(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0116632
(43) 공개일자 2016년10월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 12/24* (2006.01)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 9/3223 (2013.01)
H04L 41/28 (2013.01)
(21) 출원번호 10-2015-0044637
(22) 출원일자 2015년03월30일
심사청구일자 2015년03월30일

(71) 출원인
광운대학교 산학협력단
서울특별시 노원구 광운로 20 (월계동, 광운대학교)
(72) 발명자
박주현
서울특별시 강동구 양재대로91나길 74, 401호
정국현
서울특별시 노원구 월계로 372, 302동 605호(월계3동, 사슴아파트)
(뒷면에 계속)
(74) 대리인
임국일

전체 청구항 수 : 총 6 항

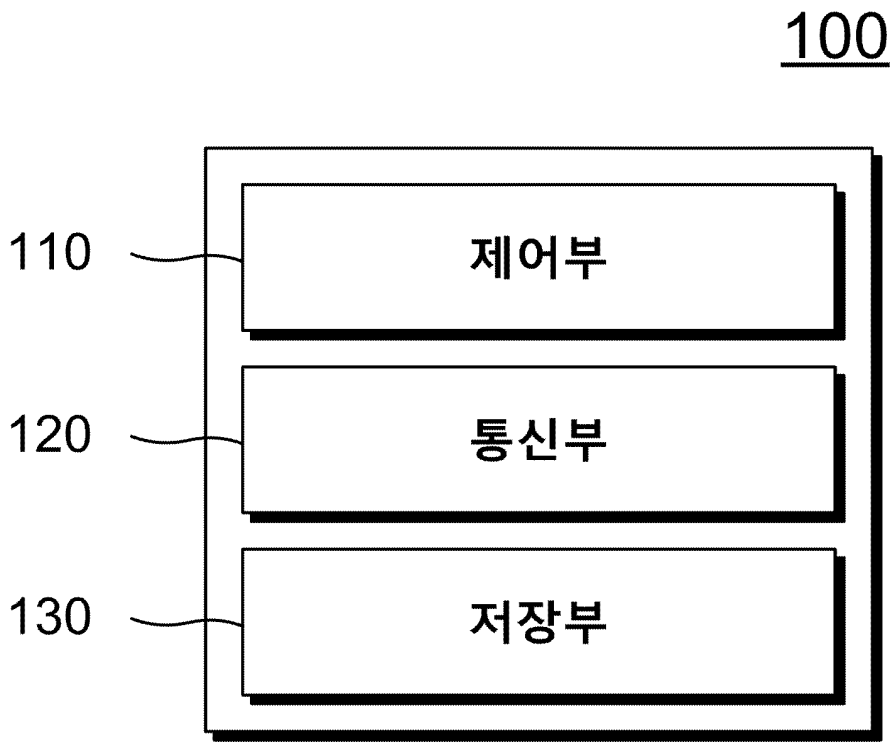
(54) 발명의 명칭 **에너지 관리 시스템을 위한 보안 서버 및 그 제어 방법**

(57) 요 약

본 발명은 에너지 관리 시스템을 위한 보안 서버 및 그 제어 방법 에 관한 것으로, 더욱 상세하게는 에너지 관리 시스템의 단말기로부터 전송된 메시지를 효율적으로 검증할 수 있는 보안 서버에 관한 기술이다. 본 발명의 실시예에 따르면, 보안 서버의 각 부를 제어하는 제어부, 외부 통신 장치와 정보를 송수신하는 통신부 및 각 단말기

(뒷면에 계속)

대 표 도 - 도1



로부터 전송되는 메시지를 검증하기 위한 보안키를 저장하는 저장부를 포함하고, 상기 제어부는 복수의 계층으로 구분되는 해시 트리를 이용하여 상기 메시지에 대한 검증을 수행하되, 상기 해시 트리의 리프 노드의 해시값은 해시값 연결 함수 및 해시 함수를 통해 상기 보안키에 대응되는 뿌리 노드의 해시값으로 변환되며, 상기 제어부는, 상기 통신부를 통해 상기 해시 트리의 리프 노드의 해시값으로 변환된 상기 단말기의 메시지를 수신하되, 상기 메시지를 검증할 때 참조되는 검증 경로 정보를 더 수신하고, 상기 리프 노드의 해시값, 상기 검증 경로 정보, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 획득된 최종 해시값이 상기 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가하되, 상기 검증 경로 정보는, 상기 해시 트리에서 상기 리프 노드와 상기 뿌리 노드를 연결하는 경로를 가정했을 때 상기 경로에 포함되는 노드의 형제 노드의 집합인 것을 특징으로 하는 보안 서버가 제공될 수 있다.

(52) CPC특허분류
H04L 63/123 (2013.01)

(72) 발명자
이선의
서울특별시 노원구 덕릉로 718, 101동902호(중계동,건영아파트)

김진영
서울특별시 강남구 선릉로 221, 410동 304호(도곡동, 도곡렉슬아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호	10041779
부처명	산업통상자원부
연구관리전문기관	한국산업기술평가관리원
연구사업명	산업융합원천기술개발사업
연구과제명	스마트 홈을 위한 에너지 그리드 반응 시스템 기술 개발
기 여 율	1/1
주관기관	한국전기연구원
연구기간	2012.06.01 ~ 2016.05.31

명 세 서

청구범위

청구항 1

에너지 관리 시스템을 위한 보안 서버에 있어서,

상기 보안 서버의 각 부를 제어하는 제어부;

상기 제어부의 제어의 의해 외부 통신 장치와 정보를 송수신하는 통신부; 및

상기 에너지 관리 시스템의 각 단말기로부터 전송되는 메시지를 검증하기 위한 보안키(security key)를 저장하는 저장부; 를 포함하고,

상기 제어부는 복수의 계층으로 구분되는 해시 트리(hash tree)를 이용하여 상기 메시지에 대한 검증을 수행하되, 상기 해시 트리의 리프 노드(leaf node)의 해시값은 해시값 연결 함수 및 해시 함수를 통해 상기 보안키에 대응되는 뿌리 노드(root node)의 해시값으로 변환되며,

상기 제어부는,

상기 통신부를 통해 상기 해시 트리의 리프 노드의 해시값으로 변환된 상기 단말기의 메시지를 수신하되, 상기 메시지를 검증할 때 참조되는 검증 경로 정보(authentication path information, API)를 더 수신하고,

상기 리프 노드의 해시값, 상기 API, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 획득된 최종 해시값이 상기 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가하되,

상기 API는,

상기 해시 트리에서 상기 리프 노드와 상기 뿌리 노드를 연결하는 경로를 가정했을 때 상기 경로에 포함되는 노드의 형제 노드의 집합인 것을 특징으로 하는 보안 서버.

청구항 2

제1항에 있어서,

상기 제어부는 적어도 두 단계 이상으로 구분된 메시지의 중요도 정보에 따른 조합 함수 정보 및 해시 함수 정보를 상기 저장부에 더 저장하고,

검증된 단말기 메시지, 상기 메시지의 중요도 정보에 따른 해시값 연결 함수, 해시 함수 및 상기 해시 트리에 기초하여 상기 각 메시지의 중요도 정보에 따른 보안키를 더 산출하고,

상기 통신부를 통해 상기 단말기로부터 검증 평가의 대상인 메시지를 수신할 때 상기 메시지의 중요도 정보를 더 수신하고,

상기 메시지의 검증을 위한 최종 해시값을 획득할 때 해당 메시지의 중요도 정보에 따른 조합 함수 및 해시 함수를 사용하고,

상기 최종 해시값이 해당 메시지의 중요도 정보에 따른 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가하는 것을 특징으로 하는 보안 서버.

청구항 3

제2항에 있어서,

상기 메시지의 중요도는 해당 메시지에 포함되는 정보의 종류 및 상기 메시지를 전송하는 단말기의 종류에 기초하여 결정되며,

상기 제어부는,

n이 2 이상의 자연수, i가 n-1 이하의 자연수이고, h_i가 n개의 계층으로 구성된 해시 트리의 제i계층의 해시값,

B_i가 hi의 형제 노드의 해시값, H_i()가 해시 함수, C_i()가 해시값 연결 함수일 때,

수식 $h_{i+1} = H_i(C_i(h_i, B_i))$을 통해 제i+1계층의 해시값 h_{i+1}를 구하되,

상기 메시지의 중요도가 높은 경우,

상기 해시 함수 H1() 내지 H_{n-1}() 중 적어도 둘 이상이 서로 상이한 것으로 선택하고,

상기 메시지의 중요도가 낮은 경우,

상기 해시 함수 H1() 내지 H_{n-1}()가 동일한 것으로 선택하는 것을 특징으로 하는 보안 서버.

청구항 4

제2항에 있어서,

상기 제어부는,

n이 2 이상의 자연수, i가 n-1 이하의 자연수이고, h_i가 n개의 계층으로 구성된 해시 트리의 제i계층의 해시값, B_i가 h_i의 형제 노드의 해시값, H_i()가 해시 함수, C_i()가 해시값 연결 함수일 때,

수식 $h_{i+1} = H_i(C_i(h_i, B_i))$을 통해 제i+1계층의 해시값 h_{i+1}를 구하되,

상기 메시지의 중요도가 높은 경우,

상기 해시값 연결 함수 C1() 내지 C_{n-1}() 중 적어도 둘 이상이 서로 상이한 것으로 선택하고,

상기 메시지의 중요도가 낮은 경우,

상기 해시값 연결 함수 C1() 내지 C_{n-1}()가 동일한 것으로 선택하는 것을 특징으로 하는 보안 서버.

청구항 5

제1항에 있어서,

n이 2 이상의 자연수이고, j가 2 이상 n 이하의 자연수이며, n 개의 계층으로 구분되되, 제1계층이 최하위 계층이고 제n계층이 최상이 계층인 해시 트리에 대하여,

상기 제어부는 검증된 리프 노드에 기초하여 상기 해시 트리의 중간 노드의 해시값을 산출하고,

상기 저장부는 상기 중간 노드의 해시값을 더 저장하고,

상기 제어부는,

상기 통신부를 통해 상기 단말기로부터 리프 노드로 변환된 메시지 및 API를 수신하고,

상기 수신된 메시지의 중요도에 기초하여 2 이상 n 이하의 자연수 j를 선택하고,

제j계층의 노드를 새로운 뿌리 노드로 하는 부분 해시 트리를 선별하되, 상기 부분 해시 트리는 상기 수신된 리프 노드를 하위 계층 노드로 포함하고,

상기 리프 노드, j-1 개의 형제 노드로 구성된 API, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 획득된 최종 해시값이 상기 새로운 뿌리 노드의 해시값과 동일하면 상기 단말기의 메시지가 유효한 것으로 평가하는 것을 특징으로 하는 보안 서버.

청구항 6

에너지 관리 시스템을 위한 보안 서버의 제어 방법에 있어서,

상기 에너지 관리 시스템의 각 단말기로부터 전송되는 메시지를 검증하기 위한 해시 트리 및 보안키를 저장하는 단계; 상기 해시 트리의 리프 노드 해시값은 기 설정된 해시값 연결 함수 및 해시 함수를 통해 상기 보안키에 대응되는 뿌리 노드의 해시값으로 변환됨,

상기 해시 트리의 리프 노드의 해시값으로 변환된 상기 단말기의 메시지를 수신하되, 상기 메시지를 검증할 때

참조되는 API를 더 수신하는 단계;

상기 리프 노드의 해시값, 상기 API, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 최종 해시값을 획득하는 단계; 및

상기 최종 해시값이 상기 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가하는 단계; 를 포함하되,

상기 API는,

상기 해시 트리에서 상기 리프 노드와 상기 뿌리 노드를 연결하는 경로를 가정했을 때 상기 경로에 포함되는 노드의 형제 노드의 집합인 것을 특징으로 하는 보안 서버의 제어 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 에너지 관리 시스템을 위한 보안 서버 및 그 제어 방법에 관한 것으로, 더욱 상세하게는 에너지 관리 시스템의 단말기로부터 전송된 메시지를 효율적으로 검증할 수 있는 보안 서버에 관한 기술이다.

배 경 기 술

[0002] 전력수요관리(Demand Side Management)란 전기소비자의 전력사용 패턴 변화를 통해 최소 비용으로 안정적인 전력수요를 충족시키기 위한 일련의 계획 및 수단을 의미한다. 전력수요관리는 일반적으로 수요반응(Demand Response)과 에너지효율향상(Energy Efficiency)으로 구분된다. 수요반응은 수요관리용 요금제 및 인센티브제도 등을 통해 피크기간 등 전력수급 상황에 따라 전기소비자의 평소 전력사용패턴 변화를 유도하는 것을 말하고, 에너지효율향상은 기존의 저효율 설비를 LED 등 고효율 설비로 교체해 전기소비 효율을 지속적으로 향상시키는 것을 의미한다. 또한 수요자원은 일련의 제도 안에서 다양한 수요반응의 모집 및 관리를 통해 에너지공급자가 운영(Control) 가능한 자원(Resource)으로 전환하는 것을 말한다.

[0003] 전술한 전력수요관리 관련 이슈들 중에서도, 최근 수요반응에 대한 연구가 다양한 방식으로 진행되고 있다. 수요반응은 전력 소비자 측에서 전기 요금이나 공급자의 요청에 따라 전력 소비를 조절하는 방식으로 작동되는데, 이 때, 전력 소비자와 전력 공급자 사이에 다양한 정보들이 송수신될 수 있다. 예를 들어, 전력 소비자 식별 정보, 사용한 전력량 정보, 사용한 전력에 대한 요금 정보, 전력 요청 정보 및 시간에 따른 전력 요금 변화 정보 등이 전력 소비자와 전력 공급자 사이에서 송수신될 수 있다. 상기 정보들은 종류에 따라서 개인 정보 등의 민감한 사항들을 포함할 수 있기 때문에 상기 정보들에 대한 보안이 중요하다. 특히, 최근 통신 네트워크를 통한 범죄가 빈번하게 발생되고 있는데, 상기 정보들을 불법으로 수집하여 악용하거나, 해킹 등을 통해 사회 기반 시설에 해당하는 전력 공급자 및 중요 전력 소비자에 대한 다양한 공격이 진행될 수도 있다.

[0004] 한편, 종래의 에너지 관리 시스템은 RSA(Rivest-Shamir-Adleman) 방식의 보안 알고리즘을 통해 암호화 및 복호화를 수행하는 경우가 있다. RSA는 큰 숫자의 소인수분해의 어려움을 이용하여 안전성을 높이는 방식으로 구성되어있으며, 별도로 구성된 공개키와 개인키를 이용하여 암호화 및 복호화를 수행한다. 하지만, 양자 컴퓨터 등 전자적 계산 장치의 성능이 높아짐에 따라 RSA 방식의 안정성이 급격하게 낮아질 수 있으며, 복잡한 암호화 및 복호화 작업으로 인한 연산 부하가 문제시 되고 있어 이를 대체할만한 보안 수단에 대한 연구가 필요한 실정이다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 상기와 같은 문제점을 해결하기 위해 안출된 것으로서, 에너지 관리 시스템의 각 구성요소 사이에 송수신되는 메시지를 효율적으로 검증할 수 있는 수단을 제공하는데 있다.

과제의 해결 수단

[0006] 상기와 같은 과제를 해결하기 위한 본 발명의 실시예에 따르면, 에너지 관리 시스템을 위한 보안 서버에 있어서, 상기 보안 서버의 각 부를 제어하는 제어부; 상기 제어부의 제어의 의해 외부 통신 장치와 정보를 송수신하는 통신부; 및 상기 에너지 관리 시스템의 각 단말기로부터 전송되는 메시지를 검증하기 위한 보안키

(security key)를 저장하는 저장부; 를 포함하고, 상기 제어부는 복수의 계층으로 구분되는 해시 트리(hash tree)를 이용하여 상기 메시지에 대한 검증을 수행하되, 상기 해시 트리의 리프 노드(leaf node)의 해시값은 해시값 연결 함수 및 해시 함수를 통해 상기 보안키에 대응되는 뿌리 노드(root node)의 해시값으로 변환되며, 상기 제어부는, 상기 통신부를 통해 상기 해시 트리의 리프 노드(leaf node)의 해시값으로 변환된 상기 단말기의 메시지를 수신하되, 상기 메시지를 검증할 때 참조되는 검증 경로 정보(authentication path information, API)를 더 수신하고, 상기 리프 노드의 해시값, 상기 API, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 획득된 최종 해시값이 상기 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가하되, 상기 API는, 상기 해시 트리에서 상기 리프 노드와 상기 뿌리 노드를 연결하는 경로를 가정했을 때 상기 경로에 포함되는 노드의 형제 노드의 집합인 것을 특징으로 하는 보안 서버가 제공될 수 있다.

[0007] 여기서, 상기 제어부는 적어도 두 단계 이상으로 구분된 메시지의 중요도 정보에 따른 조합 함수 정보 및 해시 함수 정보를 상기 저장부에 더 저장하고, 검증된 단말기 메시지, 상기 메시지의 중요도 정보에 따른 해시값 연결 함수, 해시 함수 및 상기 해시 트리에 기초하여 상기 각 메시지의 중요도 정보에 따른 보안키를 더 산출하고, 상기 통신부를 통해 상기 단말기로부터 검증 평가의 대상인 메시지를 수신할 때 상기 메시지의 중요도 정보를 더 수신하고, 상기 메시지의 검증을 위한 최종 해시값을 획득할 때 해당 메시지의 중요도 정보에 따른 조합 함수 및 해시 함수를 사용하고, 상기 최종 해시값이 해당 메시지의 중요도 정보에 따른 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가한다.

[0008] 여기서, 상기 메시지의 중요도는 해당 메시지에 포함되는 정보의 종류 및 상기 메시지를 전송하는 단말기의 종류에 기초하여 결정되며, 상기 제어부는, n이 2 이상의 자연수, i가 n-1 이하의 자연수이고, hi가 n개의 계층으로 구성된 해시 트리의 제i계층의 해시값, Bi가 hi의 형제 노드의 해시값, Hi()가 해시 함수, Ci()가 해시값 연결 함수일 때, 수식 hi+1 = Hi(Ci(hi, Bi))을 통해 제i+1계층의 해시값 hi+1를 구하되, 상기 메시지의 중요도가 높은 경우, 상기 해시 함수 H1() 내지 Hn-1() 중 적어도 둘 이상이 서로 상이한 것으로 선택하고, 상기 메시지의 중요도가 낮은 경우, 상기 해시 함수 H1() 내지 Hn-1()가 동일한 것으로 선택한다.

[0009] 여기서, n이 2 이상의 자연수, i가 n-1 이하의 자연수이고, hi가 n개의 계층으로 구성된 해시 트리의 제i계층의 해시값, Bi가 hi의 형제 노드의 해시값, Hi()가 해시 함수, Ci()가 해시값 연결 함수일 때, 수식 hi+1 = Hi(Ci(hi, Bi))을 통해 제i+1계층의 해시값 hi+1를 구하되, 상기 메시지의 중요도가 높은 경우, 상기 해시값 연결 함수 C1() 내지 Cn-1() 중 적어도 둘 이상이 서로 상이한 것으로 선택하고, 상기 메시지의 중요도가 낮은 경우, 상기 해시값 연결 함수 C1() 내지 Cn-1()가 동일한 것으로 선택한다.

[0010] 여기서, n이 2 이상의 자연수이고, j가 2 이상 n 이하의 자연수이며, n 개의 계층으로 구분되되, 제1계층이 최하위 계층이고 제n계층이 최상이 계층인 해시 트리에 대하여, 상기 제어부는 검증된 리프 노드에 기초하여 상기 해시 트리의 중간 노드의 해시값을 산출하고, 상기 저장부는 상기 중간 노드의 해시값을 더 저장하고, 상기 제어부는, 상기 통신부를 통해 상기 단말기로부터 리프 노드로 변환된 메시지 및 API를 수신하고, 상기 수신된 메시지의 중요도에 기초하여 2 이상 n 이하의 자연수 j를 선택하고, 제j계층의 노드를 새로운 뿌리 노드로 하는 부분 해시 트리를 선별하되, 상기 부분 해시 트리는 상기 수신된 리프 노드를 하위 계층 노드로 포함하고, 상기 리프 노드, j-1 개의 형제 노드로 구성된 API, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 획득된 최종 해시값이 상기 새로운 뿌리 노드의 해시값과 동일하면 상기 단말기의 메시지가 유효한 것으로 평가한다.

[0011] 본 발명의 다른 실시예에 따르면, 에너지 관리 시스템을 위한 보안 서버의 제어 방법에 있어서, 상기 에너지 관리 시스템의 각 단말기로부터 전송되는 메시지를 검증하기 위한 해시 트리 및 보안키를 저장하는 단계; 상기 해시 트리의 리프 노드 해시값은 기 설정된 해시값 연결 함수 및 해시 함수를 통해 상기 보안키에 대응되는 뿌리 노드의 해시값으로 변환됨, 상기 해시 트리의 리프 노드의 해시값으로 변환된 상기 단말기의 메시지를 수신하되, 상기 메시지를 검증할 때 참조되는 API를 더 수신하는 단계; 상기 리프 노드의 해시값, 상기 API, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 최종 해시값을 획득하는 단계; 및 상기 최종 해시값이 상기 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가하는 단계; 를 포함하되, 상기 API는, 상기 해시 트리에서 상기 리프 노드와 상기 뿌리 노드를 연결하는 경로를 가정했을 때 상기 경로에 포함되는 노드의 형제 노드의 집합인 것을 특징으로 하는 보안 서버의 제어 방법이 제공될 수 있다.

발명의 효과

[0012] 본 발명에 따르면, 단말기가 전송한 메시지의 유효성을 용이하게 검증할 수 있으며, 메시지 검증시 필요한 정보량 및 정보 전송량을 감소시킬 수 있다.

[0013] 또한, 본 발명의 실시예에 따르면, 메시지의 중요도에 기초하여 변환 과정에서 사용되는 해시 함수의 종류를 결정할 수 있다. 이에 따라 메시지의 중요도에 적합한 수준의 보안이 제공될 수 있다.

[0014] 또한, 본 발명의 실시예에 따르면, 메시지의 중요도에 기초하여 변환 과정에서 사용되는 해시값의 해시값 연결 함수를 결정할 수 있으며, 이에 따라 암호화의 복잡도를 용이하게 조정할 수 있다.

[0015] 또한, 본 발명의 실시예에 따르면, 메시지의 중요도에 기초하여 부분 해시 트리를 선별할 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 실시예에 따른 보안 서버를 나타낸 도면이다.

도 2는 본 발명의 실시예에 따른 해시 트리를 나타낸 도면이다.

도 3은 본 발명의 실시예에 따른 검증 경로 정보를 나타낸 도면이다.

도 4는 본 발명의 실시예에 따른 해시값 연결 함수를 나타낸 도면이다.

도 5는 본 발명의 실시예에 따른 부분 해시 트리를 나타낸 도면이다.

도 6은 본 발명의 실시예에 따른 보안 서버의 제어 방법을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 발명은 에너지 관리 시스템을 위한 보안 서버 및 그 제어 방법 에 관한 것으로, 더욱 상세하게는 에너지 관리 시스템의 단말기로부터 전송된 메시지를 효율적으로 검증할 수 있는 보안 서버에 관한 기술이다. 이하, 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다.

[0019] 도 1은 본 발명의 실시예에 따른 보안 서버(100)를 나타낸 도면이다. 도 1에 따르면, 본 발명의 실시예에 따른 보안 서버(100)는 제어부(110), 통신부(120) 및 저장부(130)를 포함할 수 있다. 본 발명을 실시하는 방식에 따라서, 보안 서버(100)에 포함되는 일부 구성 요소가 생략되거나 복수의 구성 요소가 하나로 구비될 수도 있다.

[0020] 본 발명에 따른 보안 서버(100)는 에너지 관리 시스템의 보안을 위한 것으로, 에너지 관리 시스템의 각 단말기로부터 전송되는 메시지를 검증할 수 있다. 이에 따라, 본 발명에 따른 보안 서버(100)는 외부의 비인증 단말기로부터 전송된 메시지 또는 비정상적인 과정을 통해 변조된 메시지가 에너지 관리 시스템의 다른 구성 요소로 전송되는 것을 차단할 수 있으며, 이를 통해 에너지 관리 시스템에서 발생될 수 있는 각종 보안 관련 문제를 사전에 방지할 수 있다.

[0021] 제어부(110)는 보안 서버(100)의 각 부를 제어할 수 있다. 제어부(110)는 하드웨어 또는 소프트웨어의 형태로 구현될 수 있으며, 하드웨어 및 소프트웨어가 결합된 형태로도 존재할 수 있다. 바람직하게는, 제어부(110)는 마이크로프로세서로 구비될 수 있으나 이에 한정되지 않는다.

[0022] 통신부(120)는 상기 제어부(110)의 제어에 의해 외부 통신장치와 무선 통신을 수행할 수 있다. 상기 외부 통신장치는 상기 에너지 관리 시스템 내의 다른 단말기뿐만 아니라 외부의 무선 단말기 및 서버도 포함할 수 있다. 또한, 외부 통신 장치는 HAN(Home Area Network) 및 HAN에 포함되는 각 가정의 단말기들을 포함할 수 있으며, 상기 제어부(110)는 상기 통신부(120)를 통해 HAN의 각 단말기의 수요전력 관련 메시지를 수신할 수 있다. 에너지 관리 시스템 내의 단말기에서 생성된 메시지는 상기 통신부(120)를 통해 상기 제어부(110)로 전송될 수 있고, 상기 제어부(110)는 전송된 메시지에 기초하여 상기 메시지의 유효성을 검증할 수 있으며, 상기 메시지의 유효성 판단 결과가 상기 통신부(120)를 통해 해당 단말기로 재전송될 수도 있다. 또한, 본 발명을 실시하는 방식에 따라서, 상기 통신부(120)는 무선 또는 유선 네트워크를 통해 정보를 송수신할 수 있다.

[0023] 저장부(130)는 상기 에너지 관리 시스템의 각 단말기로부터 전송되는 메시지를 검증하기 위한 보안키(security key)를 저장할 수 있다. 본 발명의 바람직한 실시예에 따르면, 상기 보안키는 해시 코드 또는 해시값의 형태로 구비될 수 있다. 또한, 저장부(130)가 저장할 수 있는 정보는 이에 한정되지 않으며, 후술하는 해시 트리(hash tree)의 구조 및 해시 트리를 구성하는 각 노드의 해시값도 저장할 수 있다.

[0024] 본 발명에 따른 제어부(120)는 해시 트리를 이용하여 에너지 관리 시스템의 각 단말기 또는 기타 외부 통신 장치로부터 전송되는 메시지를 검증할 수 있다. 해시 트리의 구조 및 해시 트리를 이용하여 메시지를 검증하는 방

법은 도 2 내지 도 5를 통해 보다 상세하게 설명하도록 한다.

[0025] 이 때, 제어부(110)는 메시지의 중요도에 기초하여 메시지의 유효성을 검증하는 방식을 결정할 수 있다. 여기서, 상기 메시지의 중요도는 해당 메시지에 포함되는 정보의 종류 및 상기 메시지를 전송하는 단말기의 종류에 기초하여 결정될 수 있다. 예를 들어, 단말기 사용자의 개인 정보와 관련된 정보가 상기 메시지에 포함된 경우, 해당 메시지는 중요한 것으로 판별할 수 있다. 다른 예로써, 단순한 전력 사용을 요청하는 정보가 포함된 메시지는 상대적으로 덜 중요한 정보로 판단될 수 있다. 또 다른 예로써, 병원, 교통 관제 센터, 군 시설 등 사회 기반 시설의 단말기에서 생성된 전력 관련 메시지는 안전 및 안보의 관점에서 핵심적인 정보에 해당될 수 있으므로 중요한 정보로 판별될 수 있다. 상기 메시지의 중요도는 복수의 단계로 구분될 수 있으며, 시간대 및 장소에 따라서 동일한 단말기의 동일한 메시지라도 다른 중요도로 판별될 수도 있다.

[0027] 도 2는 본 발명의 실시예에 따른 해시 트리를 나타낸 도면이다. 도 2에서 M_1 내지 M_8은 에너지 관리 시스템의 각 단말기에서 생성된 메시지를 나타내며, 특정 해시 함수(hash function)을 통해 해시값 N_1 내지 N_8로 변환될 수 있다. 이 때, 상기 해시 함수는 단방향 암호화 기법을 통해 각 단말기의 메시지를 해시값으로 변환하는 방식으로 작동할 수 있다. 도 2에서 M_1 내지 M_8에서 N_1 내지 N_8의 방향으로 도시된 파선은 상기 해시 함수에 의한 정보의 변환을 의미한다. 또한, 도 2에서 각 계층 사이의 사각형은 하위 계층의 노드의 해시값에서 상위 계층의 노드의 해시값으로 변환될 때 사용되는 해시값 연결 함수 및 해시 함수를 의미한다.

[0028] 본 발명을 실시하는 방식에 따라서, 상기 제어부는 복수의 계층으로 구분되는 해시 트리(hash tree)를 이용하여 상기 메시지에 대한 검증을 수행하되, 상기 해시 트리의 리프 노드(leaf node)의 해시값은 해시값 연결 함수 및 해시 함수를 통해 상기 보안키에 대응되는 뿌리 노드(root node)의 해시값으로 변환될 수 있다. 보다 자세히 서술하면 아래와 같다. 제어부는 2 이상의 자연수 n에 대하여 n개의 계층으로 구분되는 해시 트리를 이용하여 상기 메시지에 대한 검증을 수행할 수 있다. 도 2의 해시 트리는 n이 4일 때의 경우를 나타낸 것이다. 상기 해시 트리의 최하위 제1계층은 복수의 리프 노드로 구성되고, 상기 해시 트리의 최상위 제n계층은 하나의 뿌리 노드로 구성되며, 상기 n이 3보다 큰 경우 상기 제1계층 및 상기 제n계층을 연결하는 n - 2 개의 중간 노드 계층이 존재할 수 있다. 도 2에 따르면, 제1계층은 전술한 N_1 내지 N_8의 해시값에 해당하며, 해시 트리의 리프 노드로써 활용될 수 있다. 도 2에 따르면, 제2계층은 N_{12}, N_{34}, N_{56}, N_{78}의 중간 노드로 구비되고, 제3계층은 N_{14}, N_{58}의 중간 노드로 구비될 수 있다. 최상위 제4계층은 N_{18}의 뿌리 노드로 구비될 수 있다. 이 때, 전술한 중간 노드 및 뿌리 노드는 N_{ab}의 표기법을 통해 구분되었는데, 이것은 리프 노드 개수 미만의 자연수 a 및 a보다 크고 리프 노드 개수 이하의 자연수 b에 대하여, 해당 노드가 하위의 노드 N_a 내지 N_b로부터 생성된 것임을 나타낸다. 전술한 바와 같이, 상기 리프 노드는 N_1 내지 N_8 은 상기 단말기의 메시지로부터 변환된 해시값에 대응하고, 상기 중간 노드는 하위 계층의 리프 노드의 조합 또는 하위 계층의 중간 노드의 조합으로부터 변환된 해시값이다. 도 2에 따르면, 제2계층의 중간 노드 N_{12}는 하위의 리프 노드 N_1 및 N_2의 조합으로부터 변환된 해시값이며, 제3계층의 중간 노드 N_{14}는 하위의 중간 노드 N_{12} 및 N_{34}의 조합으로부터 변환된 해시값이다. 상기 뿌리 노드는 하위 계층의 중간 노드 조합으로부터 변환된 해시값으로 상기 저장부에 저장된 보안키에 대응될 수 있다. 도 2에 따르면, 뿌리 노드 N_{18}은 하위의 중간 노드 N_{14} 및 N_{58}의 조합으로부터 변환된 해시값일 수 있다. 이 때, 상기 중간 노드 및 뿌리 노드는 적어도 둘 이상의 하위 노드로부터 생성될 수 있으며, 본 발명을 실시하는 방식에 따라서, 오직 두 개의 하위 노드로부터 생성될 수도 있다. 각 메시지 M_1 내지 M_8이 검증을 통과한 유효한 메시지 인 경우, 상기 유효한 메시지에 기초하여 생성된 뿌리 노드 N_{18}은 전술한 보안키로써 활용될 수 있으며 저장부에 저장될 수 있다. 한편, 상기 해시 트리에서 뿌리 노드를 제외한 나머지 노드에 동일한 상위 계층의 노드와 연결된 적어도 하나의 형제 노드(brother node)가 존재할 수 있다. 예를 들어, 도 2의 리프 노드 N_3의 상위 노드는 N_{34}인데, 이 경우 N_4가 N_3의 형제 노드가 된다. 마찬가지로, N_4의 형제 노드는 N_3이며, 제3계층에서 N_{14}의 형제 노드는 N_{58}이다.

[0029] 전술한 바에 따르면, 상위 노드는 하위 노드의 해시값의 조합으로부터 변환된 해시값에 해당한다. 이를 일반화하여 서술하면, n-1 이하의 자연수 i에 대하여 제i계층의 하위 노드의 해시값은 해시값 연결 함수 $C_i()$ 및 상기 해시값 연결 함수에 의해 생성된 해시값 조합을 다른 해시값으로 변환하는 해시 함수 $H_i()$을 통해 제 i+1계층의

상위 노드의 해시값으로 변환될 수 있다.

[0030] 또한, 전술한 바에 따르면, 메시지의 중요도에 기초하여 메시지의 유효성을 검증하는 방식을 결정할 수 있는데, 본 발명을 실시하는 방식에 따라서, 상기 단말기로부터 전송된 메시지의 중요도에 기초하여 상기 i의 변화에 따른 상기 해시 함수 $H_i()$의 종류를 선택하고, 상기 선택된 해시 함수의 종류에 기초한 보안키를 개별적으로 산출할 수 있다. 상기 제어부는, 상기 메시지의 중요도가 높은 경우, 상기 해시 함수 $H_1()$ 내지 $H_{n-1}()$ 중 적어도 둘 이상이 서로 상이한 것으로 선택하고, 상기 메시지의 중요도가 낮은 경우, 상기 해시 함수 $H_1()$ 내지 $H_{n-1}()$가 동일한 것으로 선택할 수 있다.

[0031] 또한, 상기 제어부는, 상기 단말기로부터 전송된 메시지의 중요도에 기초하여 상기 i의 변화에 따른 상기 해시값 연결 함수 $C_i()$의 종류를 선택하고, 상기 선택된 해시값 연결 함수의 종류에 기초한 보안키를 개별적으로 산출할 수 있으며, 상기 메시지의 중요도가 높은 경우, 상기 해시값 연결 함수 $C_1()$ 내지 $C_{n-1}()$ 중 적어도 둘 이상이 서로 상이한 것으로 선택하고, 상기 메시지의 중요도가 낮은 경우, 상기 해시 함수 $C_1()$ 내지 $C_{n-1}()$가 동일한 것으로 선택할 수 있다. 다양한 해시값 연결 함수에 설명은 도 4를 설명할 때 상세하게 다루도록 한다.

[0032] 한편, 도 2에서는 n이 4이고 리프 노드의 수가 8인 것으로 도시되어있으나 본 발명은 이에 한정되지 않는다.

[0034] 도 3은 본 발명의 실시예에 따른 검증 경로 정보(authentication path information, API)를 나타낸 도면이다. 도 3에서 흑색 사각형은 해시 트리에서 API에 포함되는 형제 노드를 나타내며, 굵은 선으로 표시된 사각형은 리프 노드 A1(해시값 h_1)를 기초로 하여 해시값 연결 함수 및 해시 함수를 통해 최종 해시값 h_4를 산출하는 과정을 나타내고 있다. 도 2와는 달리, 각 단계 사이에 존재하는 해시값 연결 함수 및 해시 함수에 대한 표시는 생략되었다.

[0035] 도 3에서 검증의 대상이 되는 메시지는 M_5인 상황을 가정하고 있다. M_5는 특정 해시 함수를 통해 리프 노드 A1으로 변환될 수 있다. 리프 노드 A1의 유효성은 API를 통해서 검증될 수 있다. n 개의 계층으로 구분되는 해시 트리에서, API는 상기 리프 노드의 형제 노드 B_1 및 상기 리프 노드 h_1와 상기 뿌리 노드를 연결하는 n - 2 개의 중간 노드의 형제 노드 $\{B_2, \cdots B_{n-1}\}$를 하위 계층에서 상위 계층의 순서로 순차적으로 나열한 정보 $\{B_1, \cdots B_{n-1}\}$일 수 있다. 도 3에 따르면, n이 4이기 때문에 리프 노드 A1의 API는 3개의 형제 노드 정보를 포함할 수 있다. 우선, 리프 노드 A1의 형제 노드는 B_1이다. 리프 노드 A1과 뿌리 노드 A4를 연결하는 중간 노드가 각각 A2 및 A3인데, A2의 형제 노드는 B_2이며 A3의 형제 노드는 B_3이다. 즉, 리프 노드 A1의 API는 $\{B_1, B_2, B_3\}$로 구비될 수 있다. 즉, 상기 API는, 상기 해시 트리에서 상기 리프 노드 A1과 상기 뿌리 노드 A4 연결하는 경로(A1, A2, A3, A4)를 가정했을 때 상기 경로에 포함되는 노드의 형제 노드의 집합으로 구비될 수도 있다. 이 때, 뿌리 노드인 A4의 형제 노드는 존재하지 않으므로 최종적으로 3개의 형제 노드가 API에 포함될 수 있다.

[0036] 한편, 본 발명의 실시예에 따르면, 보안 서버의 제어부는 상기 API에 기초한 적어도 하나의 변환 과정을 통해 리프 노드의 해시값의 유효성을 검증할 수 있다. 이를 일반화하면, 제i변환 과정은 해시값 연결 함수 $C_i()$, 해시 함수 $H_i()$ 및 공식 $H_i(C_i(h_i,B_i))$을 통해 해시값 h_{i+1}을 산출하는 과정이다. 도 3에 따르면, 제어부는, 리프 노드 A1의 해시값 h_1으로 변환된 단말기의 메시지가 수신되면, 이를 이용하여 API의 첫 번째 형제 노드인 B_1의 해시값과 해시값 연결 함수 $C_1()$을 통해 조합하고, 해시 함수 $H_1()$을 통해 해시값 h_2를 산출하는 제1변환 과정을 수행한다. 이후, 제어부는 상기 해시값 h_2를 API의 두 번째 형제 노드인 B_2의 해시값와 해시값 연결 함수 $C_2()$을 통해 조합하고, 해시 함수 $H_2()$을 통해 해시값 h_3을 산출하는 제2변환 과정을 수행한다. 마지막으로, 제어부는 상기 해시값 h_3을 API의 세 번째 형제 노드인 B_3의 해시값과 해시값 연결 함수 $C_3()$을 통해 조합하고, 해시 함수 $H_3()$을 통해 최종 해시값 h_4을 산출하는 제3변환 과정을 수행한다. 제어부는 상기 최종 해시값 h_4가 저장부에 저장된 보안키와 동일하면 상기 단말기의 메시지 M_5가 유효한 것으로 평가하고, 상기 단말기에 포함된 정보에 기초하여 후속 처리를 수행한다. 만약 상기 최종 해시값 h_4가 상기 보안키와 상이하면, 제어부는 해당 메시지가 불법으로 생성되었거나 인증된 단말기의 메시지가 아닌 것으로 판단하고 해당 메시지를 무시하거나 소거한다.

[0037] 전술한 바에 따르면, 본 발명을 실시하는 방식에 따라서, 상기 단말기로부터 전송된 메시지의 중요도에 기초하여 상기 i의 변화에 따른 상기 해시 함수 $H_i()$의 종류를 선택하고, 상기 선택된 해시 함수의 종류에 기초한 보안키를 개별적으로 산출할 수 있다. 상기 제어부는, 상기 메시지의 중요도가 높은 경우, 상기 해시 함수 $H_1()$ 내지 $H_{n-1}()$ 중 적어도 둘 이상이 서로 상이한 것으로 선택하고, 상기 메시지의 중요도가 낮은 경우, 상기 해시 함수 $H_1()$ 내지 $H_{n-1}()$가 동일한 것으로 선택할 수 있다. 또한, 상기 제어부는, 상기 단말기로부터 전송된 메시지의 중요도에 기초하여 상기 i의 변화에 따른 상기 해시값 연결 함수 $C_i()$의 종류를 선택하고, 상기 선택된 해시값 연결 함수의 종류에 기초한 보안키를 개별적으로 산출할 수 있으며, 상기 메시지의 중요도가 높은 경우, 상기 해시값 연결 함수 $C_1()$ 내지 $C_{n-1}()$ 중 적어도 둘 이상이 서로 상이한 것으로 선택하고, 상기 메시지의 중요도가 낮은 경우, 상기 해시값 연결 함수 $C_1()$ 내지 $C_{n-1}()$가 동일한 것으로 선택할 수 있다.

[0038] 상기 해시 함수 및 해시값 연결 함수는 도 3의 경우에도 동일하게 적용될 수 있다. 즉, 전술한 사항에 따라 메시지의 중요도에 기초하여 해시 함수 또는 해시값 연결 함수가 선택된 경우, 최종 해시값 h_4을 산출하기 위한 변환 과정에 상기 선택된 해시 함수 또는 해시값 연결 함수와 동일한 해시 함수 또는 해시값 연결 함수가 사용될 수 있다. 또한, 상기 선택된 해시 함수 또는 해시값 연결 함수에 기초하여 보안키가 개별적으로 산출된 경우, 제어부는 상기 최종 해시값 h_4는 상기 개별적으로 산출된 보안키와의 일치 여부를 판별할 수 있고 이를 통해 해당 메시지의 유효성을 검증할 수 있다.

[0039] 즉, 상기 제어부는 적어도 두 단계 이상으로 구분된 메시지의 중요도 정보에 따른 조합 함수 정보 및 해시 함수 정보를 상기 저장부에 더 저장하고, 검증된 단말기 메시지, 상기 메시지의 중요도 정보에 따른 해시값 연결 함수, 해시 함수 및 상기 해시 트리에 기초하여 상기 각 메시지의 중요도 정보에 따른 보안키를 더 산출하고, 상기 통신부를 통해 상기 단말기로부터 검증 평가의 대상인 메시지를 수신할 때 상기 메시지의 중요도 정보를 더 수신하고, 상기 메시지의 검증을 위한 최종 해시값을 획득할 때 해당 메시지의 중요도 정보에 따른 조합 함수 및 해시 함수를 사용하고, 상기 최종 해시값이 해당 메시지의 중요도 정보에 따른 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가할 수 있다.

[0041] 도 4는 본 발명의 실시예에 따른 해시값 연결 함수를 나타낸 도면이다. 도 4에서 백색 사각형은 제i계층의 해시값 h_i에 해당하는 노드 또는 제i+1계층의 해시값 h_{i+1}에 해당하는 노드를 나타내고 흑색 사각형은 상기 해시값 h_i에 해당하는 노드의 형제 노드 B_i를 나타낸다.

[0042] 전술한 바와 같이, 상기 제어부는, n이 2 이상의 자연수, i가 n-1 이하의 자연수이고, h_i가 n개의 계층으로 구성된 해시 트리의 제i계층의 해시값, B_i가 h_i의 형제 노드의 해시값, $H_i()$가 해시 함수, $C_i()$가 해시값 연결 함수일 때, 수식 $h_{i+1} = H_i(C_i(h_i, B_i))$을 통해 제i+1계층의 해시값 h_{i+1}를 구하되, 상기 메시지의 중요도가 높은 경우, 상기 해시 함수 $H_1()$ 내지 $H_{n-1}()$ 중 적어도 둘 이상이 서로 상이한 것으로 선택하고, 상기 메시지의 중요도가 낮은 경우, 상기 해시 함수 $H_1()$ 내지 $H_{n-1}()$가 동일한 것으로 선택할 수 있다. 한편, 제어부는 상기 메시지의 중요도가 높은 경우, 상기 해시값 연결 함수 $C_1()$ 내지 $C_{n-1}()$ 중 적어도 둘 이상이 서로 상이한 것으로 선택하고, 상기 메시지의 중요도가 낮은 경우, 상기 해시값 연결 함수 $C_1()$ 내지 $C_{n-1}()$가 동일한 것으로 선택할 수 있다. 본 발명에 따른 보안 서버는 이를 통해 메시지의 중요도에 기초하여 메시지가 보호되는 정도를 조정할 수 있으며, 만일의 경우 일부 해시 함수 및 해시값 연결 함수가 외부에 유출되어도 효과적으로 보안 상태를 유지할 수 있다. 상기 일부 해시 함수 및 일부의 해시값 연결 함수 만으로는 보안키와 매칭이 되는 단말기 메시지를 생성할 수 없기 때문이다.

[0043] 도 4에 따르면, 제i계층의 해시값 h_i 및 그 형제 노드의 해시값 B_i은 다양한 방식으로 상호 연결될 수 있다. 도 4(a)에서는 상기 두 해시값을 줄지어 연결하는 단순한 방식으로 상기 해시값 연결 함수가 구비될 수 있다. 도 4(b)의 해시값 연결 함수는 도 4(a)의 경우와 순서가 반대인 예다. 도 4(c)의 해시값 연결 함수는 일정 길이로 분절된 해시값 h_i 및 B_i가 상호 교차되는 방식으로 연결되어있다. 이 때, 본 발명을 실시하는 방식에 따라서, 상기 두 해시값의 교차 순서 및 분절된 길이가 서로 불규칙적인 패턴으로 연결될 수도 있다. 도 4(d)의 경우, 해시값 연결 함수는 별도의 신호 처리 함수 f()인 것으로 구비될 수도 있다. 상기 함수 f()는 각 해시값의 길이를

두 배로 늘인 다음 상호 합치는 형식으로 구비될 수도 있으며, 별도의 해시 함수일 수도 있다. 하지만 상기 함수의 실시예는 이에 한정되지 않는다.

[0045] 도 5는 본 발명의 실시예에 따른 부분 해시 트리를 나타낸 도면이다. 도 5는 도 3의 경우와 마찬가지로 해시값 연결 함수 및 해시 함수에 대한 표시가 생략되어있다. 도 5에서 흑색 사각형으로 표시된 것은 단말기로부터 전송된 메시지 M5 및 메시지 M5의 해시값 N5에 해당하는 노드를 의미한다. 도 5에서 부분 해시 트리는 굵은 실선으로 표시되었으며, 부분 해시 트리에 속하지 않는 나머지 해시 트리의 부분은 점선으로 표시되었다.

[0046] 본 발명을 실시하는 방식에 따라서, n이 2 이상의 자연수이고, j가 2 이상 n 이하의 자연수이며, n 개의 계층으로 구분되되, 제1계층이 최하위 계층이고 제n계층이 최상이 계층인 해시 트리에 대하여, 제어부는 검증된 리프 노드에 기초하여 상기 해시 트리의 중간 노드의 해시값을 산출하고, 상기 저장부는 상기 중간 노드의 해시값을 더 저장할 수 있다. 이 때, 상기 제어부는, 상기 통신부를 통해 상기 단말기로부터 리프 노드로 변환된 메시지 및 API를 수신하고, 상기 수신된 메시지의 중요도 정보에 기초하여 2 이상 n 이하의 자연수 j를 선택하고, 제j 계층의 노드를 새로운 뿌리 노드로 하는 부분 해시 트리를 선별하되, 상기 부분 해시 트리는 상기 수신된 리프 노드를 하위 계층 노드로 포함하고, 상기 리프 노드, j-1 개의 형제 노드로 구성된 API, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 획득된 최종 해시값이 상기 새로운 뿌리 노드의 해시값과 동일하면 상기 단말기의 메시지가 유효한 것으로 평가할 수 있다.

[0047] 도 5(a)에서 상기 자연수 j가 4인 경우를 도시하고 있다. 즉, 해시 트리의 전 영역이 부분 해시 트리로써 활용될 수 있다. 본 발명의 바람직한 실시예에 따르면, 단말기로부터 수신된 메시지의 중요도가 높을수록 n에 가까운 자연수 j가 선택될 수 있다. 이와는 반대로, 메시지의 중요도가 낮을수록 2에 가까운 자연수 j가 선택될 수 있다. j가 n에 가까울수록 새로운 뿌리 노드의 계층이 높아지기 때문에 외부에서 에너지 관리 시스템에 침입하기 위해서 확보해야할 정보, 즉 해시 함수, 해시값 연결 함수 및 형제 노드 정보 등이 증가된다.

[0048] 도 5(b)는 상기 자연수 j가 3인 경우를 도시하고 있다. 도 5(b)에 따르면, N_{58} 노드가 새로운 뿌리 노드의 역할을 수행하게 된다. 이에 따라, 노드 N_5의 API는 N_6 및 N_{78}의 두 형제 노드로 구성되며 순차적인 해시값 조합 및 해시값 변환을 통해 N_{58}의 계층에 도달할 수 있다. 제어부는 저장부에 저장된 N_{58}의 해시값과 상기 수신된 메시지에 기초하여 생성된 N_{58}의 해시값 정보가 동일한 경우 해당 메시지가 유효한 것으로 판단할 수 있다.

[0050] 도 6은 본 발명의 실시예에 따른 보안 서버의 제어 방법을 나타낸 도면이다. 도 6에 따르면, 에너지 관리 시스템을 위한 보안 서버의 제어 방법에 상기 에너지 관리 시스템의 각 단말기로부터 전송되는 메시지를 검증하기 위한 해시 트리 및 보안키를 저장하는 단계(S110)가 포함될 수 있다. 이 때, 상기 해시 트리의 리프 노드 해시값은 기 설정된 해시값 연결 함수 및 해시 함수를 통해 상기 보안키에 대응되는 뿌리 노드의 해시값으로 변환될 수 있다. 그 후, 상기 해시 트리의 리프 노드의 해시값으로 변환된 상기 단말기의 메시지를 수신하되, 상기 메시지를 검증할 때 참조되는 API를 더 수신(S120)할 수 있다. 이 때, 상기 API는 상기 해시 트리에서 상기 리프 노드와 상기 뿌리 노드를 연결하는 경로를 가정했을 때 상기 경로에 포함되는 노드의 형제 노드의 집합일 수 있다. 그 다음, 상기 리프 노드의 해시값, 상기 API, 상기 해시값 연결 함수 및 상기 해시 함수에 기초하여 최종 해시값을 획득(S130)하고, 상기 최종 해시값이 상기 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가(S140)할 수 있다.

[0051] 이 때 본 발명을 실시하는 방식에 따라서, 상기 해시 트리 및 보안키를 저장하는 단계(S110)는 적어도 두 단계 이상으로 구분된 메시지의 중요도 정보에 따른 조합 함수 정보 및 해시 함수 정보를 더 저장할 수 있다. 이에 따라, 보안 서버는 검증된 단말기 메시지, 상기 메시지의 중요도 정보에 따른 해시값 연결 함수, 해시 함수 및 상기 해시 트리에 기초하여 상기 각 메시지의 중요도 정보에 따른 보안키를 더 산출할 수 있으며, 상기 최종 해시값을 획득하는 단계(S130)는 상기 메시지의 중요도 정보를 더 수신할 수 있다. 보안 서버는 상기 메시지의 검증을 위한 최종 해시값을 획득할 때 해당 메시지의 중요도 정보에 따른 조합 함수 및 해시 함수를 사용할 수 있으며, 상기 단말기의 메시지의 유효 여부를 평가하는 단계(S140)는 상기 최종 해시값이 해당 메시지의 중요도 정보에 따른 보안키와 동일하면 상기 단말기의 메시지가 유효한 것으로 평가할 수 있다. 이 때, 상기 메시지의 중요도는 해당 메시지에 포함되는 정보의 종류 및 상기 메시지를 전송하는 단말기의 종류에 기초하여 결정될 수 있다.

[0052] 상기 각 단계의 구체적인 설명은 도 1내지 5를 설명할 때 서술한 내용과 중복되므로 생략하도록 한다.

[0053] 본 발명에 따르면, 단말기가 전송한 메시지의 유효성을 용이하게 검증할 수 있으며, 메시지 검증시 필요한 정보량 및 정보 전송량을 감소시킬 수 있다.

[0054] 또한, 본 발명의 실시예에 따르면, 메시지의 중요도에 기초하여 변환 과정에서 사용되는 해시 함수의 종류를 결정할 수 있다. 이에 따라 메시지의 중요도에 적합한 수준의 보안이 제공될 수 있다.

[0055] 또한, 본 발명의 실시예에 따르면, 메시지의 중요도에 기초하여 변환 과정에서 사용되는 해시값의 해시값 연결 함수를 결정할 수 있으며, 이에 따라 암호화의 복잡도를 용이하게 조정할 수 있다.

[0056] 또한, 본 발명의 실시예에 따르면, 메시지의 중요도에 기초하여 부분 해시 트리를 선별할 수 있다.

[0058] 이상에서 본 발명을 구체적인 실시예를 통하여 설명하였으나, 당업자라면 본 발명의 취지를 벗어나지 않는 범위 내에서 수정, 변경을 할 수 있을 것이다. 따라서 본 발명이 속하는 기술분야에 속한 사람이 본 발명의 상세한 설명 및 실시예로부터 용이하게 유추할 수 있는 것은 본 발명의 권리범위에 속하는 것으로 해석되어야 할 것이다.

부호의 설명

[0059] 100 : 보안 서버

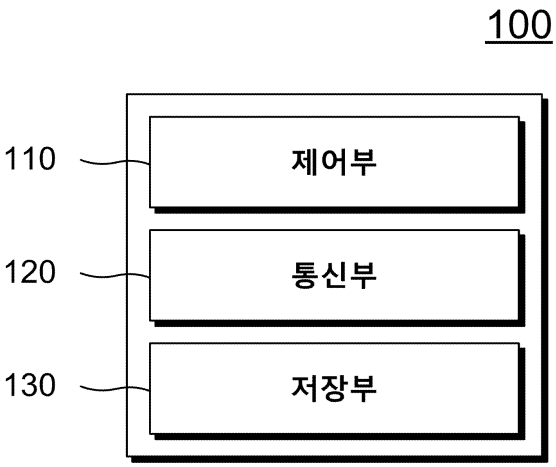
110 : 제어부

120 : 통신부

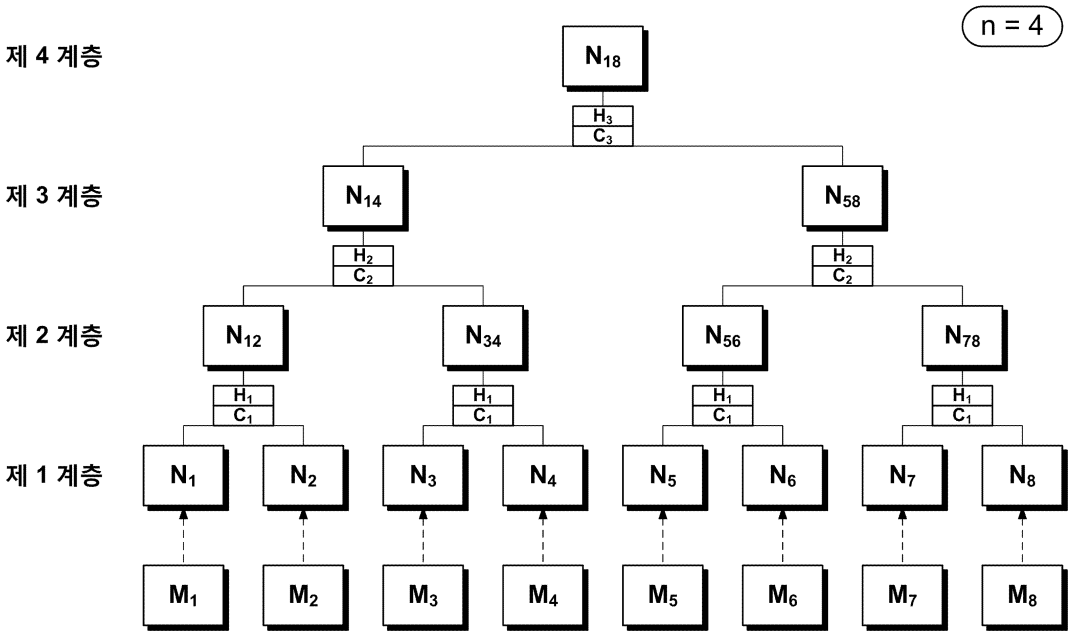
130 : 저장부

도면

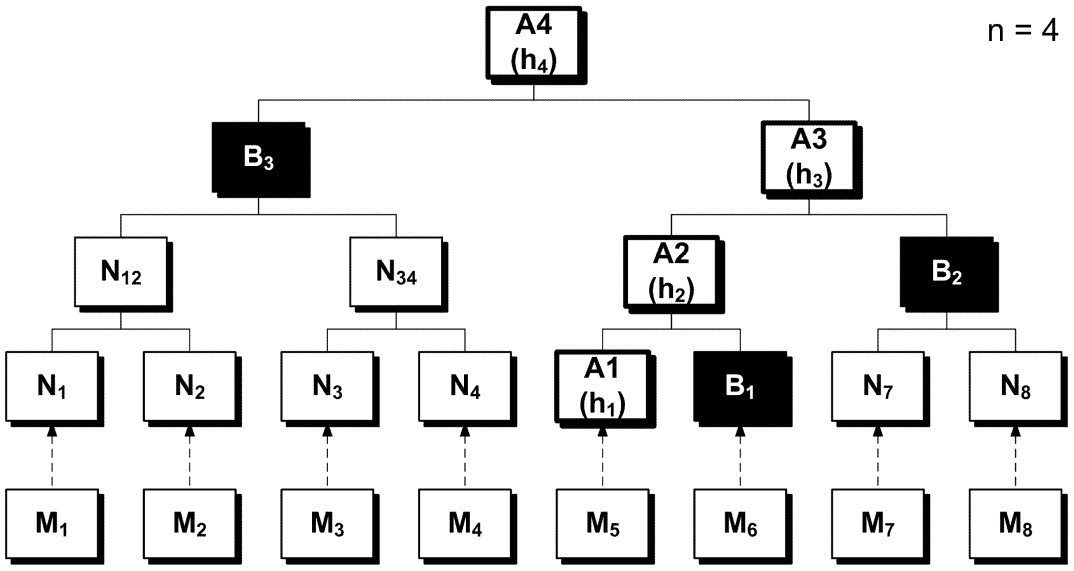
도면1



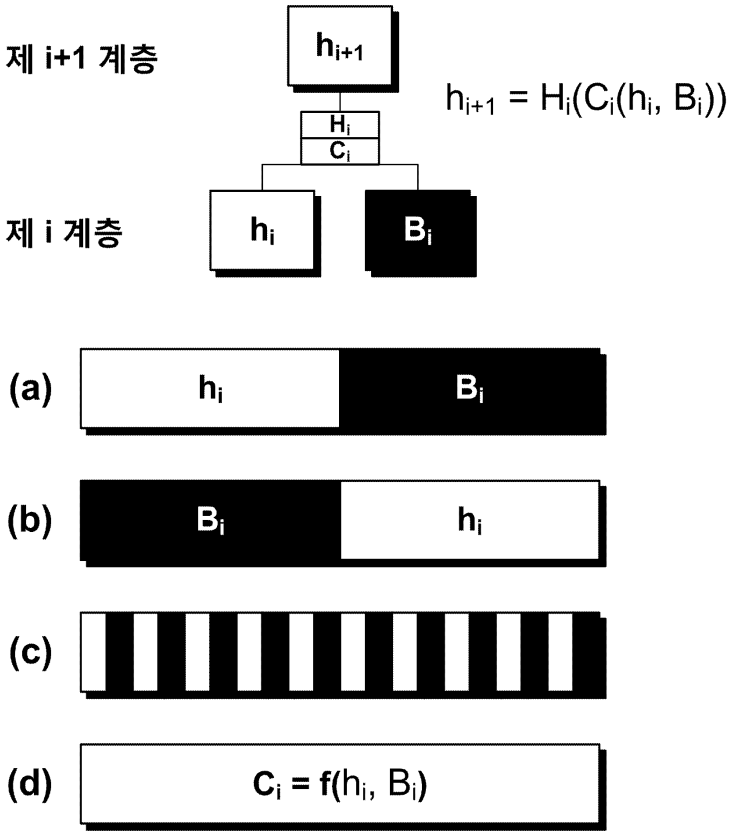
도면2


n = 4
제 4 계층
제 3 계층
제 2 계층
제 1 계층
N18
H3
C3
N14
N58
H2
C2
N12
N34
N56
N78
H1
C1
N1
N2
N3
N4
N5
N6
N7
N8
M1
M2
M3
M4
M5
M6
M7
M8

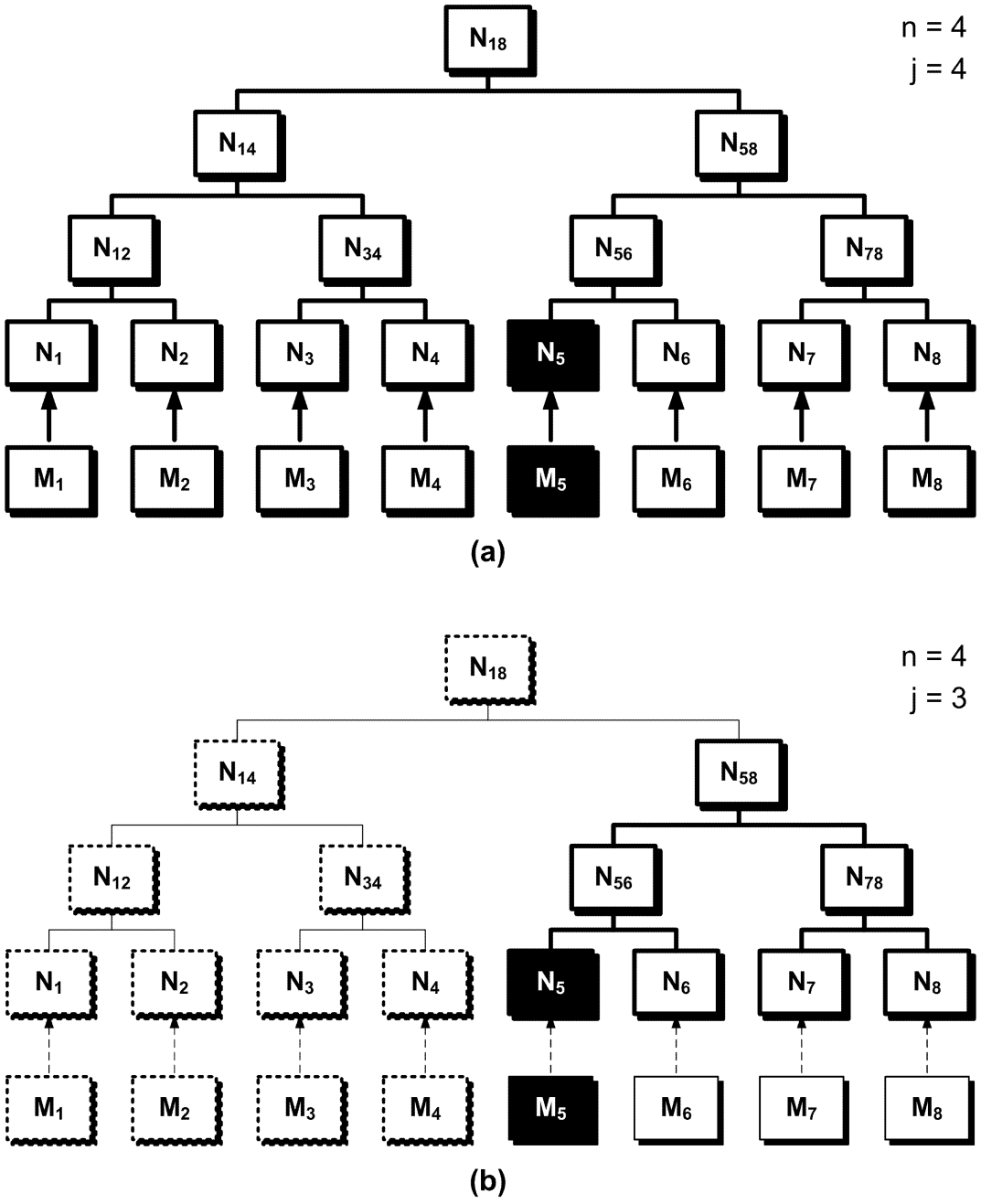
도면3


n = 4
A4
(h4)
B3
A3
(h3)
N12
N34
A2
(h2)
B2
N1
N2
N3
N4
A1
(h1)
B1
N7
N8
M1
M2
M3
M4
M5
M6
M7
M8

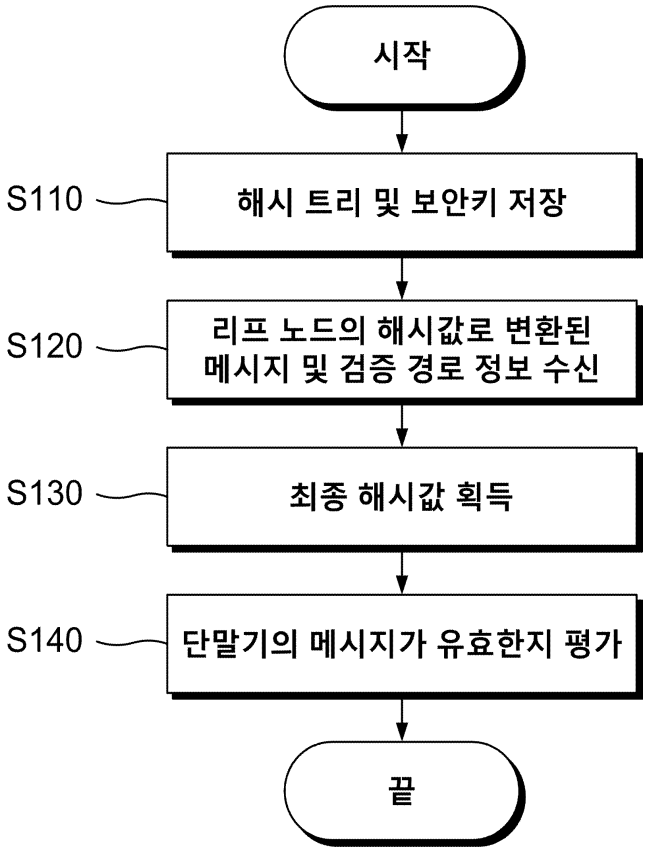
도면4


제 i+1 계층
h_{i+1}
H_i
C_i
$h_{i+1} = H_i(C_i(h_i, B_i))$
제 i 계층
h_i
B_i
(a)
h_i
B_i
(b)
B_i
h_i
(c)
(d)
$C_i = f(h_i, B_i)$

도면5


n = 4
j = 4
N18
N14
N58
N12
N34
N56
N78
N1
N2
N3
N4
N5
N6
N7
N8
M1
M2
M3
M4
M5
M6
M7
M8
(a)
n = 4
j = 3
N18
N14
N58
N12
N34
N56
N78
N1
N2
N3
N4
N5
N6
N7
N8
M1
M2
M3
M4
M5
M6
M7
M8
(b)

도면6


시작
S110
해시 트리 및 보안키 저장
S120
리프 노드의 해시값로 변환된
메시지 및 검증 경로 정보 수신
S130
최종 해시값 획득
S140
단말기의 메시지가 유효한지 평가
끝