

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0071865

(43) 공개일자 2021년06월16일

(51) 국제특허분류(Int. Cl.)

H04W 12/00 (2021.01) H04W 4/08 (2009.01)

H04W 4/46 (2018.01)

(52) CPC특허분류

H04W 12/00 (2021.01)

H04W 4/08 (2013.01)

(21) 출원번호 10-2020-0169608

(22) 출원일자 2020년12월07일

심사청구일자 2020년12월07일

(30) 우선권주장

1020190162106 2019년12월06일 대한민국(KR)

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

이동훈

서울특별시 종로구 사직로8길 34, 1404호

안나영

서울특별시 동대문구 약령시로3길 18-3, 302호 (제기동, 덕산맨션)

(74) 대리인

김홍석

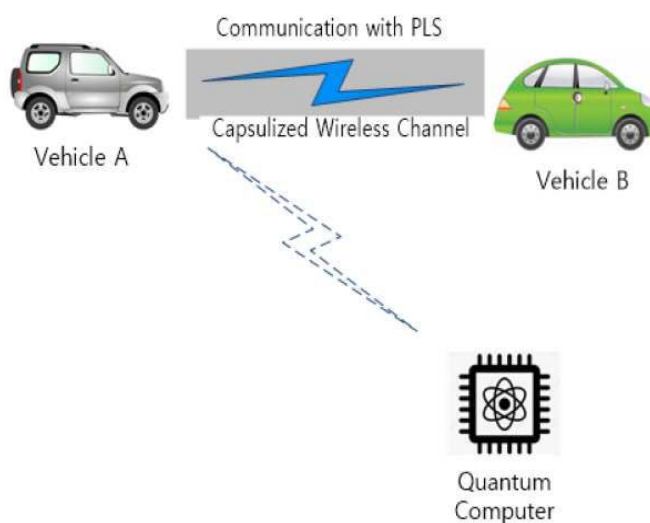
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 자율주행의 물리계층보안을 위한 차량 통신 방법 및 장치

(57) 요약

자율주행 차량의 안전한 통신을 위한 통신 장치 및 통신 방법이 개시된다. 상기 통신 장치는 인접한 차량들로 통신 개시 신호(communication-initiated signal)를 송신하고, 상기 통신 개시 신호에 대응하는 복수의 응답 메시지들을 상기 인접한 차량들로부터 수신하는 송수신부 및 상기 복수의 응답 메시지들에 기초하여 상기 인접한 차량들 각각의 보안 용량(secretcy capacity)을 계산하고, 계산된 보안 용량에 기초하여 상기 인접한 차량들 중에서 통신을 수행할 적어도 하나의 목표 차량을 결정하는 제어부를 포함한다.

대표도 - 도1



(52) CPC특허분류
H04W 4/46 (2020.05)

명세서

청구범위

청구항 1

인접한 차량들로 통신 개시 신호(communication-initiated signal)를 송신하고, 상기 통신 개시 신호에 대응하는 복수의 응답 메시지들을 상기 인접한 차량들로부터 수신하는 송수신부; 및

상기 복수의 응답 메시지들에 기초하여 상기 인접한 차량들 각각의 보안 용량(secretcy capacity)을 계산하고, 계산된 보안 용량에 기초하여 상기 인접한 차량들 중에서 통신을 수행할 적어도 하나의 목표 차량을 결정하는 제어부를 포함하는 통신 장치.

청구항 2

제1항에 있어서,

상기 제어부는 수학적 식 1을 이용하여 상기 인접한 차량들 각각의 보안 용량을 계산하고,

상기 수학적 식 1은 $VSC = \log_2(1 + SNR_{AB}) - \log_2(1 + SNR_{XOR})$ 이고,

상기 $SNR_{XOR} = \frac{\sum_{i=1}^M SNR_{Ai}}{M}$ 이고,

상기 SNR은 상기 통신 개시 신호의 신호대잡음비(signal to noise ratio)이고,

상기 M은 채널 개수이고,

상기 B는 상기 인접한 차량들 중 보안 용량을 계산할 차량이고,

상기 i는 상기 인접한 차량들의 개수인,

통신 장치.

청구항 3

제1항에 있어서,

상기 통신 장치는 자율주행 차량에 탑재되고,

상기 제어부는 상기 인접한 차량들 중에서 가장 높은 보안 용량을 갖는 적어도 하나의 차량을 목표 차량으로 결정하는,

통신 장치.

청구항 4

컴퓨팅 장치에 의해 수행되는 자율주행 차량의 통신 방법에 있어서,

인접한 차량들로 통신 개시 신호를 송신하는 단계;

상기 인접한 차량들 각각으로부터 상기 통신 개시 신호에 대응하는 응답 메시지를 수신하는 단계;

상기 응답 메시지에 기초하여, 상기 인접한 차량들 각각의 보안 용량을 계산하는 단계; 및

계산된 보안 용량에 기초하여 상기 인접한 차량들 중에서 통신을 수행할 적어도 하나의 목표 차량을 결정하는 단계를 포함하는 통신 방법.

청구항 5

제1항에 있어서,

상기 보안 용량을 계산하는 단계는 수학적 식 1을 이용하여 보안 용량을 계산하고,

상기 수학적 식 1은 $VSC = \log_2(1 + SNR_{AB}) - \log_2(1 + SNR_{XOR})$ 이고,

상기 $SNR_{XOR} = \frac{\sum_{i=1}^M SNR_{Ai}}{M}$ 이고,

상기 SNR은 상기 통신 개시 신호의 신호대잡음비(signal to noise ratio)이고,

상기 M은 채널 개수이고,

상기 B는 상기 인접한 차량들 중 보안 용량을 계산할 차량이고,

상기 i는 상기 인접한 차량들의 개수인,

통신 방법.

청구항 6

제4항에 있어서,

상기 컴퓨팅 장치는 자율주행 차량에 탑재되고,

상기 적어도 하나의 목표 차량을 결정하는 단계는 상기 인접한 차량들 중에서 가장 높은 보안 용량을 갖는 적어도 하나의 차량을 목표 차량으로 결정하는,

통신 방법.

발명의 설명

기술 분야

[0001] 본 발명은 자율주행 통신 방식 중에서 V2V 통신(Vehicle-to-Vehicle Communication)에 관한 것이다.

배경 기술

[0002] 가까운 시일 내에 모든 차량에 차량 대 차량(V2V) 통신 기능이 갖추어질 것으로 기대된다. 이를 위해 NHTSA(National Highway Traffic Safety Administration)는 최근에 새로 제조된 모든 차량에 이러한 기능이 필요하다는 제안을 발표했다. 법은 아직 통과되지 않았지만, 법에 따라 모든 모델이 V2V를 특징으로 할 필요가 있을 때 제조업체는 이 기술을 자신의 차량으로 단계적으로 구현해야 한다. 차량 외에 V2V 기능은 일반적인 5G 통신에 필수적이다. 이 기능은 기본 보안 메시지(Basic Security Message, BSM)와 같은 차량 주행 관련 정보를 공유함으로써 자율 주행 차량의 안전한 작동을 달성하는 것을 목표로 한다. V2V 기능을 보장하려면 보안이 설계의 기초가 되어야 하며 개인 정보 보호가 우선되어야 한다. 이전의 연구는 이미 차량 네트워크 계층을 넘어서 보안에 대해 상당한 진전을 이루었다. 그럼에도 불구하고, 기존 차량 보안 방법은 다수의 차량으로부터 수신 또는 전송된 데이터를 처리하는 것과 관련하여 불충분한 컴퓨팅 전력 및 큰 전력 소비를 나타낸다. 이러한 어려움을 극복하기 위해 물리 계층 보안에 관한 연구는 무선 통신 분야에서 무선 채널의 물리적 특성에 기초한 안전한 데이터 통신 방법을 개발하려고 시도했다. 물리 계층 보안의 기본 개념은 노이즈 및 페이딩을 사용하여 데이터 속도를 크게 저하시키지 않으면서 공격자로부터 데이터를 효율적으로 숨길 수 있다는 것이다. 불행히도, 차량 통신 분야에 대한 관련 연구는 여전히 이 분야에 대해서는 거의 없다. 또한, 양자 컴퓨터의 출현은 전통적인 암호화 통신 체계를 방해할 것이며, 이는 무선 통신에서 물리 계층 보안의 필요성을 점점 더 요구할 것이다.

선행기술문헌

특허문헌

[0003] (특허문헌 0001) 대한민국 공개특허 제2019-0045761호 (2019.05.03. 공개)

(특허문헌 0002) 대한민국 공개특허 제2019-0100104호 (2019.08.28. 공개)

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은 보다 안전한 차량 통신 방법 및 장치를 제안하는 데에 있다.

과제의 해결 수단

[0005] 본 발명의 일 실시예에 따른 통신 장치는 인접한 차량들로 통신 개시 신호(communication-initiated signal)를 송신하고, 상기 통신 개시 신호에 대응하는 복수의 응답 메시지들을 상기 인접한 차량들로부터 수신하는 송수신부 및 상기 복수의 응답 메시지들에 기초하여 상기 인접한 차량들 각각의 보안 용량(secretcy capacity)을 계산하고, 계산된 보안 용량에 기초하여 상기 인접한 차량들 중에서 통신을 수행할 적어도 하나의 목표 차량을 결정하는 제어부를 포함한다.

[0006] 또한, 본 발명의 일 실시예에 따른 통신 방법은 컴퓨팅 장치에 의해 수행되고, 인접한 차량들로 통신 개시 신호를 송신하는 단계, 상기 인접한 차량들 각각으로부터 상기 통신 개시 신호에 대응하는 응답 메시지를 수신하는 단계, 상기 응답 메시지에 기초하여, 상기 인접한 차량들 각각의 보안 용량을 계산하는 단계, 및 계산된 보안 용량에 기초하여 상기 인접한 차량들 중에서 통신을 수행할 적어도 하나의 목표 차량을 결정하는 단계를 포함한다.

발명의 효과

[0007] 본 발명은 일정 수준 이상의 차량용 보안 용량을 갖는 차량들의 집합인 보안 클러스터 내에서 차량 통신을 수행함으로써, 차량 통신의 보안을 향상시킬 수 있다.

도면의 간단한 설명

[0008] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

- 도 1은 물리 계층 보안을 설명하기 위한 개념도이다.
- 도 2는 차량 간의 통신에서 발생하는 SNR을 설명하기 위한 개념도이다.
- 도 3은 보안 클러스터 내에서의 차량 통신을 설명하기 위한 개념도이다.
- 도 4는 SC 기반 통신의 각 단계의 구체적인 설명을 도시한 도면이다.
- 도 5는 RSC 기반 차량 통신 알고리즘의 구체적인 설명을 도시한 도면이다.
- 도 6은 RSC 기반 차량 통신 알고리즘이 적용된 통신 환경을 도시한다.
- 도 7은 SC 클러스터 기반 차량 통신 알고리즘의 구체적인 설명을 도시한 도면이다.
- 도 8은 본 발명의 일 실시예에 따른 블록 생성 방법을 설명하기 위한 도면이다.
- 도 9는 압축 감지의 개념을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0009] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명들은 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.

[0010] 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.

[0011] 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 명명

될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0012] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있거나 "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" 있거나 "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.

[0013] 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.

[0014] 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.

[0015] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0016] 또한, 이하에서 설명되는 방법들은 자율주행 차량, 즉 호스트 차량에 의해 수행되는 방법을 의미할 수 있다.

[0018] 도 1은 안전한 V2V 통신을 설명하기 위한 도면이다.

[0019] 도 1을 참조하면, 물리 계층 보안(Physical layer security)은 방사되는 복수의 무선 채널들 중 임의의 하나를 캡슐화하는 개념으로 간주될 수 있다. 즉, 물리 계층 보안에 따르면, 도청기로 전송되는 무선 신호 또는 신호가 거의 없다. 도청기로 전송되는 신호와 완전히 다른 것은 합법적인 발신자에게 전송된다. 결과적으로, 이러한 물리 계층 보안의 역할은 송신자와 수신자 사이에 고유한 무선 채널을 할당하는 것임을 이해할 수 있다.

[0021] 차량용 보안 용량(VSC, vehicular secrecy capacity)

[0022] 도 2는 차량용 보안 용량을 설명하기 위한 개념도이다. 보안 용량 자체의 정의는 알려진 도청의 존재에 기초하기 때문에 실제 환경에서 보안 용량을 계산하는 것은 어렵다. 따라서 실제로 차량 통신에 보안 용량을 사용하려면 용어에 대한 정의가 선행되어야 한다. 실제 세계에서, 도청자는 일정한 위치에 고정되지 않고 무작위로 배치될 수 있다. 따라서, 보다 적절한 보안 용량 계산 방법이 필요하다. 일반적으로, 도청자는 호스트 차량으로부터 통신 개시 신호(communication-initiated signal, 통신 개시 메시지라 명명될 수도 있음)를 수신한 후 자신의 채널 정보에 대응하는 응답 메시지(채널 정보를 포함하는 메시지로써, 채널 정보 메시지로 명명될 수도 있음)를 송신하거나 송신하지 않을 수 있다. 응답 메시지는 통신 개시 신호의 SNR(Signal to noise ratio) 값을 포함할 수 있는 채널 상태를 통해 전송되는 채널 정보를 포함한다. 그 후, 호스트 차량은 도청자 또는 합법적인 차량으로부터 채널 정보를 수신할 수 있다. VSC 값은 도청자의 SNR 값이 평균 SNR 값보다 낮다는 가정을 기반으로 정의된다. 또한, 호스트 차량에 의해 송신되는 통신 개시 신호는 호스트 차량의 통신 범위 내에 위치하는 주위의 차량들에게 전송될 수 있다. 호스트 차량은 수신된 채널 정보의 SNR 값을 사용하여 아래 수식과 같이 VSC를 정의(또는 계산)할 수 있다.

$$VSC = \log_2(1 + SNR_{AB}) - \log_2(1 + SNR_{XOR})$$

[0023] 여기서, $SNR_{XOR} = \frac{\sum_{i=1}^M SNR_{Ai}}{M}$ 이다. 또한, M은 단위 시간 당 수신된 채널 개수를, B는 통신을 위한 타겟 차

량(target vehicle)을, i 는 호스트 차량(host vehicle)을 제외한 차량의 개수를 나타낸다(도 2 참조). 상술한 바와 같이 호스트 차량은 복수의 차량들 각각에 대한 차량용 보안 용량을 계산(또는 측정)할 수 있다.

[0025] 이후, 호스트 차량은 계산된 차량용 보안 용량(VSC)이 일정 수준 이상(또는 일정 수준 초과)인 차량들을 포함하는 보안 클러스터(Security cluster)를 형성(또는 정의)할 수 있으며, 보안 클러스터 내에서 차량들은 자유롭게 차량 통신을 수행할 수 있다. 보안 용량 외에 차량의 이동 방향이나 속도(속력) 등이 보안 클러스터를 결정하는 주요한 요인이 될 수 있다.

[0027] 상술한 통신 방법 및/또는 후술할 통신 방법을 구현하기 위하여 차량(즉, 호스트 차량으로써 자율주행 차량을 의미할 수 있음)은 통신 개시 신호를 송신하고 통신 개시 신호에 대응하는 적어도 하나의 응답 메시지를 수신하는 송수신부와 응답 메시지에 기초하여 각 차량의 보안 용량을 계산하고 계산된 보안 용량에 기초하여 적어도 하나의 목표 차량(또는 보안 클러스터)을 결정하는 제어부를 포함하는 통신 장치를 포함할 수 있다. 실시예에 따라, 통신 장치는 차량(즉, 호스트 차량) 그 자체를 의미할 수도 있다. 또한, 제어부는 기준 보안 용량에 맞도록 적어도 하나의 파라미터를 제어할 수 있다. 적어도 하나의 파라미터에 대한 제어 정보는 차량의 자율주행을 제어하는 자율주행 제어부로 전송될 수 있고, 자율주행 제어부는 수신된 적어도 하나의 파라미터에 대한 제어 신호를 생성하고 출력함으로써 차량(즉, 호스트 차량)의 자율주행을 제어할 수 있다. 이 경우, 통신 장치는 자율주행 제어부를 더 포함할 수도 있다. 통신 장치에 포함되는 제어부 및/또는 자율주행 제어부는 ECU(Electronic Control Unit)으로 구현될 수 있다.

[0029] [실시예]

[0030] 보안 용량 기반 통신(SC-based Communication)

[0031] SC(Secrecy capacity) 기반 V2V 통신은 가장 기본적인 보안 용량을 위한 통신 방법이다. 호스트 차량은 각 차량으로부터 채널 정보를 수신하고, 수신된 정보에 기초하여 차량의 보안 용량을 계산하고, 계산된 차량의 보안 용량을 사용하여 적어도 하나의 목표 차량을 선택하고, 선택된 목표 차량과의 통신을 수행한다. 여기서, 목표 차량은 복수의 차량들 중 보안 용량이 가장 큰 적어도 하나의 차량을 의미할 수 있다. 한편, 목표 차량 선택은 보안 용량에 대한 기준값을 정의하고 그에 따라 차량 통신을 수행하도록 구현될 수 있다. 즉, 목표 차량은 기준값보다 큰(또는 크거나 같은) 보안 용량을 갖는 적어도 하나의 차량일 수 있으며, 보안 용량의 크기 순서대로 복수개의 차량이 선택될 수 있다. 실시예에 따라, 선택된 적어도 하나의 목표 차량과 호스트 차량은 보안 클러스터를 형성할 수도 있다. 보안 용량 기반 통신 방법에 관한 구체적인 알고리즘은 도 4에 도시되어 있다.

[0033] RSC 기반 통신(Reference Secrecy Capacity-based Communication)

[0034] RSC(Reference Secrecy Capacity, 참조 보안 용량 또는 기준 보안 용량)는 통신 발생 여부(또는 목표 차량으로의 선택 여부)를 결정하는 기준값으로 정의될 수 있다. RSC를 사용한 차량 통신은 대상 차량의 보안 용량이 특정 값 이상인 경우에만 통신을 수행하기 위한 것이다. RSC를 확보할 수 없으면, 즉 차량의 보안 용량이 RSC보다 작다면(또는 작거나 같다면), 차량 보안 용량 매개 변수 중 적어도 하나를 이용하여 차량의 보안 용량을 증가시킬 수 있다. 차량이 특정 수준(즉, RSC 이상)의 보안 용량에 도달할 때까지 이 프로세스를 반복할 수 있다. 차량의 보안 용량은 안테나 관련 파라미터, 경로 관련 파라미터, 노이즈 관련 파라미터를 조절하거나 차량 속도(Speed), 안전 거리(Safety distance), 제한 속도(Speed limit), 및 응답 시간(Response Time or Collision avoidance time)과 같은 고유한 차량 관련 파라미터의 제어를 통해 달성될 수 있다. RSC 기반 통신 방법에 대한 구체적인 알고리즘은 도 5에 도시되어 있다. RSC를 이용한 차량 통신은 목표 차량의 보안 용량이 특정값 이상일 때만을 위한 방법이다(도 6 참조). 또한, 참조 보안 용량, 기준 보안 용량, 또는 기준값 등으로 명명되는 보안 용량은 절대적인 값이 아닌 상대적인 개념을 갖는 값을 의미할 수 있다. 따라서, 기준 보안 용량은 미리 정해진 특정 값을 가질 수 있고, 그 값은 상황이나 환경에 따라 가변되는 값일 수 있다. 예시적으로, 기준 보안 용량은 주변 차량들의 보안 용량의 평균값, 가장 높은 보안 용량의 일정 비율에 해당하는 값 등과 같이 다양한 방식으로 결정될 수도 있다.

[0036] **보안 용량 클러스터 기반 통신(SC Cluster-based Communication)**

[0037] 보안 클러스터의 개념은 단순히 특정 수준의 보안 용량을 가진 그룹이다. 이 연구의 목표는 단일 차량 통신에서 비밀 용량을 사용하여 데이터 전송이 수행되는 모델을 보여주는 것이다. 실시간 무선 통신을 통해 보안 용량을 제어할 수 있다. 이전의 연구는 일정한 비밀 용량 값을 유지함으로써 차량 간 통신을 이미 제안했다. 또한, 이 모델을 사용하면 특정 수준의 보안 용량을 가진 차량이 보안 클러스터를 형성할 수 있다. 보안 클러스터의 차량은 서로 자유롭게 통신할 수 있다. 보안 클러스터는 비밀 기준을 기본 기준으로 하여 다양한 방법으로 정의할 수 있다. 다음으로, 비밀 용량 외에도 차량 이동 방향과 속도가 주요 요인이다. RSU는 보안 클러스터를 형성할 수 있다. 블록 체인과 같은 차량 만이 보안 클러스터를 형성할 수 있다.

[0038] 차량 식별 번호 (VIN)와 같은 차량 고유의 값을 사용하여 블록 체인 기술로 보안 클러스터를 구성하는 것이 좋다. 비밀 용량에 기반한 협력적 릴레이 통신을 사용하는 새로운 V2V 통신 시스템을 제안한다.

[0040] **보안 클러스터 관리(Security Cluster Management)**

[0041] 각 차량은 V2V 통신을 수행한 보안 클러스터의 구성원을 저장하거나 관리할 수 있다. 차량은 이전 보안 클러스터 구성원을 데이터베이스에 저장한다. 차량은 데이터베이스에 현재 보안 클러스터 구성원을 저장할 수도 있다. 물론 그것은 회원의 히스토리를 관리하는 목적 중 하나이다. 현재 보안 클러스터에 포함되지 않았지만 차량 통신을 수행할 때 참조 가능한 대상 차량 후보가 선택되어야 하는 상황이 있을 수 있다. 이 경우, 히스토리 데이터베이스에 이전 보안 클러스터의 멤버에 포함된 차량이 있는 경우, 차량은 대상 차량으로 선택되어 차량 통신을 수행할 수 있다. 호스트 차량은 실시간으로 보안 클러스터를 형성하고, 이 클러스터를 사용하여 특정 기간 동안 차량과 통신할 수 있다. 여기서, 보안 클러스터는 상술 한 바와 같이 소정의 기준값 이상의 비밀 용량을 갖는 차량으로 구성될 수 있다. 비밀 용량이 필요에 따라 기준값을 만족하지 않는 차량의 경우, 이차 기준값에 기초하여 의사 클러스터가 형성될 수 있다. 이러한 의사 클러스터는 호스트 차량의 비밀 용량 파라미터를 제어함으로써 언제든지 보안 클러스터에 통합될 수 있다. 보안 클러스터는 실시간으로 형성하기 어려울 수 있다. 딥러닝 기술을 사용하여 보안 클러스터가 형성될 수 있다.

[0043] **보안 용량을 이용한 블록 검증(Block Verification Using Secrecy Capacity)**

[0044] 보안 용량을 이용하여, 생성된 블록(block)이 새로운 블록(new block)이 되는지 여부가 결정될 수 있다. 각각의 차량은 교통 정보(traffic information)를 갖는 일시적인 블록(temporary block)을 생성할 수 있다. 그러나, 일시적인 블록을 생성하는 것이 블록 체인(blockchain)을 형성하는 것을 의미하지는 않는다. 본 발명에서 제안하는 블록 체인은 보안 용량 검증(secrecy capacity verification)을 통과한 차량에 의해 생성된 블록들만으로 생성될 수 있다. 따라서, 각각의 차량은 일시적인 블록을 생성한 후에 보안 용량 검증을 수행하여야 한다.

[0045] 도 8은 본 발명의 일 실시예에 따른 블록 생성 방법을 설명하기 위한 도면이다. 보안 용량이 참조값(reference value, 참조 보안 용량을 의미할 수 있음)을 초과하는 경우에, 새로운 블록이 생성될 수 있다. 그리고, 보안 용량이 참조 값보다 작은 경우, 보안 용량 값은 보안 용량 파라미터를 제어함으로써 증가될 수 있다.

[0046] 만약 보안 용량이 참조 값보다 크지 않은 경우, 일시적인 블록은 폐기될 것이다. 그 후, 해당 차량은 보안 용량을 제어함으로써 보안 용량이 참조 값보다 크거나 같도록 조절할 수 있으며, 이에 따라 새로운 블록을 생성할 수 있다.

[0047] 제안 기법에서, 블록은 헤더 정보(header information)와 트랜잭션(transaction)으로 나뉠 수 있다. 헤더 정보는 버전 정보(version information), 이전 블록의 해시값(previous block hash value), 타임 스탬프(time stamp), 최후 논스값(last nonce value), 높이(height), 및 트랜잭션 요약(transaction summary) 중 적어도 하나를 포함할 수 있다. 트랜잭션은 트래픽 정보(traffic information)를 포함할 수 있다. 버전 정보(version information)는 소프트웨어 및/또는 프로토콜의 버전 정보를 포함할 수 있다. 블록 해시값(block hash value)은 바로 선행하는 블록체인의 블록의 해시값을 의미한다. 최후 논스값과 크기는 오퍼넌트(opponent)에 의해 블록이 검증될 때 이용될 수 있다.

[0048] 현재 블록(current block)에서, 새로운 블록으로 업데이트 정보(update information)를 추가하고자 할 때, 차량의 보안 용량이 계산될 수 있다. 차량의 보안 용량은 상술한 방식 이외의 다양한 방식에 의하여 계산될 수도 있다. 보안 용량의 계산 방법과는 무관하게, 블록을 생성하기 위해서 보안 용량은 참조 값보다 크거나 같아야

한다. 보안 용량이 참조 값보다 작은 경우, 차량 보안 용량은 보안 용량에 영향을 미치는 파라미터들을 제어함으로써 참조 값보다 크거나 같도록 조절될 수 있다.

[0049] 차량의 보안 용량이 참조 값보다 크거나 같다면, 새로운 블록은 다른 차량들에게 전파(propagating)됨으로써 블록체인 상의 새로운 블록으로 업데이트될 수 있다.

[0051] 압축 감지(Compressive Sensing)

[0052] 최근에 개발된 압축 감지를 사용하여 물리 계층 보안을 강화하는 방법을 제안한다. 압축 감지를 사용하는 물리 계층 보안은 이미지 데이터 전송에서 효율적일 것으로 예상된다. 최근에, 물리 계층 보안을 개선하기 위한 솔루션으로써 압축 감지가 제안되고 있다. 압축 감지는 샘플링과 압축을 통합하기 때문에 이론적으로 Nyquist 샘플링보다 적은 샘플링으로 압축 감지를 수행할 수 있다. 압축 감지는 $y = Ax = A\psi s = \Omega s$ 로 설명되며, 여기서 y 는 측정 벡터(measurement vector), A 는 감지 행렬(sensing matrix), x 는 신호 벡터(signal vector), ψ 는 직교 기본 행렬(orthogonal basis matrix), Ω 은 시스템 행렬(system matrix), s 는 희소 벡터(sparse vector)를 의미한다. x 가 일반 텍스트이고 A 가 암호화 키인 경우, y 는 암호 텍스트로 해석될 수 있다(도 9 참조).

[0054] 데이터 암호화를 위한 오프로딩 서비스(Offloading Service for Data Encryption)

[0055] 데이터 암호화 체계는 물리 계층 보안에서 채널을 보호하는 것과는 다른 연구 분야이다. 물리 계층 보안에서는 채널로 전송되는 데이터 자체를 보호한다. 이는 기존 암호화 기술과 다를 수 있다. 그럼에도 불구하고 압축 감지를 사용하는 기술과 함께 데이터 암호화 기술은 무선 채널을 통해 전송되는 데이터를 보호하는 데 중요한 역할을 한다. 데이터 암호화는 데이터 정보를 보호하는 가장 일반적인 방법이다. IEEE P1609.2에서 256 비트 길이의 타원 곡선 암호화 알고리즘은 응용 프로그램 관련 VANET 네트워크 및 제안된 보안 메커니즘의 관리를 제공한다. 제안된 알고리즘은 RSA 암호화 알고리즘보다 더 효과적이며 일반적인 차세대 공개 키 암호화 시스템으로 간주된다. 그러나 이 암호화 알고리즘의 서명 및 암호화는 빠르며 대규모 네트워크 응용 프로그램에서 시간 지연의 영향을 미친다. 문제는 이 데이터 암호화 기술이 기존 차량의 자율 주행 컨트롤러에서 성능을 충분히 발휘할 수 있는지 여부이다. 자율 주행으로 전송될 데이터는 짧은 긴급 메시지 일뿐만 아니라 많은 양의 이미지 또는 이미지 데이터이기 때문에 모든 관련 데이터를 암호화하는 것은 사실상 불가능하다. 차량의 자율 주행 제어기에서 이미지 데이터를 암호화하는 것이 어려울 수 있지만, 이종 네트워크에서의 오프 로딩 기술은 그러한 암호화 서비스를 충분히 제공하지 못한다. 예시적인 오프로딩 기술은 모바일 엣지 컴퓨팅(mobile edge computing; MEC) 기술이 있다.

[0057] 세이프 존을 위한 지오 펜스 Geo-Fence for Safe Zone)

[0058] 보안 클러스터 내에서 통신을 수행하는 동안 모든 차량의 보안 용량이 크게 줄어든다. 지오 펜스는 차량이 보안 클러스터를 떠나는 것을 알리는 기능을 수행할 수 있다. 일반적으로 지오 펜스는 관심 지역에서 출발하는 것을 알리는 시스템이다. 지오 펜스의 기능성에 따라, 호스트 차량은 보안 클러스터의 이탈에 대응하는 추가 대책을 수행할 수 있다. 변위된 차량에 대한 대안을 찾거나 차량을 떠난 차량을 리콜함으로써 보안 용량을 증가시키는 방법이 모색될 수 있다. 호스트 차량에서 지오 펜스를 구현하는 것이 어렵기 때문에, 지오 펜스는 오프 로딩 기술을 사용하여 근처의 RSU/BS에서 구현될 수 있다.

[0060] 본 발명은 안전한 클러스터에서 안전한 차량 간 통신 방법 또는 안전한 차량 간 통신을 수행하기 위한 클러스터 형성 방법을 제안한다. 여기서, 보안 클러스터는 특정 레벨 이상의 보안 용량을 갖는 차량 그룹을 지칭한다. 일반적으로 보안 용량을 정의하는 데 많은 어려움이 있지만 SNR 값으로만 정의된 차량의 차량 보안 용량을 정의한다. 정의된 차량 보안 용량은 V2V에서 물리 계층 보안을 달성하는 데 실용적이고 효율적이다. 일반적으로, 보안 용량은 안테나 관련 파라미터, 경로 관련 파라미터 및 노이즈 관련 파라미터에 의해 변경될 수 있다. 이러한 기존 파라미터 외에도 자율 주행과 관련하여 차량 속도, 안전 거리, 속도 제한, 응답 시간 등과 같은 고유한 차량 관련 파라미터를 다룬다. 이러한 차량 보안 파라미터는 V2V 통신의 차량 보안 용량을 실시간으로 제어할 수 있다. 차량 보안 기능을 사용하여 키템 컴퓨터와 같은 공격자로부터 안전한 차량 통신을 달성할 수 있다. 본 발명

은 자율 주행에서 경제적이고 효과적이며 효율적인 물리 계층 보안을 가능하게 한다.

[0062] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시 예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 컨트롤러, ALU(Arithmetic Logic Unit), 디지털 신호 프로세서(Digital Signal Processor), 마이크로 컴퓨터, FPA(Field Programmable array), PLU(Programmable Logic Unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(Operation System, OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(Processing Element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

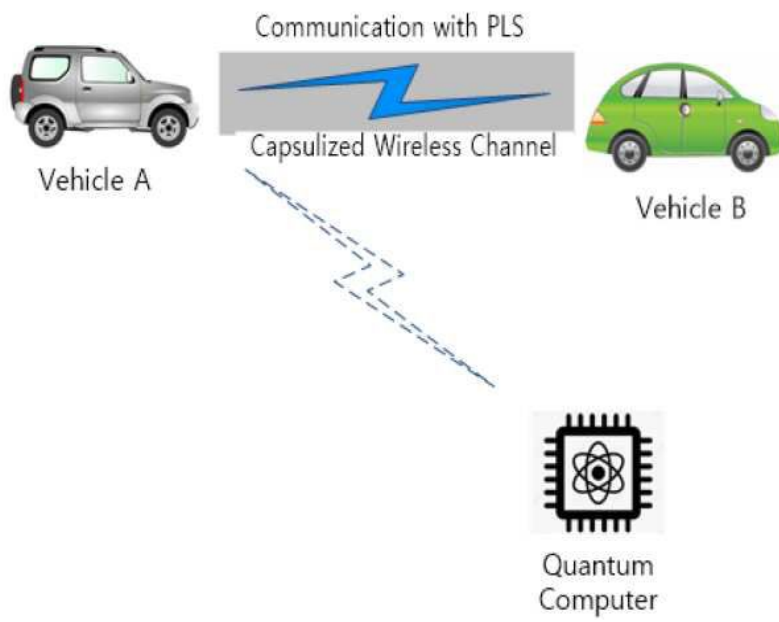
[0063] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(Signal Wave)에 영구적으로, 또는 일시적으로 구체화(Embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0064] 실시 예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시 예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-optical Media), 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시 예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

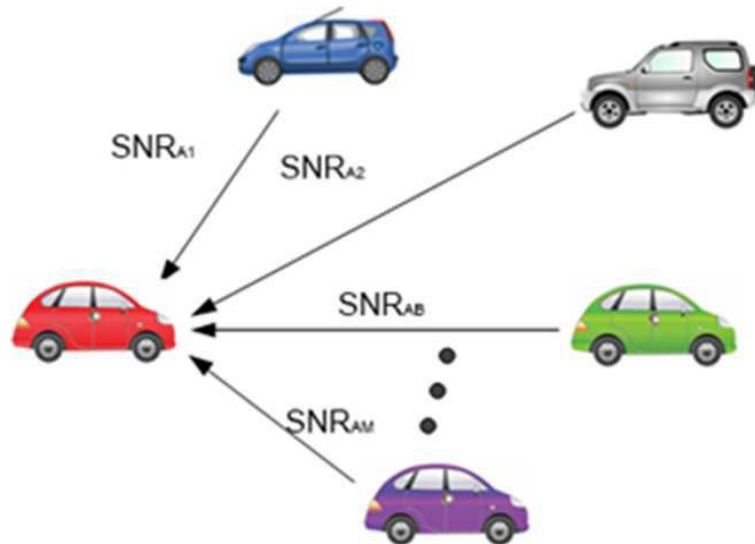
[0065] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

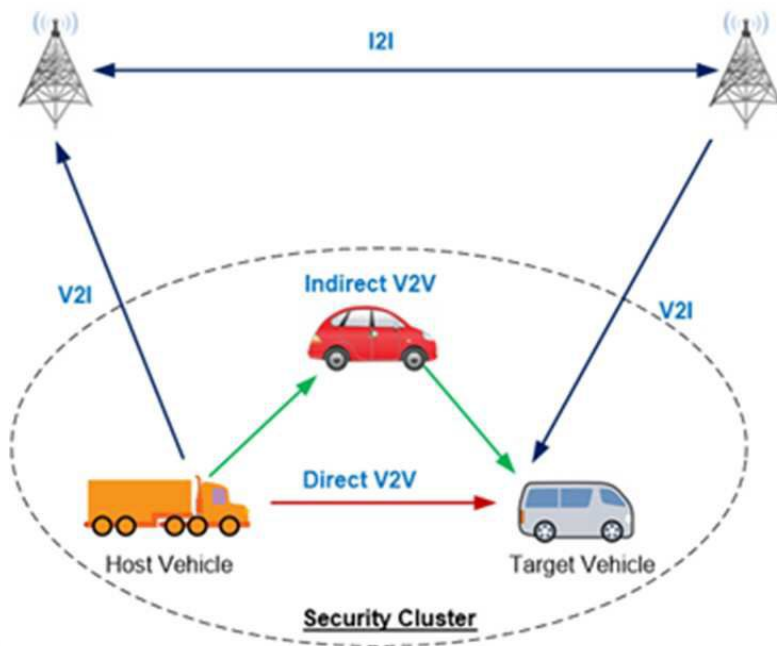
도면1



도면2



도면3



도면4

SC-based Vehicle Communication Algorithm

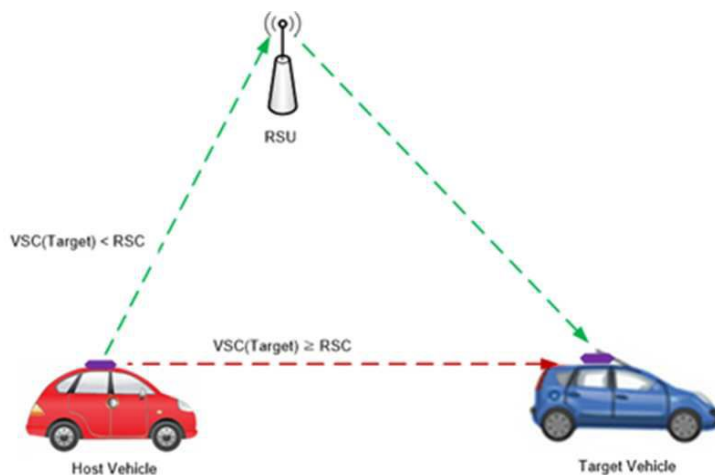
- Step 1: Receive CSI information from vehicles.
- Step 2: Calculate vehicular secrecy capacity related to each of the vehicles.
- Step 3: Select a target vehicle among the vehicles using the calculated vehicular secrecy capacity.
- Step 4: Communication with the selected target vehicle.

도면5

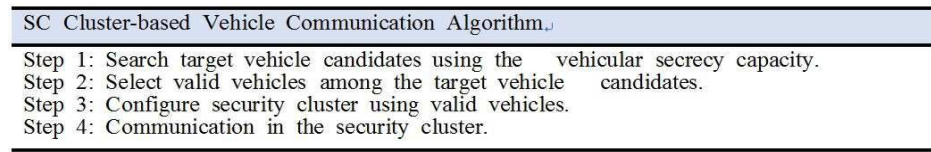
RSC-based Vehicle Communication Algorithm

- Step 1: Receive CSI information from vehicles.
- Step 2: Calculate vehicular secrecy capacity related to each of the vehicles.
- Step 3: Select a target vehicle among the vehicles using the calculated vehicular secrecy capacity.
- Step 4: Determine that $VSC(Target) \geq RSC$.
- Step 5: If $VSC(Target) \geq RSC$, communicate with the selected target vehicle.
- Step 6: Else, increase $VSC(Target)$ using vehicle secrecy parameters and repeat step 5.

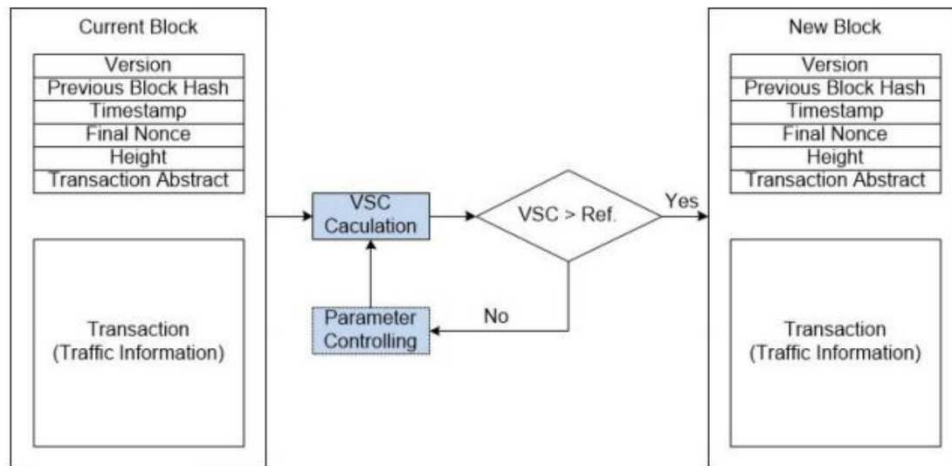
도면6



도면7



도면8



도면9

