(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년02월02일
(11) 등록번호 10-1701307
(24) 등록일자 2017년01월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 12/40* (2006.01)
(52) CPC특허분류
H04L 9/0861 (2013.01)
H04L 9/0819 (2013.01)
(21) 출원번호 10-2015-0121049
(22) 출원일자 2015년08월27일
심사청구일자 2015년08월27일
(56) 선행기술조사문헌
KR101249394 B1*
KR1020050032477 A*
KR1020150024117 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
최원석
서울특별시 강북구 삼양로 256 105동 501호 (미아동,삼성래미안미아1차아파트)
이보영
경기도 의왕시 내손로 13 106동 2103호 (내손동, 포일자이아파트)
(뒷면에 계속)
(74) 대리인
김등용, 김홍석

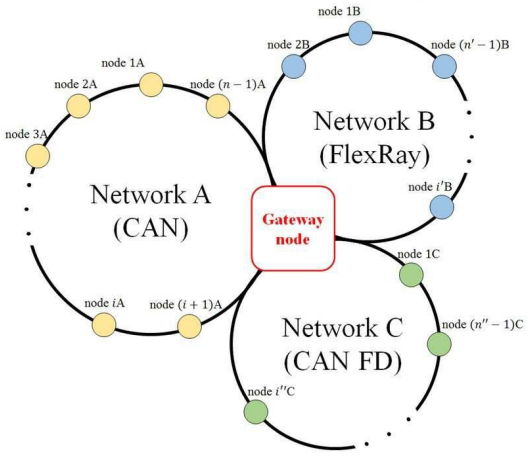
전체 청구항 수 : 총 5 항 심사관 : 윤태섭

(54) 발명의 명칭 **데이터를 송신하는 방법**

(57) 요 약

데이터를 송신하는 방법이 개시된다. 상기 데이터를 송신하는 방법은 네트워크 시스템에 포함된 제1 서브 네트워크에 포함된 송신 노드가 상기 네트워크 시스템에 포함된 제2 서브 네트워크에 포함된 수신 노드로 데이터를 송신하는 방법으로서, 상기 송신 노드가 상기 제1 서브 네트워크의 그룹키인 제1 그룹키를 이용하여 메시지를 암호화한 제1 암호문을 게이트웨이 노드로 송신하는 단계, 상기 게이트웨이 노드가 상기 제1 암호문을 상기 제2 서브 네트워크의 그룹키인 제2 그룹키로 암호화된 제2 암호문으로 변경하는 단계, 및 상기 게이트웨이 노드가 상기 제2 암호문을 상기 수신 노드로 송신하는 단계를 포함한다.

대 표 도 - 도1



10

(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 2012/40215 (2013.01)
H04L 2012/40234 (2013.01)
H04L 2012/40241 (2013.01)
(72) 발명자
조효진
서울특별시 성북구 안암로 145 자연계캠퍼스 로봇융합관 403호 (안암동5가,고려대학교안암캠퍼스)
우사무엘
서울특별시 송파구 오금로53길 7 403호 (거여동,명산주택)
서민혜
서울특별시 양천구 목동중앙남로 21-15 101동 703호 (목동,에이스아파트)
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동,경희궁의아침3단지아파트)

이 발명을 지원한 국가연구개발사업
과제고유번호 B0101150553000300 3
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신방송연구개발사업
연구과제명 자동차 전장 ECU간 보안전송기술 개발
기 여 율 1/1
주관기관 인포뱅크
연구기간 2015.03.01 ~ 2016.02.29

명 세 서

청구범위

청구항 1

네트워크 시스템에 포함된 제1 서브 네트워크에 포함된 송신 노드가 상기 네트워크 시스템에 포함된 제2 서브 네트워크에 포함된 수신 노드로 데이터를 송신하는 방법에 있어서,

상기 송신 노드가 상기 제1 서브 네트워크의 그룹키인 제1 그룹키를 이용하여 메시지를 암호화한 제1 암호문을 게이트웨이 노드로 송신하는 단계;

상기 게이트웨이 노드가 상기 제1 암호문을 상기 제2 서브 네트워크의 그룹키인 제2 그룹키로 암호화된 제2 암호문으로 변경하는 단계; 및

상기 게이트웨이 노드가 상기 제2 암호문을 상기 수신 노드로 송신하는 단계를 포함하고,

상기 게이트웨이 노드는 재암호화키를 이용하여 상기 제1 암호문을 상기 제2 암호문으로 변경하고,

상기 재암호화키는,

상기 제1 서브 네트워크에 포함된 제1 대표 노드와 상기 제2 서브 네트워크에 포함된 제2 대표 노드 각각이 제1 난수와 제2 난수를 선택하는 단계;

상기 제1 대표 노드와 상기 제2 대표 노드가, 상기 제1 대표 노드가 상기 제1 난수를 유한 그룹의 생성원에 지수승하여 연산한 제1 계산값과 상기 제2 대표 노드가 상기 제2 난수를 상기 유한 그룹의 생성원에 지수승하여 연산한 제2 계산값을 교환하는 단계;

상기 제1 대표 노드와 상기 제2 대표 노드가, 상기 제1 난수와 상기 제2 난수의 곱을 상기 유한 그룹의 생성원에 지수승한 값인 공유값을 연산하는 단계;

상기 게이트웨이 노드가 상기 제1 대표 노드로부터 상기 공유값에 상기 제1 그룹키의 역수를 곱한 값인 제3 계산값을 수신하고, 상기 제2 대표 노드로부터 상기 공유값의 역수에 상기 제2 그룹키를 곱한 값인 제4 계산값을 수신하는 단계; 및

상기 게이트웨이 노드가 상기 제3 계산값과 상기 제4 계산값의 곱인 상기 재암호화키를 생성하는 단계를 통하여 생성되는,

데이터를 송신하는 방법.

청구항 2

제1항에 있어서,

상기 네트워크 시스템은 차량용 네트워크 시스템이고,

상기 제1 서브 네트워크 또는 상기 제2 서브 네트워크는 CAN(Controller Area Network), CAN FD(CAN with Flexible Data Rate), LIN(Local Interconnect Network) 또는 Flexlay 네트워크인, 데이터를 송신하는 방법.

청구항 3

제1항에 있어서,

상기 송신 노드와 상기 수신 노드 각각은 대응되는 전자 장치의 동작을 제어하는 ECU(Electronic Control Unit)이고,

상기 게이트웨이 노드는 게이트웨이 ECU인, 데이터를 송신하는 방법.

청구항 4

제1항에 있어서,

상기 데이터를 송신하는 방법은,

상기 수신 노드가 상기 제2 그룹키를 이용하여 상기 제2 암호문을 복호화하는 단계를 더 포함하는, 데이터를 송신하는 방법.

청구항 5

제1항에 있어서,

상기 제1 그룹키는 상기 제1 서브 네트워크에 포함된 복수의 노드들 각각이 선택한 난수의 곱을 유한 그룹의 생성원(g)에 지수승한 값이고,

상기 제2 그룹키는 상기 제2 서브 네트워크에 포함된 복수의 노드들 각각이 선택한 난수의 곱을 유한 그룹의 생성원(g)에 지수승한 값인,

데이터를 송신하는 방법.

청구항 6

삭제

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 차량용 네트워크 시스템에서 데이터를 송신하는 방법에 관한 것으로, 서로 다른 서브 네트워크에 포함된 노드들 사이에서 전송되는 데이터에 대해 게이트웨이 노드에 의한 복호화 과정을 거치지 않고 데이터를 송신할 수 있는 방법에 관한 것이다.

배 경 기 술

[0002] 자동차 산업과 IT 산업의 융합이라 불릴 만큼, 최근 자동차에는 다양한 전자 제어 장치가 장착되어 판매되고 있다. 이와 같은 전자 제어 장치를 전자 제어 유닛(Electronic Control Unit; ECU)이라 한다. ECU는 마이크로프로세서(microprocessor)가 장착된 소형 컴퓨터라 할 수 있다. ECU의 기능 중 엔진 제어 유닛에 의한 엔진의 연료 분사 제어가 가장 대표적이나, 최근에는 변속기, 자세 제어, 에어백 제어, 타이어 공기압 관리 등 차량의 주행이나 관리에 필요한 거의 모든 기능들이 ECU를 통하여 제어되고 있다. 즉, 기존 차량 내부 기기는 기계식 장치가 주를 이루었던 반면, 최근에는 ECU를 포함한 전자식 장치들이 주를 이루고 있다.

[0003] 이로 인해 자동차 산업에서도 해킹이라는 용어가 사용되게 되었다. 2010년 미국의 워싱턴 대학 연구팀을 최초로 하여 차량용 ECU에 악의적인 제어 패킷을 전송하여 차량을 제어하는 사례들이 발표되기 시작하였다. 예를 들어, 차량의 가속페달이 움직이지 않은 상태에서 엔진을 담당하는 ECU에게 연료 분사 제어 패킷을 악의적으로 전송하여 차량이 가속되는 경우가 있었다.

[0004] 정보 탈취를 목표로 하는 기존 해킹과 달리 차량 해킹에 의한 영향은 운전자의 생명과 연관되어 있어 더욱 큰 문제가 되고 있다. 따라서 이러한 차량 해킹을 방어하기 위한 다양한 방법들이 연구되고 있으며, 본 발명은 이러한 차량 해킹을 근본적으로 막을 수 있는 차량 ECU들 간의 안전한 그룹 키 교환 기술에 관한 것이다. 안전하게 교환된 그룹 키를 통하여, 암호화, 메시지 인증 등과 같은 암호 프리미티브를 적용할 수 있을 것이다.

[0005] 자동차 해킹의 근본적인 원인은 차량 내부 네트워크의 각 노드들이 어떠한 암호학적 방법이 적용되지 않은 상태로 상호 통신을 하고 있다는 점에 있다. 각 ECU들은 자신의 데이터를 전송할 때, 데이터를 암호화하고 암호화된 데이터를 전송함으로써 이러한 문제를 해결할 수 있다.

[0006] 이러한 암호화 기법을 적용하기 위해서 각 ECU들이 사전에 안전하게 비밀 키를 공유하고 있어야 하며, 비밀키를 기반으로 암호화 또는 복호화를 수행할 수 있다.

[0007] 따라서, 본 발명은 차량 내부 네트워크에 속해 있는 정당한 ECU들 간에 동일한 그룹 키를 안전하게 교환할 수 있는 그룹 키 교환 프로토콜을 제안한다. 또한, 게이트웨이 ECU(gateway ECU)가 암호문을 복호화하는 과정을 거치지 아니하고 암호문의 암호화키를 변경할 수 있는 재암호화(Re-encryption) 기법을 제안한다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 공개특허 제10-2014-0078917호

발명의 내용

해결하려는 과제

[0009] 본 발명이 이루고자 하는 기술적인 과제는 서로 다른 서브 네트워크에 포함된 노드들 사이에서 암호화된 메시지를 전송할 때에, 게이트웨이 노드가 데이터를 복호화하지 않고 제1 암호화키로 암호화된 암호문을 제2 암호화키로 암호화된 암호문으로 변경하여 제공할 수 있는 데이터 전송 방법에 관한 것이다.

과제의 해결 수단

[0010] 본 발명이 실시 예에 따른 데이터를 송신하는 방법은, 네트워크 시스템에 포함된 제1 서브 네트워크에 포함된 송신 노드가 상기 네트워크 시스템에 포함된 제2 서브 네트워크에 포함된 수신 노드로 데이터를 송신하는 방법으로서, 상기 송신 노드가 상기 제1 서브 네트워크의 그룹키인 제1 그룹키를 이용하여 메시지를 암호화한 제1 암호문을 게이트웨이 노드로 송신하는 단계, 상기 게이트웨이 노드가 상기 제1 암호문을 상기 제2 서브 네트워크의 그룹키인 제2 그룹키로 암호화된 제2 암호문으로 변경하는 단계, 및 상기 게이트웨이 노드가 상기 제2 암호문을 상기 수신 노드로 송신하는 단계를 포함한다.

발명의 효과

[0011] 본 발명의 실시 예에 따른 데이터를 송신하는 방법에 의할 경우, 네트워크 시스템에 포함된 복수의 서브 네트워크들 각각에 포함된 노드들은 안전한 그룹키를 공유할 수 있는 효과가 있다.

[0012] 또한, 본 발명의 실시 예에 따른 데이터를 송신하는 방법에 의할 경우, 게이트웨이 ECU에게 암호문에 대응하는 평문을 노출시키지 않고 다른 서브 네트워크에 포함된 수신 노드로 메시지를 송신할 수 있는 효과가 있다.

도면의 간단한 설명

[0013] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 의한 네트워크 시스템을 도시한다.

도 2는 도 1에 도시된 네트워크 시스템에서 데이터 통신 방법을 설명하기 위한 흐름도이다.

도 3은 도 2에 도시된 재암호화키 생성 단계를 구체적으로 설명하기 위한 흐름도이다.

도 4a 내지 도 4e는 도 2에 도시된 그룹키 공유 단계를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0015] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0016] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0017] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0018] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0019] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0020] 우선, 본 명세서에서 사용되는 용어를 표로 정리하면 다음과 같고, 이하에서는 본 명세서에서 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

표 1

[0021]

용어	설명
GK_A	서브 네트워크 A의 그룹키
K_{AB}	그룹키 GK_A로 암호화된 암호문을 그룹키 GK_B로 암호화된 암호문으로 변경하기 위한 재암호화키(Re-encryption key)
h()	암호학적 해쉬함수
Z^*_p	유한 그룹(finite group)
g	유한 그룹의 생성원(generator)

[0022] 도 1은 본 발명의 일 실시 예에 의한 네트워크 시스템을 도시한다.

[0023] 차량용 네트워크 시스템일 수 있는 네트워크 시스템(10)은 적어도 하나 이상의 서브 네트워크를 포함할 수 있다. 상기 서브 네트워크는 CAN(Controller Area Network), LIN(Local Interconnect Network), CAN FD(CAN with Flexible Data Rate), 및 Flexlay 네트워크 중 어느 하나일 수 있고, 도 1에는 제1 서브 네트워크(Network A), 제2 서브 네트워크(Network B), 및 제3 서브 네트워크(Network C)만이 도시되어 있으나, 본 발명이 네트워크 시스템(10)에 포함되는 서브 네트워크의 개수에 제한되는 것은 아니다.

[0024] 제1 서브 네트워크(Network A)는 CAN일 수 있고, 제2 서브 네트워크(Network B)는 Flexlay 네트워크일 수 있고, 제3 서브 네트워크(Network C)는 CAN FD일 수 있다.

[0025] 각각의 서브 네트워크는 복수의 노드들을 포함하고, 서로 다른 서브 네트워크에 포함된 노드 사이에서의 통신은 게이트웨이 노드를 통하여 수행된다. 구체적으로 제1 서브 네트워크(Network A)는 n(n은 1 이상의 자연수) 개의 노드들을 포함하고, 제2 서브 네트워크(Network B)는 x(x는 1 이상의 자연수) 개의 노드들을 포함하고, 제3 서브 네트워크(Network C)는 y(y는 1 이상의 자연수) 개의 노드들을 포함할 수 있다.

[0026] 또한, 본 명세서의 노드는 각각의 전자 장치를 제어하는 ECU를 의미할 수 있고, 게이트웨이 노드는 게이트웨이 ECU를 의미할 수 있다. 또한, 상기 ECU와 상기 게이트웨이 ECU는 정보를 송수신하기 위한 송수신기를 포함하는 개념일 수 있고, 실시 예에 따라 상기 송수신기는 상기 ECU 또는 상기 게이트웨이 ECU와는 별도로 구현될 수도 있다.

[0027] 도 2는 도 1에 도시된 네트워크 시스템에서 데이터 통신 방법을 설명하기 위한 흐름도이다. 구체적으로 도 2에

서는 제1 서브 네트워크(Network A)에 포함된 송신 노드가 제2 서브 네트워크(Network B)에 포함된 수신 노드로 데이터를 전송하는 과정을 일 예로 설명한다.

[0028] 도 1과 도 2를 참조하면, 서브 네트워크에 포함된 복수의 노드들은 상기 서브 네트워크의 그룹키를 공유한다(S100). 즉, 제1 서브 네트워크(Nwtwork A)에 포함된 복수의 노드들이 제1 서브 네트워크(Network A)의 그룹키인 제1 그룹키(GK_A)를 공유하고, 제2 서브 네트워크(Network B)에 포함된 복수의 노드들이 제2 서브 네트워크(Network B)의 그룹키인 제2 그룹키(GK_B)를 공유한다. 그룹키 공유 과정에 대한 구체적인 설명은 후술하기로 한다. 단계 S100에서 공유된 그룹키는 메시지를 암호화하거나 복호화하는 과정에서 이용되는 암호화키를 의미할 수 있다.

[0029] S200 단계에서, 게이트웨이 ECU는 재암호화키를 생성한다(S200). 재암호화키 생성 과정에 대한 구체적인 설명은 후술하기로 한다.

[0030] 제1 서브 네트워크(Network A)에 포함된 송신 노드는 수신 노드로 송신하고자 하는 메시지(m)를 암호화한다(S300). 상기 송신 노드는 제1 서브 네트워크(Network A)의 그룹키(GK_A)를 이용하여 메시지(m)을 암호화할 수 있다. 구체적으로 암호문(c)은 아래의 수학식 1를 이용하여 생성될 수 있다.

수학식 1

[0031] $$c=(g^r \times m,\ g^r \times GK_A)$$

[0032] 상기 수학식 1에서, "r"은 임의의 난수이다.

[0033] 송신 노드는 생성된 암호문(c)을 게이트웨이 ECU로 송신한다(S400). 암호문(c)을 수신한 게이트웨이 ECU는 제1 그룹키(GK_A)로 암호화된 암호문(c)을 제2 그룹키(GK_B)로 암호화된 암호문(c')으로 재암호화한다(S600). 즉, 상기 게이트웨이 ECU는, 송신 노드가 암호문(c)을 복호화할 수 있도록, 암호문(c)을 상기 송신 노드가 속한 서브 네트워크인 제2 서브 네트워크(Network B)의 그룹키(GK_B)로 암호화한 암호문(c')으로 변환할 수 있다. 재암호화는 아래의 수학식 2를 이용하여 수행될 수 있다.

수학식 2

[0034] $$\begin{aligned} c' &= (g^r \times m,\ g^r \times GK_A \times K_{AB}) \\ &= (g^r \times m,\ g^r \times GK_A \times \frac{GK_B}{GK_A}) \\ &= (g^r \times m,\ g^r \times GK_B) \end{aligned}$$

[0035] 단계 S800 에서, 게이트웨이 ECU는 재암호화된 암호문(c')을 수신 노드로 송신한다.

[0036] 단계 S900에서, 제2 서브 네트워크(Network B)에 포함된 수신 노드는 게이트웨이 ECU로부터 암호문(c')을 수신하고, 수신된 암호문(c')을 복호화하여 메시지(m)을 얻을 수 있다.

[0037] 우선, 아래의 수학식 3과 같이 수신 노드는 제2 그룹키(GK_B), 보다 구체적으로는 제2 그룹키(GK_B)의 역수(GK_B^{-1})를 이용하여 암호문(c')으로부터 g^r을 계산할 수 있다.

수학식 3

[0038] $$g^r \times GK_A \times GK_A^{-1} = g^r$$

[0039] 다음으로, 아래의 수학식 4과 같이 수신 노드는 수학식 3을 통하여 얻은 g^r의 역원을 계산하고, 이를 이용하여 메시지(m)을 획득할 수 있다.

수학식 4

[0040] $$g^r \times m \times (g^r)^{-1} = m$$

[0041] 도 3은 도 2에 도시된 재암호화키 생성 단계를 구체적으로 설명하기 위한 흐름도이다.

[0042] 재암호화키(K_{AB})는 제1 서브 네트워크(Network A)의 그룹키(GK_A)로 암호화되어 있는 암호문(c)을 제2 서브 네트워크(Network B)의 그룹키(GK_B)로 암호화되어 있는 암호문(c')으로 변환할 수 있는 키로서, 실시 예에 따라 변화키로 불릴 수도 있다.

[0043] 제1 서브 네트워크(Network A)의 대표 노드인 제1 대표 노드와 제2 서브 네트워크(Network B)의 대표 노드인 제2 대표 노드 각각이 임의의 난수를 선택한다(S210). 즉, 상기 제1 대표 노드는 제1 난수(R_A)를 선택하고 상기 제2 대표 노드는 제2 난수(R_B)를 선택할 수 있다. 상기 제1 대표 노드는 제1 서브 네트워크(Network A)에 포함된 복수의 노드들 중 미리 정해진 노드일 수 있으며, 실시 예에 따라 그룹키 공유 단계에서의 제1 노드일 수도 있다. 또한, 상기 제2 대표 노드는 제2 서브 네트워크(Network B)에 포함된 복수의 노드들 중 미리 정해진 노드일 수 있으며, 실시 예에 따라 그룹키 공유 단계에서의 제1 노드일 수도 있다.

[0044] 단계 S230에서, 상기 제1 대표 노드와 상기 제2 대표 노드 각각은 유한 그룹의 생성원(g)에 선택된 난수를 지수승하여 계산된 계산값을 서로 교환한다. 즉, 상기 제1 대표 노드는 제1 난수(R_A)를 유한 그룹의 생성원(g)에 지수승하여 제1 계산값(g^{R_A})을 생성하고, 제1 계산값(g^{R_A})을 게이트웨이 ECU를 경유하여 제2 대표 노드로 송신한다. 또한, 상기 제2 대표 노드는 제2 난수(R_B)를 유한 그룹의 생성원(g)에 지수승하여 제2 계산값(g^{R_B})을 생성하고, 제2 계산값(g^{R_B})을 게이트웨이 ECU를 경유하여 제1 대표 노드로 송신한다.

[0045] 단계 S250에서, 상기 제1 대표 노드와 상기 제2 대표 노드는 상대방으로부터 수신된 계산값과 자신이 선택한 난수를 이용하여 공유값(h)을 생성할 수 있다. 즉, 상기 제1 대표 노드는 제1 난수(R_A)를 상기 제2 대표 노드로부터 수신한 제2 계산값(g^{R_B})에 지수승하여 공유값($h = g^{R_A R_B}$)을 생성하고, 상기 제2 대표 노드는 제2 난수(R_B)를 상기 제1 대표 노드로부터 수신한 제1 계산값(g^{R_A})에 지수승하여 공유값($h = g^{R_A R_B}$)을 생성할 수 있다.

[0046] 단계 S270에서, 상기 제1 대표 노드와 상기 제2 대표 노드는 자신의 그룹키의 역수와 공유값을 곱하거나 공유값의 역수와 자신의 그룹키의 곱하여 계산값을 생성하고, 생성된 계산값을 게이트웨이 ECU로 송신한다. 즉, 상기 제1 대표 노드는 공유값(h)과 제1 그룹키(GK_A)를 이용하여 제3 계산값($h*GK_A^{-1}$ 또는 $h^{-1}*GK_A$)을 생성하고 생성된 제3 계산값을 게이트웨이 ECU로 송신할 수 있다. 또한, 상기 제2 대표 노드는 고유값(h)과 제2 그룹키(GK_B)를 이용하여 제4 계산값($h^{-1}*GK_B$ 또는 $h*GK_B^{-1}$)을 생성하고 생성된 제4 계산값을 게이트웨이 ECU로 송신할 수 있다.

[0047] 단계 S290에서, 게이트웨이 ECU는 상기 제1 대표 노드와 상기 제2 대표 노드로부터 수신된 제3 계산값과 제4 계산값을 이용하여 재암호화키($GK_A^{-1}*GK_B$)를 생성할 수 있다.

[0048] 도 4a 내지 도 4e는 도 2에 도시된 그룹키 공유 단계를 설명하기 위한 도면이다. 도 4를 통하여 제1 서브 네트워크(Network A)에 포함된 노드들이 제1 그룹키(GK_A)를 공유하는 과정을 설명한다.

[0049] 우선, 제1 서브 네트워크(Network A)에 포함된 n 개(n은 2 이상의 자연수)의 노드들 각각은 자신의 난수를 선택

한다. 즉, 제1 노드(ECU 1A)는 제1 난수(r_{1A})를 선택하고 제k 노드(ECU kA, k는 1보다 크거나 같고 n보다 작거나 같은 자연수)는 제k 난수(r_{kA})를 선택한다.

[0050] 도 4a를 참조하면, 제1 ECU(ECU 1A)는 제1 난수(r_{1A})를 공개 파라미터인 유한 그룹의 생성원(g)에 지수승하여 연산값($g^{r_{1A}}$)을 계산한다. 또한, 제1 ECU(ECU 1A)는 연산값($g^{r_{1A}}$)을 제2 ECU(ECU 2A)에게 송신한다.

[0051] 도 4b를 참조하면, 제2 ECU(ECU 2A)는 제2 난수(r_{2A})를 연산값($g^{r_{1A}}$)에 지수승하여 연산값($g^{r_{1A}r_{2A}}$)을 생성한다. 또한, 제2 ECU(ECU 2A)는 $(g^{r_{1A}}, g^{r_{2A}}, g^{r_{1A}r_{2A}})$를 제3 ECU(ECU 3A)로 송신한다.

[0052] 도 4c를 참조하면, 제3 ECU(ECU 3A)는 제3 난수(r_{3A})와 제2 ECU(ECU 2A)로부터 수신된 값을 이용하여 연산을 수행하고, $(g^{r_{1A}r_{3A}}, g^{r_{2A},r_{3A}}, g^{r_{1A},r_{2A}}, g^{r_{1A},r_{2A},r_{3A}})$를 제4 ECU(ECU 4A)로 송신한다.

[0053] 도 4d를 참조하면, 제4 ECU(ECU 4A)는 제4 난수(r_{4A})와 제3 ECU(ECU 3A)로부터 수신된 값을 이용하여 연산을 수행하고, $(g^{r_{1A}r_{3A}r_{4A}}, g^{r_{2A},r_{3A},r_{4A}}, g^{r_{1A},r_{2A},r_{4A}}, g^{r_{1A},r_{2A},r_{3A}}, g^{r_{1A},r_{2A},r_{3A},r_{4A}})$를 제5 ECU(ECU 5A)로 송신한다.

[0054] 이후에 이전 노드로부터 연산 결과를 수신한 노드(ECU kA)는 자신이 선택한 난수(r_{kA})를 상기 이전 노드로부터 수신한 연산 결과에 지수승한 연산값을 다음 노드(ECU (k+1)A)로 송신할 수 있다. 마찬가지로 도 4e를 참조하면, 제n 노드는 제(n-1) 노드로부터 $(g^{r_{1A}r_{3A}r_{4A}\cdots r_{n-1A}}, g^{r_{2A}r_{3A}r_{4A}\cdots r_{n-1A}}, g^{r_{1A}r_{2A}r_{4A}\cdots r_{n-1A}}, g^{r_{1A},r_{2A},r_{3A}\cdots r_{n-2A}}, g^{r_{1A},r_{2A},r_{3A},r_{4A}\cdots r_{n-1A}})$를 수신하고, 수신된 값에 제n 난수($r_{nA}$)를 지수승하여 $(g^{r_{1A}r_{3A}r_{4A}\cdots r_{nA}}, g^{r_{2A}r_{3A}r_{4A}\cdots r_{nA}}, g^{r_{1A}r_{2A}r_{4A}\cdots r_{nA}}, g^{r_{1A},r_{2A},r_{3A}\cdots r_{n-1A}}, g^{r_{1A},r_{2A},r_{3A},r_{4A}\cdots r_{nA}})$를 연산한다.

[0055] 또한, 제n ECU(ECU nA)는 $g^{r_{1A}r_{2A}\cdots r_{nA}/r_{iA}}$ 연산하고, 연산값을 제i ECU(ECU iA)로 송신한다. 즉, 제n ECU(ECU nA)는 제1 ECU(ECU 1A)로 $g^{r_{2A}\cdots r_{nA}}$를 전송하고, 제2 ECU(ECU 2A)로 $g^{r_{1A}r_{3}\cdots r_{nA}}$를 전송하고, 제3 ECU(ECU 3A)로 $g^{r_{1A}r_{2A}r_{4A}\cdots r_{nA}}$를 전송할 수 있다.

[0056] 제n 노드(ECU nA)를 제외한 노드들 각각은 자신이 선택한 난수를 제n 노드(ECU nA)로부터 수신된 값에 지수승함으로써 그룹키(GK_A)를 생성할 수 있다. 즉, 제1 서브 네트워크(Network A)의 그룹키($GK_A = g^{r_{1A}\cdots r_{nA}}$)는 제1 서브 네트워크(Network A)에 포함된 모든 노드들 각각이 선택한 난수들의 곱을 유한 그룹의 생성원(g)에 지수승한 값이 될 수 있다.

[0057] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0058] 10 : 네트워크 시스템

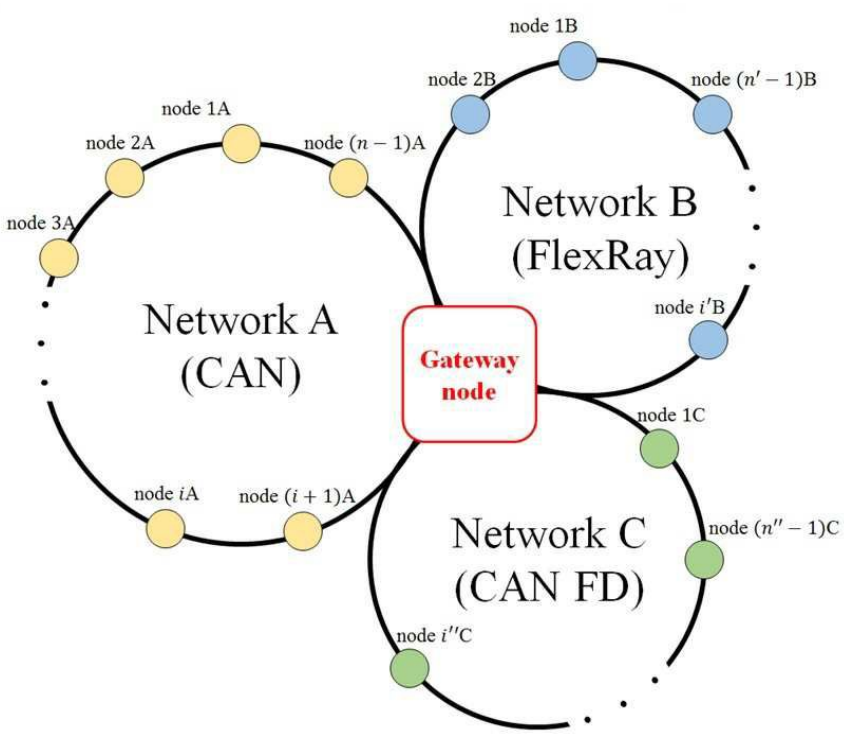
Network A : 제1 서브 네트워크

Network B : 제2 서브 네트워크

Network C : 제3 서브 네트워크

도면

도면1

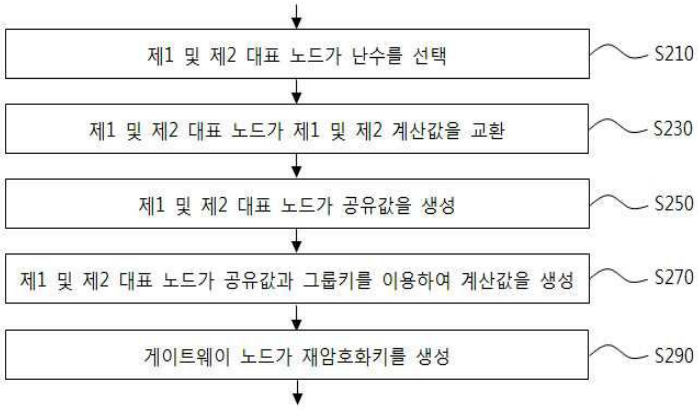


10

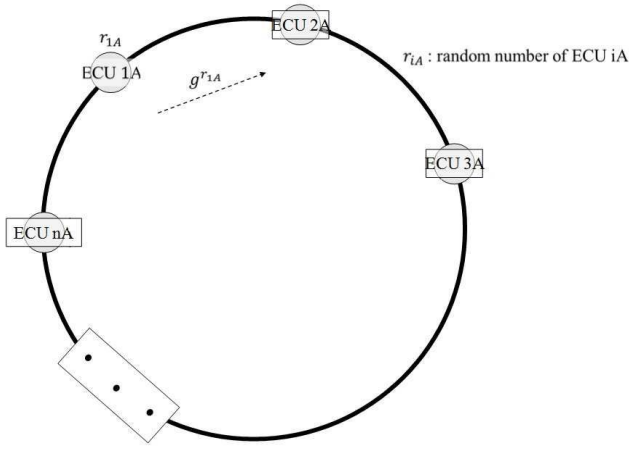
도면2


시작
그룹키 공유 단계
S100
재암호화키 생성 단계
S200
메시지(m)를 암호화
S300
송신 노드가 암호문(c)을 게이트웨이 노드로 송신
S400
암호문(c)을 재암호화하여 암호문(c')을 생성
S600
암호문(c')을 수신 노드로 송신
S800
수신 노드가 암호문(c')을 복호화
S900
종료

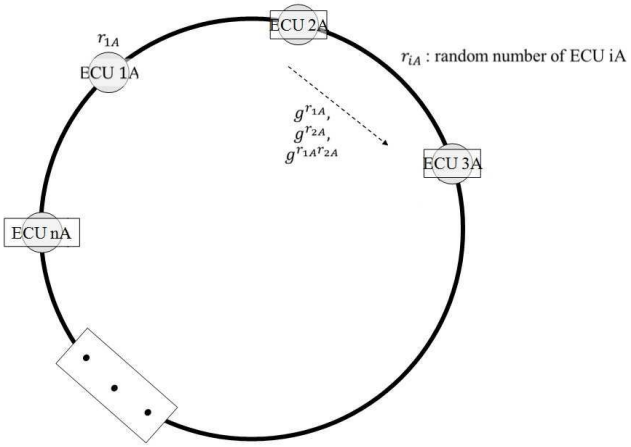
도면3


제1 및 제2 대표 노드가 난수를 선택
S210
제1 및 제2 대표 노드가 제1 및 제2 계산값을 교환
S230
제1 및 제2 대표 노드가 공유값을 생성
S250
제1 및 제2 대표 노드가 공유값과 그룹키를 이용하여 계산값을 생성
S270
게이트웨이 노드가 재암호화키를 생성
S290

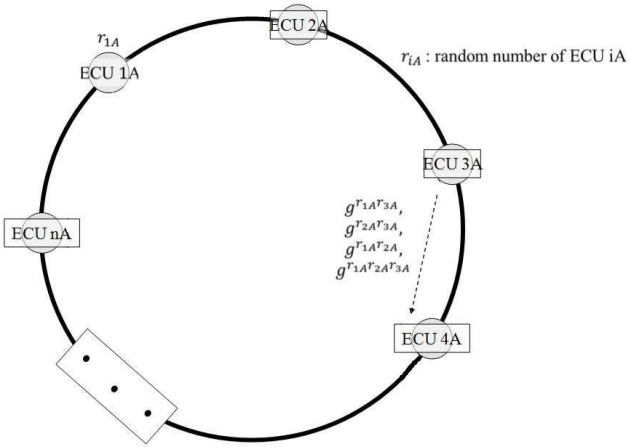
도면4a


r_{1A}
ECU 1A
$g^{r_{1A}}$
ECU 2A
r_{iA} : random number of ECU iA
ECU 3A
ECU nA

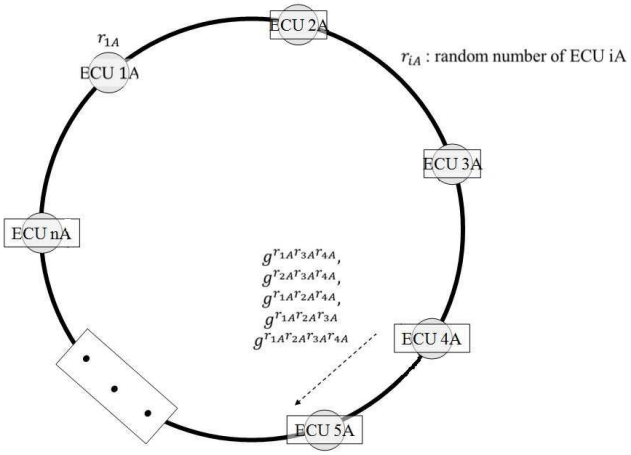
도면4b



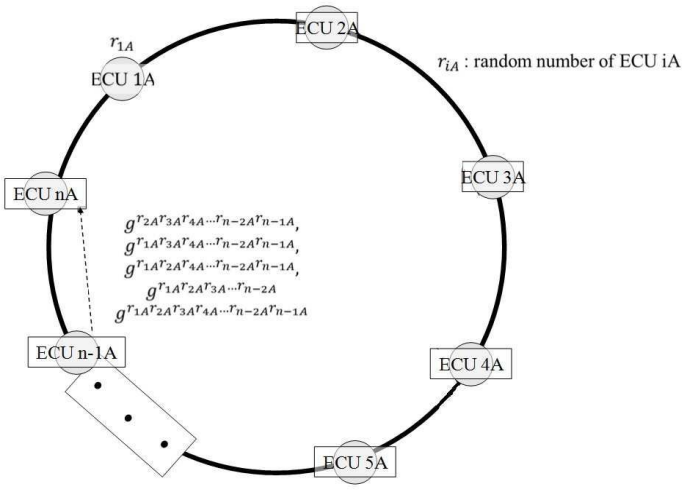
도면4c



도면4d



도면4e


r_{1A}
ECU 1A
ECU 2A
r_{iA} : random number of ECU iA
ECU 3A
ECU nA
$g^{r_{2A}r_{3A}r_{4A}\cdots r_{n-2A}r_{n-1A}}$,
$g^{r_{1A}r_{3A}r_{4A}\cdots r_{n-2A}r_{n-1A}}$,
$g^{r_{1A}r_{2A}r_{4A}\cdots r_{n-2A}r_{n-1A}}$,
$g^{r_{1A}r_{2A}r_{3A}\cdots r_{n-2A}}$
$g^{r_{1A}r_{2A}r_{3A}r_{4A}\cdots r_{n-2A}r_{n-1A}}$
ECU n-1A
ECU 4A
ECU 5A