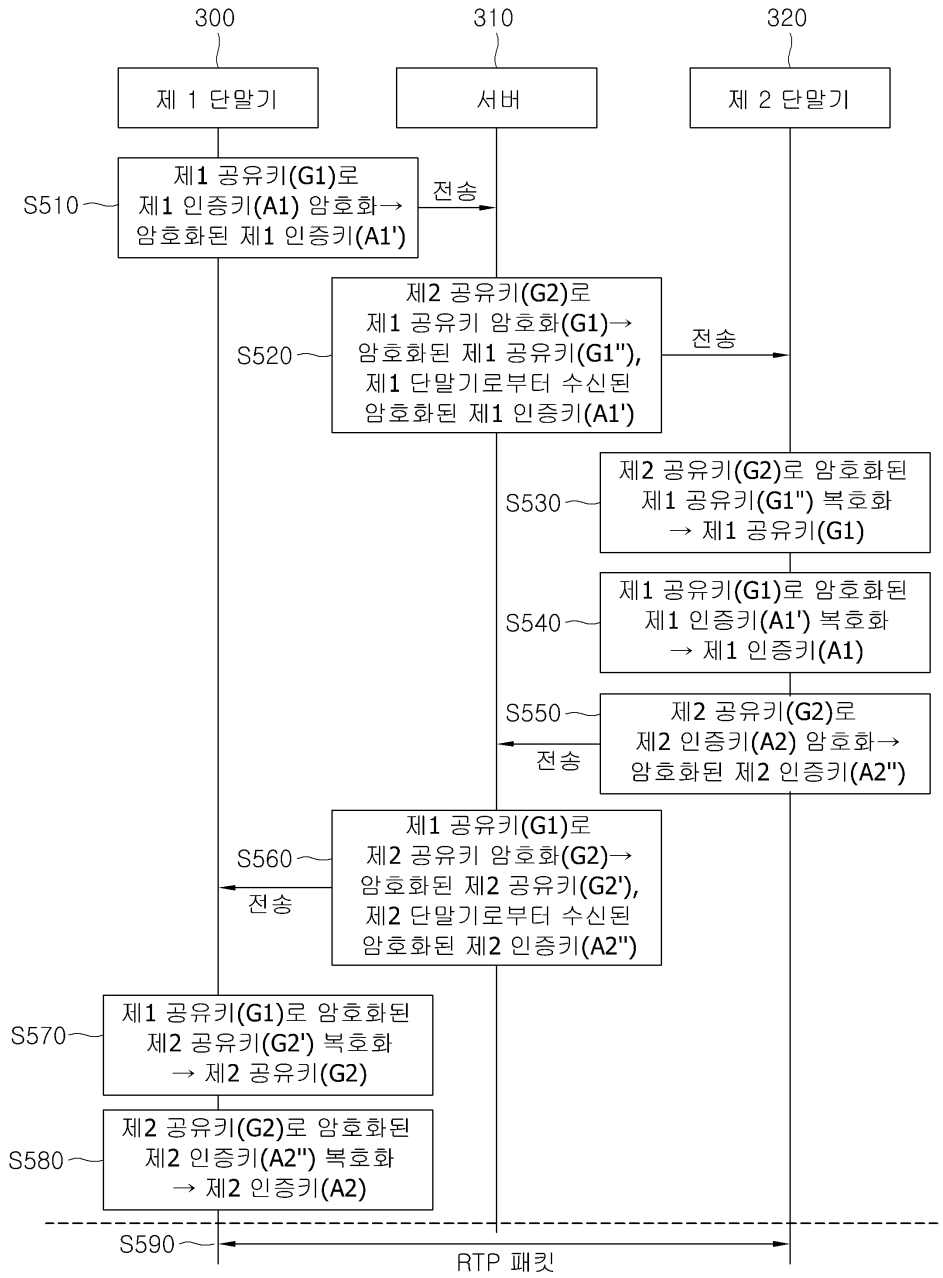
도면3


100
110
120
제 1 단말기
서버
제 2 단말기
S210
SIP INVITE 메시지
S220
SIP INVITE 메시지
S230
SIP 200 OK 메시지
S240
SIP 200 OK 메시지
S250
RTP 패킷

도면4


100
110
120
제 1 단말기
서버
제 2 단말기
S410
제1 공유키(G1)로
제1 인증키(A1) 암호화→
암호화된 제1 인증키(A1')
전송
S420
제1 공유키(G1)로 암호화된
제1 인증키(A1') 복호화
→ 제1 인증키(A1)
S430
제2 공유키(G2)로
제1 인증키(A1) 암호화→
암호화된 제1 인증키(A1'')
전송
S440
제2 공유키(G2)로 암호화된
제1 인증키(A1'') 복호화
→ 제1 인증키(A1)
S450
전송
제2 공유키(G2)로
제2 인증키(A2) 암호화→
암호화된 제2 인증키(A2'')
S460
제2 공유키(G2)로 암호화된
제2 인증키(A2'') 복호화
→ 제2 인증키(A2)
S470
전송
제1 공유키(G1)로
제2 인증키(A2) 암호화→
암호화된 제2 인증키(A2')
S480
제1 공유키(G1)로 암호화된
제2 인증키(A2') 복호화
→ 제2 인증키(A2)
S490
RTP 패킷

도면5


300
310
320
제 1 단말기
서버
제 2 단말기
S510
제1 공유키(G1)로
제1 인증키(A1) 암호화→
암호화된 제1 인증키(A1')
전송
S520
제2 공유키(G2)로
제1 공유키 암호화(G1)→
암호화된 제1 공유키(G1''),
제1 단말기로부터 수신된
암호화된 제1 인증키(A1')
전송
S530
제2 공유키(G2)로 암호화된
제1 공유키(G1'') 복호화
→ 제1 공유키(G1)
S540
제1 공유키(G1)로 암호화된
제1 인증키(A1') 복호화
→ 제1 인증키(A1)
S550
제2 공유키(G2)로
제2 인증키(A2) 암호화→
암호화된 제2 인증키(A2'')
전송
S560
제1 공유키(G1)로
제2 공유키 암호화(G2)→
암호화된 제2 공유키(G2'),
제2 단말기로부터 수신된
암호화된 제2 인증키(A2'')
전송
S570
제1 공유키(G1)로 암호화된
제2 공유키(G2') 복호화
→ 제2 공유키(G2)
S580
제2 공유키(G2)로 암호화된
제2 인증키(A2'') 복호화
→ 제2 인증키(A2)
S590
RTP 패킷