



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0033716
(43) 공개일자 2019년04월01일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 12/40 (2006.01)
(52) CPC특허분류
H04L 9/0816 (2013.01)
H04L 12/40104 (2013.01)
(21) 출원번호 10-2017-0122210
(22) 출원일자 2017년09월22일
심사청구일자 2017년09월22일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
박수용
서울특별시 마포구 독막로18길 5, 101동 1001호(상수동, 상수두산위브아파트)
이준하
서울특별시 마포구 독막로38길 32, 102동 202호(대흥동, 마포나루타운)
(74) 대리인
특허법인충현

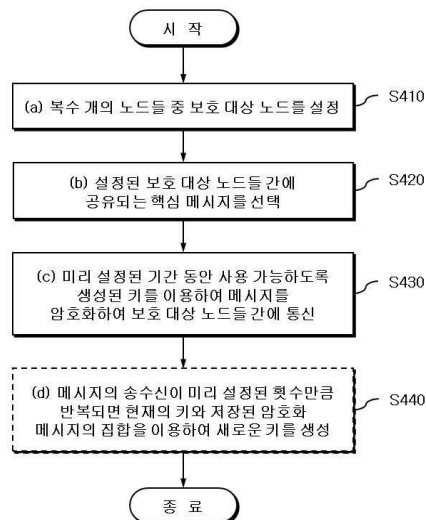
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 블록체인을 이용한 메시지 히스토리 기반의 보안 키를 이용하는 통신 장치 및 방법

(57) 요약

본 발명은 네트워크 또는 버스를 통해 암호화된 통신을 수행하는 기술에 관한 것으로, 네트워크 또는 버스(BUS)를 통해 연결된 노드(node)들 간에 보안 키(key)를 이용한 통신 방법은, 복수 개의 노드들 중 보호 대상 노드를 설정하고, 설정된 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하며, 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 메시지를 암호화하여 보호 대상 노드들 간에 통신하되, 보호 대상 노드들 각각은 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 핵심 메시지를 저장하여 블록(block)을 생성하고 생성된 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적된다.

대표도 - 도4



(52) CPC특허분류

H04L 2209/12 (2013.01)

H04L 2209/38 (2013.01)

(72) 발명자

박지우

서울특별시 서초구 서초중앙로24길 33, 106동 140
2호(서초동, 서초교대이편한세상)

이진환

서울특별시 광진구 아차산로76길 31, 103동 1503
호(광장동, 광나루현대아파트)

이우승

경기도 고양시 일산동구 산두로 26, 403동 105호(
마두동, 정발마을4단지건영빌라)

명세서

청구범위

청구항 1

네트워크 또는 버스(BUS)를 통해 연결된 노드(node)들 간에 보안 키(key)를 이용한 통신 방법에 있어서,

- (a) 복수 개의 노드들 중 보호 대상 노드를 설정하는 단계;
- (b) 설정된 상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하는 단계; 및
- (c) 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 메시지를 암호화하여 상기 보호 대상 노드들 간에 통신하는 단계를 포함하고,

상기 보호 대상 노드들 각각은 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적되는 것을 특징으로 하는 보안 키를 이용한 통신 방법.

청구항 2

제 1 항에 있어서,

상기 (a) 단계는,

복수 개의 노드들 중 미리 설정된 보안 기능에 연관된 노드를 보호 대상 노드로 설정하거나,

복수 개의 노드들 중 하나의 시스템 내에 위치하는 노드를 보호 대상 노드로 설정하거나, 또는

하나의 시스템 내에 위치하는 노드 및 그와 상호 작용하는 노드를 보호 대상 노드로 설정하는 것을 특징으로 하는 보안 키를 이용한 통신 방법.

청구항 3

제 1 항에 있어서,

상기 (b) 단계는,

설정된 상기 보호 대상 노드들 간에 송수신되는 메시지들의 집합 중 가장 많은 보호 대상 노드에 송수신되는 메시지를 핵심 메시지로 선택하는 단계를 포함하는 보안 키를 이용한 통신 방법.

청구항 4

제 3 항에 있어서,

상기 (b) 단계는,

상기 보호 대상 노드들 중에서 상기 핵심 메시지를 공유하지 않는 노드가 존재한다면, 해당 노드에 상기 핵심 메시지를 전송하는 단계를 더 포함하는 보안 키를 이용한 통신 방법.

청구항 5

제 1 항에 있어서,

상기 (c) 단계는,

상기 보호 대상 노드들이 각각 자신이 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 송신 메시지를 생성하거나 수신 메시지를 검증하는 것을 특징으로 하는 보안 키를 이용한 통신 방법.

청구항 6

제 1 항에 있어서,

상기 (c) 단계는,

(c2) 전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호함으로써 새로운 암호화 메시지를 생성하는 단계; 및

(c3) 생성된 새로운 암호화 메시지를 전송하고자 하는 메시지에 첨부하여 수신 노드에 전송하는 단계를 포함하는 보안 키를 이용한 통신 방법.

청구항 7

제 6 항에 있어서,

상기 (c) 단계는,

(c4) 상기 수신 노드가 수신된 메시지와 자신이 저장하고 있는 이전 기간의 암호화 메시지를 자신이 저장하고 있는 현재 기간 동안 사용 가능한 키를 이용하여 암호화한 후, 수신된 새로운 암호화 메시지와 비교함으로써 보안 여부를 검증하는 단계를 더 포함하는 보안 키를 이용한 통신 방법.

청구항 8

제 6 항에 있어서,

상기 (c) 단계는,

(c1) 상기 보호 대상 노드들이 최초 기동되는 시점에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 마지막으로 저장된 키 및 암호화 메시지를 독출하여 상기 보호 대상 노드들 간의 일치성을 검증하는 단계를 더 포함하는 보안 키를 이용한 통신 방법.

청구항 9

제 1 항에 있어서,

(d) 상기 (c) 단계를 통해 메시지의 송수신이 미리 설정된 횟수만큼 반복되면, 상기 보호 대상 노드들 각각은 동일한 키 생성 규칙에 따라 현재의 키와 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유하는 단계를 더 포함하는 보안 키를 이용한 통신 방법.

청구항 10

제 1 항 내지 제 9 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 11

네트워크 또는 버스(BUS)를 통해 통신하는 송신 노드(node)에 있어서,

미리 설정된 기간 동안 사용 가능하도록 생성된 키와 암호화된 메시지를 저장하는 비휘발성 메모리;

상기 비휘발성 메모리의 저장 공간에 대응하는 저장 공간을 형성하되, 상기 비휘발성 메모리에 저장된 키와 암호화된 메시지를 독출하여 연산을 수행하거나 연산 결과를 상기 비휘발성 메모리에 저장하는 휘발성 메모리; 및

보호 대상 노드들 간에 암호화된 통신을 수행하는 제어부를 포함하고,

상기 제어부는,

상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하고, 상기 핵심 메시지로부터 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 전송하고자 하는 메시지를 암호화하여 상기 보호 대상 노드들 중 수신 노드에 전송하되,

상기 수신 노드와 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적되는 것을 특징으로 하는 송신 노드.

청구항 12

제 11 항에 있어서,

상기 제어부는,

상기 비휘발성 메모리에 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 송신 메시지를 생성하는 것을 특징으로 하는 송신 노드.

청구항 13

제 11 항에 있어서,

상기 제어부는,

전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호함으로써 새로운 암호화 메시지를 생성하고,

생성된 새로운 암호화 메시지를 전송하고자 하는 메시지에 첨부하여 상기 수신 노드에 전송하는 것을 특징으로 하는 송신 노드.

청구항 14

제 13 항에 있어서,

상기 제어부는,

상기 보호 대상 노드들이 최초 기동되는 시점에 상기 비휘발성 메모리에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 상기 휘발성 메모리로부터 상기 비휘발성 메모리에 마지막으로 저장된 키 및 암호화 메시지를 상기 휘발성 메모리에 독출하여 상기 보호 대상 노드들 간의 일치성을 검증하는 것을 특징으로 하는 송신 노드.

청구항 15

제 11 항에 있어서,

상기 제어부는,

메시지의 송신이 미리 설정된 횟수만큼 반복되면, 상기 수신 노드와 동일한 키 생성 규칙에 따라 현재의 키와 상기 휘발성 메모리에 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유하는 것을 특징으로 하는 송신 노드.

청구항 16

네트워크 또는 버스(BUS)를 통해 통신하는 수신 노드(node)에 있어서,

미리 설정된 기간 동안 사용 가능하도록 생성된 키와 암호화된 메시지를 저장하는 비휘발성 메모리;

상기 비휘발성 메모리의 저장 공간에 대응하는 저장 공간을 형성하되, 상기 비휘발성 메모리에 저장된 키와 암호화된 메시지를 독출하여 연산을 수행하거나 연산 결과를 상기 비휘발성 메모리에 저장하는 휘발성 메모리; 및

보호 대상 노드들 간에 암호화된 통신을 수행하는 제어부를 포함하고,

상기 제어부는,

상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하고, 상기 핵심 메시지로부터 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 암호화된 메시지를 상기 보호 대상 노드들 중 송신 노드로부터 수신하되,

상기 송신 노드와 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적되는 것을 특징으로 하는 수신 노드.

청구항 17

제 16 항에 있어서,

상기 제어부는,

상기 송신 노드가 전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호화함으로써 새로운 암호화 메시지를 생성하고, 생성된 새로운 암호화 메시지가 첨부된 메시지를 상기 송신 노드로부터 수신하되,

상기 휘발성 메모리에 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 수신된 메시지를 검증하는 것을 특징으로 하는 수신 노드.

청구항 18

제 17 항에 있어서,

상기 제어부는,

상기 수신된 메시지와 상기 이전 기간의 암호화 메시지를 휘발성 메모리에 저장하고 있는 현재 기간 동안 사용 가능한 키를 이용하여 암호화한 후, 상기 송신 노드로부터 수신된 새로운 암호화 메시지와 비교함으로써 보안 여부를 검증하는 것을 특징으로 하는 수신 노드.

청구항 19

제 17 항에 있어서,

상기 제어부는,

상기 보호 대상 노드들이 최초 기동되는 시점에 상기 휘발성 메모리에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 상기 휘발성 메모리로부터 상기 휘발성 메모리에 마지막으로 저장된 키 및 암호화 메시지를 상기 휘발성 메모리에 독출하여 상기 보호 대상 노드들 간의 일치성을 검증하는 것을 특징으로 하는 수신 노드.

청구항 20

제 16 항에 있어서,

상기 제어부는,

메시지의 수신이 미리 설정된 횟수만큼 반복되면, 상기 송신 노드와 동일한 키 생성 규칙에 따라 현재의 키와 상기 휘발성 메모리에 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유하는 것을 특징으로 하는 수신 노드.

발명의 설명

기술 분야

[0001] 본 발명은 네트워크 또는 버스를 통해 암호화된 통신을 수행하는 기술에 관한 것으로, 특히 시스템 내부 네트워크를 구성하는 노드(node)들 또는 시스템 내부 네트워크 상의 노드와 상호 작용하는 외부의 노드의 보안 통신을 보장하기 위한 암호화 키(key)를 생성하여 송수신하는 노드, 이들 노드 간의 통신 방법 및 그 방법을 기록한 기록매체에 관한 것이다.

배경 기술

[0002] 자동차, 드론 등의 제어 기반 시스템은 작은 컴퓨터가 서로 통신하면서 동작하는 분산 시스템이다. 최근 자동차, 드론 등의 제어 기반 시스템의 기능이 늘어나고 복잡해짐에 따라 이러한 시스템의 네트워크는 데이터를 전달하기 쉬운 버스 형태를 가지게 되었다.

[0003] 하지만 버스 형태의 네트워크의 특성상 누가 보낸 데이터인지 구별하지 못하기 때문에 메시지를 전송하면 모든 노드(node)가 메시지 진위 여부와 관계없이 메시지를 처리하게 된다. 그렇기 때문에 버스가 해킹되어 비 인가된

노드가 버스에 접근하여 메시지를 전송하면 노드가 비 인가된 노드가 내리는 명령을 시행하는 오작동 하게 되어 사람의 생명에 위협이 될 수 있다. 특히 최근 떠오르고 있는 자율 주행 시스템 혹은 드론 등에서는 사람이 아닌 노드가 모든 상황을 통제하고 차량을 조정하기 때문에 보안 위협이 발생하였을 때 그 문제가 더욱 심각할 수 있다.

- [0004] 현재까지는 시스템의 네트워크가 폐쇄되어 외부에 노출되지 않았기 때문에 이러한 보안 위협의 가능성이 적었지만 최근 IoT, 자율주행 시스템 등의 기술의 발전에 따라 시스템 네트워크가 외부로 노출되어 보안에 대한 요구가 더욱 강조되고 있다. 따라서 비 인가된 노드가 시스템의 네트워크에 접근하여 전송하는 메시지를 식별할 수 있는 기술이 요구된다.

선행기술문헌

비특허문헌

- [0005] (비특허문헌 0001) Kleberger, Pierre, Tomas Olovsson, and Erland Jonsson. "Security aspects of the in-vehicle network in the connected car." Intelligent Vehicles Symposium (IV), 2011 IEEE. IEEE, 2011.

발명의 내용

해결하려는 과제

- [0006] 본 발명이 해결하고자 하는 기술적 과제는, 시스템 내부 네트워크에 적용된 종래의 고정된 대칭 키 기술에서 키가 노출될 경우 심각한 보안 위협이 되거나 네트워크에서 메시지를 가로채는 재전송 공격(Replay Attack)에 취약하다는 한계를 극복하고, 종래의 동적 키 기술에서 키나 키 생성을 위한 시드(seed) 값이 네트워크에 노출되기 때문에 도청 공격(Spoofing Attack)에 취약하며 네트워크 속도 저하 내지 오버헤드를 야기하는 문제를 해결하고자 한다.

과제의 해결 수단

- [0007] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 네트워크 또는 버스(BUS)를 통해 연결된 노드(node)들 간에 보안 키(key)를 이용한 통신 방법은, (a) 복수 개의 노드들 중 보호 대상 노드를 설정하는 단계; (b) 설정된 상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하는 단계; 및 (c) 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 메시지를 암호화하여 상기 보호 대상 노드들 간에 통신하는 단계를 포함하고, 상기 보호 대상 노드들 각각은 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적된다.
- [0008] 일 실시예에 따른 보안 키를 이용한 통신 방법에서, 상기 (a) 단계는, 복수 개의 노드들 중 미리 설정된 보안 기능에 연관된 노드를 보호 대상 노드로 설정하거나, 복수 개의 노드들 중 하나의 시스템 내에 위치하는 노드를 보호 대상 노드로 설정하거나, 또는 하나의 시스템 내에 위치하는 노드 및 그와 상호 작용하는 노드를 보호 대상 노드로 설정할 수 있다.
- [0009] 일 실시예에 따른 보안 키를 이용한 통신 방법에서, 상기 (b) 단계는, 설정된 상기 보호 대상 노드들 간에 송수신되는 메시지들의 집합 중 가장 많은 보호 대상 노드에 송수신되는 메시지를 핵심 메시지로 선택하는 단계를 포함할 수 있다. 또한, 상기 (b) 단계는, 상기 보호 대상 노드들 중에서 상기 핵심 메시지를 공유하지 않는 노드가 존재한다면, 해당 노드에 상기 핵심 메시지를 전송하는 단계를 더 포함할 수 있다.
- [0010] 일 실시예에 따른 보안 키를 이용한 통신 방법에서, 상기 (c) 단계는, 상기 보호 대상 노드들이 각각 자신이 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 송신 메시지를 생성하거나 수신 메시지를 검증할 수 있다.
- [0011] 일 실시예에 따른 보안 키를 이용한 통신 방법에서, 상기 (c) 단계는, (c2) 전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호함으로써 새로운 암호화 메시지를 생성하는 단계; 및 (c3) 생성된 새로운 암호화 메시지를 전송하고자 하는 메시지에 첨부하여 수신 노드에 전송하는 단계를 포함할 수 있다. 또한, 상기 (c) 단계는, (c4) 상기 수신 노드가 수신된 메시지와 자신이

저장하고 있는 이전 기간의 암호화 메시지를 자신이 저장하고 있는 현재 기간 동안 사용 가능한 키를 이용하여 암호화한 후, 수신된 새로운 암호화 메시지와 비교함으로써 보안 여부를 검증하는 단계를 더 포함할 수 있다. 나아가, 상기 (c) 단계는, (c1) 상기 보호 대상 노드들이 최초 기동되는 시점에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 마지막으로 저장된 키 및 암호화 메시지를 독출하여 상기 보호 대상 노드들 간의 일치성을 검증하는 단계를 더 포함할 수 있다.

[0012] 일 실시예에 따른 보안 키를 이용한 통신 방법은, (d) 상기 (c) 단계를 통해 메시지의 송수신이 미리 설정된 횟수만큼 반복되면, 상기 보호 대상 노드들 각각은 동일한 키 생성 규칙에 따라 현재의 키와 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유하는 단계를 더 포함할 수 있다.

[0013] 한편, 이하에서는 상기 기재된 보안 키를 이용한 통신 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

[0014] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 네트워크 또는 버스(BUS)를 통해 통신하는 송신 노드(node)는, 미리 설정된 기간 동안 사용 가능하도록 생성된 키와 암호화된 메시지를 저장하는 비휘발성 메모리; 상기 비휘발성 메모리의 저장 공간에 대응하는 저장 공간을 형성하되, 상기 비휘발성 메모리에 저장된 키와 암호화된 메시지를 독출하여 연산을 수행하거나 연산 결과를 상기 비휘발성 메모리에 저장하는 휘발성 메모리; 및 보호 대상 노드들 간에 암호화된 통신을 수행하는 제어부를 포함하고, 상기 제어부는, 상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하고, 상기 핵심 메시지로부터 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 전송하고자 하는 메시지를 암호화하여 상기 보호 대상 노드들 중 수신 노드에 전송하되, 상기 수신 노드와 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적된다.

[0015] 일 실시예에 따른 네트워크 또는 버스를 통해 통신하는 송신 노드에서, 상기 제어부는, 상기 비휘발성 메모리에 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 송신 메시지를 생성할 수 있다.

[0016] 일 실시예에 따른 네트워크 또는 버스를 통해 통신하는 송신 노드에서, 상기 제어부는, 전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호함으로써 새로운 암호화 메시지를 생성하고, 생성된 새로운 암호화 메시지를 전송하고자 하는 메시지에 첨부하여 상기 수신 노드에 전송할 수 있다. 또한, 상기 제어부는, 상기 보호 대상 노드들이 최초 기동되는 시점에 상기 비휘발성 메모리에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 상기 휘발성 메모리로부터 상기 비휘발성 메모리에 마지막으로 저장된 키 및 암호화 메시지를 상기 휘발성 메모리에 독출하여 상기 보호 대상 노드들 간의 일치성을 검증할 수 있다.

[0017] 일 실시예에 따른 네트워크 또는 버스를 통해 통신하는 송신 노드에서, 상기 제어부는, 메시지의 송신이 미리 설정된 횟수만큼 반복되면, 상기 수신 노드와 동일한 키 생성 규칙에 따라 현재의 키와 상기 휘발성 메모리에 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유할 수 있다.

[0018] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 네트워크 또는 버스(BUS)를 통해 통신하는 수신 노드(node)는, 미리 설정된 기간 동안 사용 가능하도록 생성된 키와 암호화된 메시지를 저장하는 비휘발성 메모리; 상기 비휘발성 메모리의 저장 공간에 대응하는 저장 공간을 형성하되, 상기 비휘발성 메모리에 저장된 키와 암호화된 메시지를 독출하여 연산을 수행하거나 연산 결과를 상기 비휘발성 메모리에 저장하는 휘발성 메모리; 및 보호 대상 노드들 간에 암호화된 통신을 수행하는 제어부를 포함하고, 상기 제어부는, 상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하고, 상기 핵심 메시지로부터 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 암호화된 메시지를 상기 보호 대상 노드들 중 송신 노드로부터 수신하되, 상기 송신 노드와 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적된다.

[0019] 일 실시예에 따른 네트워크 또는 버스를 통해 통신하는 수신 노드에서, 상기 제어부는, 상기 송신 노드가 전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호함으로써 새로운 암호화 메시지를 생성하고, 생성된 새로운 암호화 메시지가 첨부된 메시지를 상기 송신 노드로부터 수신하되, 상기 비휘발성 메모리에 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사

용 가능하도록 미리 저장된 키를 이용하여 수신된 메시지를 검증할 수 있다. 또한, 상기 제어부는, 상기 수신된 메시지와 상기 이전 기간의 암호화 메시지를 휘발성 메모리에 저장하고 있는 현재 기간 동안 사용 가능한 키를 이용하여 암호화한 후, 상기 송신 노드로부터 수신된 새로운 암호화 메시지와 비교함으로써 보안 여부를 검증할 수 있다. 나아가, 상기 제어부는, 상기 보호 대상 노드들이 최초 기동되는 시점에 상기 비휘발성 메모리에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 상기 휘발성 메모리로부터 상기 비휘발성 메모리에 마지막으로 저장된 키 및 암호화 메시지를 상기 휘발성 메모리에 독출하여 상기 보호 대상 노드들 간의 일치성을 검증할 수 있다.

[0020]

일 실시예에 따른 네트워크 또는 버스를 통해 통신하는 수신 노드에서, 상기 제어부는, 메시지의 수신에 미리 설정된 횟수만큼 반복되면, 상기 송신 노드와 동일한 키 생성 규칙에 따라 현재의 키와 상기 휘발성 메모리에 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유할 수 있다.

발명의 효과

[0021]

본 발명의 실시예들은, 네트워크를 통해 송수신하는 메시지를 이용하여 동적으로 키를 생성하되 송수신 메시지를 각각의 노드가 개별적으로 일정 기간 동안 적재하여 블록을 생성하고 생성된 블록과 이전 단계에서 생성된 키를 기반으로 블록 체인 형태로 연속적으로 연결된 키를 생성함으로써, 해커가 해당 키를 알아내기 어렵게 할 수 있을 뿐만 아니라 손상된 키 공격, 재전송 공격, 도청 공격 등에 있어서 용이하고 효과적인 방어 수단이 될 수 있으며 인증에 소요되는 오버헤드를 현저히 감소시킴으로써 실시간성을 보장할 수 있다.

도면의 간단한 설명

[0022]

도 1은 시스템의 내부 네트워크 구조를 도시한 블록도이다.

도 2는 시스템의 내부 네트워크에서 동적으로 키를 생성하는 일례를 설명하기 위한 도면이다.

도 3은 본 발명의 실시예들이 채택하고 있는 블록 체인을 이용하여 인증 키를 생성하는 아이디어를 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 네트워크 또는 버스(BUS)를 통해 연결된 시스템 노드(node) 간에 보안 키(key)를 이용한 통신 방법을 도시한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 도 4의 통신 방법에서 보호 대상 노드를 선택하는 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 도 4의 통신 방법에서 보호 대상 노드 간의 키 및 암호화 메시지의 일치성을 검증하는 과정을 설명하기 위한 도면이다.

도 7은 본 발명의 일 실시예에 따른 도 4의 통신 방법에서 키를 이용한 메시지의 송수신 과정을 설명하기 위한 도면이다.

도 8은 본 발명의 일 실시예에 따른 도 4의 통신 방법에서 히스토리 큐를 이용하여 새로운 키를 생성하는 과정을 설명하기 위한 도면이다.

도 9 및 도 10은 블록 체인에 기반한 보안 키를 이용한 도 4의 통신 방법의 일례를 보다 구체적으로 도시한 흐름도이다.

도 11은 본 발명의 일 실시예에 따른 네트워크 또는 버스(BUS)를 통해 통신하는 시스템 노드를 도시한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0023]

본 발명의 실시예들을 설명하기에 앞서, 시스템 내부 네트워크에 관한 기술에서의 보안 이슈를 살펴보고, 네트워크를 구성하는 노드(node) 간의 암호화 키에 관한 종래 기술의 문제점들을 검토한 후, 이들 문제점을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 기술적 수단을 순차적으로 소개하도록 한다.

[0024]

도 1은 시스템의 내부 네트워크 구조를 도시한 블록도로서, 복수 개의 노드(110)와 이들을 연결하는 데이터 버스(120)로 구성된다. 앞서 간략히 소개한 바와 같이 버스(120)를 통해 수신한 메시지를 인증하기 위한 연구가 활발히 이루어지고 있으나, 메시지를 인증하는 작업은 일반적으로 네트워크 성능을 저하시킨다. 각각의 노드(110)는 서로 약속한 시간 이내에 메시지를 주고 받는 실시간 시스템이기 때문에 메시지 인증에서 발생하는 오

버헤드가 동시에 고려되어야 한다.

- [0025] 비 인가된 노드가 송신하는 메시지를 걸러내기 위해서 많은 연구가 이루어지고 있는데, 이러한 연구들은 주로 메시지 인증에서 발생하는 오버헤드를 줄이기 위해 대칭키를 기반으로 인증을 수행하고 있다. 대칭키 기반의 연구는, 고정된 대칭 키를 사용하는 연구와 동적으로 대칭 키를 생성하고 각각의 노드들이 생성된 대칭 키를 공유하는 연구로 나눌 수 있다.
- [0026] 고정된 대칭 키 기반의 연구는 고정된 키를 사용하는 방식인데, 이는 내부자를 통해 키가 노출될 경우 심각한 보안 위협이 있을 수 있고, 키를 모르더라도 네트워크에서 메시지를 가로채서 그대로 재전송하는 재전송 공격(Replay Attack)에 취약하다는 한계를 가지고 있다. 이러한 한계를 극복하기 위해 노드들이 동적으로 생성된 키를 생성하고 네트워크를 통해 공유하거나 키 생성을 위한 시드(seed) 값을 공유하는 방식으로 개선되었다. 그러나 이러한 연구는 키나 키 생성을 위한 시드(seed) 값이 네트워크에 노출되기 때문에, 네트워크 감시를 통해 정보를 갈취하는 도청 공격(Spoofing Attack)에 한계를 가진다. 또한 네트워크를 통해 정보를 공유하기 때문에 성능에 오버헤드가 발생할 수 있어 전체 네트워크를 느리게 할 수 있다는 단점이 있다.
- [0027] 실시간 시스템에서 메시지를 인증은 효율성을 고려하여 보내고자 하는 메시지에 MAC(Message Authentication Code)를 붙여 전송할 수 있다. MAC은 송신자 측에서 보내고자 하는 메시지를 수신자와 공유하고 있는 키를 이용하여 암호화하여 생성하고, 수신자 측에서는 공유된 키로 MAC을 복호화하여 수신한 메시지와 일치하는지 검사한다. 만약 복호화한 메시지와 수신한 메시지가 일치하지 않으면 적합하지 않은 메시지로 간주한다. MAC을 이용하여 메시지를 인증하기 위해서는 반드시 송신자와 수신자가 동일한 키를 공유해야 하는데, 키를 공유하는 방법은 크게 ① 개발 시에 수신자 노드와 송신자 노드가 가지는 키를 고정시켜 공유하는 방법과 ② 송신자 노드가 동적으로 키를 생성하고 이를 수신자 노드와 네트워크를 통해 공유하는 방법으로 분류될 수 있다.
- [0028] 도 2는 시스템의 내부 네트워크에서 동적으로 키를 생성하는 일례를 설명하기 위한 도면으로서, 시스템 내부 네트워크의 보안을 위한 대칭키 기반의 기술들 중 세션 키를 채택한 방식(Symmetric Session Encryption Key Exchange)을 소개하고 있다.
- [0029] 도 2에 예시된 방법은 해시 함수와 랜덤 알고리즘을 이용하여 키를 생성한다. 각 노드는 서로 비밀 키를 공유하고 있고 메시지를 보낼 노드는 랜덤 알고리즘을 통해 새로운 숫자를 생성한다. 새로운 숫자를 생성한 뒤 자신이 가지고 있는 비밀 키와 숫자를 같이 해시 함수를 통해 해시를 수행하게 된다. 이러한 해시 수행 결과는 새로운 세션 키가 되고, 예를 들어 AES 알고리즘을 통해 암호화 처리한다. 그런 다음, 암호화된 메시지와 자신이 생성한 랜덤한 숫자를 함께 보내게 되는데, 메시지를 전달받는 수신 측에서는 자신이 받은 숫자와 자신이 가지고 있는 비밀 키를 통해 이 메시지가 올바른 노드에서 온 메시지인지 검사한다.
- [0030] 그러나, 도 2에 예시된 세션 키를 이용하는 방식을 이용할 경우, 해시 함수와 랜덤 알고리즘을 실행하는 시간만큼 성능이 감소하게 된다. 또한, 비밀 키를 직접 이용하여 암호화를 하는 것은 아니지만 비밀 키는 변하지 않기 때문에 키가 어떠한 이유로 노출된다면 시스템 보안이 취약해 질 수 있다는 약점을 가진다.
- [0031] 요약하건대, 시스템 내부 네트워크의 보안을 위한 종래의 기술들은 고정된 대칭키를 사용하거나 동적으로 대칭키를 생성하는 방식을 채택하였다. 비록 재전송 공격이나 키 유출의 한계를 극복하기 위해 키를 동적으로 생성하는 방식을 채택하였음에도, 동적으로 생성된 키나 키를 생성하기 위한 시드(seed) 값을 네트워크를 통해 공유하여 도청 공격에 노출될 수 있다는 한계를 보였다.
- [0032] 따라서, 이하에서 기술되는 본 발명의 실시예들은 시스템 노드가 특정 메시지 자체를 시드(seed) 값으로 하여 각각의 노드 스스로가 독립적이고 동적으로 동일한 키를 생성하는 보안 키 생성 기술을 제안한다. 이러한 방법을 통해 원래 송신하고 있던 메시지 이외에 생성된 키나 키 생성을 위한 시드 값을 네트워크에 노출시키지 않으면서도 실시간성을 보장하는 통신 방법을 제시한다. 이를 위해 본 발명의 실시예들이 제안하는 보안 통신 방법은, 공격자로부터 보호하고자 하는 노드들을 선정하여 해당 노드들과 가장 밀접한 관련이 있는 메시지를 지정하고, 그 메시지를 기반으로 하여 키를 동적으로 생성하게 되며 이 메시지들의 순서는 예측할 수 없기 때문에 키의 기밀성이 증가하게 된다. 또한, 각각의 노드들은 공통된 메시지와 키를 가지고 있기 때문에 내부 네트워크에 키가 노출되지 않고 서로 동일한 동적 키를 가질 수 있게 된다. 구현의 관점에서, 본 발명의 실시예들은 블록체인(block chain) 알고리즘의 구조를 일부 채용하였다.
- [0033] 도 3은 본 발명의 실시예들이 채택하고 있는 블록 체인을 이용하여 인증 키를 생성하는 아이디어를 설명하기 위한 도면이다.
- [0034] 2008년 사토시 나카모토에 의해 제시된 비트코인은 다른 신뢰된 보증기관이나 서버 없이 분산된 환경에서 디지털

털로 거래가 가능한 암호화 화폐라고 할 수 있다. 비트코인은 P2P, PKI, 분산합의 과정 등 여러 핵심기술이 존재한다. 하지만 각 거래의 신뢰도를 보장하기 위해서 블록체인이라는 것을 사용하였는데 그것은 각 거래 내역을 체인 형태로 이어 붙여서 이전 거래 내역을 위조하지 못하게 만들어 주는 기술이다. 즉, 거래 내역들을 블록이라는 구조로 만들어 순서를 부여함으로써 과거 내역을 바꾸지 않고는 현재 내역을 바꿀 수 없게 만든 것이다. 또한, 발급된 비트코인은 코인끼리 연결이 되어있기 때문에 발급처가 불분명한 코인이 발생할 수 없는 형태를 가지고 있다. 또한 비트코인의 노드들은 각자의 데이터는 각자가 판단하는 특징을 가지고 있다. 즉, 다른 누군가의 판단을 믿지 않고 자신의 판단을 믿음으로써 각자 자신이 옳다고 생각하는 데이터를 유지하는 시스템이다. 그것을 통해 데이터의 변조가 일어나더라도 복구할 수 있는 것이다. 즉, 블록체인은 P2P 환경에서 서로 신뢰할 수 없는 노드들끼리 신뢰된 거래를 하기 위한 구조라고 볼 수 있는 것이다.

[0035] 블록 체인에 기반한 비트코인과 같이 거래 내역이 모여 블록을 이루는 점에 착안하여, 시스템 내부 네트워크에 관한 각각의 메시지 내역들이 모여 새로운 키를 생성하는 메커니즘을 제안하고자 한다. 즉, 블록(분산 장부) 대신 키를 생성하는 것이다. 블록 체인의 경우, 새로운 블록의 생성시 이전 블록에 대한 정보(해시 값)에 기반하기 때문에 블록들 간의 연결성이 부여되므로, 올바르게 생성된 블록들은 첫 번째 블록부터 가장 최근의 블록까지 일정한 연결성을 갖는다.

[0036] 도 3을 참조하면, 본 발명의 실시예들은, 분산된 환경에서 중앙화된 관리 장치 없이 동작하는 노드들로 구성된 네트워크를 전체로 한다. 전체 노드들 중에서 이후 소개할 보호 대상 노드들로 선정된 노드들은 동일한 데이터(시스템 제어 메시지 및 인증 키를 포함하는 블록)를 유지한다. 만약 새로운 암호화 키를 생성할 경우, 이전 메시지들에 대한 정보와 이전 키를 바탕으로 키 생성이 이루어지기 때문에, 새롭게 생성된 인증 키들 간의 연결성이 부여된다. 즉, 올바르게 생성된 키는 시스템 동작 시작 시점부터 키 생성 시점까지의 메시지 내역 간의 연결성을 가진다. 따라서, 인증 키를 알아내거나 메시지를 조작하기 위해서는 시스템 동작 시작 시점부터 현재까지의 메시지 및 키를 모두 알아내야 하며, 이러한 구조하에서 보안성과 기밀성이 보장된다.

[0037] 이하에서는 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명하도록 한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 덧붙여, 명세서 전체에서, 어떤 구성 요소를 '포함'한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라, 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0038] 본 발명에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0039] 특별히 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미이다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미인 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0040] 한편, 본 발명의 실시예들에서 시스템 노드는 구현의 관점에서 설명의 편의를 위해 비휘발성 메모리인 EEPROM과 휘발성 메모리인 레지스터(register)를 갖는다고 예시하였다.

[0041] 도 4는 본 발명의 일 실시예에 따른 네트워크 또는 버스(BUS)를 통해 연결된 노드(node) 간에 보안 키(key)를 이용한 통신 방법을 도시한 흐름도로서, 도시된 3개의 과정(S410, S420, S430)을 포함하되, 새로운 키를 생성하는 과정(S440)을 더 포함할 수 있다.

[0042] S410 단계에서, (a) 복수 개의 노드들 중 보호 대상 노드를 설정한다. 여기서, 상기 (a) 단계는, 복수 개의 노드들 중 미리 설정된 보안 기능에 연관된 노드를 보호 대상 노드로 설정하거나, 복수 개의 노드들 중 하나의 이동체(moving body) 내에 위치하는 노드를 보호 대상 노드로 설정하거나, 또는 하나의 이동체 내에 위치하는 노드 및 그와 상호 작용하는 노드를 보호 대상 노드로 설정하는 것이 바람직하다. 이러한 보호 대상 노드를 크리티컬 클러스터(Critical Cluster)라고 명명(또는 태깅)하여 공격자로부터 지키고 싶은 노드들과 그것과 관련된 노드들의 집합을 식별할 수 있다.

[0043] S420 단계에서, (b) 설정된 상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택한다. 상기 (b) 단계는,

설정된 상기 보호 대상 노드들 간에 송수신되는 메시지들의 집합 중 발생 빈도가 가장 높은 메시지를 핵심 메시지로 선택하되, 상기 보호 대상 노드들 중에서 상기 핵심 메시지를 공유하지 않는 노드가 존재한다면, 해당 노드에 상기 핵심 메시지를 전송하는 것이 바람직하다. 즉, 핵심 메시지는 크리티컬 클러스터에 속한 노드들끼리 주고받는 메시지 중 특정한 메시지들을 말한다.

[0044] 보호 대상 노드를 선택하기 위해서는 공격자로부터 보호하고 싶은 노드들을 선정한 다음, 그 노드들이 많이 사용하는 메시지들을 살펴보게 된다. 살펴본 메시지들 중 핵심 메시지를 선정할 수 있다. 예를 들어, 메시지들 중 N개(N은 자연수)를 핵심 메시지로 선정하고 핵심 메시지들을 키 생성을 위한 시드로 설정한다. 키를 만드는 시드이자 보호 대상 노드에 가장 많은 영향을 주는 핵심 메시지를 고른 다음 최소에 설정된 보호 대상 노드에는 포함되어 있지 않지만 핵심 메시지들을 처리하는 다른 노드들도 보호 대상 노드에 포함시키는 것이 바람직하다. 반면, 보호 대상 노드에는 포함되어 있지만 핵심 메시지를 송수신하지 않는 노드가 존재할 수 있다. 이러한 노드들은 키를 생성하기 위해 핵심 메시지를 주고 받아야 하기 때문에 강제로 핵심 메시지를 송수신하도록 동작시키는 것이 바람직하다.

[0045] 이상과 같이 보호 대상 노드와 핵심 메시지를 선정할 때 고려해야 할 사항이 있다. 만약 핵심 메시지의 수를 많이 선정한다면 키가 자주 바뀌게 되는데, 키가 자주 바뀐다는 것은 보안성은 높아지지만 성능은 낮아질 수 있다는 것을 의미한다. 이러한 작업들은 도메인이나 작업 목적에 따라 달라질 수 있기 때문에 보호 대상 노드와 핵심 메시지의 선정 작업은 구현 환경에 따라 시스템의 요구 사항에 부합하도록 미리 설정될 수 있다.

[0046] 이상에서 보호 대상 노드와 핵심 메시지를 선정했다면 이제 비휘발성 메모리에 존재하는 히스토리 큐에 대한 크기를 결정해야 한다. 히스토리 큐의 크기는 메시지가 얼마나 쌓일 경우 키를 새로 생성할 것인지를 결정하는 인자로서, 히스토리 큐는 핵심 메시지의 메시지 내역을 저장하는 큐를 말한다. 만약 히스토리 큐에 대한 크기를 크게 한다면 키는 천천히 바뀌게 되지만 평균적인 메시지 처리 속도는 증가할 것이다. 반면, 히스토리 큐 크기를 작게 한다면 키가 자주 바뀌어 보안성이 높아지지만 상대적으로 성능이 저하될 것이다. 이러한 보안성과 성능 간의 트레이드 오프(trade-off)를 고려하여 히스토리 큐의 크기를 결정해야 할 것이다. 따라서, 히스토리 큐(history queue)의 크기를 설정하는 과정은, 요구되는 키의 갱신 주기에 반비례하고, 요구되는 메시지 처리 속도에 비례하며, 요구되는 보안 수준에 반비례하여 상기 히스토리 큐의 크기를 설정하는 것이 바람직하다.

[0047] S430 단계에서, (c) 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 메시지를 암호화하여 상기 보호 대상 노드들 간에 통신한다. 여기서, 상기 보호 대상 노드들 각각은 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적된다. 이러한 S430 단계는, 상기 보호 대상 노드들이 각각 자신이 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 송신 메시지를 생성하거나 수신 메시지를 검증한다.

[0048] 보다 구체적으로, 메시지를 전송하는 송신측 노드는 메시지를 키로 암호화하여 전송하며, 이때 수신측 노드에서 MAC(Message Authentication Code)을 사용하여 메시지의 변조를 찾아낸다. 또한 메시지를 전송할 때 이전 메시지를 함께 첨부함으로써 자신이 보낸 메시지가 다시 사용될 수 있는 재사용 공격에 대해 대비한다. 수신측 노드는 메시지를 수신하여 자신이 가지고 있는 키를 사용하여 메시지의 유효성을 판단하고 이전 메시지가 올바른지 여부도 검사하게 된다. 이전 메시지와 메시지가 올바르다고 판단되면 각 노드의 레지스터에 있는 히스토리 큐에 암호화된 메시지를 넣고 메시지를 처리하게 된다.

[0049] 요약하건대, S430 단계는, (c2) 전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호함으로써 새로운 암호화 메시지를 생성하고, (c3) 생성된 새로운 암호화 메시지를 전송하고자 하는 메시지에 첨부하여 수신 노드에 전송한다. 나아가, S430 단계는, (c4) 상기 수신 노드가 수신된 메시지와 자신이 저장하고 있는 이전 기간의 암호화 메시지를 자신이 저장하고 있는 현재 기간 동안 사용 가능한 키를 이용하여 암호화한 후, 수신된 새로운 암호화 메시지와 비교함으로써 보안 여부를 검증하는 과정을 더 포함할 수 있다.

[0050] 한편, S430 단계는, (c1) 상기 보호 대상 노드들이 최초 기동되는 시점에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 마지막으로 저장된 키 및 암호화 메시지를 독출하여 상기 보호 대상 노드들 간의 일치성을 검증할 수 있다. 처음 시스템을 작동시킬 때, 각 노드들은 같은 내역을 가지고 있어야 한다. 이를 위해 해시 함수를 이용하여 각 비휘발성 메모리의 내역들을 확인한다. 시스템 작동시 각 저장 내역과 키를 해시 함수를 통해 해시한 뒤 해시 값들을 비교한다. 모두 같은 해시 값을 가지고 있다면 비휘발성 메모리에 저

장되어 있는 내역들을 휘발성 메모리 영역으로 옮기고 시스템이 시작되게 된다.

[0051] S440 단계에서, (d) 보호 대상 노드들 간에 통신하는 상기 (c) 단계를 통해 메시지의 송수신이 미리 설정된 횟수만큼 반복되면, 상기 보호 대상 노드들 각각은 동일한 키 생성 규칙에 따라 현재의 키와 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유할 수 있다. 보다 구체적으로, S440 단계는, 메시지의 송수신이 발생할 때마다 미리 설정된 임계 조건(메시지의 송수신 횟수 제한)을 검사하고, 상기 임계 조건에 따른 횟수만큼 메시지의 송수신이 반복된 경우, 상기 보호 대상 노드들 각각은 동일한 키 생성 규칙에 따라 현재의 키와 저장된 암호화 메시지의 집합을 시드(seed)로서 활용하여 새로운 키를 생성함으로써 기존의 키를 대체할 수 있다.

[0052] 구현의 관점에서, 메시지를 송수신하는 과정을 거치면 히스토리 큐에 메시지가 점점 쌓이게 된다. 각 노드들은 메시지를 송수신할 때마다 자신의 레지스터에 있는 메시지 히스토리 큐를 살펴보는 과정을 거친다. 만약 히스토리 큐의 메시지가 가득 찬다면 그동안 쌓아온 암호화된 메시지들과 키를 시드 값으로 하여 새로운 키를 생성한다. 이 과정은 키를 예측할 수 없는 시드로 동적으로 생성하는 과정이라고 볼 수 있다. 새로운 키의 동적 생성 및 키 갱신 과정을 통해 최초의 키가 유출되어도 그 동안의 모든 메시지 내역과 키 생성을 위한 히스토리 큐의 크기를 모르는 한 키를 유추할 수 없게 된다.

[0053] 한편, 상기된 일련의 메시지 송수신 및 키 갱신 과정이 수행되는 도중 또는 완료된 이후 시스템(예를 들어 자동차 또는 드론)의 시동이 꺼지는 상황(시스템의 종료)에 관한 후처리 과정이 필요할 수 있다. 만약 상기 시스템의 기동이 종료되는 경우, 상기 보호 대상 노드들은 각각 자신이 보유하고 있는 현재의 키와 저장된 암호화 메시지를 이용하여 생성된 새로운 키를 상호 비교하여 일치성이 검증된 경우 해당 키를 저장한다. 즉, 이전 과정을 통해 메시지를 주고 받던 중 시스템에 시동을 정지하는 종료 메시지가 온다면, 각 노드들은 자신의 레지스터에 있는 값들을 해시 함수를 통해 해시한다. 그리고 각 노드들은 버스에 자신의 해시값을 보내 다른 보호 대상 노드들의 내역과 비교한다. 각 노드들은 전송되어 온 해시 값들을 비교하고 서로 일치할 경우 비휘발성 메모리에 해당 값들을 저장한 후 프로세스를 종료하게 된다.

[0054] 이상에서 기술된 도 4의 통신 방법에서 노드들은 송수신하는 메시지를 각각 축적하고 이를 기반으로 각자 키를 동적으로 생성하였다. 이하에서는 설계 단계에서 고려해야 할 사항을 먼저 기술한 후, 이를 기반으로 노드들이 운용 중에 동적으로 키를 동적으로 생성하는 실행 단계의 프로세스에 대해서 자세히 기술한다.

[0056] (1) 설계 단계

[0057] 본 발명의 실시예들에서 각각의 노드들은 서로 송수신하는 메시지를 기반으로 하여 동적으로 키를 생성한다. 이를 위해 설계 단계에서는, 보호하고자 하는 노드를 선정하고, 키를 생성하는데 사용될 메시지를 선정해야 하며, 키를 생성하기 위한 하드웨어 제약사항을 고려하여야 한다.

[0058] 메시지를 암호화하여 암호화 및 복호화하는 과정은 성능 오버헤드가 큰 작업이다. 따라서 엔진이나 조향을 제어하는 노드와 같이 보안 속성이 중요한 노드만 선별하여 본 기법을 적용하는 것이 성능 및 비용 측면에서 효율적이라고 할 수 있다. 이를 위해서 설계 단계에서 엔지니어가 보안이 적용되어야 하는 보호 대상 노드들을 선정하고 그룹을 선정해 주어야 한다. 또한 선정된 보호 대상 노드들이 수신하는 메시지를 기반으로 핵심 메시지를 선정한다. 보호 대상 노드는 엔지니어가 선정한 보안이 적용되어야 하는 노드들과 더불어 선정된 노드에 메시지를 전송하는 노드 또한 포함한다. 보다 정형화된 정의를 위해, 전체 메시지의 집합을

$M = \{m_1, m_2, \dots, m_i\}$ 이라고 하고, 전체 노드의 집합을 $E = \{e_1, e_2, \dots, e_j\}$ 라고 하고, 엔지니어가

선정한 보호 대상 노드의 집합을 $PE \subset E = \{pe_1, pe_2, \dots, pe_x\}$ 라고 정의하자. 더불어 노드 e_j

가 수신하는 메시지의 집합을 $\overleftarrow{M}_{e_j} \subset M$ 이라고 하고, 메시지 m_i 를 노드 e_j 로 송신하는 노드의 집합을

$E_{m_i \rightarrow e_j} \subset E$ 이라고 정의하고 메시지 m_i 를 수신하는 노드의 집합을 $E_{\overleftarrow{m_i}} \subset E$ 이라고 할 때, 핵심 메시지

P는 아래의 수학적 식 1과 같이 정의될 수 있다.

수학식 1

$$P = \operatorname{argmax}_{m_k \in \overleftarrow{PE}} |E_{m_k} \subset PE|, \text{ where } \overleftarrow{PE} = \bigcup_{e_j \in PE} \overleftarrow{M} e_j$$

수학식 1을 통해 주어진 핵심 메시지 P로부터 보호 대상 노드 CE는 아래의 수학식 2와 같이 정의될 수 있다.

수학식 2

$$CE = PE \cup E_{P \rightarrow e_j \in PE}$$

위와 같이 핵심 메시지와 보호 대상 노드를 정의하였을 때, 보호 대상 노드 내의 노드들 중 핵심 메시지 P를 수신하지 않는 노드가 존재할 수 있다. 이러한 노드 내부 알고리즘에서는 핵심 메시지를 이용하지 않을지라도 키 생성만을 목적으로 버스에서 핵심 메시지 P를 수신하도록 설계해야 한다. 이러한 노드에서는 알고리즘에 이용되지 않는 메시지를 받고 있어 오버헤드가 발생할 수 있지만 PE 내의 노드가 수신하는 메시지 중 가장 공통적으로 수신되는 메시지를 핵심 메시지로 정의했으므로 그 오버헤드는 최소화되었다고 할 수 있다.

도 5는 본 발명의 일 실시예에 따른 도 4의 통신 방법에서 보호 대상 노드를 선택하는 과정을 설명하기 위한 도면으로서, 네트워크(120) 또는 버스를 통해 연결된 10개의 노드가 서로 메시지를 송수신하고 있는 상황을 가정하였다. 또한, 이들 노드들 중 4개의 보호 대상 노드(115)가 사전에 PE로 지정되었음을 가정하였다.

도 5를 참조하면, 보호되어야 하는 4, 5, 6, 7번 노드가 수신하는 메시지의 합집합 $\overleftarrow{PE}$ 는 {0x01, 0x02, 0x03, 0x04}으로 정의될 수 있다. 이 메시지 중 '0x01' 메시지는 가장 많은 보호 대상 노드가 수신하는 메시지로 핵심 메시지 P로 선정되었다. 또한, 보호 대상 노드가 수신하는 메시지를 송신하는 보호대상 노드가 아닌 노드는 0, 1, 2번 노드이고, 결국 보호 대상 노드는 0, 1, 2, 4, 5, 6, 그리고 7번 노드로 선정된다. 여기서, 2, 4번 노드는 핵심 메시지로 선정된 '0x01' 메시지를 송신하거나 수신하고 있지 않기 때문에, 메시지 인증을 위해 강제로 '0x01' 메시지를 수신하도록 한다.

핵심 메시지와 보호 대상 노드의 선정과 더불어 하드웨어 제약 사항이 고려되어야 한다. 본 발명의 실시예들이 제안하고 있는 바와 같이, 메시지를 기반으로 한 블록을 저장하고 이를 체인 형태로 관리하여 동적으로 키를 생성하기 위해서는 메시지와 생성된 키를 저장할 수 있는 비휘발성 메모리(예를 들어, EEPROM)와 휘발성 메모리(예를 들어, 레지스터)가 탑재되어 있어야 한다. EEPROM과 레지스터는 각각 키를 저장할 수 있는 크기가 $1 \times \tau$ (단, τ 는 암호화한 메시지 크기)인 공간과 k개의 메시지를 저장할 수 있는 크기가 $k \times \tau$ 인 공간을 가져야 한다. 보안 모듈을 통한 메시지는 실제 노드가 수행하는 기능을 구현한 제어부(예를 들어, MCU로 구현될 수 있다)로 전달된다. 물리적인 EEPROM과 레지스터(register)는 보안 모듈 내에 포함될 수 있고, 필요에 따라 보안 모듈도 MCU 내에 구현될 수 있다.

(2) 실행 단계

본 발명의 실시예들이 제안하는 보안 통신 방법의 실행 단계는 시스템의 시동이 켜지면서 시작되고 시동이 꺼지면서 종료된다. 시동이 켜질 때부터 시동이 꺼진 때까지의 기간을 사이클(Cycle)이라고 명명하자. Cycle₀은 시스템가 출고되어 처음으로 시동이 켜지고 꺼질 때까지의 기간을 의미한다.

2.1) 초기화 단계

Cycle_n의 초기화 단계에서는 EEPROM에 저장되어 있는 키와 k개의 암호화된 메시지를 레지스터로 옮겨 온다. EEPROM에 저장되어 있는 데이터는 Cycle_(n-1)에서 레지스터에 저장되어 있던 키와 k개의 암호화된 메시지를 EEPROM으로 옮겨온 값이다. Cycle₀에서의 EEPROM의 데이터는 엔지니어가 임의로 삽입한 초기 키와 k개의 메시지

가 저장된다. Cycle_(n-1)의 종료 단계에서 레지스터의 데이터를 EEPROM으로 옮길 때 보호 대상 노드 내의 노드들이 가지고 있는 레지스터의 데이터의 일치성을 검증한 후 EEPROM으로 옮기기 때문에 Cycle_n의 초기화 단계에서 EEPROM의 데이터는 모두 같은 값을 가지고 있다는 것이 보장된다.

[0072] 도 6은 본 발명의 일 실시예에 따른 도 4의 통신 방법에서 보호 대상 노드 간의 키 및 암호화 메시지의 일치성을 검증하는 과정을 설명하기 위한 도면으로서, 보호 대상 노드(115) 각각에 저장된 키 및 암호화 메시지를 이용한 해시 값을 버스를 통해 전송하고 서로 일치하는지 여부를 검사하는 과정을 예시하고 있다.

[0074] 2.2) 메시지 송수신 단계

[0075] 도 7은 본 발명의 일 실시예에 따른 도 4의 통신 방법에서 키를 이용한 메시지의 송수신 과정을 설명하기 위한 도면으로서, 송신측 노드를 통해 암호화된 메시지를 수신하여 수신측 노드에서 이를 검증하는 과정을 보여준다.

[0076] 우선, EPROM의 모든 데이터가 레지스터로 옮겨오면 노드는 메시지를 송수신할 수 있는 상태에 놓인다. 메시지를 암호화하여 전송하기 위해 전송 노드에서는 보내고자 하는 메시지와 레지스터의 가장 상단에 저장된 암호화된 메시지를 레지스터에 저장된 키를 이용하여 암호화하여 암호화 메시지 MAC을 생성한다. 이때 MAC의 길이 등을 고려하여 기존의 SHA256이나 AES과 같은 암호화를 위한 다양한 알고리즘이 선택될 수 있으며, 개별적인 암호화 알고리즘의 적용 과정은 본 발명의 본질을 흐릴 우려가 있으며 여기서는 자세한 설명을 생략한다.

[0077] 암호화 메시지 MAC을 정형화하여 표현하기 위해 전송하고자 하는 n번째 메시지를 m_n이라 하고, 레지스터의 가장 상단에 적재되어 있는 암호화된 메시지를 MAC_(n-1)이라고 하자. 현재 레지스터에 저장되어 있는 키를 key_x이라고 하고 임의의 암호화 알고리즘을 $\cdot$ 이라고 할 때, 보내고자 하는 메시지 m_n을 암호화한 MAC_n은 아래의 수학적 식 3과 같이 정의될 수 있다.

수학적 식 3

$$MAC_n = key_x \cdot (m_n, MAC_{n-1})$$

[0078]

[0079] 전송 노드는 위의 정의에 따라 MAC_n을 생성한 후 생성된 MAC_n을 보내고자 하는 메시지 m_n에 첨부시켜서 버스로 전송하고 새로 생성된 MAC_n을 레지스터의 암호화 메시지 저장소의 최상단에 저장시키고 최하단의 암호화 메시지를 삭제한다.

[0080] 전송 노드에서 m_n에 MAC_n을 첨부하여 보내면 수신 노드에서는 자신의 레지스터에 저장되어 있는 key_x와 암호화 메시지 저장소의 최상단에 저장되어 있는 MAC_(n-1)을 이용하여 전송받은 m_n의 MAC_n'을 생성한다. 생성된 MAC_n'을 전송받은 MAC_n과 비교하여 양자가 서로 일치하면 전송받은 메시지 m_n을 정상적으로 처리하고, 일치하지 않으면 비정상 처리한다. 일치하는 경우 전송받은 MAC_n을 자신의 레지스터의 최상단에 저장하고, 최하단의 MAC은 삭제하여, 전송한 측의 레지스터의 MAC 저장소와 같은 MAC이 적재되게 만든다. 만약 MAC_n'과 MAC_n가 일치하지 않는다면 버스로 롤백(Rollback) 메시지를 전송한다. 보호 대상 노드의 노드들이 롤백 메시지를 수신하면 EEPROM에 저장된 키와 k개의 MAC을 레지스터로 옮겨 초기화한다. 이러한 과정을 통해 항상 보호 대상 노드의 노드들이 같은 키와 같은 암호화 메시지를 가진다는 것을 보장한다.

[0081] 메시지 송신측과 수신측에서 암호화 메시지 MAC_n을 생성하기 위해 이전 메시지 m_(n-1)를 암호화한 MAC_(n-1)을 이용하는 이유는 해커가 이전에 보낸 메시지를 네트워크에서 가로채어 그대로 재전송하는 공격인 재전송 공격(Replay Attack)을 막기 위함이다. 해커가 재전송 공격을 성공시키기 위해서는 현재의 키 key_x를 알아야 하고, 또한 이전 메시지의 암호화된 코드 MAC_(n-1)을 알아야 한다. 그러나 이전 메시지의 암호화된 코드 MAC_(n-1)은 그 이전 메시지의 암호화된 코드 MAC_(n-2)를 기반으로 생성되기 때문에, 결국 MAC₀부터 추적해야 재전송 공격을 성공시킬 수 있는데, 이는 시스템(예를 들어, 자동차 내지 드론)의 출고부터 추적할 수 있어야 한다는 것을 의미하기 때문에 매우 어려운 일이라고 할 수 있다.

[0083] 2.3) 동적 키 생성 단계

[0084] 도 8은 본 발명의 일 실시예에 따른 도 4의 통신 방법에서 히스토리 큐를 이용하여 새로운 키를 생성하는 과정을 설명하기 위한 도면이다. 메시지의 송수신 과정을 반복하면 히스토리 큐에 메시지가 누적되게 되며, 각 노드들은 메시지의 송수신 때마다 자신의 레지스터에 누적된 메시지 히스토리 큐를 살펴본 후, 해당 큐가 가득 찬 경우 이미 쌓인 암호화 메시지들과 키를 시드 값으로 하여 새로운 키를 생성하게 된다.

[0085] 즉, 메시지 송수신을 임의의 지정된 수 k 만큼 반복하면 현재의 키 key_x 와 레지스터의 k 개의 MAC의 집합 $SMAC_x = \{MAC_n \dots MAC_{n+k}\}$ 을 이용하여 새로운 키 $key_{(x+1)}$ 를 생성한다. 메시지 송수신 단계에서 보호 대상 노드의 모든 노드의 레지스터는 항상 같은 키와 MAC의 리스트를 가지는 것이 보장이 되기 때문에, 보호 대상 노드 내의 모든 노드들은 항상 같은 키를 가진다는 것 또한 보장된다. 아래의 수학적 식 4는 동적으로 생성되는 새로운 키 $key_{(x+1)}$ 를 정형화하여 정의한다.

수학적 식 4

[0086]
$$key_{x+1} = key_x \cdot (MAC_n \dots MAC_{n+k})$$

[0087] 위의 정의에 따라 생성된 키 $key_{(x+1)}$ 를 이용하여 메시지를 임의의 지정된 수인 k 번 만큼 송수신한 후 새로운 키 $key_{(x+2)}$ 를 동적으로 생성한다. 이러한 과정을 반복하여 주기적으로 새로운 키를 생성한다. 보호 대상 노드 내의 모든 노드들이 가지는 레지스터에 저장된 SMAC 내의 값들이 항상 같은 값을 가지게 되므로 항상 모든 노드들이 같은 키를 생성하는 것이 보장된다.

[0089] 2.4) 종료 단계

[0090] 네트워크에 엔진을 종료시키기 위한 신호가 감지되면 보호 대상 노드는 종료 단계를 수행한다. 종료 단계에서는 레지스터에 저장된 k 개의 MAC과 레지스터에 저장되어 있던 현재의 키를 각각 EEPROM으로 옮기고 다음 사이클(Cycle)에서 이용한다. 이때, 보호 대상 노드 내의 모든 노드의 레지스터-MAC의 k 개의 MAC이 같다는 것을 검증하기 위해 보호 대상 노드 내의 모든 노드가 수학적 식 4의 방법으로 새로운 키를 생성하여 버스로 송신하고 미리 정해진 시간 t 만큼 대기한다. 미리 정해진 시간 t 이내에 보호 대상 노드 내의 임의의 노드 e_n 는 버스를 통해 다른 노드로부터 수신한 $n-1$ 개의 새로 생성된 키를 수신하고, 자신이 새로 생성한 키와의 일치성을 검사한다. 검사 결과 모두 일치하면 자신의 레지스터의 모든 값을 EEPROM으로 옮긴다. 만약 수신하지 못한 키가 있거나 하나라도 일치하지 않는 키가 존재하면 롤백(Rollback) 메시지를 버스로 송신하고, 레지스터의 값을 EEPROM으로 옮기지 않고 종료한다. 임의의 노드 e_n 이 EEPROM에 데이터를 옮기기 전에 대기하는 시간 t 동안 롤백 메시지를 받으면 레지스터의 값을 EEPROM으로 옮기지 않고 종료한다. 보호 대상 노드 내의 모든 노드의 EEPROM의 데이터는 다음 사이클에서 키로 사용되거나 키를 만드는 시드로 사용되기 때문에, 보호 대상 노드 내의 모든 노드의 EEPROM의 데이터는 항상 같다는 것을 보장해주어야 한다. 시간 t 가 너무 짧게 설정되는 경우 다른 노드가 송신한 롤백 메시지를 놓칠 수 있기 때문에 t 값은 시스템이 요구하는 최소 수준의 시간 이상으로 설정해주어야 한다.

[0092] 도 9 및 도 10은 블록 체인에 기반한 보안 키를 이용한 도 4의 통신 방법의 일례를 보다 구체적으로 도시한 흐름도이다.

[0093] 도 9를 참조하면, 크리티컬 클러스터(보호 대상 노드)를 선택(S410)하고, 핵심 메시지를 선택(S420)하며, 히스토리 큐의 크기를 선택하는 일련의 전처리 과정이 별도로 기술되어 있다. 이러한 전처리 과정이 수행된 이후, 본격적인 노드들이 구동이 시작되면, 최초에 노드 간 비휘발성 메모리 내역을 확인하는 과정이 실행된다. 이후, 키를 이용한 송수신 과정(S430)이 반복되며 메시지의 개수가 증가되며, 증가된 메시지의 개수가 미리 전처리 과정을 통해 설정된 히스토리 큐의 크기에 도달하면, 새로운 키를 동적으로 생성(S440)하게 된다. 한편, 시스템의

종료 메시지가 감지되면, 비휘발성 메모리에 보호 대상 노드의 모든 내역과 키를 기록하고 시스템을 종료한다.

- [0094] 도 10은 이전 사이클의 결과가 현재의 사이클에 영향을 미치는 구조를 보여주고 있는데, 특히 메시지 송수신 과정(S430)에 관하여 전송 노드 및 수신 노드로 구분하여 세부 프로세스를 도시하였다. 도 10을 참조하면, 전송 노드에서 생성된 MAC을 암호화 메시지와 결합하여 수신 노드에 전송하며, 최상단 레지스터에 MAC을 저장하고 있음을 보여준다. 또한, 수신 노드에서는 수신 메시지에서부터 MAC을 분리하여 복호화하며, 복호화된 MAC과 자신이 저장하고 있는 암호화 메시지가 일치하는 경우 MAC을 최상단 레지스터에 저장하고, 반면 양자가 일치하지 않는 경우 롤백 메시지를 전송하게 됨을 보여준다.
- [0095] 도 11은 본 발명의 일 실시예에 따른 네트워크 또는 버스(BUS)를 통해 통신하는 노드를 도시한 블록도이다. 앞서 소개된 바와 같이, 핵심 메시지와 보호 대상 노드의 선정과 더불어 하드웨어 제약 사항이 고려되어야 하는데, 도 11은 노드 내부의 EEPROM(10)과 레지스터(register)(20)의 논리적인 구성을 예시하였다. 시스템 노드들이 메시지를 기반으로 한 블록을 저장하고 이를 체인 형태로 관리하여 동적으로 키를 생성하기 위해서는 메시지와 생성된 키를 저장할 수 있는 비휘발성 메모리(예를 들어, EEPROM)와 휘발성 메모리(예를 들어, 레지스터)가 탑재되어 있어야 한다. EEPROM과 레지스터는 각각 키를 저장할 수 있는 크기가 $1 \times \tau$ (단, τ 는 암호화한 메시지 크기)인 공간과 k 개의 메시지를 저장할 수 있는 크기가 $k \times \tau$ 인 공간을 가져야 한다. 보안 모듈(security module)을 통한 메시지는 실제 노드가 수행하는 기능을 구현한 제어부(예를 들어, MCU(micro controller unit)(30)로 구현될 수 있다)로 전달된다. 물리적인 EEPROM과 레지스터(register)는 보안 모듈 내에 포함될 수 있고, 필요에 따라 보안 모듈도 MCU(30) 내에 구현될 수 있다.
- [0096] 도 11의 노드 또는 보호 대상 노드(115)는 앞서 도 4를 통해 기술한 시스템 노드들 간에 보안 키를 이용한 통신 방법의 각 과정을 하드웨어 구현의 관점에서 제시된 것으로서, 여기서는 설명의 중복을 피하고자 각 구성의 주요 동작과 기능을 송신 노드 및 수신 노드의 관점에서 요약하도록 한다.
- [0097] 네트워크 또는 버스(BUS)를 통해 통신하는 송신 노드 및 수신 노드는 상황에 따라 송신측 및 수신측의 어느 역할로도 동작할 수 있으므로 기본적인 하드웨어 구성은 동일하다.
- [0098] 첫째, 송신 노드의 구성을 살펴보자.
- [0099] 비휘발성 메모리(예를 들어, EEPROM)(10)는, 미리 설정된 기간 동안 사용 가능하도록 생성된 키와 암호화된 메시지를 저장하는 수단이다.
- [0100] 휘발성 메모리(예를 들어, 레지스터)(20)는, 상기 비휘발성 메모리(10)의 저장 공간에 대응하는 저장 공간을 형성하되, 상기 비휘발성 메모리(10)에 저장된 키와 암호화된 메시지를 독출하여 연산을 수행하거나 연산 결과를 상기 비휘발성 메모리(10)에 저장하는 수단이다.
- [0101] 제어부(예를 들어, MCU)(30)는, 보호 대상 노드들 간에 암호화된 통신을 수행하는 구성으로서, 상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하고, 상기 핵심 메시지에서부터 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 전송하고자 하는 메시지를 암호화하여 상기 보호 대상 노드들 중 수신 노드에 전송하되, 상기 수신 노드와 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적된다.
- [0102] 상기 제어부(30)는, 상기 비휘발성 메모리에 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 송신 메시지를 생성할 수 있다.
- [0103] 상기 제어부(30)는, 전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호함으로써 새로운 암호화 메시지를 생성하고, 생성된 새로운 암호화 메시지를 전송하고자 하는 메시지에 첨부하여 상기 수신 노드에 전송할 수 있다. 또한, 상기 제어부(30)는, 상기 보호 대상 노드들이 최초 기동되는 시점에 상기 비휘발성 메모리에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 상기 휘발성 메모리로부터 상기 비휘발성 메모리에 마지막으로 저장된 키 및 암호화 메시지를 상기 휘발성 메모리에 독출하여 상기 보호 대상 노드들 간의 일치성을 검증할 수 있다.
- [0104] 상기 제어부(30)는, 메시지의 송신이 미리 설정된 횟수만큼 반복되면, 상기 수신 노드와 동일한 키 생성 규칙에 따라 현재의 키와 상기 휘발성 메모리에 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유할 수 있다.

- [0105] 둘째, 수신 노드의 구성을 살펴보자.
- [0106] 비휘발성 메모리(예를 들어, EEPROM)(10), 휘발성 메모리(예를 들어, 레지스터)(20) 및 제어부(예를 들어, MCU)(30)는 기본적으로 송신 노드의 구성과 동일하다. 다만, 동작 역할의 관점에서 약간의 차이점이 존재하는데, 제어부(30)는, 상기 보호 대상 노드들 간에 공유되는 핵심 메시지를 선택하고, 상기 핵심 메시지로부터 미리 설정된 기간 동안 사용 가능하도록 생성된 키를 이용하여 암호화된 메시지를 상기 보호 대상 노드들 중 송신 노드로부터 수신하되, 상기 송신 노드와 동일한 키 생성 규칙에 따라 미리 설정된 기간 동안 상기 핵심 메시지를 저장하여 블록(block)을 생성하고, 생성된 상기 블록과 현재 사용 중인 키를 기반으로 새로운 키를 생성하여 보유함으로써, 이전 메시지 및 이전 키에 관한 정보가 새로운 키에 순차적으로 누적된다.
- [0107] 상기 제어부(30)는, 상기 송신 노드가 전송하고자 하는 메시지와 이전 기간의 암호화 메시지를 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 암호함으로써 새로운 암호화 메시지를 생성하고, 생성된 새로운 암호화 메시지가 첨부된 메시지를 상기 송신 노드로부터 수신하되, 상기 비휘발성 메모리에 저장하고 있는 이전 기간의 암호화 메시지 및 현재 기간 동안 사용 가능하도록 미리 저장된 키를 이용하여 수신된 메시지를 검증할 수 있다. 또한, 상기 제어부(30)는, 상기 수신된 메시지와 상기 이전 기간의 암호화 메시지를 휘발성 메모리에 저장하고 있는 현재 기간 동안 사용 가능한 키를 이용하여 암호화한 후, 상기 송신 노드로부터 수신된 새로운 암호화 메시지와 비교함으로써 보안 여부를 검증할 수 있다. 나아가, 상기 제어부(30)는, 상기 보호 대상 노드들이 최초 기동되는 시점에 상기 비휘발성 메모리에 미리 저장되어 있던 초기 키 및 암호화 메시지 또는 지난 종료 시점에 상기 휘발성 메모리로부터 상기 비휘발성 메모리에 마지막으로 저장된 키 및 암호화 메시지를 상기 휘발성 메모리에 독출하여 상기 보호 대상 노드들 간의 일치성을 검증할 수 있다.
- [0108] 상기 제어부(30)는, 메시지의 수신에 미리 설정된 횟수만큼 반복되면, 상기 송신 노드와 동일한 키 생성 규칙에 따라 현재의 키와 상기 휘발성 메모리에 저장된 암호화 메시지의 집합을 이용하여 새로운 키를 생성하여 보유할 수 있다.
- [0109] 상기된 본 발명의 실시예들에 따르면, 네트워크를 통해 송수신하는 메시지를 이용하여 동적으로 키를 생성하되 송수신 메시지를 각각의 노드가 개별적으로 일정 기간 동안 적재하여 블록을 생성하고 생성된 블록과 이전 단계에서 생성된 키를 기반으로 블록 체인 형태로 연속적으로 연결된 키를 생성함으로써, 해커가 해당 키를 알아내기 어렵게 할 수 있을 뿐만 아니라 손상된 키 공격, 재전송 공격, 도청 공격 등에 있어서 용이하고 효과적인 방어 수단이 됨과 동시에 인증에 소요되는 오버헤드를 현저히 감소시킴으로써 실시간성을 보장할 수 있다.
- [0110] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.
- [0111] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.
- [0112] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

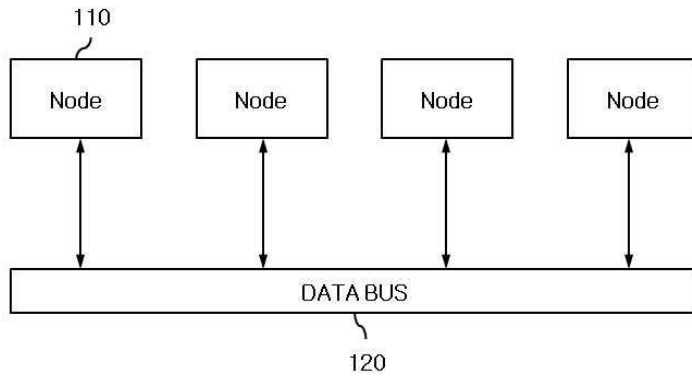
부호의 설명

- [0113] 110: 노드 (node)
- 120: 네트워크 또는 버스(BUS)
- 115: 보호 대상 노드 (크리티컬 클러스터)
- 10: 비휘발성 메모리 (EEPROM)
- 20: 휘발성 메모리 (register)

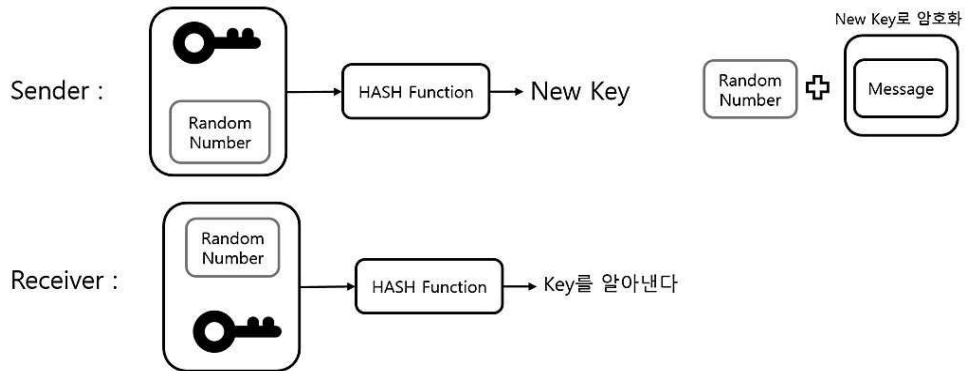
30: 제어부 (MCU)

도면

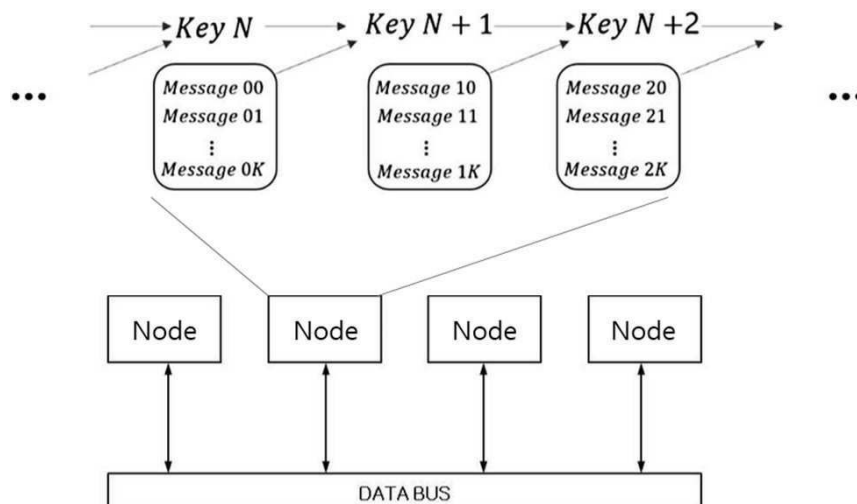
도면1



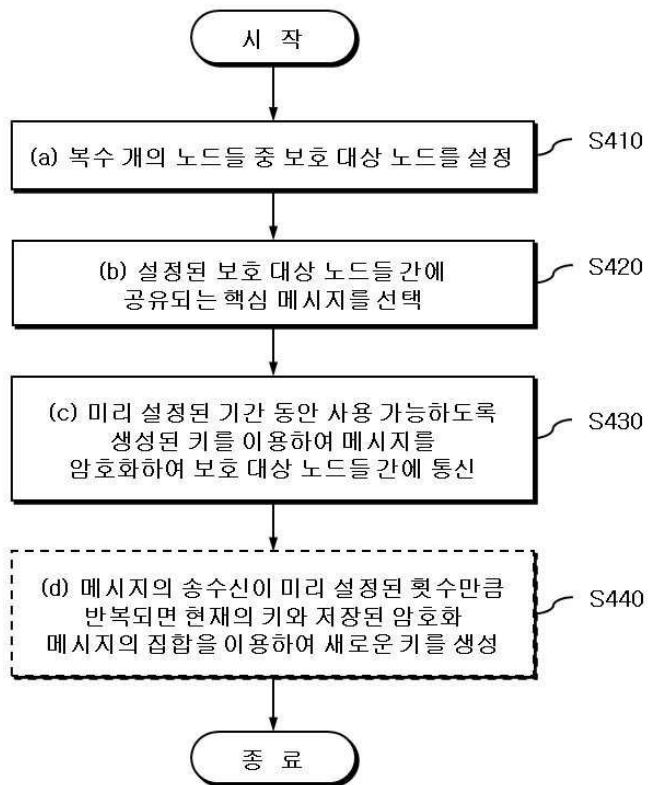
도면2



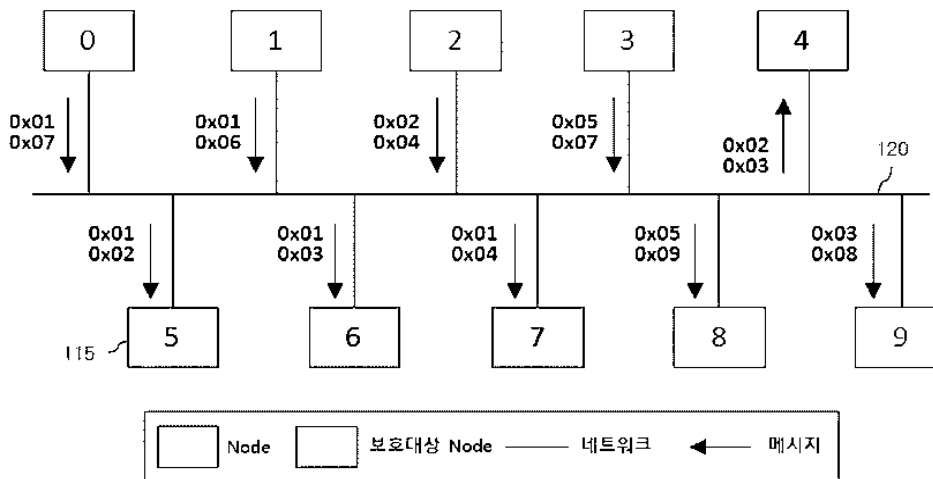
도면3



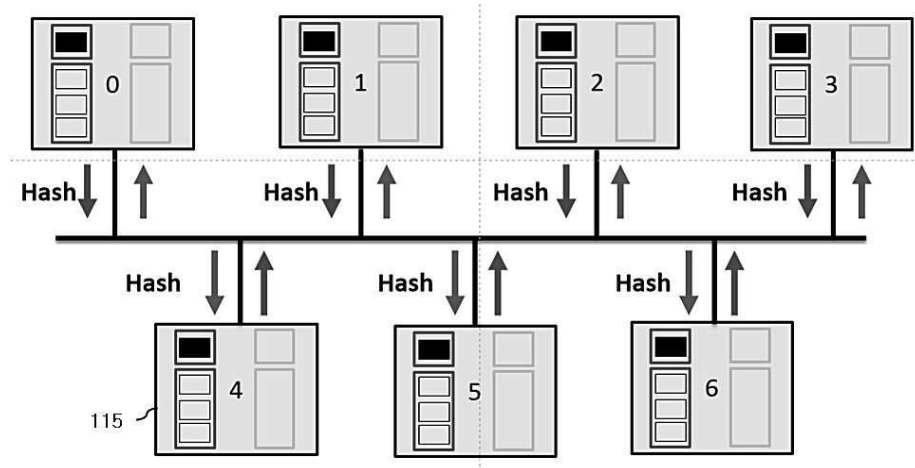
도면4



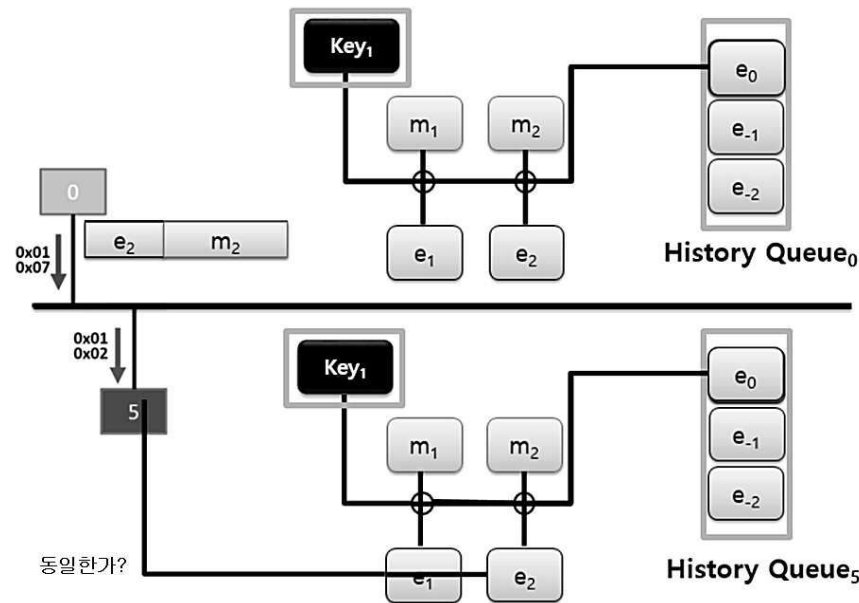
도면5



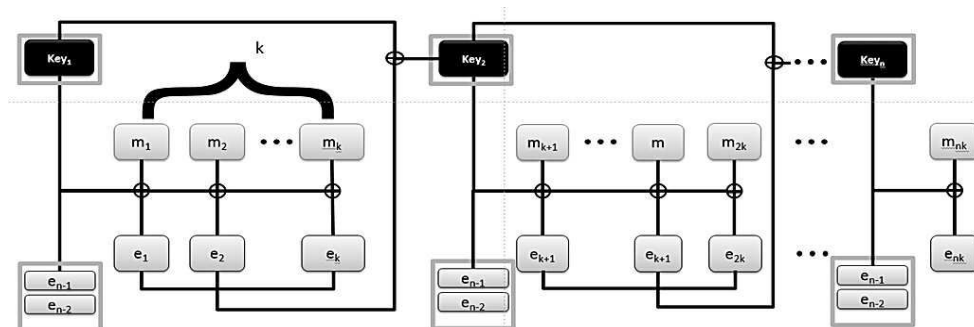
도면6



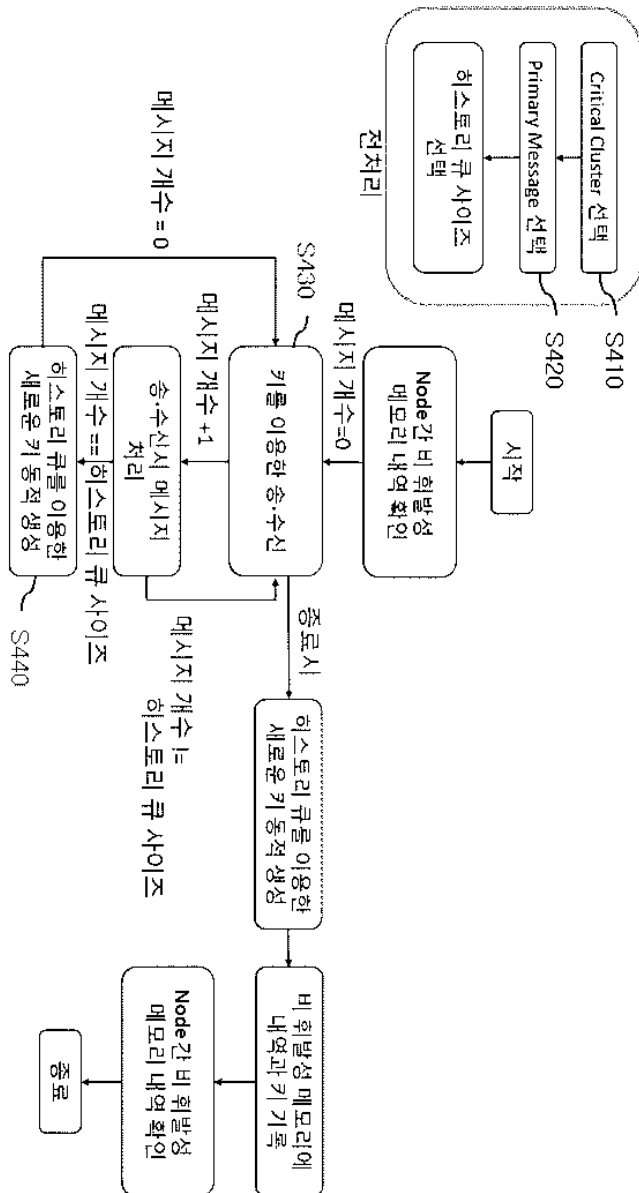
도면7



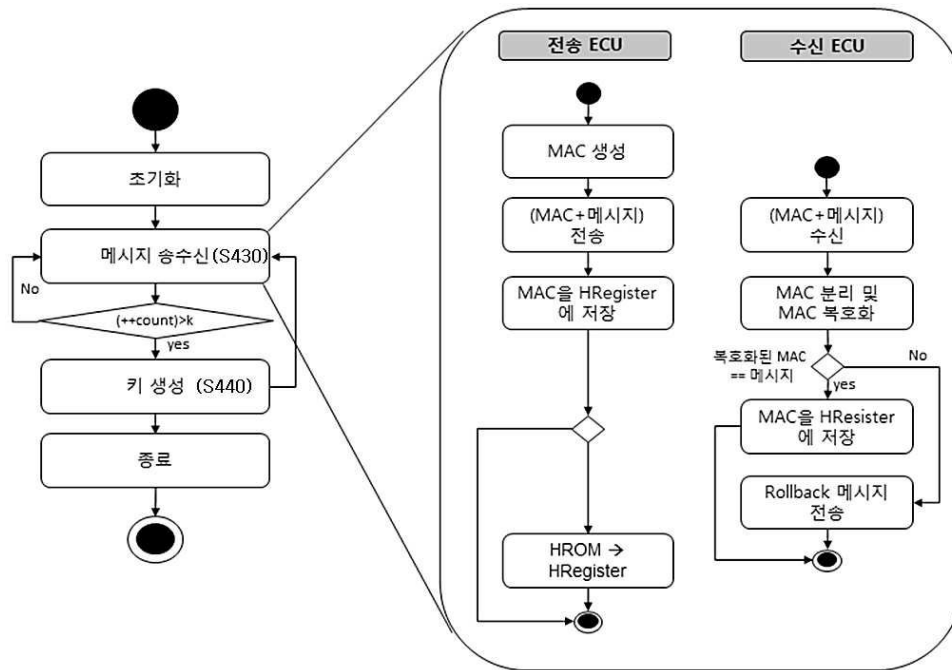
도면8



도면9



도면10



도면11

