(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0097397
(43) 공개일자 2023년07월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06F 11/07* (2006.01)
G06F 21/55 (2013.01) *H04L 12/40* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 63/14 (2013.01)
G06F 11/0757 (2013.01)
(21) 출원번호 10-2021-0186865
(22) 출원일자 2021년12월24일
심사청구일자 없음

(71) 출원인
현대모비스 주식회사
서울특별시 강남구 테헤란로 203 (역삼동)
(72) 발명자
이재영
경기도 용인시 기흥구 마북로240번길 17-2
(74) 대리인
특허법인아주

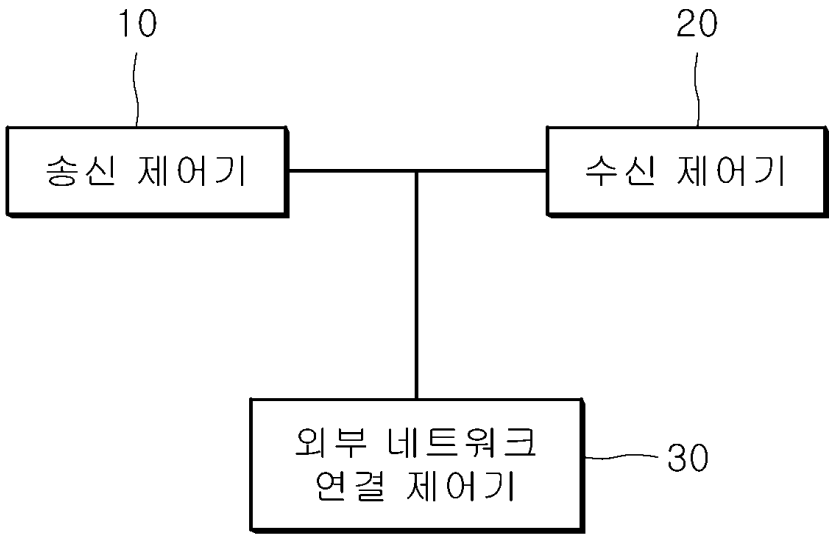
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **차량 네트워크 침입 탐지 시스템 및 그 방법**

(57) 요 약

본 발명은 차량 네트워크 침입 탐지 시스템 및 그 방법이 개시된다. 본 발명의 차량 네트워크 침입 탐지 시스템은, 차량 네트워크를 통해 암호 처리 요청 메시지를 송신하고 수신된 암호 처리 응답 메시지를 통해 외부 침입을 판단하는 송신 제어기; 및 송신 제어기로부터 암호 처리 요청 메시지를 수신하여 암호 처리를 수행한 결과와 외부 네트워크 연결 제어기 내부에서 침입을 감지하는 SW 와치독의 밸리데이트(validate)를 수행한 결과를 기반으로 암호 처리 응답 메시지를 생성하여 송신 제어기로 전송하는 수신 제어기;를 포함하는 것을 특징으로 한다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/55 (2013.01)
H04L 12/40013 (2013.01)
H04L 12/40104 (2013.01)
H04L 63/1408 (2013.01)
H04L 9/0869 (2013.01)
H04L 2209/84 (2013.01)

명 세 서

청구범위

청구항 1

차량 네트워크를 통해 암호 처리 요청 메시지를 송신하고 수신된 암호 처리 응답 메시지를 통해 외부 침입을 판단하는 송신 제어기; 및

상기 송신 제어기로부터 상기 암호 처리 요청 메시지를 수신하여 암호 처리를 수행한 결과와 외부 네트워크 연결 제어기 내부에서 침입을 감지하는 SW 와치독의 밸리데이트(validate)를 수행한 결과를 기반으로 상기 암호 처리 응답 메시지를 생성하여 상기 송신 제어기로 전송하는 수신 제어기;를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 2

제 1항에 있어서, 상기 암호 처리 요청 메시지는, 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함하고,

상기 암호 처리 응답 메시지는, 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 3

제 2항에 있어서, 상기 수신 제어기는, 상기 암호 처리 요청 메시지를 수신하여 메시지 수신 대상을 확인한 후 상기 암호 알고리즘에 따라 상기 시드값에 대해 암호 처리를 수행하고, 상기 SW 와치독의 밸리데이트를 수행하여 상기 제어기의 상태를 확인한 후 상기 암호 처리 응답 메시지를 생성하여 상기 송신 제어기로 전송하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 4

제 2항에 있어서, 상기 송신 제어기는, 상기 암호 처리 요청 메시지의 상기 암호 알고리즘과 상기 시드값을 기반으로 예상결과를 생성하여 브로드캐스팅한 후 수신된 상기 암호 처리 응답 메시지를 통해 응답시간, 시드값 처리 결과 및 상기 제어기의 상태를 기반으로 상기 수신 제어기의 제어권 상실여부를 판단하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 5

제 4항에 있어서, 상기 송신 제어기는, 응답시간이 설정시간을 초과하거나 상기 시드값 처리결과가 상기 예상결과와 다른 경우 상기 수신 제어기의 전체 제어권 상실로 판단하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 6

제 5항에 있어서, 상기 송신 제어기는, 상기 수신 제어기의 전체 제어권 상실로 판단한 경우 해당 수신 제어기와 통신신호를 사용하지 않는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 7

제 5항에 있어서, 상기 송신 제어기는, 응답시간이 설정시간 이내 수신되고, 상기 시드값 처리결과가 상기 예상 결과와 동일하나 상기 제어기의 상태가 정상이 아닌 경우, 상기 수신 제어기의 일부 제어권 상실로 판단하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 8

제 7항에 있어서, 상기 송신 제어기는, 상기 수신 제어기의 일부 제어권 상실로 판단한 경우, 해당 수신 제어기로 전달하는 신호는 사용하고 해당 수신 제어기로부터 수신되는 신호를 사용하지 않는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 9

제 1항에 있어서, 상기 수신 제어기는, 상기 차량 네트워크로부터 메시지가 수신된 경우, 현재 상태가 송신상태인지 판단하여 수신된 수신 메시지 ID와 상기 수신 제어기의 송신 메시지 ID와의 동일여부를 판단하여 NM(Network Management) 메시지의 제어기 상태를 업데이트하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 10

제 9항에 있어서, 상기 수신 제어기는, 현재 상태가 송신상태가 아닌 경우 상기 수신 메시지 ID와 상기 송신 메시지 ID가 동일하면 상기 NM(Network Management) 메시지의 제어기 상태에 외부침입으로 업데이트하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 11

제 9항에 있어서, 상기 NM 메시지는, 수신제어기, 명령어, 슬립 진입 여부 및 제어기 상태를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 시스템.

청구항 12

수신 제어기가 차량 네트워크를 통해 송신 제어기로부터 암호 처리 요청 메시지를 수신받아 수신 대상을 판단하는 단계;

상기 수신 제어기가 상기 수신 대상이 일치할 경우, 암호 알고리즘에 따라 시드값에 대해 암호 처리를 수행하는 단계;

상기 수신 제어기가 암호 처리를 수행한 후 외부 네트워크 연결 제어기 내부에서 침입을 감지하는 SW 와치독의 밸리데이트(validate)를 수행하여 제어기 상태를 확인하는 단계; 및

상기 수신 제어기가 상기 시드값에 대해 암호 처리를 수행한 결과와 제어기 상태를 확인한 결과를 기반으로 암호 처리 응답 메시지를 생성하여 전송하는 단계;를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

청구항 13

제 12항에 있어서, 상기 암호 처리 요청 메시지는, 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함하고,

상기 암호 처리 응답 메시지는, 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

청구항 14

송신 제어기가 암호 처리 요청 메시지의 암호 알고리즘과 시드값을 기반으로 예상결과를 생성하여 차량 네트워크로 브로드캐스팅하는 단계;

상기 송신 제어기가 수신 제어기로부터 상기 암호 처리 응답 메시지를 수신하여 응답시간이 설정시간을 초과하는지 판단하는 단계;

상기 송신 제어기가 상기 응답시간이 설정시간을 초과하는지 판단하여 상기 설정시간을 초과한 경우, 상기 수신 제어기의 전체 제어권 상실로 판단하는 단계;

상기 송신 제어기가 상기 응답 시간이 설정시간을 초과하는지 판단하여 상기 설정시간 이하인 경우, 상기 암호 처리 응답 메시지의 시드값 처리결과를 판단하는 단계;

상기 송신 제어기가 상기 시드값 처리결과를 판단하여 상기 시드값 처리결과가 상기 예상결과와 동일하지 않은 경우, 상기 수신 제어기의 전체 제어권 상실로 판단하는 단계;

상기 송신 제어기가 상기 시드값 처리결과를 판단하여 상기 시드값 처리결과가 상기 예상결과와 동일한 경우, 상기 암호 처리 응답 메시지의 제어기 상태를 판단하는 단계; 및

상기 송신 제어기가 상기 제어기 상태를 판단하여 정상이 아닌 경우, 상기 수신 제어기의 일부 제어권 상실로 판단하는 단계;를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

청구항 15

제 14항에 있어서, 상기 수신 제어기의 전체 제어권 상실로 판단하는 단계는, 상기 송신 제어기가 해당 수신 제어기와 통신신호를 사용하지 않는 단계;를 더 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

청구항 16

제 15항에 있어서, 상기 수신 제어기의 일부 제어권 상실로 판단하는 단계는, 상기 송신 제어기가 해당 수신 제어기로 전달하는 신호는 사용하고 해당 수신 제어기로부터 수신되는 신호를 사용하지 않는 단계;를 더 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

청구항 17

제 14항에 있어서, 상기 암호 처리 요청 메시지는, 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함하고,

상기 암호 처리 응답 메시지는, 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

청구항 18

수신 제어기가 차량 네트워크를 통해 수신 메시지를 수신하는 단계;

상기 수신 제어기가 현재 상태가 송신상태인지 판단하는 단계;

상기 수신 제어기가 상기 현재 상태가 송신 상태인지 판단하여 상기 송신상태가 아닌 경우, 수신 메시지 ID와 상기 수신 제어기의 송신 메시지 ID의 동일여부를 판단하는 단계; 및

상기 수신 제어기가 송신 메시지 ID의 동일여부를 판단하여 NM(Network Management) 메시지의 제어기 상태를 업데이트하는 단계;를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

청구항 19

제 18항에 있어서, 상기 제어기 상태를 업데이트하는 단계는, 상기 수신 메시지 ID와 상기 송신 메시지 ID가 동일한 경우, 상기 수신 제어기가 상기 NM(Network Management) 메시지의 상기 제어기 상태에 외부침입으로 업데이트하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

청구항 20

제 18항에 있어서, 상기 NM 메시지는, 수신제어기, 명령어, 슬립 진입 여부 및 제어기 상태를 포함하는 것을 특징으로 하는 차량 네트워크 침입 탐지 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 차량 네트워크 침입 탐지 시스템 및 그 방법에 관한 것으로서, 보다 상세하게는 외부 네트워크와 연결된 제어기에서 제어기 간 송수신되는 메시지를 기반으로 제어권의 상실 여부를 판단하여 차량 네트워크의 침입을 탐지하는 차량 네트워크 침입 탐지 시스템 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로, 차량은 다수의 제조업체에서 제작된 부품들이 조립되어 만들어지기 때문에 다양한 SW 개발 방법으로 만들어진 기능들이 호환되도록 제어기 사이에 약한 연결 관계를 갖는다. 또한 실시간 제어를 위하여 제어기 사이에 전송하는 데이터를 고도로 암호화하기 어렵기 때문에 쉽게 해킹의 위험에 노출될 수 있다. 더욱이 차량의 기능이 고도화 되면서 무선 통신망을 통하여 외부 네트워크에 접속함에 따라 사이버 보안의 중요성은 더욱 더 커지고 있다.

[0003] 차량용 제어기는 외부 침입에 대하여 강건성을 확보하기 위하여 HSM(Hardware Security Module)이 적용된 MCU(Micro Controller Unit)/AP(Application Processor)등을 사용하여 secure boot나 secure flash 기능을 구현한다. Secure boot는 firmware 영역을 SHA-256 등의 방법을 사용하여 검사함으로써 변경이 없을 때에만 boot를 시작하며, secure flash는 인증된 장비나 사용자만 flash write가 가능하도록 함으로써 침입자에 의하여 비휘발성 메모리(non-volatile memory) 영역 변경을 할 수 없도록 한다.

[0004] 외부 침입자의 공격에 의하여 제어기 동작 제어권을 빼앗겼을 경우, 침입자의 SW는 휘발성 메모리(volatile memory) 영역에 존재하게 된다. 따라서 제어기에 전원이 유지되는 상황에서는 침입자에 의하여 차량 내부 망에 잘못된 데이터가 전송되어 차량이 악의적으로 제어될 수 있다. 제어권을 빼앗긴 제어기가 전송 주기가 짧은 메시지를 전송하여 차량 제어를 정상적으로 수행하지 못하게 하는 것은 약속된 주기가 아닌 메시지를 검출만 하면 되므로 검출이 쉽다.

[0005] 하지만 외부 네트워크와 직접 연결되어 있는 CCU(Central Communication Unit)의 제어권을 빼앗겼을 경우, 게이트웨이(gateway) 과정에서 이상 데이터를 전송하게 되므로 차량 내부 다른 망에 연결된 제어기에 잘못된 정보를 송신하여 차량이 이상 제어될 수 있다. 특히 이더넷으로 연결된 제어기는 스위치와 1대 1로 연결되어 있으므로, 스위치가 장착된 CCU의 제어권을 빼앗겼을 경우 통신을 통한 입력 정보를 믿을 수 없게 된다.

[0006] 이에, 차량이 외부 네트워크에 연결되면서 악의적인 외부 침입을 방지하기 위하여 사이버 보안이 강조되고 있다. 하지만 차량에 적용된 사이버 보안 대응 방법은 비휘발성 메모리(non-volatile memory)나 이상 주기를 갖는 신호 탐지에 국한되어 있으므로 외부 침입자의 공격에 의하여 휘발성 메모리(volatile memory) 영역 침입 감지에는 취약하다. 이로 인해 제어기의 동작 중에 외부 침입자에 의하여 차량 내부 망에 잘못된 데이터가 전송되어 차량이 악의적으로 제어되는 문제가 발생한다.

[0007] 본 발명의 배경기술은 대한민국 공개특허공보 제10-2021-0075386호(2021.06.23. 공개, 차량 네트워크에 대한 경량화된 침입탐지 방법 및 장치)에 개시되어 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 상기와 같은 문제점들을 개선하기 위하여 안출된 것으로, 일 측면에 따른 본 발명의 목적은 외부 네트워크와 연결된 제어기에서 제어기 간 송수신되는 메시지를 기반으로 제어권의 상실 여부를 판단하여 차량 네트워크의 침입을 탐지하는 차량 네트워크 침입 탐지 시스템 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 일 측면에 따른 차량 네트워크 침입 탐지 시스템은, 차량 네트워크를 통해 암호 처리 요청 메시지를 송신하고 수신된 암호 처리 응답 메시지를 통해 외부 침입을 판단하는 송신 제어기; 및 송신 제어기로부터 암호 처리 요청 메시지를 수신하여 암호 처리를 수행한 결과와 외부 네트워크 연결 제어기 내부에서 침입을 감지하는 SW 와치독의 밸리데이트(validate)를 수행한 결과를 기반으로 암호 처리 응답 메시지를 생성하여 송신 제어기로 전송하는 수신 제어기;를 포함하는 것을 특징으로 한다.

[0010] 본 발명에서 암호 처리 요청 메시지는, 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함하고, 암호 처리 응답 메시지는, 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함하는 것을 특징으로 한다.

[0011] 본 발명에서 수신 제어기는, 암호 처리 요청 메시지를 수신하여 메시지 수신 대상을 확인한 후 암호 알고리즘에 따라 시드값에 대해 암호 처리를 수행하고, SW 와치독의 밸리데이트를 수행하여 제어기의 상태를 확인한 후 암호 처리 응답 메시지를 생성하여 송신 제어기로 전송하는 것을 특징으로 한다.

[0012] 본 발명에서 송신 제어기는, 암호 처리 요청 메시지의 암호 알고리즘과 시드값을 기반으로 예상결과를 생성하여 브로드캐스팅한 후 수신된 암호 처리 응답 메시지를 통해 응답시간, 시드값 처리 결과 및 제어기의 상태를 기반으로 수신 제어기의 제어권 상실여부를 판단하는 것을 특징으로 한다.

[0013] 본 발명에서 송신 제어기는, 응답시간이 설정시간을 초과하거나 시드값 처리결과가 예상결과와 다른 경우, 수신 제어기의 전체 제어권 상실로 판단하는 것을 특징으로 한다.

[0014] 본 발명에서 송신 제어기는, 수신 제어기의 전체 제어권 상실로 판단한 경우 해당 수신 제어기와 통신신호를 사용하지 않는 것을 특징으로 한다.

[0015] 본 발명에서 송신 제어기는, 응답시간이 설정시간 이내 수신되고, 시드값 처리결과가 예상결과와 동일하나 제어기의 상태가 정상이 아닌 경우, 수신 제어기의 일부 제어권 상실로 판단하는 것을 특징으로 한다.

[0016] 본 발명에서 송신 제어기는, 수신 제어기의 일부 제어권 상실로 판단한 경우, 해당 수신 제어기로 전달하는 신호는 사용하고 해당 수신 제어기로부터 수신되는 신호를 사용하지 않는 것을 특징으로 한다.

[0017] 본 발명에서 수신 제어기는, 차량 네트워크로부터 메시지가 수신된 경우, 현재 상태가 송신상태인지 판단하여 수신된 수신 메시지 ID와 수신 제어기의 송신 메시지 ID와의 동일여부를 판단하여 NM(Network Management) 메시지의 제어기 상태를 업데이트하는 것을 특징으로 한다.

[0018] 본 발명에서 수신 제어기는, 현재 상태가 송신상태가 아닌 경우, 수신 메시지 ID와 송신 메시지 ID가 동일하면 NM(Network Management) 메시지의 제어기 상태에 외부침입으로 업데이트하는 것을 특징으로 한다.

[0019] 본 발명에서 NM 메시지는, 수신제어기, 명령어, 슬립 진입 여부 및 제어기 상태를 포함하는 것을 특징으로 한다.

[0020] 본 발명의 다른 측면에 따른 차량 네트워크 침입 탐지 방법은, 수신 제어기가 차량 네트워크를 통해 송신 제어기로부터 암호 처리 요청 메시지를 수신받아 수신 대상을 판단하는 단계; 수신 제어기가 수신 대상이 일치할 경우, 암호 알고리즘에 따라 시드값에 대해 암호 처리를 수행하는 단계; 수신 제어기가 암호 처리를 수행한 후 외부 네트워크 연결 제어기 내부에서 침입을 감지하는 SW 와치독의 밸리데이트(validate)를 수행하여 제어기 상태를 확인하는 단계; 및 수신 제어기가 시드값에 대해 암호 처리를 수행한 결과와 제어기 상태를 확인한 결과를 기반으로 암호 처리 응답 메시지를 생성하여 전송하는 단계;를 포함하는 것을 특징으로 한다.

[0021] 본 발명에서 암호 처리 요청 메시지는, 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함하고, 암호 처리 응답 메시지는, 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함하는 것을 특징으로 한다.

[0022] 본 발명의 또 다른 측면에 따른 차량 네트워크 침입 탐지 방법은, 송신 제어기가 암호 처리 요청 메시지의 암호 알고리즘과 시드값을 기반으로 예상결과를 생성하여 차량 네트워크로 브로드캐스팅하는 단계; 송신 제어기가 수신 제어기로부터 암호 처리 응답 메시지를 수신하여 응답시간이 설정시간을 초과하는지 판단하는 단계; 송신 제어기가 응답시간이 설정시간을 초과하는지 판단하여 설정시간을 초과한 경우, 수신 제어기의 전체 제어권 상실로 판단하는 단계; 송신 제어기가 응답 시간이 설정시간을 초과하는지 판단하여 설정시간 이하인 경우, 암호 처리 응답 메시지의 시드값 처리결과를 판단하는 단계; 송신 제어기가 시드값 처리결과를 판단하여 시드값 처리결과가 예상결과와 동일하지 않은 경우, 수신 제어기의 전체 제어권 상실로 판단하는 단계; 송신 제어기가 시드값 처리결과를 판단하여 시드값 처리결과가 예상결과와 동일한 경우, 암호 처리 응답 메시지의 제어기 상태를 판단하는 단계; 및 송신 제어기가 제어기 상태를 판단하여 정상이 아닌 경우, 수신 제어기의 일부 제어권 상실로 판단하는 단계;를 포함하는 것을 특징으로 한다.

[0023] 본 발명에서 수신 제어기의 전체 제어권 상실로 판단하는 단계는, 송신 제어기가 해당 수신 제어기와 통신신호를 사용하지 않는 단계;를 더 포함하는 것을 특징으로 한다.

[0024] 본 발명에서 수신 제어기의 일부 제어권 상실로 판단하는 단계는, 송신 제어기가 해당 수신 제어기로 전달하는 신호는 사용하고 해당 수신 제어기로부터 수신되는 신호를 사용하지 않는 단계;를 더 포함하는 것을 특징으로 한다.

[0025] 본 발명에서 암호 처리 요청 메시지는, 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함하고, 암호 처리 응답 메시지는, 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함하는 것을 특징으로 한다.

[0026] 본 발명의 또 다른 측면에 따른 차량 네트워크 침입 탐지 방법은, 수신 제어기가 차량 네트워크를 통해 수신 메시지를 수신하는 단계; 수신 제어기가 현재 상태가 송신 상태인지 판단하는 단계; 수신 제어기가 현재 상태가 송신 상태인지 판단하여 송신상태가 아닌 경우, 수신 메시지 ID와 수신 제어기의 송신 메시지 ID의 동일여부를 판단하는 단계; 및 수신 제어기가 송신 메시지 ID의 동일여부를 판단하여 NM(Network Management) 메시지의 제어기 상태를 업데이트하는 단계;를 포함하는 것을 특징으로 한다.

[0027] 본 발명에서 제어기 상태를 업데이트하는 단계는, 수신 메시지 ID와 송신 메시지 ID가 동일한 경우, 수신 제어기가 NM(Network Management) 메시지의 제어기 상태에 외부침입으로 업데이트하는 것을 특징으로 한다.

[0028] 본 발명에서 NM 메시지는, 수신제어기, 명령어, 슬립 진입 여부 및 제어기 상태를 포함하는 것을 특징으로 한다.

발명의 효과

[0029] 본 발명의 일 측면에 따른 차량 네트워크 침입 탐지 시스템 및 그 방법은 외부 네트워크와 연결된 제어기에서 제어기 간 송수신되는 메시지를 기반으로 제어권의 상실 여부를 판단하여 차량 네트워크의 침입을 탐지함으로써, 외부 침입자의 SW가 휘발성 메모리(volatile memory)에 상주하는 경우도 감지 가능하므로 외부 침입에 강건한 차량 네트워크를 구성할 수 있을 뿐만 아니라 외부 침입에 의하여 이상 동작한 경우나 SW 버그 등에 의한 이상 동작도 모니터링 가능하므로 최근 점점 더 복잡해지는 차량용 SW 생태계에서 필수적인 고장 감지 및 해결 방법이 될 수 있다.

도면의 간단한 설명

[0030] 도 1은 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 시스템을 나타낸 블록 구성도이다.

도 2는 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 시스템에서의 암호 처리 요청 메시지와 암호 처리 응답 메시지 구조를 나타낸 도면이다.

도 3은 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 시스템에서의 NM 메시지 구조를 나타낸 도면이다.

도 4는 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 방법에서 수신 제어기의 암호 처리 방법을 설명하기 위한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 방법에서 송신 제어기의 침입 상태 판단 과정을 설명하기 위한 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 방법에서 수신 제어기의 통신망 감시 과정을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 이하, 첨부된 도면들을 참조하여 본 발명에 따른 차량 네트워크 침입 탐지 시스템 및 그 방법을 설명한다. 이 과정에서 도면에 도시된 선들의 두께나 구성요소의 크기 등은 설명의 명료성과 편의상 과장되게 도시되어 있을 수 있다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례에 따라 달라질 수 있다. 그러므로 이러한 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0032] 도 1은 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 시스템을 나타낸 블록 구성도이고, 도 2는 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 시스템에서의 암호 처리 요청 메시지와 암호 처리 응답 메시지 구조를 나타낸 도면이며, 도 3은 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 시스템에서의 NM 메시지 구조를 나타낸 도면이다.

[0033] 도 1에 도시된 바와 같이 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 시스템은, 송신 제어기(10) 및 수신 제어기(20)를 포함할 수 있다.

[0034] 외부 네트워크와 연결된 외부 네트워크 연결 제어기(30) 내부에서 SW 와치독을 사용하여 침입을 감지하였을 때, 통신을 사용하여 차량 내부의 제어기들에게 알려야 한다. 이때 통신과 같이 외부와 연결된 채널은 침입자에 의하여 감지 및 변조될 수 있으므로 암호화 절차가 필요하다.

[0035] 따라서 본 실시예에서는 다수의 암호와 알고리즘을 사용하여 차량 내부의 송신 제어기(10)와 수신 제어기(20)들이 전체 처리에 영향을 주지 않을 정도의 긴 주기를 가지고 통신 기반으로 암호 처리 요청 메시지와 암호 처리 응답 메시지를 송수신하여 외부 침입을 감지할 수 있다.

[0036] 송신 제어기(10)는 차량 네트워크를 통해 암호 처리 요청 메시지를 송신하고 수신된 암호 처리 응답 메시지를 통해 외부 침입을 판단할 수 있다.

[0037] 또한, 수신 제어기(20)는 송신 제어기(10)로부터 암호 처리 요청 메시지를 수신하여 암호 처리를 수행한 결과와 외부 네트워크 연결 제어기(30) 내부에서 침입을 감지하는 SW 와치독의 밸리데이트(validate)를 수행한 결과를 기반으로 암호 처리 응답 메시지를 생성하여 송신 제어기(10)로 전송할 수 있다.

[0038] 여기서, 암호 처리 요청 메시지는 도 2의 (a)와 같이 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함하고, 암호 처리 응답 메시지는 도 2의 (b)와 같이 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함할 수 있다.

[0039] 이와 같이 송신 제어기(10)와 수신 제어기(20)간 통신 기반으로 외부 침입을 판단할 수 있다. 이를 보다 구체적으로 설명하면 다음과 같다.

[0040] 먼저, 수신 제어기(20)는 암호 처리 요청 메시지를 수신하여 메시지 수신 대상을 확인한 후 암호 알고리즘에 따라 시드값에 대해 암호 처리를 수행할 수 있다.

[0041] 그리고, 수신 제어기(20)는 외부 네트워크 연결 제어기(30) 내부에서 침입을 감지하는 SW 와치독의 밸리데이트를 수행하여 제어기의 상태를 확인한 후 암호 처리한 암호 알고리즘 선택, 시드값에 대한 암호 처리결과 및 제어기의 상태를 포함하는 암호 처리 응답 메시지를 생성하여 송신 제어기(10)로 전송할 수 있다.

[0042] 다음으로 송신 제어기(10)는 암호 처리 요청 메시지의 암호 알고리즘과 시드값을 기반으로 예상결과를 생성하여 암호 처리 요청 메시지를 브로드캐스팅한다.

[0043] 이후 차량 네트워크를 통해 수신된 암호 처리 응답 메시지를 통해 응답시간, 시드값 처리 결과 및 제어기의 상태를 기반으로 수신 제어기(20)의 제어권 상실여부를 판단할 수 있다.

[0044] 보다 구체적으로 송신 제어기(10)는 응답시간이 설정시간을 초과하거나 시드값 처리결과가 예상결과와 다른 경우, 수신 제어기(20)의 전체 제어권이 상실된 것으로 판단할 수 있다.

[0045] 이와 같이 수신 제어기(20)의 전체 제어권이 상실된 것으로 판단할 경우, 송신 제어기(10)는 해당 수신 제어기(20)와 통신신호를 사용하지 않는다.

[0046] 또한, 송신 제어기(10)는 응답시간이 설정시간 이내 수신되고, 시드값 처리결과가 예상결과와 동일하나 제어기의 상태가 정상이 아닌 경우, 수신 제어기(20)의 일부 제어권 상실로 판단할 수 있다.

[0047] 이렇게 수신 제어기(20)의 일부 제어권 상실로 판단한 경우, 송신 제어기(10)는 해당 수신 제어기(20)로 전달하는 신호는 사용하지만, 해당 수신 제어기(20)로부터 수신되는 신호는 사용하지 않는다.

[0048] 한편, 통신망을 상호 감시하여 네트워크 침입을 감지할 수 있다.

[0049] 차량 내부 통신에서 정해진 ID는 약속된 제어기만 송신해야 한다. 이때 차량 내부 통신은 CAN/CANFD와 같이 버스로 구성된 경우가 많으므로 외부 침입에 의하여 특정 제어기의 제어권이 빼앗긴 경우, 잘 알려진 ID의 메시지를 짧은 주기로 송신하게 되면, 내부 망에 연결된 모든 제어기에 잘못된 정보를 전달 할 수 있다.

[0050] 예를 들어, 휠 속도 정보가 담긴 ID를 원래 주기보다 1/10 간격으로 값을 0으로 넣어서 통신망에 송신하면, 내부 제어기는 차가 달리고 있음에도 정차된 것으로 판단 할 수 있다.

[0051] 따라서 각 제어기가 송신하지 않을 때, 제어기가 송신해야 할 신호가 수신된다면 통신망에 침입자가 있는 것으로 판단할 수 있다.

[0052] 이와 같이 수신 제어기(20)는 차량 네트워크로부터 메시지가 수신된 경우, 현재 상태가 송신상태인지 판단하여 수신된 수신 메시지 ID와 수신 제어기의 송신 메시지 ID와의 동일여부를 판단하여 NM(Network Management) 메시지의 제어기 상태를 업데이트함으로써 통신망의 침입을 감지할 수 있다.

[0053] 이때 NM 메시지 구조는 도 3에 도시된 바와 같이 수신제어기, 명령어, 슬립 진입 여부 및 제어기 상태를 포함할 수 있다.

[0054] 여기서, 수신 제어기(20)는 현재 상태가 송신상태가 아닌 경우, 수신 메시지 ID와 송신 메시지 ID가 동일하면 NM(Network Management) 메시지의 제어기 상태에 외부침입으로 업데이트하여 자신이 송신할 신호를 생성하는 제어기가 있음을 통신망에 연결된 다른 제어기에 알림으로써 침입에 강건한 통신망을 구성할 수 있다.

[0055] 상술한 바와 같이, 본 발명의 실시예에 의한 차량 네트워크 침입 탐지 시스템에 따르면, 외부 네트워크와 연결된 제어기에서 제어기 간 송수신되는 메시지를 기반으로 제어권의 상실 여부를 판단하여 차량 네트워크의 침입을 탐지함으로써, 외부 침입자의 SW가 휘발성 메모리(volatile memory)에 상주하는 경우도 감지 가능하므로 외부 침입에 강건한 차량 네트워크를 구성할 수 있을 뿐만 아니라 외부 침입에 의하여 이상 동작한 경우나 SW 버그 등에 의한 이상 동작도 모니터링 가능하므로 최근 점점 더 복잡해지는 차량용 SW 생태계에서 필수적인 고장 감지 및 해결 방법이 될 수 있다.

[0056] 도 4는 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 방법에서 수신 제어기의 암호 처리 방법을 설명하기 위한 흐름도이다.

[0057] 도 4에 도시된 바와 같이 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 방법에서는 먼저, 수신 제어기(20)가 차량 네트워크를 통해 송신 제어기(10)로부터 암호 처리 요청 메시지를 수신 받는다(S10).

[0058] 여기서, 암호 처리 요청 메시지는 도 2의 (a)와 같이 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함할 수 있다.

[0059] S10 단계에서 암호 처리 요청 메시지를 수신 받은 후 수신 제어기(20)는 암호 처리 요청 메시지에서 메시지 수신 대상을 확인하여 수신 대상이 맞는지 판단한다(S20).

[0060] S20 단계에서 수신 대상이 맞는지 판단하여 수신 대상이 맞는 경우, 수신 제어기(20)는 암호 처리 요청 메시지의 암호 알고리즘 선택에 따라 선택된 암호 알고리즘으로 시드값에 대해 암호 처리를 수행한다(S30).

[0061] S30 단계에서 시드값에 대해 암호 처리를 수행한 후 수신 제어기(20)는 외부 네트워크 연결 제어기(30) 내부에서 침입을 감지하는 SW 와치독의 밸리데이트(validate)를 수행하여 제어기 상태를 확인한다(S40).

[0062] S40 단계에서 제어기 상태를 확인한 후 수신 제어기(20)는 암호 처리 요청 메시지에 따라 암호화 알고리즘으로 시드값에 대해 암호화한 결과와 제어기 상태를 확인한 결과를 기반으로 암호 처리 응답 메시지를 생성하여 송신 제어기(10)로 전송한다(S50).

[0063] 여기서, 암호 처리 응답 메시지는 도 2의 (b)와 같이 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함할 수 있다.

[0064] 도 5는 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 방법에서 송신 제어기의 침입 상태 판단 과정을 설명하기 위한 흐름도이다.

[0065] 도 5에 도시된 바와 같이 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 방법에서는 먼저, 송신 제어기(10)가 암호 처리 요청 메시지의 암호 알고리즘과 시드값을 기반으로 예상결과를 생성한다(S110).

[0066] S110 단계에서 예상결과를 생성한 후 송신 제어기(10)는 적용한 암호 알고리즘 선택과 시드값을 포함하는 암호 처리 요청 메시지를 차량 네트워크로 브로드캐스팅한다(S120).

[0067] 여기서, 암호 처리 요청 메시지는 도 2의 (a)와 같이 메시지 수신 대상, 암호 처리를 수행할 암호 알고리즘 선택 및 암호 처리할 시드값(seed)을 포함할 수 있다.

[0068] S120 단계에서 암호 처리 요청 메시지를 브로드캐스팅한 후 송신 제어기(10)는 수신 제어기(20)로부터 암호 처리 응답 메시지를 수신한다(S130).

[0069] S130 단계에서 암호 처리 응답 메시지를 수신한 후 송신 제어기(10)는 응답시간이 설정시간을 초과하는지 판단한다(S140).

[0070] S140 단계에서 응답시간이 설정시간을 초과하는지 판단하여 초과하는 경우, 송신 제어기(10)는 수신 제어기(20)의 전체 제어권이 상실된 것으로 판단한다(S170).

[0071] S170 단계에서 수신 제어기(20)의 전체 제어권이 상실된 것으로 판단한 경우, 송신 제어기(10)는 해당 수신 제어기(20)와 통신신호를 사용하지 않도록 한다(S180).

[0072] 한편, S140 단계에서 응답시간이 설정시간을 초과하는지 판단하여 초과하지 않는 경우, 송신 제어기(10)는 암호 처리 응답 메시지로부터 시드값 처리결과를 확인하여 예상결과와 동일한지 비교한다(S150).

[0073] 여기서, 암호 처리 응답 메시지는 도 2의 (b)와 같이 메시지 수신 대상, 암호 처리를 수행한 암호 알고리즘 선택, 시드값에 대한 암호 처리 결과 및 제어기의 상태를 포함할 수 있다.

[0074] S150 단계에서 시드값 처리결과와 예상결과를 비교하여 동일하지 않은 경우, 송신 제어기(10)는 수신 제어기(20)의 전체 제어권이 상실된 것으로 판단한다(S170).

[0075] 반면, S150 단계에서 시드값 처리결과와 예상결과를 비교하여 동일한 경우, 송신 제어기(10)는 암호 처리 응답 메시지로부터 제어기 상태를 확인하여 정상인지 판단한다(S160).

[0076] S160 단계에서 제어기 상태를 확인하여 정상인 경우, 송신 제어기(10)는 수신 제어기(20)를 정상으로 판단한다(S210).

[0077] 반면, S160 단계에서 제어기 상태를 확인하여 정상이 아닌 경우, 송신 제어기(10)는 수신 제어기(20)의 일부 제어권 상실로 판단한다(S190).

[0078] S190 단계에서 수신 제어기(20)의 일부 제어권 상실로 판단한 경우, 송신 제어기(10)는 해당 수신 제어기로 전달하는 신호는 사용하지만, 해당 수신 제어기로부터 수신되는 신호를 사용하지 않는다(S200).

[0079] 도 6은 본 발명의 일 실시예에 따른 차량 네트워크 침입 탐지 방법에서 수신 제어기의 통신망 감시 과정을 설명하기 위한 흐름도이다.

[0080] 도 6에 도시된 바와 같이 차량 네트워크 침입 탐지 방법에서는 먼저, 수신 제어기(20)가 차량 네트워크를 통해 수신 메시지를 수신한다(S310).

[0081] S310 단계에서 수신 메시지를 수신하면 수신 제어기(20)는 현재 상태가 송신상태인지 판단한다(S320).

[0082] S320 단계에서 현재 상태가 송신상태인지 판단하여 송신상태인 경우, 수신 제어기(20)는 침입 탐지를 종료한다.

[0083] 반면, S320 단계에서 현재 상태가 송신상태인지 판단하여 송신상태가 아닌 경우, 수신 제어기(20)는 수신 메시지의 수에 따라 반복하여 수신 메시지 ID와 수신 제어기(20)의 송신 메시지 ID의 동일여부를 판단한다(S330).

[0084] S330 단계에서 수신 메시지 ID와 수신 제어기(20)의 송신 메시지 ID의 동일여부를 판단하여 동일한 경우, 수신 제어기(20)는 NM(Network Management) 메시지의 제어기 상태를 외부침입으로 업데이트한다(S340).

[0085] 반면, S330 단계에서 수신 메시지 ID와 수신 제어기(20)의 송신 메시지 ID의 동일여부를 판단하여 동일하지 않은 경우, 수신 제어기(20)는 NM(Network Management) 메시지의 제어기 상태를 정상으로 업데이트한다(S350).

[0086] 이때 NM 메시지 구조는 도 3에 도시된 바와 같이 수신제어기, 명령어, 슬립 진입 여부 및 제어기 상태를 포함할 수 있다.

[0087] 상술한 바와 같이, 본 발명의 실시예에 의한 차량 네트워크 침입 탐지 시스템에 따르면, 외부 네트워크와 연결된 제어기에서 제어기 간 송수신되는 메시지를 기반으로 제어권의 상실 여부를 판단하여 차량 네트워크의 침입을 탐지함으로써, 외부 침입자의 SW가 휘발성 메모리(volatile memory)에 상주하는 경우도 감지 가능하므로 외부 침입에 강건한 차량 네트워크를 구성할 수 있을 뿐만 아니라 외부 침입에 의하여 이상 동작한 경우나 SW 버그 등에 의한 이상 동작도 모니터링 가능하므로 최근 점점 더 복잡해지는 차량용 SW 생태계에서 필수적인 고장 감지 및 해결 방법이 될 수 있다.

[0088] 본 명세서에서 설명된 구현은, 예컨대, 방법 또는 프로세스, 장치, 소프트웨어 프로그램, 데이터 스트림 또는 신호로 구현될 수 있다. 단일 형태의 구현의 맥락에서만 논의(예컨대, 방법으로서만 논의)되었더라도, 논의된 특징의 구현은 또한 다른 형태(예컨대, 장치 또는 프로그램)로도 구현될 수 있다. 장치는 적절한 하드웨어, 소프트웨어 및 펌웨어 등으로 구현될 수 있다. 방법은, 예컨대, 컴퓨터, 마이크로프로세서, 집적 회로 또는 프로그래밍 가능한 로직 디바이스 등을 포함하는 프로세싱 디바이스를 일반적으로 지칭하는 프로세서 등과 같은 장치에서 구현될 수 있다. 프로세서는 또한 최종-사용자 사이에 정보의 통신을 용이하게 하는 컴퓨터, 셀 폰, 휴대용/개인용 정보 단말기(personal digital assistant: "PDA") 및 다른 디바이스 등과 같은 통신 디바이스를 포함한다.

[0089] 본 발명은 도면에 도시된 실시예를 참고로 하여 설명되었으나, 이는 예시적인 것에 불과하며, 당해 기술이 속하는 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다.

[0090] 따라서 본 발명의 진정한 기술적 보호범위는 아래의 청구범위에 의해서 정하여져야 할 것이다.

부호의 설명

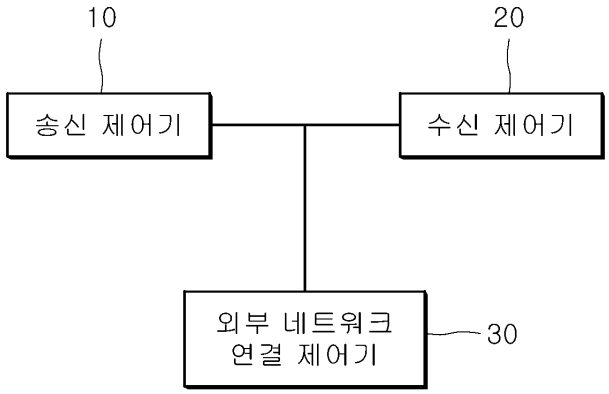
[0091] 10 : 송신 제어기

20 : 수신 제어기

30 : 외부 네트워크 연결 제어기

도면

도면1



도면2

(a)

ID	Byte					
	0	1	2	3	4	5
암호 처리 요청 메시지	수신 제어기	알고리즘 선택	Seed			

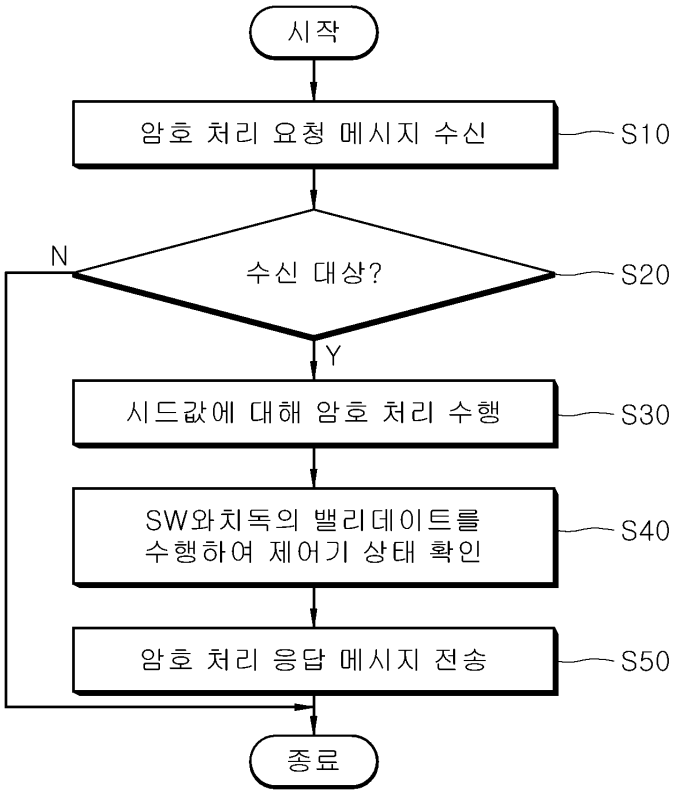
(b)

ID	Byte						
	0	1	2	3	4	5	6
암호 처리 응답 메시지	송신 제어기	알고리즘 선택	Seed 처리 결과				제어기 상태

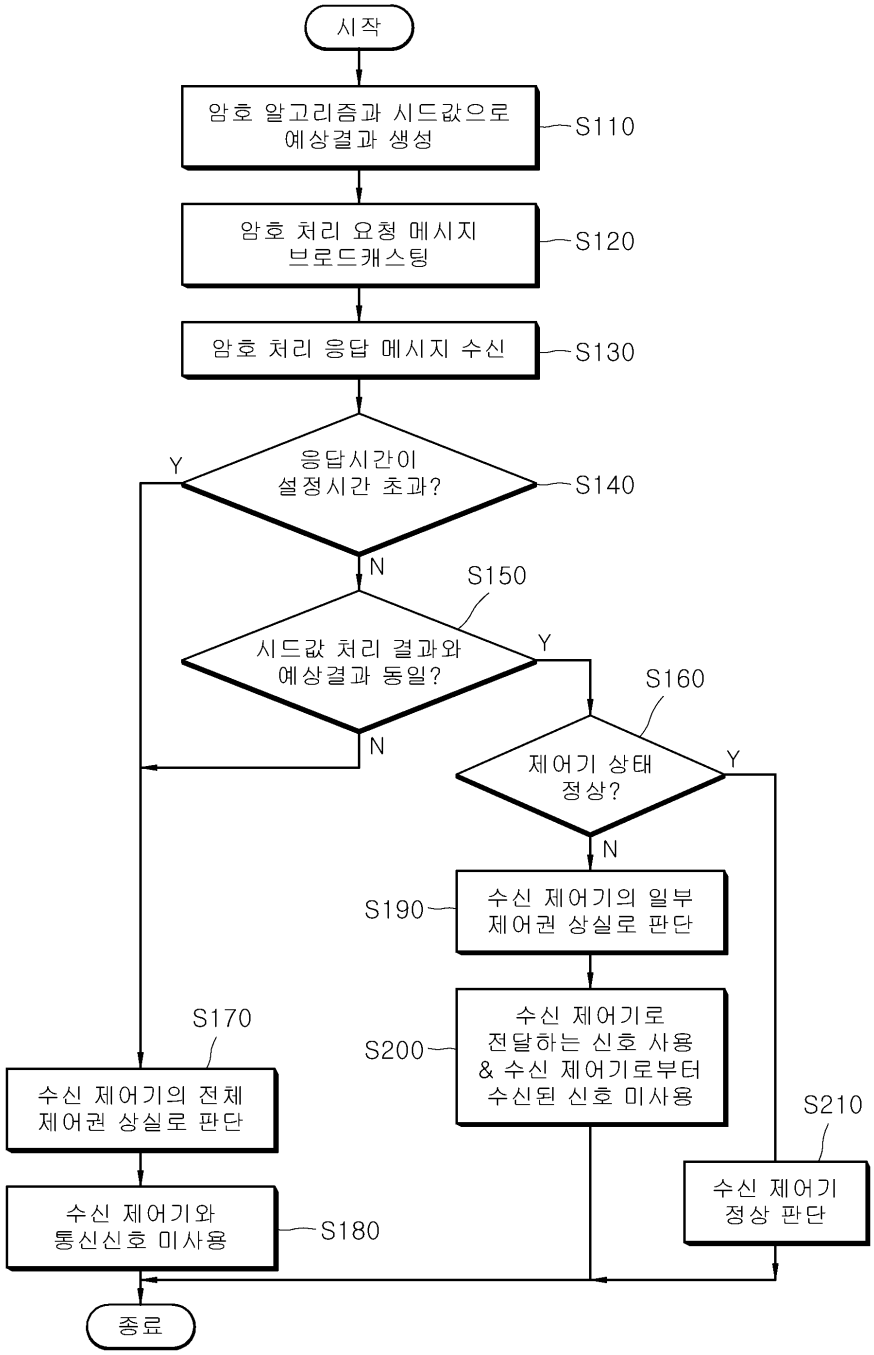
도면3

ID	Byte			
	0	1	2	3
Network Management 메시지	수신 제어기	명령어	슬립 진입 여부	제어기 상태

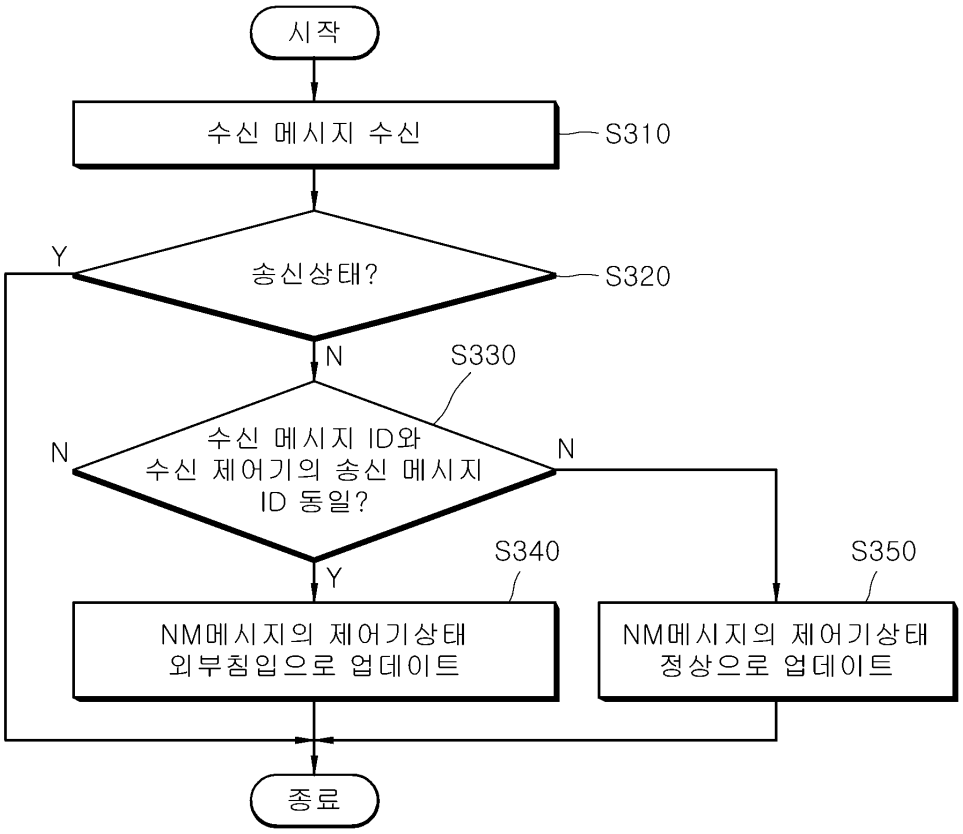
도면4



도면5


시작
암호 알고리즘과 시드값으로 예상결과 생성
S110
암호 처리 요청 메시지 브로드캐스팅
S120
암호 처리 응답 메시지 수신
S130
응답시간이 설정시간 초과?
S140
Y
N
S150
시드값 처리 결과와 예상결과 동일?
Y
N
S160
제어기 상태 정상?
Y
N
S190
수신 제어기의 일부 제어권 상실로 판단
S200
수신 제어기로 전달하는 신호 사용 & 수신 제어기로부터 수신된 신호 미사용
S210
수신 제어기 정상 판단
S170
수신 제어기의 전체 제어권 상실로 판단
수신 제어기와 통신신호 미사용
S180
종료

도면6


시작
수신 메시지 수신
S310
송신상태?
S320
Y
N
S330
수신 메시지 ID와
수신 제어기의 송신 메시지
ID 동일?
N
N
Y
S340
NM메시지의 제어기상태
외부침입으로 업데이트
S350
NM메시지의 제어기상태
정상으로 업데이트
종료