



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년04월23일
(11) 등록번호 10-1256114
(24) 등록일자 2013년04월12일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/08 (2006.01)
(21) 출원번호 10-2011-0115131
(22) 출원일자 2011년11월07일
심사청구일자 2011년11월07일
(56) 선행기술조사문헌
KR1020070118282 A
KR1020080065633 A
KR1020090015736 A
KR1020070074231 A

(73) 특허권자
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
김휘강
서울특별시 서초구 양재동
김형석
경기도 부천시 소사구 범안로96번길 23, 405동
2103호 (범박동, 현대홈타운)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 10 항

심사관 : 양종필

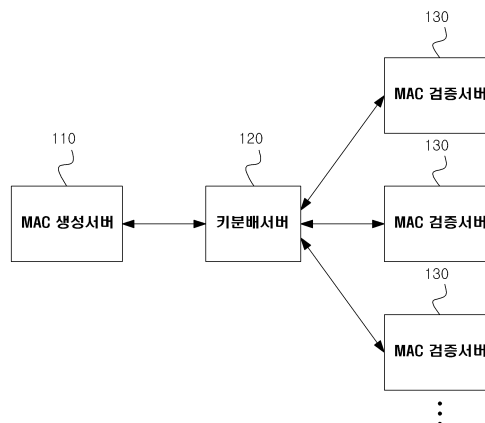
(54) 발명의 명칭 다수의 MAC 검증서버에 의한 메시지인증코드 검증 방법 및 시스템

(57) 요약

본 발명은 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템 및 방법에 관한 것으로, 보다 구체적으로는 MAC(Message Authentication Code)생성서버가 키분배서버로부터 타임스탬프값을 수신하여, 수신한 타임스탬프값의 주기 초과여부를 확인하는 주기확인단계; 상기 MAC생성서버가 고유한 아이디정보와 이전 타임스탬프값 및 대칭키를 상기 키분배서버로 전송하는 대칭키전송단계; 상기 MAC생성서버가 상기 대칭키를 해시하여 기준 메시지인증코드를 생성하는 MAC생성단계; 상기 MAC생성서버가 고유한 아이디정보와 이전 타임스탬프값 및 상기 기준 메시지인증코드를 데이터에 포함하고, 상기 데이터를 적어도 하나의 MAC검증서버로 전송하는 데이터전송단계; 상기 MAC검증서버가 상기 키분배서버로부터 타임스탬프값을 수신하고, 수신한 타임스탬프값과 상기 MAC생성서버로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 같거나 작은 경우, 상기 키분배서버로부터 수신한 타임스탬프값이 유효하다고 판단하는 유효성판단단계; 상기 MAC검증서버가 상기 MAC생성서버로부터 수신한 상기 데이터 내 고유한 아이디정보 및 이전 타임스탬프값을 상기 키분배서버로 전송하고, 상기 키분배서버로부터 상기 고유의 아이디정보 및 이전 타임스탬프값에 대응하는 대칭키를 수신하는 대칭키공유단계; 및 상기 MAC검증서버가 수신한 대칭키를 이용하여 비교 메시지인증코드를 생성한 후, 생성된 비교 메시지인증코드와 상기 MAC생성서버로부터 수신한 데이터 내 기준 메시지인증코드를 상호 비교하여 동일여부에 따라 상기 기준 메시지인증코드에 대한 검증을 수행하는 MAC검증단계;를 포함한다.

이러한 구성에 의해, 본 발명의 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템은 동일한 대칭키를 다수의 사용자 즉, 다수의 MAC검증서버가 키분배서버를 통해 공유하여, 메시지 인증 코드의 조작여부를 용이하게 검증할 수 있는 효과가 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	ITAC109011110002000
부처명	정보통신산업진흥원
연구사업명	대학IT연구센터육성지원사업
연구과제명	스마트 그리드 보안 연구센터(스마트 그리드 보안기술 개발)
주관기관	고려대학교 산학협력
연구기간	2011.01.01 ~ 2011.12.31

특허청구의 범위

청구항 1

MAC(Message Authentication Code)생성서버가 키분배서버로부터 타임스탬프값을 수신하여, 수신한 타임스탬프값의 주기 초과여부를 확인하는 주기확인단계;

상기 MAC생성서버가 고유한 아이디정보와 이전 타임스탬프값 및 대칭키를 상기 키분배서버로 전송하는 대칭키전송단계;

상기 MAC생성서버가 상기 대칭키를 해시하여 기준 메시지인증코드를 생성하는 MAC생성단계;

상기 MAC생성서버가 고유한 아이디정보와 이전 타임스탬프값 및 상기 기준 메시지인증코드를 데이터에 포함하고, 상기 데이터를 적어도 하나의 MAC검증서버로 전송하는 데이터전송단계;

상기 MAC검증서버가 상기 키분배서버로부터 타임스탬프값을 수신하고, 수신한 타임스탬프값과 상기 MAC생성서버로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 같거나 작은 경우, 상기 키분배서버로부터 수신한 타임스탬프값이 유효하다고 판단하는 유효성판단단계;

상기 MAC검증서버가 상기 MAC생성서버로부터 수신한 상기 데이터 내 고유한 아이디정보 및 이전 타임스탬프값을 상기 키분배서버로 전송하고, 상기 키분배서버로부터 상기 고유의 아이디정보 및 이전 타임스탬프값에 대응하는 대칭키를 수신하는 대칭키공유단계; 및

상기 MAC검증서버가 수신한 대칭키를 이용하여 비교 메시지인증코드를 생성한 후, 생성된 비교 메시지인증코드와 상기 MAC생성서버로부터 수신한 데이터 내 기준 메시지인증코드를 상호 비교하여 동일여부에 따라 상기 기준 메시지인증코드에 대한 검증을 수행하는 MAC검증단계;

를 포함하는 다수의 MAC검증서버에 의한 메시지인증코드 검증방법.

청구항 2

제1항에 있어서,

상기 주기확인단계는

상기 MAC생성서버가 상기 키분배서버로부터 수신한 타임스탬프값을 기생성된 대칭키에 대한 이전 타임스탬프값 및 타임스탬프 주기의 합과 비교하는 비교과정;

상기 MAC생성서버가 수신한 타임스탬프값이 기생성된 대칭키에 대한 이전 타임스탬프값과 타임스탬프 주기의 합보다 큰 경우, 상기 타임스탬프값이 주기를 초과하였다고 판단하는 주기판단과정;

상기 MAC생성서버는 상기 타임스탬프값이 주기를 초과하였다고 판단함에 따라 신규 대칭키를 생성하는 대칭키생성과정; 및

상기 MAC생성서버는 상기 기생성된 대칭키에 대한 이전 타임스탬프값을 상기 타임스탬프값으로 갱신하는 갱신과정;

을 포함하는 것을 특징으로 하는 다수의 MAC검증서버에 의한 메시지인증코드 검증방법.

청구항 3

제2항에 있어서,

상기 주기판단과정은

상기 MAC생성서버가 상기 키분배서버로부터 수신한 타임스탬프값이 기생성된 대칭키에 대한 이전 타임스탬프값과 타임스탬프 주기의 합보다 같거나 작은 경우, 상기 타임스탬프값이 주기를 초과하지 않는다고 판단하는 과정;

정을 더 포함하는 것을 특징으로 하는 다수의 MAC검증서버에 의한 메시지인증코드 검증방법.

청구항 4

제1항에 있어서,

상기 유효성판단단계는

상기 MAC검증서버가 상기 키분배서버로부터 수신한 타임스탬프값과 상기 MAC생성서버로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 큰 경우, 상기 키분배서버로부터 수신한 타임스탬프값이 유효하지 않다고 판단하고, 상기 기준 메시지인증코드가 조작되었다고 판단하는 과정을 더 포함하는 것을 특징으로 하는 다수의 MAC검증서버에 의한 메시지인증코드 검증방법.

청구항 5

제1항에 있어서,

상기 MAC생성서버와 키분배서버 및 상기 MAC검증서버와 키분배서버는 상호간에 SSL(Secure Sockets Layer) 통신을 수행하는 것을 특징으로 하는 다수의 MAC검증서버에 의한 메시지인증코드 검증방법.

청구항 6

제1항 내지 제5항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

청구항 7

키분배서버로부터 타임스탬프값을 수신하고, 대칭키를 이용하여 기준 메시지인증코드(MAC: Message Authentication Code)를 생성한 후, 고유한 아이디정보와 이전 타임스탬프값 및 기준 메시지인증코드를 포함하는 데이터를 적어도 하나의 MAC검증서버로 전송하는 하나의 MAC생성서버;

상기 MAC생성서버의 요청에 응답하여 상기 타임스탬프값을 전송하고, 상기 MAC생성서버로부터 고유한 아이디정보와 이전 타임스탬프값 및 대칭키를 수신하며, 수신한 상기 대칭키를 적어도 하나의 MAC검증서버로 전송하는 하나의 키분배서버; 및

상기 키분배서버로부터 타임스탬프값 및 대칭키를 수신하고, 상기 타임스탬프값에 대한 유효성을 판단한 후, 상기 대칭키를 이용하여 비교 메시지인증코드를 생성한 후, 생성한 비교 메시지인증코드를 상기 기준 메시지인증코드와 비교하여 상기 기준 메시지인증코드에 대한 검증을 수행하는 적어도 하나의 MAC검증서버;

를 포함하는 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템.

청구항 8

제7항에 있어서,

상기 MAC생성서버는

상기 키분배서버로부터 수신한 타임스탬프값을 기생성된 대칭키에 대한 이전 타임스탬프값 및 타임스탬프 주기의 합과 비교하는 주기비교모듈;

상기 수신한 타임스탬프값이 기생성된 대칭키에 대한 이전 타임스탬프값과 타임스탬프 주기의 합보다 큰 경우에는 상기 수신한 타임스탬프값이 주기를 초과하였다고 판단하는 주기판단모듈;

상기 수신한 타임스탬프값이 주기를 초과하였다고 판단되는 경우에는 신규 대칭키를 생성하는 대칭키생성모듈;

및

상기 기생성된 대칭키에 대한 이전 타임스탬프값을 상기 수신한 타임스탬프값으로 갱신하는 갱신모듈;
을 포함하는 것을 특징으로 하는 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템.

청구항 9

제7항에 있어서,

상기 MAC검증서버는

상기 키분배서버로부터 수신한 타임스탬프값과 상기 MAC생성서버로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 큰 경우에, 상기 수신한 타임스탬프값이 유효하지 않다고 판단하고, 상기 기준 메시지인증코드가 조작되었다고 판단하는 것을 특징으로 하는 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템.

청구항 10

제7항에 있어서,

상기 MAC생성서버와 키분배서버 및 상기 MAC검증서버와 키분배서버는

상호 간에 SSL(Secure Sockets Layer) 통신을 수행하는 것을 특징으로 하는 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템.

명세서

기술 분야

[0001] 본 발명은 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템은 특정 서버가 생성한 메시지인증코드에 대하여 다수의 서버가 용이하게 검증할 수 있는 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템에 관한 것이다.

배경 기술

[0002] IT 기술의 발전에 따라 사용자는 자신의 개인정보를 외부의 각종 서버 또는 단말에 전송하여 사용자 본인인증을 수행한 후, 인증이 완료되면 원하는 서비스를 제공받고 있다. 하지만 이처럼, 사용자의 개인정보를 외부의 서버 또는 단말로 전송하여, 사용자의 본인 인증을 수행하는데 있어서, 해커 또는 공격자에 의해 상기 개인정보가 노출되어 각종 범죄에 악용되는 사례가 급속도로 많아지고 있다. 이를 방지하고자 상기 사용자의 개인정보를 외부의 서버 또는 단말로 전송할 때, 암호화하여 전송하는 방법이 주로 사용되고 있다. 특히, 이러한 개인정보의 보안을 위해, 메시지 인증 코드가 주로 사용된다.

[0003] 이때, 상기 메시지 인증 코드(MAC: Message Authentication Code)란, 컴퓨터 보안에서 메시지의 내용, 작성자, 발신처 등과 같은 속성이 정당한지 여부를 검증하도록 메시지와 함께 전송되는 값을 말한다. 또한 상기 메시지 인증 코드는 컴퓨터 보안기법에서 주로 사용되는 암호 기법 중 하나로서, 하나의 인증 알고리즘을 통해 데이터를 처리해서 생성된 수 또는 값을 말하며, 디지털 서명부호를 나타내기도 한다. 이러한 메시지 인증 코드 기술은 대칭키 알고리즘을 통해 송수신하는 데이터의 인증과 무결성을 보장한다. 특히, 메시지인증코드를 생성 및 검증하기 위하여 대칭키를 이용한 대칭키 알고리즘이 사용된다.

[0004] 이와 같이, 대칭키 알고리즘을 이용하는 메시지 인증 코드 기술은 생성과 검증에 동일한 대칭키를 사용하기 때문에, 다수의 사용자가 메시지 인증 코드를 검증하기 위해서는 상기 다수의 사용자가 동일한 대칭키를 상호 공유해야한다. 따라서, 상기 대칭키를 알고 있는 사용자가 상기 대칭키를 악용하는 경우, 메시지 인증 코드가 조

작되어, 전송하고자 하는 데이터 내 사용자의 개인정보가 외부로 노출되는 문제점이 발생한다.

[0005] 상술한 바와 같이, 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템에 대한 선행기술을 살펴보면 다음과 같다.

[0006] 선행기술 1은 한국공개특허공보 제2006-0127333호(2006.12.12)로서, 이동통신망을 통해 전송되는 데이터 암호화 방법에 관한 것이다. 이러한 선행기술 1은 NTP 타임스탬프(Timestamp) 값과 ESN 값을 나머지(modulo) 연산하여 비밀키를 생성하는 이동통신망을 통해 전송되는 데이터 암호화 방법 및 서버가 이동통신 단말기로부터 NTP 타임스탬프 값이 포함된 데이터 요청 신호를 수신하고, 상기 서버에서 상기 NTP 타임스탬프 값과 상기 이동통신 단말기의 ESN 값을 나머지(modulo) 연산하여 비밀키를 생성하고, 상기 서버에서 상기 이동통신 단말기로 전송하고자 하는 원문 데이터와 상기 비밀키를 배타적 논리합 연산하여 암호문 데이터를 생성하고, 상기 서버가 상기 암호문 데이터를 상기 이동통신 단말기로 전송하여, 이동통신망을 통해 전송되는 데이터를 암호화한다.

[0007] 또한, 선행기술 2는 한국등록특허공보 제0581590호(2006.05.12)로서, 이중 요소 인증된 키 교환 방법 및 이를 이용한 인증방법과 그 방법을 포함하는 프로그램이 저장된 기록매체에 관한 것이다. 이러한 선행기술 2는 가입자 단말기가 자신의 식별자와 인증 서버의 공개키를 사용하여 생성된 값을 인증 서버로 송신하고, 인증 서버는 가입자 단말기로부터 수신된 값을 사용하여 가입자 관련 패스워드 및 대칭키와 인증 서버의 비밀키를 검출하고, 난수를 생성하여 가입자 단말기로 송신한 후, 가입자 단말기는 수신된 난수와 패스워드 및 대칭키를 사용하여 특정 값을 암호화한 값과 생성된 가입자측 인증자를 인증 서버로 송신하며, 상기 인증 서버는 패스워드, 대칭키 및 난수를 사용하여 생성한 제2 특정 값을 복호화 키로 하여 상기 수신된 암호화 값을 복호화하고, 복호된 값에 기초하여 가입자측 인증자에 대한 인증을 수행하며, 인증이 성공되는 경우에는 패스워드, 대칭키 및 공개키를 사용하여 생성된 인증 서버측 인증자를 가입자 단말기로 송신하고, 가입자 단말기는 대칭키와 패스워드를 사용하여 인증 서버측 인증자에 대한 인증을 수행한다.

발명의 내용

해결하려는 과제

[0008] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 다수의 검증서버가 타임스탬프값의 주기 및 유효성 확인을 통해 동일한 대칭키를 키분배서버로부터 제공받아 이를 이용하여 메시지 인증 코드의 검증을 용이하게 수행하는 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템을 제공하고자 한다.

과제의 해결 수단

[0009] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법은 MAC(Message Authentication Code)생성서버가 키분배서버로부터 타임스탬프값을 수신하여, 수신한 타임스탬프값의 주기 초과여부를 확인하는 주기확인단계; 상기 MAC생성서버가 고유한 아이디정보와 이전 타임스탬프값 및 대칭키를 상기 키분배서버로 전송하는 대칭키전송단계; 상기 MAC생성서버가 상기 대칭키를 해시하여 기준 메시지인증코드를 생성하는 MAC생성단계; 상기 MAC생성서버가 고유한 아이디정보와 이전 타임스탬프값 및 상기 기준 메시지인증코드를 데이터에 포함하고, 상기 데이터를 적어도 하나의 MAC검증서버로 전송하는 데이터전송단계; 상기 MAC검증서버가 상기 키분배서버로부터 타임스탬프값을 수신하고, 수신한 타임스탬프값과 상기 MAC생성서버로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 같거나 작은 경우, 상기 키분배서버로부터 수신한 타임스탬프값이 유효하다고 판단하는 유효성판단단계; 상기 MAC검증서버가 상기 MAC생성서버로부터 수신한 상기 데이터 내 고유한 아이디정보 및 이전 타임스탬프값을 상기 키분배서버로 전송하고, 상기 키분배서버로부터 상기 고유의 아이디정보 및 이전 타임스탬프값에 대응하는 대칭키를 수신하는 대칭키공유단계; 및 상기 MAC검증서버가 수신한 대칭키를 이용하여 비교 메시지인증코드를 생성한 후, 생성된 비교 메시지인증코드와 상기 MAC생성서버로부터 수신한 데이터 내 기준 메시지인증코드를 상호 비교하여 동일여부에 따라 상기 기준 메시지인증코드에 대한 검증을 수행하는 MAC검증단계;를 포함한다.

[0010] 보다 바람직하게는 상기 MAC생성서버가 상기 키분배서버로부터 수신한 타임스탬프값을 기생성된 대칭키에 대한 이전 타임스탬프값 및 타임스탬프 주기의 합과 비교하는 비교과정; 상기 MAC생성서버가 수신한 타임스탬프값이 기생성된 대칭키에 대한 이전 타임스탬프값과 타임스탬프 주기의 합 보다 큰 경우, 상기 타임스탬프값이 주기를

초과하였다고 판단하는 주기판단과정; 상기 MAC생성서버는 상기 타임스탬프값이 주기를 초과하였다고 판단함에 따라 신규 대칭키를 생성하는 대칭키생성과정; 및 상기 MAC생성서버는 상기 기생성된 대칭키에 대한 이전 타임스탬프값을 상기 타임스탬프값으로 갱신하는 갱신과정;을 포함하는 주기확인단계를 포함할 수 있다.

[0011] 특히, 상기 MAC생성서버가 상기 키분배서버로부터 수신한 타임스탬프값이 기생성된 대칭키에 대한 이전 타임스탬프값과 타임스탬프 주기의 합 보다 같거나 작은 경우, 상기 타임스탬프값이 주기를 초과하지 않는다고 판단하는 과정을 더 포함하는 주기판단과정을 포함할 수 있다.

[0012] 보다 바람직하게는 상기 MAC검증서버가 상기 키분배서버로부터 수신한 타임스탬프값과 상기 MAC생성서버로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 큰 경우, 상기 키분배서버로부터 수신한 타임스탬프값이 유효하지 않다고 판단하고, 상기 기준 메시지인증코드가 조작되었다고 판단하는 과정을 더 포함하는 유효성판단단계를 포함할 수 있다.

[0013] 특히, 상기 MAC생성서버와 키분배서버 및 상기 MAC검증서버와 키분배서버는 상호간에 SSL(Secure Sockets Layer) 통신을 수행할 수 있다.

[0014] 위와 같은 과제를 해결하기 위한 본 발명의 다른 실시 예에 따른 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템은 키분배서버로부터 타임스탬프값을 수신하고, 대칭키를 이용하여 기준 메시지인증코드(MAC: Message Authentication Code)를 생성한 후, 고유한 아이디정보와 이전 타임스탬프값 및 기준 메시지인증코드를 포함하는 데이터를 적어도 하나의 MAC검증서버로 전송하는 하나의 MAC생성서버; 상기 MAC생성서버의 요청에 응답하여 상기 타임스탬프값을 전송하고, 상기 MAC생성서버로부터 고유한 아이디정보와 이전 타임스탬프값 및 대칭키를 수신하며, 수신한 상기 대칭키를 적어도 하나의 MAC검증서버로 전송하는 하나의 키분배서버; 및 상기 키분배서버로부터 타임스탬프값 및 대칭키를 수신하고, 상기 타임스탬프값에 대한 유효성을 판단한 후, 상기 대칭키를 이용하여 비교 메시지인증코드를 생성한 후, 생성한 비교 메시지인증코드를 상기 기준 메시지인증코드와 비교하여 상기 기준 메시지인증코드에 대한 검증을 수행하는 적어도 하나의 MAC검증서버;를 포함한다.

[0015] 보다 바람직하게는 상기 키분배서버로부터 수신한 타임스탬프값을 기생성된 대칭키에 대한 이전 타임스탬프값 및 타임스탬프 주기의 합과 비교하는 주기비교모듈; 상기 수신한 타임스탬프값이 기생성된 대칭키에 대한 이전 타임스탬프값과 타임스탬프 주기의 합보다 큰 경우에는 상기 수신한 타임스탬프값이 주기를 초과하였다고 판단하는 주기판단모듈; 상기 수신한 타임스탬프값이 주기를 초과하였다고 판단되는 경우에는 신규 대칭키를 생성하는 대칭키생성모듈; 및 상기 기생성된 대칭키에 대한 이전 타임스탬프값을 상기 수신한 타임스탬프값으로 갱신하는 갱신모듈;을 포함하는 MAC생성서버를 포함할 수 있다.

[0016] 특히, 상기 키분배서버로부터 수신한 타임스탬프값과 상기 MAC생성서버로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 큰 경우에, 상기 수신한 타임스탬프값이 유효하지 않다고 판단하고, 상기 기준 메시지인증코드가 조작되었다고 판단하는 MAC검증서버를 포함할 수 있다.

[0017] 특히, 상기 MAC생성서버와 키분배서버 및 상기 MAC검증서버와 키분배서버는 상호 간에 SSL(Secure Sockets Layer) 통신을 수행할 수 있다.

발명의 효과

[0018] 본 발명의 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템은 동일한 대칭키를 다수의 사용자 즉, 다수의 MAC검증서버가 키분배서버를 통해 공유하여, 메시지 인증 코드의 조작여부를 용이하게 검증할 수 있는 효과가 있다.

[0019] 또한, 본 발명의 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템은 메시지인증코드의 데이터 무결성 검증을 통해 전송하고자 하는 데이터가 외부로 노출되는 것을 방지함에 따라, 각종 범죄에 악용되는 것을 미연에 방지할 수 있는 효과가 있다.

[0020] 더불어, 본 발명의 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템은 다수의 MAC검증서버가 동일한 대칭키를 이용하여 데이터와 함께 송수신되는 메시지인증코드를 검증함으로써, 빠른 검증과정을 통해 다량의 데이터를 실시간으로 서명할 수 있는 효과가 있다.

도면의 간단한 설명

- [0021] 도 1은 본 발명의 일 실시 예에 따른 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템의 블록도이다.
- 도 2는 도 1의 MAC생성서버의 블록도이다.
- 도 3은 본 발명의 다른 실시 예에 따른 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법의 순서도이다.
- 도 4는 도 3의 수신한 타임스탬프값에 대한 주기초과여부 확인과정을 나타낸 순서도이다.
- 도 5는 도 3의 수신한 타임스탬프값에 대한 유효성을 판단하는 과정을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0022] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.
- [0023] 이하, 도 1을 참조하여, 먼저 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템에 대하여 살펴보도록 한다.
- [0024] 도 1은 본 발명의 일 실시 예에 따른 다수의 MAC검증서버에 의한 메시지인증코드 검증 시스템의 블록도이다.
- [0025] 도 1에 도시된 바와 같이, 본 발명의 다수의 MAC 검증서버에 의한 메시지인증코드 검증 시스템은 전송하는 데이터의 무결성을 판단하기 위한 메시지인증코드를 생성하는 하나의 MAC생성서버(110)와, 대칭키를 공유하는 하나의 키분배서버(120) 및 생성된 메시지인증코드를 검증하는 적어도 하나의 MAC검증서버(130)를 포함한다.
- [0026] MAC생성서버(110)는 상기 키분배서버(120)로 메시지인증코드 생성 시 필요한 타임스탬프값을 요청하여 수신하고, 이전 생성되거나 신규 생성된 대칭키를 이용하여 기준 메시지인증코드(MAC: Message Authentication Code)를 생성한 후, 자신의 고유한 아이디정보와 이전 수신한 이전 타임스탬프값 및 기준 메시지인증코드를 포함하는 데이터를 적어도 하나의 MAC검증서버(130)로 전송한다. 이때, 요청되는 타임스탬프는 어느 시점에 데이터가 존재했다는 사실을 증명하기 위하여, 특정 위치에 표시하는 시각을 나타내는 것으로서, 공통적으로 참고하는 시각에 대해 시간의 기점을 표시하는 시간 변위 매개변수를 나타낸다.
- [0027] 이하, 도 2를 참조하여, 상기 MAC생성서버에 대하여 자세히 살펴보도록 한다.
- [0028] 도 2는 도 1의 MAC생성서버의 블록도이다.
- [0029] 도 2에 도시된 바와 같이, 본 발명의 MAC생성서버(110)는 주기비교모듈(112), 주기판단모듈(114), 대칭키생성모듈(116) 및 갱신모듈(118)을 포함한다.
- [0030] 주기비교모듈(112)은 상기 키분배서버(120)로 요청하여 수신한 타임스탬프값을 기생성된 대칭키를 생성 시 사용되었던 이전 타임스탬프값 및 기설정된 타임스탬프 주기의 합과 비교한다.
- [0031] 주기판단모듈(114)은 상기 수신한 타임스탬프값이 기생성된 대칭키를 생성할 때 사용되었던 이전 타임스탬프값과 기설정된 타임스탬프 주기의 합보다 큰 경우에는 상기 수신한 타임스탬프값이 주기를 초과하였다고 판단하며, 상기 수신한 타임스탬프값이 상기 이전 타임스탬프값과 타임스탬프 주기의 합보다 같거나 작은 경우에는 상기 키분배서버(120)로부터 수신한 타임스탬프값이 주기를 초과하지 않는다고 판단한다.
- [0032] 대칭키생성모듈(116)은 상기 수신한 타임스탬프값이 주기를 초과하였다고 판단되는 경우에는 이전 생성된 대칭키는 더 이상 유효하지 않는다고 판단하여 신규 대칭키를 생성한다.
- [0033] 갱신모듈(118)은 이전 생성된 대칭키가 상기 대칭키생성모듈(116)을 통해 수신한 타임스탬프값이 주기를 초과하였다고 판단하여 더 이상 유효하지 않다고 판단됨에 따라, 상기 이전 생성된 대칭키를 생성할 때 사용되었던 이전 타임스탬프값을 상기 키분배서버(120)로부터 수신한 타임스탬프값으로 갱신한다.
- [0034] 다시 도 1로 돌아가서, 키분배서버(120)는 상기 MAC생성서버(110)의 요청에 응답하여 저장하고 있는 타임스탬프값을 전송하고, 상기 MAC생성서버(110)로부터 고유한 아이디정보와 이전 타임스탬프값 및 대칭키를 수신하며, 수신한 상기 대칭키를 적어도 하나의 MAC검증서버(130)로 전송한다.
- [0035] MAC검증서버(130)는 상기 키분배서버(120)로부터 타임스탬프값 및 대칭키를 수신하고, 상기 타임스탬프값에 대

한 유효성을 판단한 후, 상기 대칭키를 이용하여 비교 메시지인증코드를 생성한 후, 생성한 비교 메시지인증코드를 상기 MAC생성서버(110)로부터 수신한 데이터 내 기준 메시지인증코드와 비교함으로써, 상기 기준 메시지인증코드에 대한 검증을 수행한다. 이러한 MAC검증서버(130)는 상기 키분배서버(120)로부터 수신한 타임스탬프값과 상기 MAC생성서버(110)로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 같거나 작은 경우에 상기 수신한 타임스탬프값이 유효하다고 판단하며, 이와 달리 상기 키분배서버(120)로부터 수신한 타임스탬프값과 상기 MAC생성서버(110)로부터 수신한 데이터 내 이전 타임스탬프값의 차이가 기설정된 타임스탬프 유효시간보다 큰 경우에, 상기 수신한 타임스탬프값이 유효하지 않다고 판단하며, 이에 따라 상기 기준 메시지인증코드가 조작되었다고 판단한다.

- [0036] 특히, 이러한 상기 MAC생성서버(110)와 키분배서버(120) 및 상기 MAC검증서버(130)와 키분배서버(120)는 상호간에 SSL(Secure Sockets Layer) 통신을 수행한다. 이러한 SSL통신은 보안소켓 계층을 나타내는 것으로서, 인터넷에서 데이터를 안전하게 전송하기 위한 인터넷 통신규약 프로토콜이다. 특히, 상기 SSL통신은 인터넷 상거래시, 요구되는 개인정보와 신용카드정보의 보안유지에 널리 사용되고 있는 프로토콜이다.
- [0037] 이하, 도 3을 참조하여, 다수의 MAC검증서버에 의한 메시지인증코드 검증방법에 대하여 자세히 살펴보도록 한다.
- [0038] 도 3은 본 발명의 다른 실시 예에 따른 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법의 순서도이다.
- [0039] 도 3에 도시된 바와 같이, 본 발명의 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법은 먼저, 메시지인증코드를 생성하고자 하는 MAC생성서버(110)가 전송하는 데이터의 무결성을 판단하기 위한 메시지인증코드 생성시 필요한 타임스탬프값의 전송을 키분배서버(120)로 요청한다(S210). 이때, 요청되는 상기 타임스탬프란, 어느 시점에 데이터가 존재했다는 사실을 증명하기 위하여, 특정 위치에 표시하는 시각을 나타내는 것으로서, 공통적으로 참고하는 시각에 대해 시간의 기점을 표시하는 시간 변위 매개변수를 나타낸다.
- [0040] 이에 따라, 상기 MAC생성서버(110)는 상기 키분배서버(120)로부터 요청한 타임스탬프값을 수신한다(S220).
- [0041] 이후, 상기 MAC생성서버(110)는 상기 키분배서버(120)로부터 수신한 타임스탬프값에 대하여 주기가 초과하였는지 여부를 확인한다(S230).
- [0042] 이하, 도 4를 참조하여 타임스탬프값의 주기 초과여부 확인과정을 자세히 살펴보면 다음과 같다.
- [0043] 도 4는 도 3의 수신한 타임스탬프값에 대한 주기초과여부 확인과정을 나타낸 순서도이다.
- [0044] 도 4에 도시된 바와 같이, 상기 MAC생성서버(110)는 수신한 타임스탬프값이 기생성된 대칭키를 생성할 때 사용되었던 이전 타임스탬프값과 기설정된 타임스탬프 주기를 합한 값보다 큰 지 비교한다(S231).
- [0045] 이때, 상기 MAC생성서버(110)가 수신한 타임스탬프값이 이전 타임스탬프값과 기설정된 타임스탬프 주기를 합한 값보다 큰 경우, 상기 MAC생성서버(110)는 앞서 S220과정에서 수신한 타임스탬프값이 미리 설정된 주기를 초과하였다고 판단한다(S232).
- [0046] 이에 따라, 상기 MAC생성서버(110)는 앞서 S232과정에서 수신한 타임스탬프값이 주기를 초과하였다고 판단함에 따라, 이전 생성된 대칭키는 유효하지 않는다고 판단하고, 기생성된 대칭키를 대신하여 신규 대칭키를 생성한다(S233).
- [0047] 이어서, 상기 MAC생성서버(110)는 기생성된 대칭키를 생성할 때 사용되었던 이전 타임스탬프값을 앞서 S220과정에서 키분배서버(120)로부터 수신한 타임스탬프값으로 갱신한다(S234).
- [0048] 하지만 상기 S231과정에서 상기 MAC생성서버(110)가 수신한 타임스탬프값이 이전 타임스탬프값과 기설정된 타임스탬프 주기를 합한 값보다 같거나 작은 경우, 상기 MAC생성서버(110)는 앞서 S220과정에서 수신한 타임스탬프값이 미리 설정된 주기를 초과하지 않았다고 판단한다(S235).
- [0049] 이에 따라, 상기 MAC생성서버(110)는 별도의 신규 대칭키 생성과정을 수행하지 않고, 이전 생성된 대칭키를 대칭키로서 그대로 사용한다(S236).
- [0050] 다시 도 3으로 돌아와서, 이와 같이, 상기 MAC생성서버(110)가 상기 키분배서버(120)로부터 수신한 타임스탬프값에 대한 주기 초과여부에 대한 확인을 완료함에 따라, 상기 MAC생성서버(110)는 자신의 고유한 아이디정보와, 이전 타임스탬프값 및 이전 생성되었거나 신규 생성된 대칭키를 상기 키분배서버(120)로 전송한다(S240).
- [0051] 이후, 상기 MAC생성서버(110)는 앞서 S240과정을 통해 상기 키분배서버(120)로 전송한 대칭키를 해시하여 메시

지인증코드를 생성한다(S250). 이때, 생성된 상기 메시지인증코드는 추후 MAC검증서버(130)에서 생성되는 메시지인증코드와의 구별을 위해, 기준 메시지인증코드라고 정의한다.

- [0052] 이와 같이, 기준 메시지인증코드를 생성한 상기 MAC생성서버(110)는 자신의 고유한 아이디정보와, 이전 타임스탬프값 및 앞서 S250과정에서 생성한 기준 메시지인증코드를 전송하고자 하는 데이터에 저장한다(S260).
- [0053] 이후, 상기 MAC생성서버(110)는 자신의 고유한 아이디정보와, 이전 타임스탬프값 및 기준 메시지인증코드를 포함하는 데이터를 다수의 MAC검증서버(130)로 전송한다(S270).
- [0054] 상기 MAC생성서버(110)로부터 데이터를 수신한 다수의 MAC검증서버(130) 중 수신한 데이터 내 포함되는 메시지인증코드의 데이터 무결성을 검증하고자 하는 MAC검증서버(130)가 상기 키분배서버(120)로 메시지인증코드 생성 시 필요한 타임스탬프값의 전송을 요청한다(S280).
- [0055] 상기 키분배서버(120)는 상기 MAC검증서버(130)로부터의 타임스탬프값 전송요청에 응답하여 저장하고 있는 타임스탬프값을 상기 MAC검증서버(130)로 전송한다(S290).
- [0056] 이와 같이, 상기 키분배서버(120)로 요청하여 타임스탬프값을 수신한 MAC검증서버(130)는 수신한 타임스탬프값에 대하여 유효성 여부를 확인한다(S300).
- [0057] 이하, 도 5를 참조하여, 타임스탬프값에 대한 유효성 확인과정에 대하여 보다 자세히 살펴보도록 한다.
- [0058] 도 5는 도 3의 수신한 타임스탬프값의 유효성을 판단하는 과정을 나타낸 순서도이다.
- [0059] 도 5에 도시된 바와 같이, 상기 MAC검증서버(130)가 상기 키분배서버(120)로부터 수신한 타임스탬프값에서 상기 MAC생성서버(110)로부터 수신한 데이터에 포함된 이전 타임스탬프값을 차감하고, 그 차이값이 기설정된 타임스탬프 유효시간 보다 큰 지 여부를 비교한다(S301).
- [0060] 이때, 상기 MAC검증서버(130)가 수신한 타임스탬프값에서 상기 MAC생성서버(110)로부터 수신한 데이터에 포함된 이전 타임스탬프값을 차감하고, 그 차이값이 기설정된 타임스탬프 유효시간 보다 큰 경우, 앞서 S220과정을 통해 상기 키분배서버(120)로부터 수신한 타임스탬프값이 유효하지 않다고 판단한다(S302).
- [0061] 이에 따라, 상기 MAC검증서버(130)는 상기 MAC생성서버(110)로부터 수신한 데이터 내 포함된 기준 메시지인증코드가 조작되었다고 판단한다(S303).
- [0062] 하지만 이와 달리, 상기 S301과정에서, 상기 MAC검증서버(130)가 수신한 타임스탬프값에서 상기 MAC생성서버(110)로부터 수신한 데이터에 포함된 이전 타임스탬프값을 차감하고, 그 차이값이 기설정된 타임스탬프 유효시간 보다 같거나 작은 경우에는 상기 MAC검증서버(130)는 상기 키분배서버(120)로부터 수신한 타임스탬프값이 유효하다고 판단한다(S304).
- [0063] 다시 도 3으로 돌아가서, 과정 S300과 같이, 상기 MAC검증서버(130)가 상기 키분배서버(120)로부터 수신한 타임스탬프값에 대한 유효성 여부를 확인한 후, 상기 MAC생성서버(110)로부터 수신한 데이터 내 포함된 고유한 아이디정보와 이전 타임스탬프값을 상기 키분배서버(120)로 전송한다(S310).
- [0064] 이에 따라, 상기 키분배서버(120)는 앞서 S240과정을 통해, 상기 MAC생성서버(110)로부터 수신한 고유한 아이디정보, 이전 타임스탬프값 및 대칭키를 저장함에 따라, 상기 MAC검증서버(130)로부터 고유한 아이디정보와 이전 타임스탬프값을 수신하면, 저장하고 있는 정보 중 수신한 MAC생성서버(110)의 고유한 아이디정보와 이전 타임스탬프값에 대응하는 대칭키를 검색하여, 대응하는 대칭키를 상기 MAC검증서버(130)로 전송한다(S320).
- [0065] 이후, 상기 MAC검증서버(130)는 상기 키분배서버(120)로부터 대칭키를 수신함에 따라, 수신한 대칭키를 해시하여 메시지인증코드를 생성한다(S330). 이때, 상기 MAC검증서버(130)가 생성한 메시지인증코드는 앞서 MAC생성서버(110)가 생성한 기준 메시지인증코드의 검증을 확인하기 위한 비교데이터로서 생성됨에 따라, 이하 비교 메시지인증코드라고 정의된다.
- [0066] 이와 같이, 비교 메시지인증코드를 생성한 상기 MAC검증서버(130)는 자신이 생성한 비교 메시지인증코드와, 상기 MAC생성서버(110)로부터 수신한 데이터 내 포함된 기준 메시지인증코드를 상호 비교한다(S340). 이때, 상기 MAC검증서버(130)는 자신이 생성한 비교 메시지인증코드와, 상기 MAC생성서버(110)로부터 수신한 데이터 내 포함된 기준 메시지인증코드가 상호 동일한 경우, 상기 기준 메시지인증코드는 조작되지 않고, 정상이라고 판단한다. 또는 이와 달리, 상기 MAC검증서버(130)가 자신이 생성한 비교 메시지인증코드와, 상기 MAC생성서버(110)로부터 수신한 데이터 내 포함된 기준 메시지인증코드가 상호 동일하지 않다고 판단한 경우에는 상기 기준 메시지

인증코드가 정상이 아닌 조작되었다고 판단한다.

[0067] 결국, 다수의 사용자가 다수의 MAC검증서버를 통해 키분배서버로부터 동일한 대칭키를 공유함으로써, 메시지인 증코드의 검증을 용이하게 수행할 수 있게 된다.

[0068] 본 발명의 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템은 동일한 대칭키를 다수의 사용자 즉, 다수의 MAC검증서버가 키분배서버를 통해 공유하여, 메시지 인증 코드의 조작여부를 용이하게 검증할 수 있는 효과가 있다.

[0069] 또한, 본 발명의 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템은 메시지인증코드의 데이터 무결성 검증을 통해 전송하고자 하는 데이터가 외부로 노출되는 것을 방지함에 따라, 각종 범죄에 악용되는 것을 미연에 방지할 수 있는 효과가 있다.

[0070] 더불어, 본 발명의 다수의 MAC검증서버에 의한 메시지인증코드 검증 방법 및 시스템은 다수의 MAC검증서버가 동일한 대칭키를 이용하여 데이터와 함께 송수신되는 메시지인증코드를 검증함으로써, 빠른 검증과정을 통해 다량의 데이터를 실시간으로 서명할 수 있는 효과가 있다.

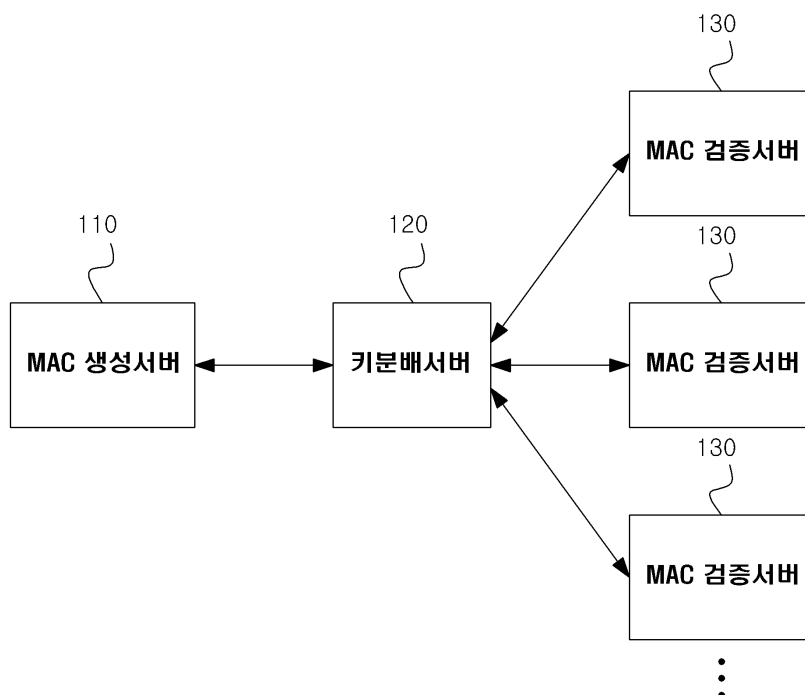
[0071] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

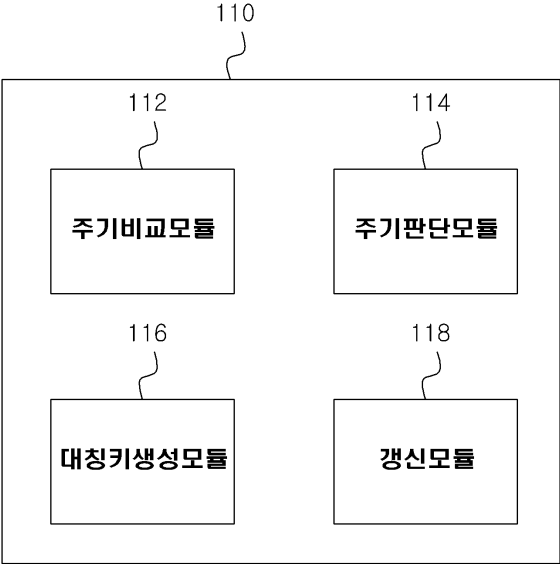
[0072] 110: MAC생성서버 120: 키분배서버
130: MAC검증서버

도면

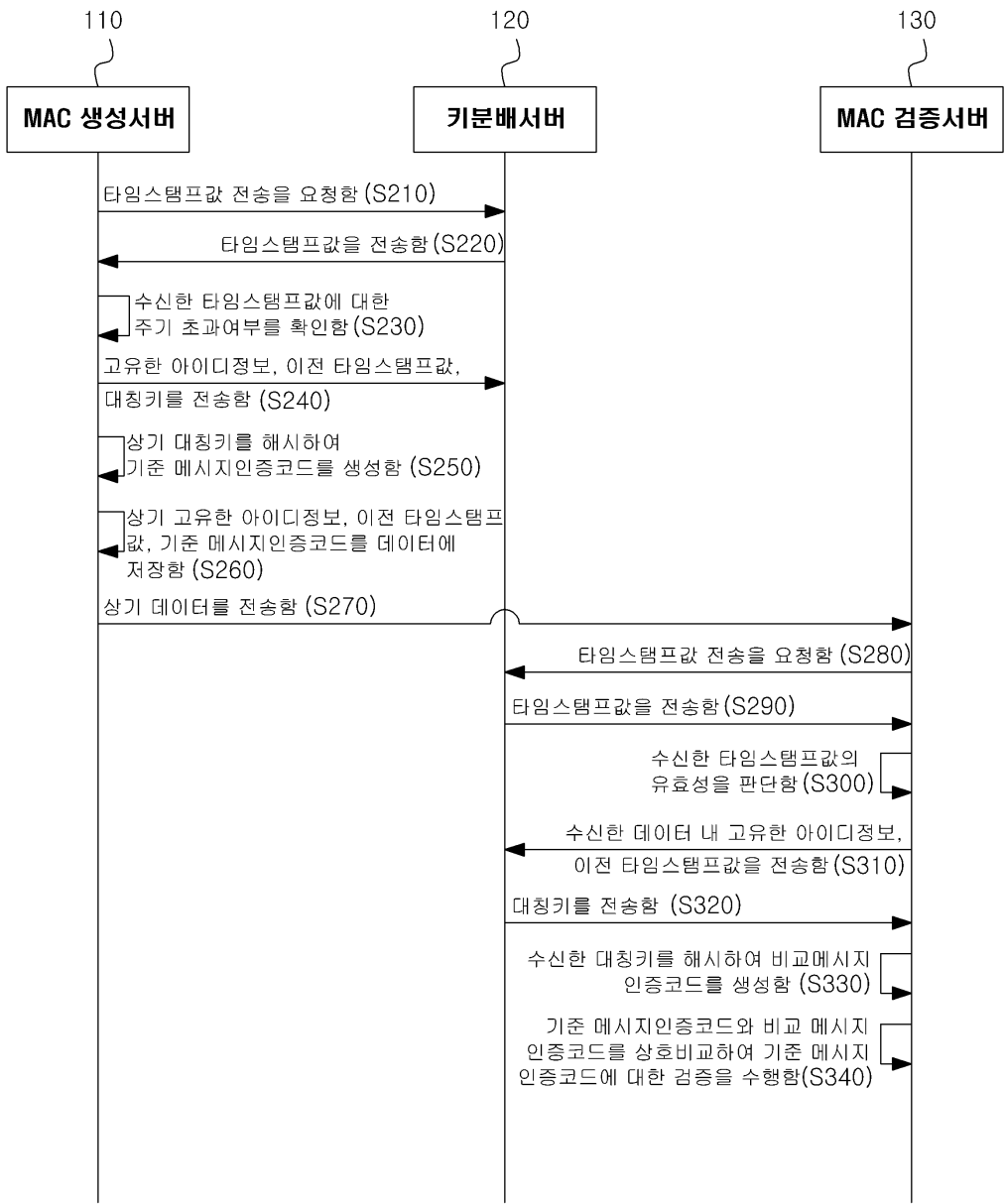
도면1



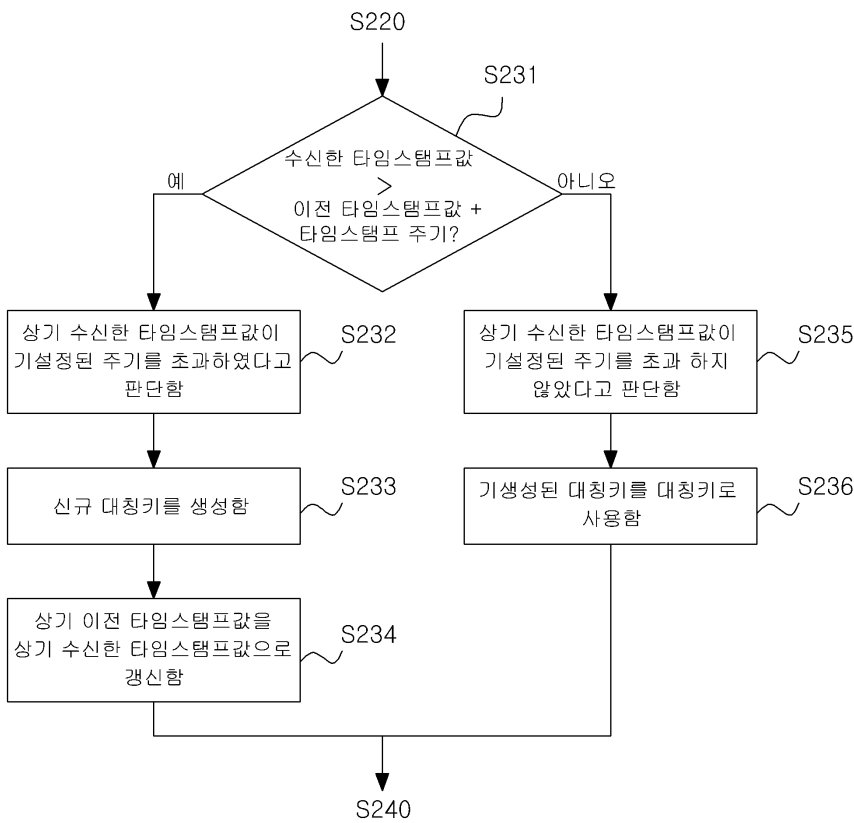
도면2



도면3



도면4



도면5

