(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0102876
(43) 공개일자 2023년07월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 12/40* (2006.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
H04L 63/123 (2013.01)
(21) 출원번호 10-2021-0193332
(22) 출원일자 2021년12월30일
심사청구일자 2021년12월30일

(71) 출원인
부경대학교 산학협력단
부산광역시 남구 용소로 45, 부경대학교내 (대연동)
(72) 발명자
이경창
부산광역시 기장군 정관읍 모전1길 9, 304동 601호(정관동일스위트3차)
장현준
부산광역시 남구 수영로322번길 49-11, 202호(대연동, 정동빌라)
(뒷면에 계속)
(74) 대리인
오위환, 나성곤, 정기택

전체 청구항 수 : 총 11 항

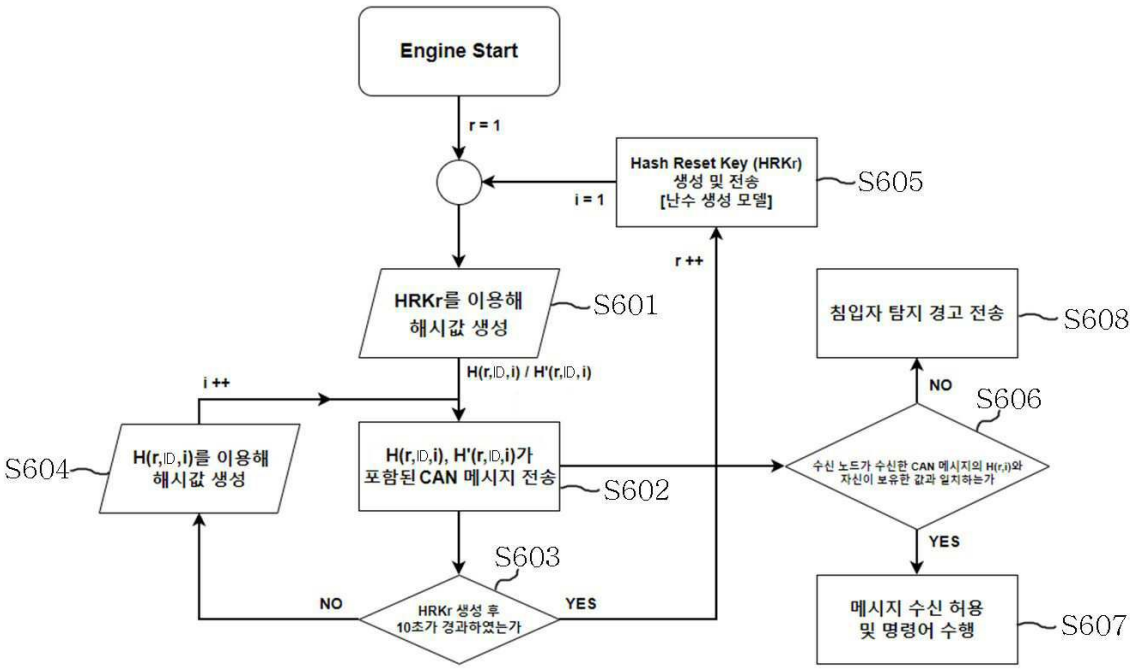
(54) 발명의 명칭 **해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법**

(57) 요 약

본 발명은 별도의 보안 프로토콜을 제공하지 않는 차량 네트워크 기술인 CAN에서 해시 함수를 활용한 메시지 기반 보안으로 악의적 메시지를 효율적으로 검출할 수 있도록 한 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법에 관한 것으로, 임의의 노드에서 HRK_r(Hash Reset Key)를 전송하면 수신한 HRK_r와 자신이 송수신 할

(뒷면에 계속)

대 표 도 - 도6



ID를 이용해 해시값 H(r,ID,i)/H'(r,ID,i)을 생성하는 해시값 생성부;해시값 H(r,ID,i)/H'(r,ID,i)이 포함된 CAN 메시지를 전송하는 CAN 메시지 전송부;CAN 메시지를 수신한 노드가 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하는지를 판단하는 유효성 판단부;유효성 판단부에서 유효성이 있는 것으로 판단되면 메시지 수신을 허용하고 명령어를 수행하는 메시지 수신 및 실행부;유효성 판단부에서 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하지 않아 유효성이 없는 것으로 판단되면 침입자 탐지 경고 전송을 하는 경고 전송부;를 포함하는 것이다.

(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/50 (2022.05)
H04L 2012/40215 (2013.01)
H04L 2012/40273 (2013.01)
H04L 2209/84 (2013.01)

(72) 발명자
김형준
부산광역시 부산진구 백양관문로 10, 313동 1302호(당감동, 주공아파트3단지)
김현희
부산광역시 남구 분포로 113, 233동 1301호(용호동, 엘지메트로시티)
신은혜
부산광역시 수영구 남천바다로 51, 714호

이 발명을 지원한 국가연구개발사업

과제고유번호	1425157665
과제번호	S3038447
부처명	중소벤처기업부
과제관리(전문)기관명	한국산학연협회
연구사업명	중소기업연구인력지원(R&D)
연구과제명	프로젝트기반 로봇융합 스마트제조 인력양성사업
기 여 율	1/1
과제수행기관명	부경대학교산학협력단
연구기간	2021.03.01 ~ 2022.02.28

명 세 서

청구범위

청구항 1

임의의 노드에서 HRK_r(Hash Reset Key)를 전송하면 수신한 HRK_r와 자신이 송수신 할 ID를 이용해 해시값 H(r,ID,i)/H'(r,ID,i)을 생성하는 해시값 생성부;

해시값 H(r,ID,i)/H'(r,ID,i)이 포함된 CAN 메시지를 전송하는 CAN 메시지 전송부;

CAN 메시지를 수신한 노드가 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하는지를 판단하는 유효성 판단부;

유효성 판단부에서 유효성이 있는 것으로 판단되면 메시지 수신을 허용하고 명령어를 수행하는 메시지 수신 및 실행부;

유효성 판단부에서 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하지 않아 유효성이 없는 것으로 판단되면 침입자 탐지 경고 전송을 하는 경고 전송부;를 포함하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치.

청구항 2

제 1 항에 있어서, 해시값 생성부에서의 해시값 생성 시점부터 설정 시간이 경과되었는 지를 판단하는 생성 시간 판단부를 더 포함하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치.

청구항 3

제 2 항에 있어서, 생성 시간 판단부에서 설정 시간이 경과된 것으로 판단되면 난수 생성 모델을 통하여 HRK_r(Hash Reset Key)를 생성하는 해시 리셋키 생성부와,

설정 시간이 경과되지 않았다면 H(r,ID,i)를 이용해 해시값을 생성하여 CAN 메시지 전송부로 전송하는 해시값 재생성부를 더 포함하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치.

청구항 4

제 1 항에 있어서, 마스터로 선정된 노드에서 초기화 메시지를 주기적으로 전송하고,

하위 슬레이브 노드는 초기화 메시지에 저장된 값에 따라 각각의 메시지 ID별로 해시값을 생성하고, CAN 노드는 생성된 해시값에서 차출된 4bit를 차량제어 메시지에 포함하여 전송하고,

수신 노드는 메시지 수신시 해당 4bit 값이 기존 해시값과 일치하는지를 판단하여 악의적 메시지를 검출하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치.

청구항 5

제 1 항에 있어서, HRK_r(Hash Reset Key)를 생성하는 해시 ECU는,

하위 통신 노드에게 HRK(Hash Reset Key)를 전송하고, 하위 노드들은 수신한 HRK와 자신이 송수신 할 ID를 이용해 해시값을 생성하고,

해시 함수는 입력값이 동일할 때 출력값이 동일하므로 각 노드들은 자신들이 통신할 ID에 해당하는 해시값을 동일하게 생성 및 보유하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치.

청구항 6

제 5 항에 있어서, HRK를 수신한 ECU는 2개의 해시값 $H_{(r,ID,i)}$와, $H'_{(r,ID,i)}$을 생성하고,

$H_{(r,ID,i)}$는 HRK, ID를 입력으로 하는 해시함수의 반환값이며, $H'_{(r,ID,i)}$는 HRK, ID, Salt를 입력으로 하는 해시함

수의 반환값이고,

Salt 값은 사용자가 임의로 지정 가능한 파라미터로, 해시함수의 복잡도를 올리기 위한 고정된 값인 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치.

청구항 7

임의의 노드에서 HRK_r(Hash Reset Key)를 전송하면 해시값 생성부에서 수신한 HRK_r와 자신이 송수신 할 ID를 이용해 해시값 H(r,ID,i)/H'(r,ID,i)을 생성하는 단계;

CAN 메시지 전송부에서 해시값 H(r,ID,i)/H'(r,ID,i)을 받아 해시값 H(r,ID,i)/H'(r,ID,i)이 포함된 CAN 메시지를 전송하는 단계;

CAN 메시지를 수신한 노드가 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하는지를 판단하는 단계;

유효성이 있는 것으로 판단되면 메시지 수신을 허용하고 명령어를 수행하고, 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하지 않아 유효성이 없는 것으로 판단되면 침입자 탐지 경고 전송을 하는 단계;를 포함하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법.

청구항 8

제 7 항에 있어서, 해시값 생성부에서의 해시값 생성 시점부터 설정 시간이 경과되었는 지를 판단하여,

설정 시간이 경과된 것으로 판단되면 난수 생성 모델을 통하여 HRK_r(Hash Reset Key)를 생성하고, 설정 시간이 경과되지 않았다면 H(r,ID,i)를 이용해 해시값을 생성하여 CAN 메시지 전송부로 전송하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법.

청구항 9

제 7 항에 있어서, 마스터로 선정된 노드에서 초기화 메시지를 주기적으로 전송하고,

하위 슬레이브 노드는 초기화 메시지에 저장된 값에 따라 각각의 메시지 ID별로 해시값을 생성하고, CAN 노드는 생성된 해시값에서 차출된 4bit를 차량제어 메시지에 포함하여 전송하고,

수신 노드는 메시지 수신시 해당 4bit 값이 기존 해시값과 일치하는지를 판단하여 악의적 메시지를 검출하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법.

청구항 10

제 7 항에 있어서, HRK_r(Hash Reset Key)를 생성하는 해시 ECU는,

하위 통신 노드에게 HRK(Hash Reset Key)를 전송하고, 하위 노드들은 수신한 HRK와 자신이 송수신 할 ID를 이용해 해시값을 생성하고,

해시 함수는 입력값이 동일할 때 출력값이 동일하므로 각 노드들은 자신들이 통신할 ID에 해당하는 해시값을 동일하게 생성 및 보유하는 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법.

청구항 11

제 10 항에 있어서, HRK를 수신한 ECU는 2개의 해시값 $H_{(r,ID,i)}$와, $H'_{(r,ID,i)}$을 생성하고,

$H_{(r,ID,i)}$는 HRK, ID를 입력으로 하는 해시함수의 반환값이며, $H'_{(r,ID,i)}$는 HRK, ID, Salt를 입력으로 하는 해시함수의 반환값이고,

Salt 값은 사용자가 임의로 지정 가능한 파라미터로, 해시함수의 복잡도를 올리기 위한 고정된 값인 것을 특징으로 하는 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 CAN(Controller Area Network) 보안에 관한 것으로, 구체적으로 별도의 보안 프로토콜을 제공하지 않는 차량 네트워크 기술인 CAN에서 해시 함수를 활용한 메시지 기반 보안으로 악의적 메시지를 효율적으로 검출할 수 있도록 한 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] ECU(Electronic Control Unit)의 등장 이후 연료 공급이 전자제어를 통한 직분사 방식(GDI, MPI, EUI, CRDi 등)으로 대체되기 시작하면서 현재는 엔진제어, 차세제어, ABS 등 수많은 차량 내 전자제어 시스템이 탑재되고, 이에 따라 차량 내 ECU의 수는 지속적으로 증가하고 있다.

[0003] 이와 같이, 차량에 탑재된 ECU들은 CAN, LIN, FlexRay 등의 방식을 이용해 상호 통신하고 있다. 이중 CAN은 한 쌍의 꼬임선을 이용해 차동전압 방식으로 통신하기 때문에 전기적 외란으로부터 매우 강인한 물리적 특성을 장점으로 가지고 있어 차량 통신에 가장 안정적으로 이용되며, 주요 데이터를 송수신 하는데 사용되고 있다.

[0004] 최근에는 차량의 ECU를 단순한 차량의 제어에 사용하는 것뿐 아니라 각종 편의기능을 제공하고 탑승자와 상호작용을 하며 차량 운행시간을 보다 효율적으로 활용할 수 있는 서비스 탑재하는데도 활용하고 있다.

[0005] 특히, 반자율주행 및 온라인 서비스를 제공하기 위해 고성능의 ECU의 개발 및 탑재도 꾸준히 연구되고 있다. 이러한 서비스의 제공을 위해서는 통신사의 무선 네트워크 연결이 필요한데, 차량의 ECU중 일부를 온라인에 연결하여 다양한 서비스를 제공받기도 한다.

[0006] 이와 같이 현재의 차량은 차량 내부의 단순제어부터 차량 외부와의 상호 통신까지 넓은 범위의 통신을 수행하고 있는데, 이것이 사이버 공격의 대상으로 주목받고 있으며, 공격자의 침입이 이루어지게 되는 경우 차량의 정상 운행이 불가능해지거나 오작동으로 인한 피해로 이어질 수 있다.

[0007] 특히 CAN 의 경우 별도의 보안 사양이 적용되어 있지 않기 때문에 어떤 방식으로든 공격자가 CAN BUS에 침투하게 되는 경우 모든 시스템이 무력화 될 수 있으며, 이를 통해 수많은 차량을 마비시키거나 제어권한을 탈취 할 수 있는 위험에 빠지게 된다.

[0008] 무선 통신 시스템을 이용하여 다양한 서비스를 제공하는 것은 사용자에게 있어 매우 중요한 차량 구매 결정 요소가 될 수 있다. 일반 사용자의 경우 네비게이션 기반 스마트 크루즈 기능을 통해 반자율주행 시스템을 공급받을 수 있는 등 최대의 편의사양을 누릴 수 있으며, 기업 사용자의 경우 자동 물류 시스템 및 군집 주행 등을 통해 생산 시스템의 효율을 극대화 할 수 있다.

[0009] 이렇게 많은 분야에서 차량의 무선 통신 서비스는 4차산업을 뛰어넘어 5차산업을 항하는 현대 사회에 가장 필요한 기술중 하나로 꾸준히 조명받고 있다.

[0010] 하지만 이러한 무선 통신은 해커의 타겟이 되기 쉽기 때문에 무선 네트워크 통신상의 보안을 철저히 강화하고 있다. 특히 5G 및 6G를 통해 온라인 제어 및 모니터링 서비스를 제공하기 위해 많은 통신사들이 무선 통신 보안을 지속적으로 발전시키고 있지만, 언젠가 한번 보안이 무력화 되는 순간 그 피해는 상상을 초월할 수 있다. 즉, 완벽한 시스템은 존재하지 않는다는 것이다.

[0011] 따라서, 무선 게이트웨이 레벨에서 공격자의 침입을 허용한 상황을 대비하기 위해 내부 유선 네트워크의 보안도 강화할 필요가 있다.

[0012] 비교적 대역폭이나 통신속도가 빠른 이더넷, FelxRay등은 보안사양을 추가하는 것이 가능하지만, CAN은 현재 보안사양이 일절 존재하지 않으며, 프로토콜 특성상 보안사양을 탑재는 것이 다소 어렵다.

[0013] 따라서 하드웨어 레벨에서 보안을 설정해야 하지만 이는 막대한 비용의 원인이 되기 때문에 소프트웨어 레벨에서의 보안 사양 개발도 필요한 시점이다.

[0014] CAN 프로토콜에 보안사양을 탑재하는 것은 어려운 일이지만, 이를 극복하고 보안 솔루션을 탑재하려는 연구들이 매년 진행되고 있다.

[0015] 통신이 수행되기 전에 적용되는 보안 기법은 인증서 및 대칭키 타입의 암호학적 방법이 있고, 통신이 수행된 후에 그것을 모니터링 함으로써 공격자의 침입을 검출하는 침입 검출 기법이 있다.

[0016] 하지만, 전자의 경우 CAN의 실시간성을 보장 못할 가능성이 있거나, 용량적 한계를 극복하지 못한 사례들이 다

수 있으며, 후자의 경우 공격자가 우회를 시도하였을 때 탐지하지 못할 가능성이 존재한다.

[0017] 따라서, 주기적으로 제어 메시지가 송수신되는 차량 네트워크 환경에 적합하고, 지연의 최소화 및 모든 메지시에 적용할 수 있는 강화된 새로운 보안 기술의 개발이 요구되고 있다.

선행기술문헌

특허문헌

[0018] (특허문헌 0001) 대한민국 공개특허 제10-2020-0075604호

(특허문헌 0002) 대한민국 공개특허 제10-2011-0057348호

(특허문헌 0003) 대한민국 등록특허 제10-2194469호

발명의 내용

해결하려는 과제

[0019] 본 발명은 종래 기술의 CAN(Controller Area Network) 보안 기술의 문제점을 해결하기 위한 것으로, 별도의 보안 프로토콜을 제공하지 않는 차량 네트워크 기술인 CAN에서 해시 함수를 활용한 메시지 기반 보안으로 악의적 메시지를 효율적으로 검출할 수 있도록 한 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 제공하는데 그 목적이 있다.

[0020] 본 발명은 주기적으로 제어 메시지가 송수신되는 차량 네트워크 환경에 적합하고, 지연의 최소화 및 모든 메지시에 적용할 수 있는 강화된 보안 특성을 갖도록 한 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 제공하는데 그 목적이 있다.

[0021] 본 발명은 해시 함수를 통해 생성된 값을 주기적으로 전송되는 메시지에 할당하여 동일한 ID의 메시지를 체인으로 연결하는 메시지 체인 기반 보안 방법으로 연산량의 증가없이 다양한 네트워크에 적용할 수 있도록 한 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 제공하는데 그 목적이 있다.

[0022] 본 발명은 CAN BUS 구성에 HASH ECU가 하나만 추가하여 구현 가능하도록 하여 큰 비용없이 하드웨어 구성을 할 수 있도록 한 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 제공하는데 그 목적이 있다.

[0023] 본 발명은 수신한 메시지에서 올바른 해시비트 위치에 정확한 해시비트가 저장되어있는지 비교하고, 일치하는 경우 메시지 명령어를 수행하며 불일치하는 경우 네트워크에 침입자 경고 메시지를 송출하여 주기적으로 제어 메시지가 송수신되는 차량 네트워크 환경에서의 보안성을 높인 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 제공하는데 그 목적이 있다.

[0024] 본 발명은 한번 사용한 해시값은 활용된 후에 바로 제거하여 기록을 누적하여 값을 검증하지 않고 오직 메시지를 송수신 하는 순간에만 활용하여 강인한 보안 특성을 갖도록 한 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 제공하는데 그 목적이 있다.

[0025] 본 발명의 다른 목적들은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0026] 상기와 같은 목적을 달성하기 위한 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치는 임의의 노드에서 HRK_r(Hash Reset Key)를 전송하면 수신한 HRK_r와 자신이 송수신 할 ID를 이용해 해시값 H(r,ID,i)/H'(r,ID,i)을 생성하는 해시값 생성부;해시값 H(r,ID,i)/H'(r,ID,i)이 포함된 CAN 메시지를 전송하는 CAN 메시지 전송부;CAN 메시지를 수신한 노드가 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하는지를 판단하는 유효성 판단부;유효성 판단부에서 유효성이 있는 것으로 판단되면 메시지 수신을 허용하고 명령어를 수행하는 메시지 수신 및 실행부;유효성 판단부에서 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하지 않아 유효성이 없는 것으로 판단되면 침입자 탐지 경고 전송을 하는 경고 전송부;를 포함하는 것을 특징으로 한다.

[0027] 여기서, 해시값 생성부에서의 해시값 생성 시점부터 설정 시간이 경과되었는 지를 판단하는 생성 시간 판단부를 더 포함하는 것을 특징으로 한다.

[0028] 그리고 생성 시간 판단부에서 설정 시간이 경과된 것으로 판단되면 난수 생성 모델을 통하여 HRK_r(Hash Reset Key)를 생성하는 해시 리셋키 생성부와, 설정 시간이 경과되지 않았다면 H(r,ID,i)를 이용해 해시값을 생성하여 CAN 메시지 전송부로 전송하는 해시값 재생성부를 더 포함하는 것을 특징으로 한다.

[0029] 그리고 마스터로 선정된 노드에서 초기화 메시지를 주기적으로 전송하고, 하위 슬레이브 노드는 초기화 메시지에 저장된 값에 따라 각각의 메시지 ID별로 해시값을 생성하고, CAN 노드는 생성된 해시값에서 차출된 4bit를 차량제어 메시지에 포함하여 전송하고, 수신 노드는 메시지 수신시 해당 4bit 값이 기존 해시값과 일치하는지를 판단하여 악의적 메시지를 검출하는 것을 특징으로 한다.

[0030] 그리고 HRK_r(Hash Reset Key)를 생성하는 해시 ECU는, 하위 통신 노드에게 HRK(Hash Reset Key)를 전송하고, 하위 노드들은 수신한 HRK와 자신이 송수신 할 ID를 이용해 해시값을 생성하고, 해시 함수는 입력값이 동일할 때 출력값이 동일하므로 각 노드들은 자신들이 통신할 ID에 해당하는 해시값을 동일하게 생성 및 보유하는 것을 특징으로 한다.

[0031] 그리고 HRK를 수신한 ECU는 2개의 해시값 $H_{(r,ID,i)}$와, $H'_{(r,ID,i)}$을 생성하고, $H_{(r,ID,i)}$는 HRK, ID를 입력으로 하는 해시함수의 반환값이며, $H'_{(r,ID,i)}$는 HRK, ID, Salt를 입력으로 하는 해시함수의 반환값이고, Salt 값은 사용자가 임의로 지정 가능한 파라미터로, 해시함수의 복잡도를 올리기 위한 고정된 값인 것을 특징으로 한다.

[0032] 다른 목적을 달성하기 위한 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법은 임의의 노드에서 HRK_r(Hash Reset Key)를 전송하면 해시값 생성부에서 수신한 HRK_r와 자신이 송수신 할 ID를 이용해 해시값 H(r,ID,i)/H'(r,ID,i)을 생성하는 단계;CAN 메시지 전송부에서 해시값 H(r,ID,i)/H'(r,ID,i)을 받아 해시값 H(r,ID,i)/H'(r,ID,i)이 포함된 CAN 메시지를 전송하는 단계;CAN 메시지를 수신한 노드가 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하는지를 판단하는 단계;유효성이 있는 것으로 판단되면 메시지 수신을 허용하고 명령어를 수행하고, 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하지 않아 유효성이 없는 것으로 판단되면 침입자 탐지 경고 전송을 하는 단계;를 포함하는 것을 특징으로 한다.

[0033] 여기서, 해시값 생성부에서의 해시값 생성 시점부터 설정 시간이 경과되었는 지를 판단하여, 설정 시간이 경과된 것으로 판단되면 난수 생성 모델을 통하여 HRK_r(Hash Reset Key)를 생성하고, 설정 시간이 경과되지 않았다면 H(r,ID,i)를 이용해 해시값을 생성하여 CAN 메시지 전송부로 전송하는 것을 특징으로 한다.

[0034] 그리고 마스터로 선정된 노드에서 초기화 메시지를 주기적으로 전송하고, 하위 슬레이브 노드는 초기화 메시지에 저장된 값에 따라 각각의 메시지 ID별로 해시값을 생성하고, CAN 노드는 생성된 해시값에서 차출된 4bit를 차량제어 메시지에 포함하여 전송하고, 수신 노드는 메시지 수신시 해당 4bit 값이 기존 해시값과 일치하는지를 판단하여 악의적 메시지를 검출하는 것을 특징으로 한다.

[0035] 그리고 HRK_r(Hash Reset Key)를 생성하는 해시 ECU는, 하위 통신 노드에게 HRK(Hash Reset Key)를 전송하고, 하위 노드들은 수신한 HRK와 자신이 송수신 할 ID를 이용해 해시값을 생성하고, 해시 함수는 입력값이 동일할 때 출력값이 동일하므로 각 노드들은 자신들이 통신할 ID에 해당하는 해시값을 동일하게 생성 및 보유하는 것을 특징으로 한다.

[0036] 그리고 HRK를 수신한 ECU는 2개의 해시값 $H_{(r,ID,i)}$와, $H'_{(r,ID,i)}$을 생성하고, $H_{(r,ID,i)}$는 HRK, ID를 입력으로 하는 해시함수의 반환값이며, $H'_{(r,ID,i)}$는 HRK, ID, Salt를 입력으로 하는 해시함수의 반환값이고, Salt 값은 사용자가 임의로 지정 가능한 파라미터로, 해시함수의 복잡도를 올리기 위한 고정된 값인 것을 특징으로 한다.

발명의 효과

[0037] 이상에서 설명한 바와 같은 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법은 다음과 같은 효과가 있다.

[0038] 첫째, 별도의 보안 프로토콜을 제공하지 않는 차량 네트워크 기술인 CAN에서 해시 함수를 활용한 메시지 기반 보안으로 악의적 메시지를 효율적으로 검출할 수 있도록 한다.

[0039] 둘째, 주기적으로 제어 메시지가 송수신되는 차량 네트워크 환경에 적합하고, 지연의 최소화 및 모든 메시지에 적용할 수 있는 강화된 보안 특성을 갖도록 한다.

[0040] 셋째, 해시 함수를 통해 생성된 값을 주기적으로 전송되는 메시지에 할당하여 동일한 ID의 메시지를 체인으로 연결하는 메시지 체인 기반 보안 방법으로 연산량의 증가없이 다양한 네트워크에 적용할 수 있도록 한다.

[0041] 넷째, CAN BUS 구성에 HASH ECU가 하나만 추가하여 구현 가능하도록 하여 큰 비용없이 하드웨어 구성을 할 수 있도록 한다.

[0042] 다섯째, 수신한 메시지에서 올바른 해시비트 위치에 정확한 해시비트가 저장되어있는지 비교하고, 일치하는 경우 메시지 명령어를 수행하며 불일치하는 경우 네트워크에 침입자 경고 메시지를 송출하여 주기적으로 제어 메시지가 송수신되는 차량 네트워크 환경에서의 보안성을 높인다.

[0043] 여섯째, 한번 사용한 해시값은 활용된 후에 바로 제거하여 기록을 누적하여 값을 검증하지 않고 오직 메시지를 송수신 하는 순간에만 활용하여 강인한 보안 특성을 갖도록 한다.

도면의 간단한 설명

[0044] 도 1은 CAN 프레임 구성도

도 2는 해시 함수의 I/O 특성을 나타낸 구성도

도 3은 블록체인 특성을 나타낸 구성도

도 4는 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 기술의 개념을 나타낸 구성도

도 5는 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 시스템의 구성도

도 6은 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법을 나타낸 플로우 차트

도 7은 해시 리셋 키 분배 및 해시 코드 업데이트 과정을 나타낸 구성도

도 8은 각각의 ECU들이 내부에서 해시값을 생성하는 과정을 나타낸 구성도

도 9는 본 발명에 따른 인증 및 침입 탐지 성능 평가 특성을 나타낸 그래프

발명을 실시하기 위한 구체적인 내용

[0045] 이하, 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법의 바람직한 실시 예에 관하여 상세히 설명하면 다음과 같다.

[0046] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법의 특징 및 이점들은 이하에서의 각 실시 예에 대한 상세한 설명을 통해 명백해질 것이다.

[0047] 도 1은 CAN 프레임 구성도이고, 도 2는 해시 함수의 I/O 특성을 나타낸 구성도이다.

[0048] 그리고 도 3은 블록체인 특성을 나타낸 구성도이다.

[0049] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법은 별도의 보안 프로토콜을 제공하지 않는 차량 네트워크 기술인 CAN에서 해시 함수를 활용한 메시지 기반 보안으로 악의적 메시지를 효율적으로 검출할 수 있도록 한 것이다.

[0050] 이를 위하여, 본 발명은 해시 함수를 통해 생성된 값을 주기적으로 전송되는 메시지에 할당하여 동일한 ID의 메시지를 체인으로 연결하는 메시지 체인 기반 보안 방법으로 연산량의 증가없이 다양한 네트워크에 적용할 수 있도록 하는 구성을 포함할 수 있다.

[0051] 본 발명은 CAN BUS 구성에 HASH ECU가 하나만 추가하여 구현 가능하도록 하여 큰 비용없이 하드웨어 구성을 할 수 있도록 하는 구성을 포함할 수 있다.

[0052] 본 발명은 수신한 메시지에서 올바른 해시비트 위치에 정확한 해시비트가 저장되어 있는지 비교하고, 일치하는 경우 메시지 명령어를 수행하며 불일치하는 경우 네트워크에 침입자 경고 메시지를 송출하여 주기적으로 제어 메시지가 송수신되는 차량 네트워크 환경에서의 보안성을 높이는 구성을 포함할 수 있다.

[0053] 본 발명은 한번 사용한 해시값은 활용된 후에 바로 제거하여 기록을 누적하여 값을 검증하지 않고 오직 메시지

를 송수신하는 순간에만 활용하여 강인한 보안 특성을 갖도록 하는 구성을 포함할 수 있다.

[0054] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 구현하기 위한 CAN 프레임 구조를 설명하면 다음과 같다.

[0055] CAN은 차동 전압 방식을 통해 통신하기 위해 CANH, CANL 신호를 이용한다.

[0056] Dominant 상태에서는 CANH-CANL 전압차가 0.9V 이상 발생하게 되며 도 1에서와 같이 CANL 이 Dominant 상태에서는 0V로 본다.

[0057] Recessive State는 CANH-CANL 전압차가 0.5V 이하가 되고, VCC/2 상태로 CANL가 중간전압으로 상승하게 된다. 반대로 CANH의 경우 Dominant 상태일 때 5V가 되며, Recessive 상태일때에는 CANL과 동일하게 VCC/2 즉, 2.5V가 된다.

[0058] 따라서 일반적으로 CANL의 전압을 기준으로 0V일 때 LOGIC 0, 2.5V 일 때 LOGIC 1로 표현한다.

[0059] CAN 프로토콜은 Start-of-Frame 으로 시작하여 End-of-Frame 으로 끝난다.

[0060] SoF 이후 Arbitration Field가 위치하는데, 이는 메시지의 ID가 포함되어 있으며 트랜시버가 이것을 읽고 자신과 엮인 ECU가 수신할 메시지인지 아닌지 판단한다. 수신 목록에 있는 ID인 경우 해당 신호를 ECU 명령어로 변환하여 전달한다.

[0061] 수신목록에 없는 경우 해당 메시지의 EoF가 수신될 때까지 대기상태가 된다.

[0062] Control Field는 해당 메시지가 데이터 프레임인지 리모트 프레임인지에 대한 정보를 담고 있다. 데이터 프레임은 데이터 값을 메시지에 포함하여 전송하는 메시지 프레임이며, 리모트 프레임은 다른 노드에게 데이터 값 송신을 요청하는 메시지 프레임이다.

[0063] CAN은 Arbitration Field에 담긴 메시지 ID값을 통해 메시지의 우선순위를 결정한다.

[0064] 이는 CAN 프로토콜이 P2P 방식으로 송신 ECU에서 수신 ECU로 직접 전달하는 것이 아닌, 공유된 CAN BUS를 통해 메시지를 전달하기 때문이다. 공유된 CAN BUS에 수십개의 ECU 노드들이 접속되어 있는데, CAN은 송신시 수신 노드의 주소를 이용하지 않고, 메시지에 ID를 담아 송신한다.

[0065] 해당 BUS에 있는 ECU들은 모두 해당 메시지를 읽고, 자신이 수신할 목록에 있는 ID인 경우에만 해당 메시지를 수용한다.

[0066] 그리고 CAN 프로토콜을 이용하는 ECU는 트랜시버를 내장하고 있거나, 추가로 트랜시버를 요구한다. 트랜시버는 CAN BUS 상에 전달되고 있는 데이터의 Arbitration 값을 읽고, 자신과 엮인 ECU가 수신할 메시지 ID인지 판단하는 역할을 수행한다. 자신이 수신할 메시지 ID가 아닌 경우 해당 메시지를 무시하고, 자신이 수신할 메시지인 경우 ECU에서 사용 가능하도록 전기 신호를 변환해준다.

[0067] 메시지 우선순위 경쟁의 역할도 트랜시버가 수행하는데, 트랜시버에서 송신하는 비트값과 수신하는 비트값을 비교하여 Dominant 상태인지, Recessive 상태인지 확인하는데 이때 동일한 상태이면 송신을 지속한다.

[0068] 서로 다른 상태일 때 자신이 Dominant 이며 다른 노드가 Recessive 일 때에는 자신이 우선권을 갖고있다고 인식하여 송신을 계속하고, 자신이 Recessive 일 때 다른 노드가 Dominant 이면 자신이 우선권을 빼앗겼다고 판단하여 송신을 중단하며 수신 상태로 전환한다.

[0069] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 구현하기 위한 해시 함수에 관하여 설명하면 다음과 같다.

[0070] 해시 알고리즘 또는 해시함수 알고리즘으로도 불리는 해시 함수는 임의의 길이의 데이터를 지정된 길이의 데이터로 맵핑을 수행하는 함수이다.

[0071] 해시함수의 반환값은 해시값, 해시코드, 해시 체크섬으로 불리는데 이를 간단히 해시라고 칭한다. 해시함수의 큰 특징은 다음과 같다.

[0072] 첫째, 입력이 같을 경우 결과가같다.

[0073] 둘째, 출력값을 통해 입력값을 추론하는 것이 힘들다.

[0074] 셋째, 두 해시값이 다르면 원 데이터는 같지 않다.

[0075] 넷째, 두 개의 입력이 다르더라도 같은 해시값이 반환될 수 있다.

[0076] 해시함수는 동일한 입력에 대해 입력값에 아주 사소한 변화라도 있는 경우 이전과 매우 다른 결과값을 반환한다. 따라서 데이터의 내용에 변화가 있는 경우 해당 파일의 해시값을 통해 알 수 있으므로, 파일의 위변조를 쉽게 검출할 수 있다.

[0077] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법을 구현하기 위한 블록체인에 관하여 설명하면 다음과 같다.

[0078] 블록체인은 관리하고자 하는 데이터를 순서를 가진 체인 형태로 운용되는 '블록'에 저장하는 데이터 관리 기법이다.

[0079] 블록은 P2P 환경에서 생성되며, 누구라도 임의로 수정이 불가능하지만 누구든지 데이터의 변경 내용을 열람할 수 있는 분산 컴퓨팅 기반의 원장 관리 기술이다.

[0080] 이는 근본적으로 분산 데이터 저장기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의해 임의의 조작이 불가능하도록 고안되었다.

[0081] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 기술의 개념을 구체적으로 설명하면 다음과 같다.

[0082] 도 4는 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 기술의 개념을 나타낸 구성도이다.

[0083] 본 발명에서 제안하는 CAN 보안 알고리즘의 핵심은 해시체인 기법인데, 이는 블록체인의 아이디어를 이용한 것이다.

[0084] 현재 전송될 메시지는 이전 메시지의 값을 입력으로 한 해시 반환값을 포함한다.

[0085] 다음 메시지는 현재 메시지의 값을 입력으로 한 해시 반환값을 포함한다. 따라서 모든 메시지는 이전 메시지 및 이후의 메시지와 서로 유기적인 연관관계를 가지고 있다.

[0086] 다만, 블록체인 기법은 해시 블록 데이터가 모든 사용자들에게 분산되어 저장되기 때문에 공간적인 암호화 방식으로 볼 수 있지만, 본 발명에서 제안하는 CAN 보안 알고리즘은 한번 사용한 해시값은 다음 메시지를 위해 활용된 후에 바로 제거되기 때문에 기록을 누적하여 값을 검증하지 않는다.

[0087] 오직 메시지를 송수신 하는 순간에만 활용하게 되므로 본 알고리즘은 시간적인 개념으로 해석하는 바람직하다.

[0088] 이는 시간의 흐름에 따라 메시지가 전송되고, 이 메시지들간의 연관관계가 해시라는 매개변수로 이어지기 때문에 시간의 흐름에 따라 운용되는 알고리즘인 것이다.

[0089] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 시스템을 구체적으로 설명하면 다음과 같다.

[0090] 도 5는 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 시스템의 구성도이다.

[0091] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 시스템은 임의의 노드에서 HRK_r(Hash Reset Key)를 전송하면 수신한 HRK_r와 자신이 송수신 할 ID를 이용해 해시값 H(r,ID,i)/H'(r,ID,i)을 생성하는 해시값 생성부(10)와, 해시값 H(r,ID,i)/H'(r,ID,i)이 포함된 CAN 메시지를 전송하는 CAN 메시지 전송부(50)와, CAN 메시지를 수신한 노드가 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하는지를 판단하는 유효성 판단부(60)와, 유효성 판단부(60)에서 유효성이 있는 것으로 판단되면 메시지 수신을 허용하고 명령어를 수행하는 메시지 수신 및 실행부(70)와, 유효성 판단부(60)에서 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하지 않아 유효성이 없는 것으로 판단되면 침입자 탐지 경고 전송을 하는 경고 전송부(80)를 포함한다.

[0092] 여기서, 해시값 생성부(10)에서의 해시값 생성 시점부터 설정 시간이 경과되었는 지를 판단하는 생성 시간 판단부(20)와, 설정 시간이 경과된 것으로 판단되면 난수 생성 모델을 통하여 HRK_r(Hash Reset Key)를 생성하는 해시 리셋키 생성부(30)와, 설정 시간이 경과되지 않았다면 H(r,ID,i)를 이용해 해시값을 생성하여 CAN 메시지 전송부(50)로 전송하는 해시값 재생성부(40)를 더 포함한다.

[0093] 이와 같은 구성을 갖는 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치는 마스터로 선정된 노드에서 초기화 메시지를 주기적으로 전송하고, 하위 슬레이브 노드는 초기화 메시지에 저장된 값에 따라 각각의 메시지 ID별로 해시값을 생성하고, CAN 노드는 생성된 해시값에서 차출된 4bit를 차량제어 메시지에 포함하

여 전송하고, 수신 노드는 메시지 수신시 해당 4bit 값이 기존 해시값과 일치하는지를 판단하여 악의적 메시지를 검출하는 할 수 있다.

[0094] 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법을 구체적으로 설명하면 다음과 같다.

[0095] 도 6은 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 방법을 나타낸 플로우 차트이다.

[0096] 먼저, 임의의 노드에서 HRK_r(Hash Reset Key)를 전송하면 해시값 생성부(10)에서 수신한 HRK_r와 자신이 송수신할 ID를 이용해 해시값 H(r,ID,i)/H'(r,ID,i)을 생성한다.(S601)

[0097] 이어, CAN 메시지 전송부(50)에서 해시값 H(r,ID,i)/H'(r,ID,i)을 받아 해시값 H(r,ID,i)/H'(r,ID,i)이 포함된 CAN 메시지를 전송한다.(S602)

[0098] 그리고 CAN 메시지를 수신한 노드가 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하는지를 판단한다.(S606)

[0099] 유효성이 있는 것으로 판단되면 메시지 수신을 허용하고 명령어를 수행하고(S607), 수신한 CAN 메시지의 H(r,ID,i)와 자신이 보유한 값이 일치하지 않아 유효성이 없는 것으로 판단되면 침입자 탐지 경고 전송을 한다.(S608)

[0100] 여기서, 해시값 생성부(10)에서의 해시값 생성 시점부터 설정 시간이 경과되었는 지를 판단하여(S603), 설정 시간이 경과된 것으로 판단되면 난수 생성 모델을 통하여 HRK_r(Hash Reset Key)를 생성하고, 설정 시간이 경과되지 않았다면 H(r,ID,i)를 이용해 해시값을 생성하여 CAN 메시지 전송부(50)로 전송한다.(S604)

[0101] 해시 초기화 및 ID별 해시 관리에 관하여 설명하면 다음과 같다.

[0102] 도 7은 해시 리셋 키 분배 및 해시 코드 업데이트 과정을 나타낸 구성도이다.

[0103] 해시 ECU는 하위 통신 노드에게 HRK(Hash Reset Key)를 전송한다. 하위 노드들은 수신한 HRK와 자신이 송수신할 ID를 이용해 해시값을 생성한다.

[0104] 해시 함수는 입력값이 동일할 때 출력값이 동일하므로 각 노드들은 자신들이 통신할 ID에 해당하는 해시값을 동일하게 생성 및 보유할 수 있다.

[0105] 도 8은 각각의 ECU들이 내부에서 해시값을 생성하는 과정을 나타낸 구성도이다.

[0106] HRK를 수신한 ECU는 2개의 해시값을 생성해야 하는데, 이를 각각 $H_{(r,ID,i)}$와, $H'_{(r,ID,i)}$라고 명명한다. $H_{(r,ID,i)}$는 HRK, ID를 입력으로 하는 해시함수의 반환값이며, $H'_{(r,ID,i)}$는 HRK, ID, Salt를 입력으로 하는 해시함수의 반환값이다.

[0107] 이때, Salt 값은 사용자가 임의로 지정 가능한 파라미터로, 해시함수의 복잡도를 올리기 위한 고정된 값이다. 필요에 따라 변수로 설정이 가능하다.

[0108] 표 1은 HRK가 123이고, ID는 0x478, salt값은 ‘ 일때의 경우를 표현한 것이다

표 1

ex) in case of [HRKr=123], [ID = 0x478], [Salt = ']

$Hr_{,1}$ = 81DC9BDB52D04DC20036DBD8313ED055
$H'_{r,1}$ = 52AC6A0EACC6CA4FCB3F8726E8BEA0B6

HP_1 = $Hash_Postion_1$ = 1st value of h1
$HashCode_1$ = HP_1^{th} value of h2

#define $HashCode_1$ HC_1
#define $Position_Value_1$ PV_1
in this case, HC_1 = E = $1110_{(2)}$
PV1 = 1, PV2 = D, PV3 = C, PV4 = 9

$PV_1 = PV_1+1$
// PV_1 => 0~F -> 1~16

$P1_1 = PV1_1$
$P2_1 = P1_1 + PV2_1$
$P3_1 = P2_1 + PV3_1$
$P4_1 = P3_1 + PV4_1$
so $P1_1$~$P4_1$ = 2, 16, 29, 39

then, insert HC_1 in 'Pn_1'th CAN DATA Field as below

CAN DATA FIELD : X1XXXXXX XXXXXXX0 XXXXXXXX XXXX0XXX
XXXXXX0X XXXXXXXX XXXXXXXX XXXXXXXX

[0109]

[0110] 임의의 0x478를 수신하는 임의의 노드는 HRK값(123)을 수신하고, $H_{(r,ID,i)}$, $H'_{(r,ID,i)}$를 생성한다. 이때 $H_{(r,ID,i)}$의 첫 번째 값인 8을 이용해 $H'_{(r,ID,i)}$의 8번째 문자인 E를 해시비트로 추출한다. 이때 E는 이진수로 1110이며, 이 1110 값을 해시비트로 이용한다.

[0111] 해시비트 4bit가 위치할 자리는 $H_{(r,ID,i)}$의 2~5번째 값을 통해 지정하는데, 순서대로 Position Value(PV) 1~4로 지정한다.

[0112] 따라서 PV1~4는 각각 1,D,C,9 가 되는데 이를 10진수로 표현하면 1, 13, 12, 9 이다. 경우에 따라서 이 값이 0이 될 수 있는데, 0번째 자리는 존재하지 않으므로 PV=PV+1을 수행한다. 따라서 PV 1~4는 각각 2, 14, 15, 10이 된다.

[0113] 이후 해시비트가 실제로 들어가 비트 위치를 지정하는데, 이는 PV 1~4를 누적한 P 1~4 값에 따라 정해지고, 현재의 경우 각각 2, 16, 29, 39이다. 따라서 해시비트는 DATA Field 64bit 중 2, 16, 29, 39번째 비트 위치에 1, 1, 1, 0이 각각 들어간다.

[0114] 이렇게 CAN 메시지에 저장될 해시비트와 해시비트의 위치가 정해졌으면 해시비트를 해당 위치에 저장한 후 송신한다.

[0115] 수신 노드에서도 이 과정을 동일하게 수행하기 때문에, 수신한 메시지에서 올바른 해시비트 위치에 정확한 해시비트가 저장되어있는지 비교하고, 일치하는 경우 메시지 명령어를 수행하며 불일치하는 경우 네트워크에 침입자 경고 메시지를 송출한다.

[0116] 본 발명에 따른 인증 및 침입 탐지 성능 평가 특성에 관하여 설명하면 다음과 같다.

[0117] 도 9는 본 발명에 따른 인증 및 침입 탐지 성능 평가 특성을 나타낸 그래프이다.

[0118] 평가 과정은 수신노드 중 하나가 메시지를 수신할 때 해시 값을 비교하며 이때 해시가 일치하는 경우 해당 ID의 해시값을 업데이트하고, 일치하지 않는 경우 해시값을 업데이트 하지 않으며 침입자 경고 메시지를 전송하는 방

식으로 진행한다.

[0119] 평가 진행 전, 해시 ECU에서 HRK를 송신한 후, 송신 ECU 및 수신 ECU에서 같은 ID에 대해 동일한 해시코드를 반환하는 과정을 100회 진행하였으며, 100회 모두 동일한 값을 반환함을 확인하였다.

[0120] 이후 침입자 ECU에서 각 ID별로 1000회씩 악의적 메시지를 난수공격으로 수행하였고, 그중 0x100 ID로 수행된 악의적 메시지 400회에 대한 검출 결과는 도 9에서와 같다.

[0121] 0 값은 송신 ECU가 수신한 악의적 메시지 중 해시코드가 일치하지 않아 공격자 메시지로 검출하여 방어에 성공한 것이고, 1 값은 해시값이 일치하여 공격자 메시지를 수용해 공격자가 공격에 성공한 것을 의미한다.

[0122] 표 2는 CAN DB 상의 각 NAME별로 수행된 실험 결과를 정리한 것이다.

표 2

[0123]

	수신된 메시지	검출된 메시지	수용된 메시지	검출율
AAA	4000	3758	242	0.9395
BBB	6000	5608	392	0.934667
CCC	5000	4697	303	0.9394
DDD	4000	3780	220	0.945
EEE	2000	1877	123	0.9385
FFF	4000	3736	264	0.934
GGG	3000	2795	205	0.931667
HHH	3000	2818	182	0.939333
합계	31000	29069	1931	0.93771

[0124] CAN 프로토콜의 Data Field 중 4bit 공간에 HASH Code를 저장함으로써 메시지 인증 과정을 수행하였다.

[0125] 평가 결과 총 31000회에 걸친 악의적 메시지 검출 실험에서 29069개의 악의적 악의적 메시지를 검출하였고, 1931개의 악의적 메시지를 검출 실패 및 수용하였다. 인증코드 용량이 4bit임에 따라 난수 공격에 대한 코드 일치 확률은 이론상 1/16(6.25%) 이며 실제 결과는 1931/31000(6.229%)이므로 오차 0.4%미만의 정확도를 보인다.

[0126] 이상에서 설명한 본 발명에 따른 해시함수가 적용된 메시지 체인 기반 CAN 보안 장치 및 방법은 별도의 보안 프로토콜을 제공하지 않는 차량 네트워크 기술인 CAN에서 해시 함수를 활용한 메시지 기반 보안으로 악의적 메시지를 효율적으로 검출할 수 있도록 한 것으로, 해시 함수를 통해 생성된 값을 주기적으로 전송되는 메시지에 할당하여 동일한 ID의 메시지를 체인으로 연결하는 메시지 체인 기반 보안 방법으로 연산량의 증가없이 다양한 네트워크에 적용할 수 있도록 한다.

[0127] 이상에서의 설명에서와 같이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 본 발명이 구현되어 있음을 이해할 수 있을 것이다.

[0128] 그러므로 명시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 하고, 본 발명의 범위는 전술한 설명이 아니라 특허청구 범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

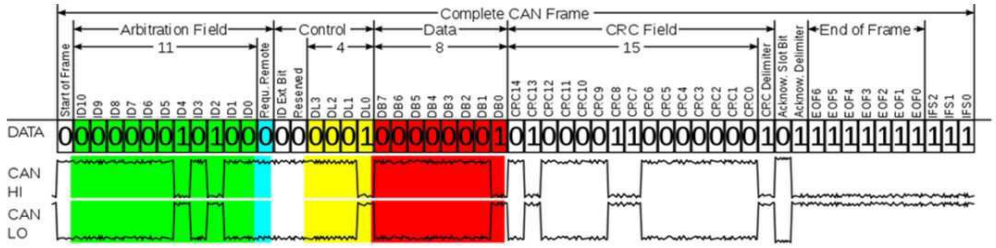
부호의 설명

[0129]

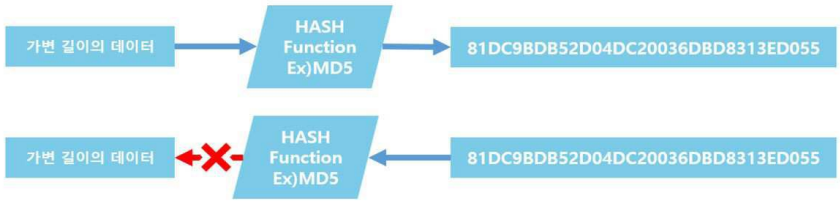
10. 해시값 생성부
20. 생성 시간 판단부
30. 해시 리셋키 생성부
40. 해시값 재생성부
50. CAN 메시지 전송부
60. 유효성 판단부
70. 메시지 수신 및 실행부
80. 경고 전송부

도면

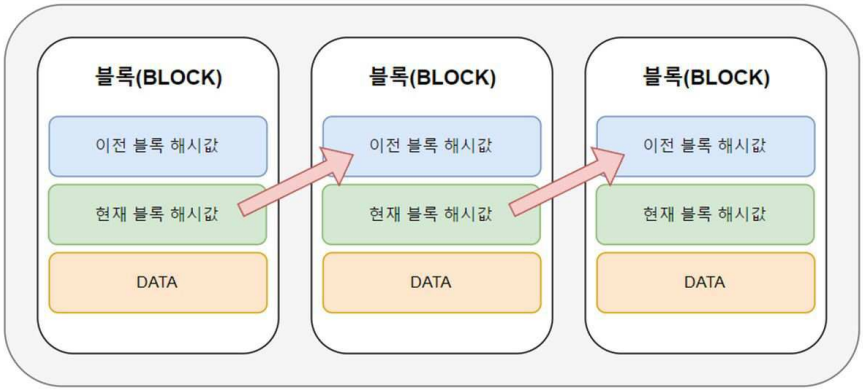
도면1



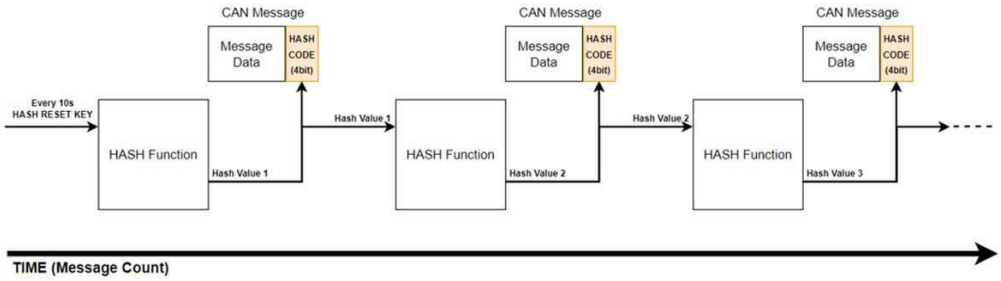
도면2



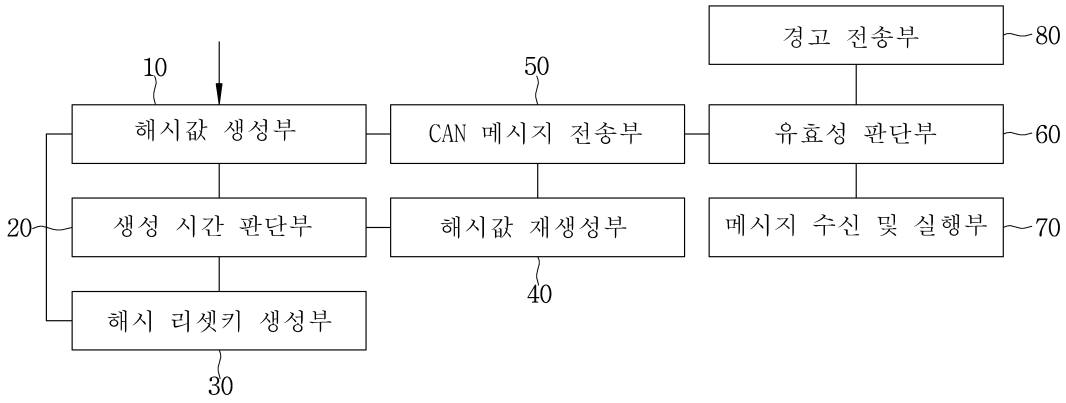
도면3



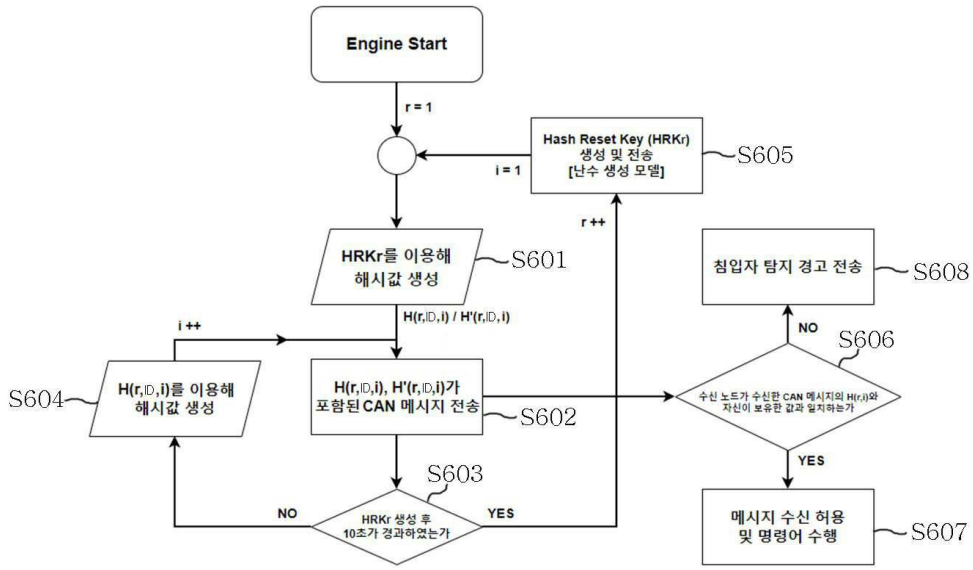
도면4



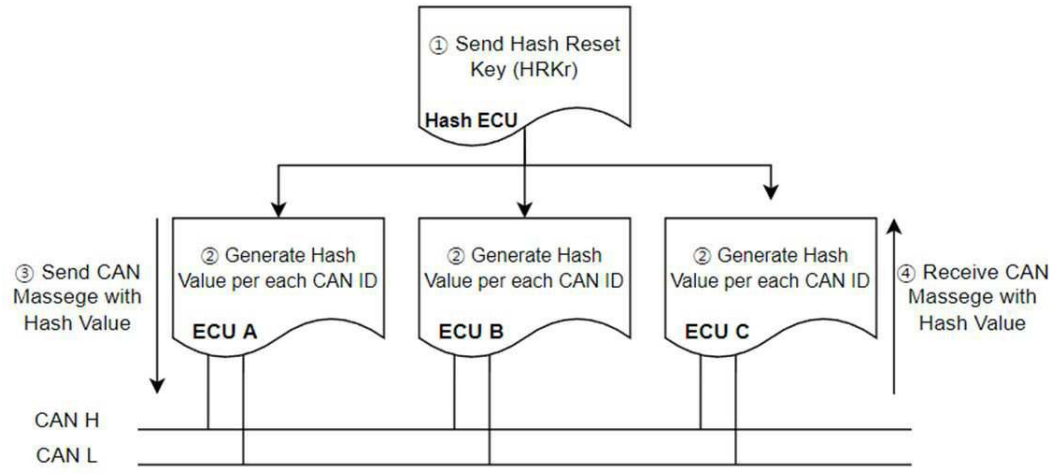
도면5


경고 전송부
80
10
50
해시값 생성부
CAN 메시지 전송부
유효성 판단부
60
20
생성 시간 판단부
해시값 재생성부
메시지 수신 및 실행부
70
40
해시 리셋키 생성부
30

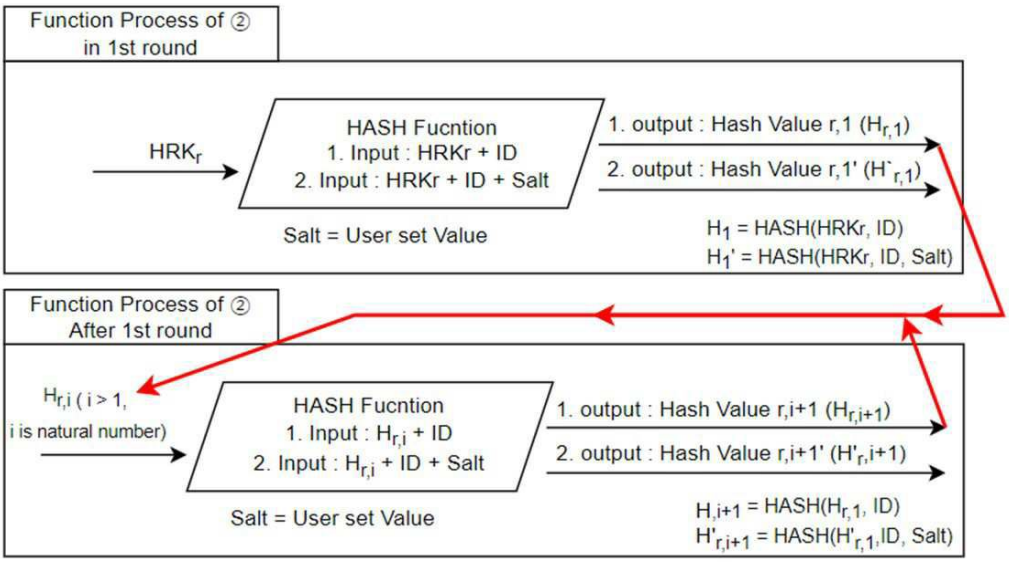
도면6


Engine Start
r = 1
Hash Reset Key (HRKr)
생성 및 전송
[난수 생성 모델]
S605
i = 1
r ++
HRKr를 이용해
해시값 생성
S601
침입자 탐지 경고 전송
S608
H(r,ID,i) / H'(r,ID,i)
i ++
NO
S606
S604
H(r,ID,i)를 이용해
해시값 생성
H(r,ID,i), H'(r,ID,i)가
포함된 CAN 메시지 전송
S602
수신 노드가 수신한 CAN 메시지의 H(r,i)와
자신이 보유한 값과 일치하는가
YES
S603
NO
HRKr 생성 후
10초가 경과하였는가
YES
메시지 수신 허용
및 명령어 수행
S607

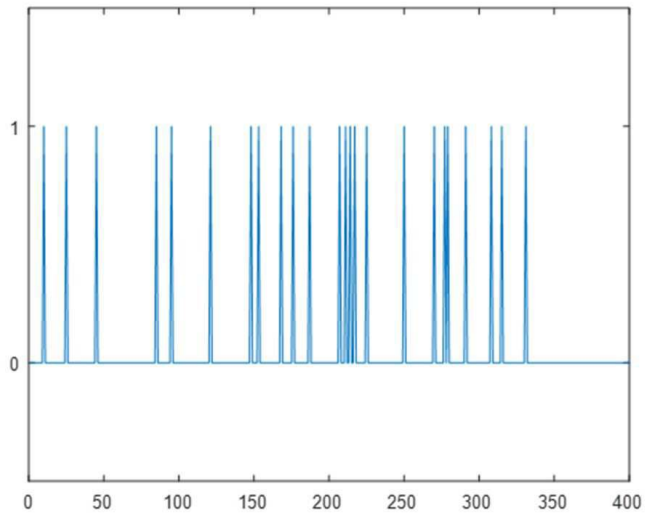
도면7


① Send Hash Reset
Key (HRKr)
Hash ECU
③ Send CAN
Massege with
Hash Value
② Generate Hash
Value per each CAN ID
ECU A
② Generate Hash
Value per each CAN ID
ECU B
② Generate Hash
Value per each CAN ID
ECU C
④ Receive CAN
Massege with
Hash Value
CAN H
CAN L

도면8


Function Process of ②
in 1st round
HRK$_r$
HASH Fucntion
1. Input : HRKr + ID
2. Input : HRKr + ID + Salt
Salt = User set Value
1. output : Hash Value r,1 ($H_{r,1}$)
2. output : Hash Value r,1' ($H`_{r,1}$)
H_1 = HASH(HRKr, ID)
H_1' = HASH(HRKr, ID, Salt)
Function Process of ②
After 1st round
$H_{r,i}$ (i > 1,
i is natural number)
HASH Fucntion
1. Input : $H_{r,i}$ + ID
2. Input : $H_{r,i}$ + ID + Salt
Salt = User set Value
1. output : Hash Value r,i+1 ($H_{r,i+1}$)
2. output : Hash Value r,i+1' ($H'_{r,i+1}$)
$H_{,i+1}$ = HASH($H_{r,1}$, ID)
$H'_{r,i+1}$ = HASH($H'_{r,1}$,ID, Salt)

도면9


1
0
0
50
100
150
200
250
300
350
400