(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0122432
(43) 공개일자 2019년10월30일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04W 4/40* (2018.01)
(52) CPC특허분류
H04W 12/08 (2019.01)
H04W 4/40 (2018.02)
(21) 출원번호 10-2018-0046196
(22) 출원일자 2018년04월20일
심사청구일자 2018년04월20일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
안나영
서울특별시 동대문구 제기로6길 9-13(제기동)
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
(74) 대리인
김홍석

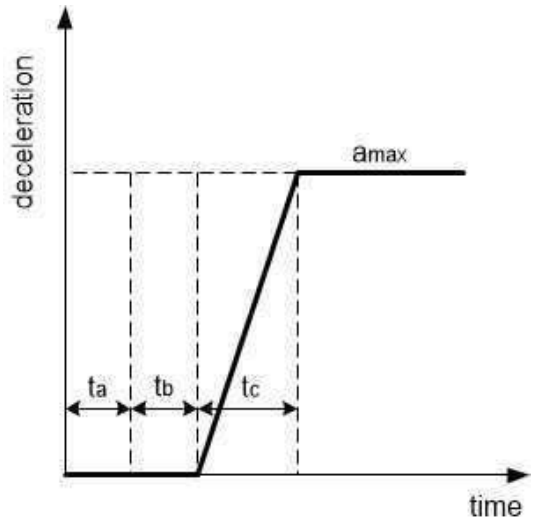
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 **보안용량을 이용한 차량 통신**

(57) 요 약

본 발명에 따른 자율 주행 차량의 통신 방법은, 채널 상태 정보를 이용하여 보안 용량을 계산하는 단계, 및 상기 계산된 보안 용량을 기준값 이하 일 때, 상기 보안 용량을 상기 기준값 이상으로 유지시키는 단계를 포함하고, 상기 차량의 속도, 전송 전력, 및 릴레이 통신 모드 중 적어도 하나를 조절함으로써 상기 보안 용량이 변화되는 것을 특징으로 한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

자율 주행 차량의 통신 방법에 있어서:

채널 상태 정보를 이용하여 보안 용량을 계산하는 단계; 및

상기 계산된 보안 용량을 기준값 이하 일 때, 상기 보안 용량을 상기 기준값 이상으로 조절하는 단계를 포함하고,

상기 차량의 속도, 전송 전력, 및 릴레이 통신 모드 중 적어도 하나를 조절함으로써 상기 보안 용량이 변화되는 것을 특징으로 하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안용량을 이용한 차량 통신에 관한 것이다.

배 경 기 술

[0002] 지능형 교통 시스템 (Intelligent Transportation Systems; ITS)은 모든 스마트 도시의 도로 안전과 교통 효율성을 향상시킬 수 있다. ITS의 발전으로 차량 무선 네트워크는 잠재적 인 중요성을 가지고 있다. 차량 무선 네트워크 보안은 실제로 ITS를 배치하는 데있어 매우 중요하다. 이전 차량 무선 네트워크 보안 기술들은 주로 전송 신뢰성을 높이고, 엔드-투-엔드 처리량을 향상 시키거나, 차량 네트워크의 서비스 범위를 확장하기 위해 협동 중계의 사용에 중점을 두었다. 그러나, 차량 채널의 개방성은 도청 자뿐만 아니라 불법 사용자에게 전송 데이터를 제공한다. 따라서 데이터 전송의 기밀성을 보장하는 것도 중요하다. IEEE 1609.2는 차량용 무선 네트워크에서 보안 메시지 및 해당 암호 절차의 형식을 지정한다. 그러나 비밀 키를 관리하려면 차량 네트워크에서 만족하기 어려운 복잡한 네트워크 아키텍처와 프로토콜은 물론 신뢰할 수 있는 제 3자의 인증이 필요하다. 이기종 ITS에 대한 블록 키 기반 동적 키 관리기 소개되기도 한다. 암호 기반 보안 대신 물리 계층 보안 (physical layer security; PLS)이 최근에 도입되었다.

선행기술문헌

비특허문헌

[0003] (비특허문헌 0001) Li Sun and Qinghe Du, “ “Secure Data Dissemination for Intelligent Transportation Systems,” ” Secure and Trustworthy Transportation Cyber-Physical Systems, Springer Briefs in Computer Science, PP. 99-140, 2017.

(비특허문헌 0002) Faith Saki, and Sevil Sen, “ “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” ” Ad Hoc Networks 61, 2017.

éáñ(비특허문헌 0003) Fernando Camacho, Cesar Crdenas and David Muoz, “challenges for intelligent transportation systems: 5G, HetNets, and SDN” ”, Int J Interact Des Manu, Springer, 2017.

(비특허문헌 0004) William Whyte, Andr´ ´e Weimerskirch, Virendra Kumar, and Thorsten Hehn , “ “A Security Credential Management System for V2V Communications,” ” Vehicular Networking Conference (VNC), 2013 IEEE, 2013.

(비특허문헌 0005) Ao Lei, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P. Anyigor Ogah, and Zhili Sun, “ “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” ” IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 6, DECEMBER 2017.

(비특허문헌 0006) Le Liang, Haixia Peng, Geoffrey Ye Li, and Xuemin (Sherman) Shen, ""Vehicular Communications: A Physical Layer Perspective,"" IEEE Transactions on Vehicular Technology, 2017.

(비특허문헌 0007) Di Han, Bo Bai, and Wei Chen, ""Secure V2V Communications via Relays: Resource Allocation and Performance Analysis,"" IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 6, NO. 3, JUNE 2017.

(비특허문헌 0008) Mohammed E. Eltayeb, Junil Choi, Tareq Y. Al-Naffouri, and Robert W. Heath, Jr., ""Enhancing Secrecy with Multi-Antenna Transmission in Millimeter Wave Vehicular Communication Systems,"" IEEE Transactions on Vehicular Technology, 2017.

(비특허문헌 0009) Freddy A. Mullakkal-Babu, Meng Wang, Bart van Arem, Riender Happee, ""Design and Analysis of Full Range Adaptive Cruise Control with Integrated Collision Avoidance Strategy,"" 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2016.

(비특허문헌 0010) Sutao Duan, and Jian Zhao, "A Model Based on Hierarchical Safety Distance Aigorithm for ACC Control Mode Switching Strategy," 2017 2nd International Conference on Image, Vision and Computing, 2017.

(비특허문헌 0011) Guiping Wang, Lili Zhao, Yi Hao and Jinyu Zhu, ""Design of Active Safety Warning System for Hazardous Chemical Transportation Vehicle,"" Information Technology and Intelligent Transportation System, Springer, pp. 11-21, 2017.

(비특허문헌 0012) Dongbin Zhao, Zhongpu Xia, Qichao Zhang, ""Model-free Optimal Control based Intelligent Cruise Control with Hardware-in-the-loop Demonstration,"" IEEE Computational Intelligence magazine, May 2017.

ã(비특허문헌 0013) Matthieu Bloch, Joao Barros, Miguel R. D. Rodrigues, and Steven W. McLaughlin, "" ¡*j* IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 54, NO. 6, JUNE 2008Yulong Zou, Jia Zhu, Xianbin Wang, and Victor C.M. Leung, ""Improving Physical-Layer Security in Wireless Communications Using Diversity Techniques,"" IEEE Network, January/February 2015.

(비특허문헌 0014) Xiaoming Chen, Derrick Wing Kwan Ng, Wolfgang H. Gerstacker, and Hsiao-Hwa Chen, ""A Survey on Multiple-Antenna Techniques for Physical Layer Security,"" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 19, NO. 2, SECOND QUARTER 2017.

(비특허문헌 0015) Yue Wu1, Wuling Liu, Siyi Wang, Weisi Guo and Xiaoli Chu, ""Network Coding in Device-to-device (D2D) Communications Underlaying Cellular Networks,"" IEEE ICC 2015-Wireless Communication Symposium, 2015.

(비특허문헌 0016) Furqan Jameel, Faisal, M. Asif Ali Haider, Aamir Aziz Butt, ""Performance Analysis of VANETs under Rayleigh, Rician, Nakagami and Weibull Fading,"" 2017 International Conference on Communication, Computing and Digital Systems (C-CODE), 2017.

(비특허문헌 0017) Hazer Inaltekin, Mung Chiang, H. Vincent Poor, and Stephen B. Wicker, ""On Unbounded Path-Loss Models: Effects of Singularity on Wireless Network Performance,"" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 27, NO. 7, SEPTEMBER 2009.

(비특허문헌 0018) Aiqing Zhang and Xiaodong Lin, ""Security-Aware and Privacy-Preserving D2D Communications in 5G,"" IEEE Network, July/August 2017.

(비특허문헌 0019) Aiqing Zhang, Lei Wang, Xinrong Ye and Liang Zhou, ""Secure content delivery over device-to-device communications underlaying cellular networks,"" WIRELESS COMMUNICATIONS AND MOBILE COMPUTING, 27, June 2016.

(비특허문헌 0020) Shunya Iwata, Tooaki Ohtsuki, and Pool-Tuen Kam, ""A Lower Bound on Secrecy Capacity for MIMO Wiretap Channel Aided by a Cooperative Jammer With Channel Estimation Error,"" IEEE Access, Volume 5, 2017.

(비특허문헌 0021) Yingbin Liang, H. Vincent Poor, and Shlomo Shamai (Shitz), ""Secure Communication Over Fading Channels,"" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 54, NO. 6, JUNE 2008.

(비특허문헌 0022) H. Vincent Poora, and Rafael F. Schaeferb, ""Wireless physical layer security,"" PNAS, January 3, 2017, vol. 114, no. 1, pp. 19-26, 2017.

(비특허문헌 0023) Xiaohu Ge, Hui Cheng, Guoqiang Mao, Yang Yang, and Song Tu, ""Vehicular Communications for 5G Cooperative Small-Cell Networks,"" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 65, NO. 10, OCTOBER 2016.

(비특허문헌 0024) Gong Shiqi, Xing ChengWen, Fei ZeSong and Kuang JingMing, ""Cooperative Beamforming Design for Physical-Layer Security of Multi-Hop MIMO Communications"" SCIENCE CHINA Information Sciences, 2015.

(비특허문헌 0025) Dongyang Xu, Pinyi Ren, Qinghe Du and Li Sun, ""Hybrid secure beamforming and vehicle selection using hierarchical agglomerative clustering for C-RAN-based vehicle-to-infrastructure communications in vehicular cyber-physical systems,"" International Journal of Distributed Sensor Networks, 2016.

(비특허문헌 0026) Tanjil Amin, ""Performance Analysis of Secondary Users in Heterogeneous Cognitive Radio Network,"" Georgia Southern University Digital Commons@Georgia Southern, 2016.

(비특허문헌 0027) Jinho Choi, ""Channel-Aware Randomized Encryption and Channel Estimation Attack,"" IEEE Access, Volume 5, 2017.

(비특허문헌 0028) Jinho Choi, ""Secure Transmissions via Compressive Sensing in Multicarrier Systems,"" IEEE SIGNAL PROCESSING LETTERS, VOL. 23, NO. 10, OCTOBER, 2016.

(비특허문헌 0029) Nam Yul Yu, ""Indistinguishability of Compressed Encryption With Circulant Matrices for Wireless Security,"" IEEE SIGNAL PROCESSING LETTERS, VOL. 24, NO. 2, FEBRUARY 2017.

óó(비특허문헌 0030) Joan Enric Barcelo-Llad, Antoni Morell, and Gonzalo Seco-Granados, "a " ¡ ± IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 5, MAY 2014.

(비특허문헌 0031) AthiraV, Sudhish N George, Deepthi P P, ""A Novel Encryption Method Based on Compressive Sensing,"" Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on 2013.

(비특허문헌 0032) Yaron Rachlin and Dror Baron, ""The Secrecy of Compressed Sensing Measurements,"" Communication, Control, and Computing, 2008 46th Annual Allerton Conference on 2008.

(비특허문헌 0033) Ruslan Dautov and Gill R Tsouri, ""Establishing Secure Measurement Matrix For Compressed Sensing Using Wireless Physical Layer Security,"" 2013 International Conference on Computing, Networking and Communications, Communications and Information Security Symposium, 2013.

(비특허문헌 0034) Shuai Chang, Jialun Li, Xiaomei Fu, and Liang Zhang, ""Energy Harvesting for Physical Layer Security in Cooperative Networks Based on Compressed Sensing,"" Entropy 2017, 19, 420, 2017.

(비특허문헌 0035) Jie Guo, Bin Song, Ying He, Fei Richard, ""A Survey on Compressed Sensing in Vehicular Infotainment Systems,"" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 19, NO. 4, FOURTH QUARTER 2017.

(비특허문헌 0036) Junqing Zhang, Trung Q. Duong, Roger Woods and Alan Marshall, ""Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview,"" Entropy 2017, 19, 420, 2017.

(비특허문헌 0037) David L. Donoho, ""Compressed Sensing,"" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 52, NO. 4, APRIL 2006.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은 안전성을 향상시키는 차량 통신 및 그것의 동작 방법을 제공하는데 있다.

과제의 해결 수단

[0005] 본 발명의 실시 예에 따른 자율 주행 차량의 통신 방법은: 채널 상태 정보를 이용하여 보안 용량을 계산하는 단계; 및 상기 계산된 보안 용량을 기준값 이하 일 때, 상기 보안 용량을 상기 기준값 이상으로 조절하는 단계를 포함하고, 상기 차량의 속도, 전송 전력, 및 릴레이 통신 모드 중 적어도 하나를 조절함으로써 상기 보안 용량이 변화되는 것을 특징으로 한다.

발명의 효과

[0006] 본 발명의 실시 예에 따른 차량 통신 방법은 보안 용량을 일정하게 유지하도록 함으로써, 도청자로부터의 데이터 안정성을 확보할 수 있다.

도면의 간단한 설명

[0007] 이하에 첨부되는 도면들은 본 실시 예에 관한 이해를 돕기 위한 것으로, 상세한 설명과 함께 실시 예들을 제공한다. 다만, 본 실시예의 기술적 특징이 특정 도면에 한정되는 것은 아니며, 각 도면에서 개시하는 특징들은 서로 조합되어 새로운 실시 예로 구성될 수 있다.

도 1은 호스트 차량의 제동 과정을 예시적으로 보여주는 도면이다.

도 2는 충돌을 방지하기 위한 차량 안전 거리에 대한 개념을 설명하는 도면이다.

도 3는 도청자가 멀리 떨어져 있을 때 시스템 모델을 예시적으로 보여주는 도면이다.

도 4는 차량 속도 v에 따른 보안 용량 Cs를 예시적으로 보여준다.

도 5는 차량 속도에 따른 보안 용량을 변화를 예시적으로 보여주는 도면이다.

도 6는 서로 다른 전송 전력에서 차량 속도에 따른 보안 용량의 변화를 예시적으로 보여주는 도면이다.

도 7은 서로 다른 차량의 응답 속도에서 차량 속도에 따른 보안 용량의 변화를 예시적으로 보여주는 도면이다.

도 8은 호스트 차량 (A)과 타겟 차량 (B) 사이에 하나의 릴레이 (R)를 포함하는 것을 시스템 모델을 보여주는 도면이다.

도 9는 릴레이 존재 유무에 따른 보안 용량의 변화를 예시적으로 보여주는 도면이다.

도 10은 평균 보안 용량 및 AWGN(additive white Gaussian noise) 채널 용량을 예시적으로 비교한 도면이다.

도 11은 본 발명의 실시 예에 따른 차량 통신을 예시적으로 보여주는 도면이다.

도 12는 압축 센싱을 이용한 물리 계층 보안을 증대시키는 방법을 개념적으로 설명하는 도면이다.

도 13은 본 발명의 실시 예에 따른 차량 통신 방법을 예시적으로 보여주는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0008] 아래에서는 도면들을 이용하여 본 발명의 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있을 정도로 본 발명의 내용을 명확하고 상세하게 기재할 것이다.

[0009] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 특정 실시 예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 제 1, 제 2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다.

[0010] 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위로부터 이탈되지 않은 채 제 1 구성요소는 제 2 구성요소로 명명될 수 있고, 유사하게 제 2 구성요소도 제 1 구성요소로 명명될 수 있다. 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 혹은 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0011] 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 혹은 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다. 본 출원에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[0012] 본 출원에서, "포함하다" 혹은 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 혹은 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 혹은 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 혹은 이들을 조합한 것들의 존재 혹은 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다. 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 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.

[0013] 본 발명의 실시 예에 따른 차량 통신은 보안 용량(secrecy capacity)을 사용하여 수행될 수 있다. 아래에서는 차량 무선 네트워크의 보안 용량을 결정하는 다양한 유형의 매개 변수와 보안 용량 간의 관계를 밝힌다. 예를 들어, 차량 속도와 보안 용량 사이의 관계, 자율 차량의 응답 시간과 보안 용량 사이의 관계 및 송신 전력과 보안 용량 간의 관계를 조사한다. 특히, 자율 주행 차량은 차량의 속도가 안전 거리와 관련되어 있다는 가정하에 시스템 모델링을 설정한다. 다양한 매개 변수에 따라 일정 수준의 보안 용량을 유지하기 위해 새로운 차량 통신이 제안된다. 결과적으로 5G 통신에서 자율 차량의 안전한 통신 보안을 기대할 수 있다.

[0014] 보안 용량에 기반한 물리적 계층 보안을 사용하여 V2V (vehicle-to-vehicle) 통신을 보다 깊이 연구한다. 이 발명은 다음과 같이 설명된다. 먼저 안전 거리와 차량 속도 사이의 관계를 개시하고, 다음으로, 차속에 따라 보안 용량을 계산하는 시스템이 모델링 된다. 그 후 다양한 매개 변수에 따른 보안 용량의 관계를 개시하고, 다음으로, 보안 용량을 이용한 차량 통신의 개념이 개시된다. 마지막으로 차량 통신의 보안 기능에 따른 물리적 계층 보안 외에도 물리 계층 보안을 향상시키는 방법이 개시된다.

[0015] **차량 속도 기반 안전 거리(SAFETY DISTANCE BASED ON VELOCITY)**

[0016] 자율 주행 차량은 ACC (Adaptive Cruise Control)가 매우 중요한 기술이다. ACC는 차량 속도와 적어도 두 대의 차량 사이의 거리를 조정하도록 구성된다. ACC 시스템은 다양한 상황에서 충돌 회피 조건을 충족시켜야 할 수도 있다. 예를 들어, 정지 및 이동 시나리오, 비상 제동 시나리오 및 커팅 시나리오의 세 가지 시나리오가 있다. 이러한 모든 시나리오에는 기본적으로 선행 차량과 후속 차량 간의 제동 거리가 포함된다. 일반적으로 제동 거리는 차량이 초기 제동 점에서 완전히 정지하는 거리를 나타낸다. 제동 거리(braking distance)는 기본적으로 호스트 차량과 목표 차량 사이의 안전 거리를 포함한다. 즉, 적어도 안전 거리는 제동 거리보다 길다.

[0017] 도 1은 호스트 차량의 제동 과정을 예시적으로 보여주는 도면이다. 도 1을 참조하면, 자율 주행 차량은 도시된 제동 과정을 수행 할 수 있다. 도 1에 도시된 바와 같이, a_{max}는 제동 과정에서의 최대 감속도이다. 제동 과정은 응답 주기 t_a, 제동 간극 주기 t_b 및 차단력 인가 주기 t_c를 포함한다. 이 때 이론적인 제동 거리 d_L은 다음과 같이 계산된다.

[0018] $$d_L = v_0\left(t_a + t_b + \frac{t_c}{2}\right) + \frac{v_0^2}{2a_{max}}$$

[0019] 여기서 v_0는 호스트 차량의 초기 속도이다.

[0020] 도 2는 충돌을 방지하기 위한 차량 안전 거리에 대한 개념을 설명하는 도면이다. 도 2에서, 제동 안전 거리는

호스트 차량 (A)과 후행하는 차량 (B) 사이의 충돌을 방지하기 위해 도시된다.

[0021] 도 2에 도시 된 바와 같이, 호스트 차량 (A)이 2 대의 차량 (A, B)이 충돌 확률을 검출 할 때, ACC 시스템에서 안전 가드를 자동으로 작동시킬 것이다. 이제, 호스트 차량 (A)이 초기 속도 (V_1)에 있다고 가정하면, 가속기 (a_1); 목표 차량 (B)은 초기 속도 (V_2), 가속도 (a_2); 안전 거리는 d_s이다. 안전 거리 d_s는 다음과 같이 계산된다.

[0022] $$d_s = v_1 \tau + \frac{V_1^2}{2a_1} - \frac{V_2^2}{2a_2}$$

[0023] 여기서 τ 는 ACC의 상수 파라미터이다.

[0024] 주요 관심사는 안전한 V2V 통신이다. 따라서 ACC 시스템에 기반한 호스트 차량 A와 목표 차량 B는 일정한 동작과 동일한 속도를 갖는다고 가정할 수 있다. 호스트 차량 (A) 및 목표 차량 (B)의 각각의 ACC 시스템은 제 1 차량 (A)의 전방 범퍼와 제 2 차량 (B)의 후방 범퍼 사이의 이격 거리를 유지하도록 제어하기 때문이다. 그러면, $V_1 = V_2$ 및 $a_1 = a_2$이다. 결과적으로, 호스트 차량 A의 속도를 기반으로 한 안전 거리는 다음과 같습니다.

[0025] $$d_s = v_1 \tau$$

[0026] 결과적으로, 안전 거리 d_s는 V2V 통신에서 호스트 차량 A의 초기 속도 v1에 비례한다는 것을 확인할 수 있다. 즉, 자율 주행 차량의 속도는 안전 거리에 비례한다.

[0027] **차량 통신에서 보안 용량(SECRECY CAPACITY FOR V2V COMMUNICATION)**

[0028] 정보 이론에서 채널 (또는 새넌) 용량은 무선 채널을 통해 전송할 수있는 최대 정보량으로 알려져 있습니다. 일반적으로, 채널 용량은 다음과 같이 주어진다:

[0029] $$C = W\log\ (1 + SNR)$$

[0030] 여기서, W는 채널 대역폭이고, SNR은 신호 대 잡음비이다. 보안 용량은 합법적인 채널의 채널 용량이 도청 채널의 채널 용량을 차감한다는 것을 의미한다. 즉, 보안 용량은 합법적 인 TX-RX 쌍 사이에서 달성 할 수 있는 최대 데이터 전송률이며 비인가 수신자가 얻을 수 있는 정보에 대한 제약이 따른다. 가우스 도청 채널에서, 보안 용량 C_s는 다음과 같이 주어진다.

[0031] $$C_s = \frac{1}{2}\log\left(1 + \frac{P}{N_m}\right) - \frac{1}{2}\log\left(1 + \frac{P}{N_w}\right)$$

[0032] 여기서 P는 송신기의 전력, N_m은 수신기의 잡음, N_w는 도청 자의 잡음이다.

[0033] **차량 속도 기반 시스템 모델(SYSTEM MODEL BASED ON VELOCITY)**

[0034] 호스트 차량 (A)과 목표 차량 (B) 사이의 거리는 자율 주행 시스템의 안전 거리 (Ds)보다 길 것이다. 도 3는 도청자가 멀리 떨어져 있을 때 시스템 모델을 예시적으로 보여주는 도면이다.

[0035] 즉, 도청자 (E)와 자기 차량 (A) 사이의 거리 (r)는 목표 차량 (B)과 도청자 (E) 사이의 거리 (r)와 유사하다 호스트 차량 (A)과 목표 차량 (B) 사이의 거리 (D)는 $r\Theta$이다. 제 1 선분(AE) 및 제 2 선분 (AB)에 의해 형성되는 제 3 선분 (D)을 포함한다. 도청자의 V2V 통신 시나리오를 고려한다. 페이딩 시나리오에서의 보안 용량 C_s는 다음과 같다.

[0036] $$C_s = \log_2\left(1 + \frac{P\,|h_{AB}|^2}{N_0}\right) - \log_2\left(1 + \frac{P|h_{AE}|^2}{N_0}\right)$$

[0037] 여기서, P는 자 차량 A의 송신 전력, h_{AB}는 자 차량 A와 목표 차량 B 사이의 페이딩 채널 계수, h_{AE}는 자 차량 A와 도청 자 E 사이의 페이딩 채널 계수이며, N_0는 분산 AWGN (Additive White Gaussian Noise)이다.

[0038] 일반적으로 Rayleigh, Rician 및 Nakagami의 세 가지 페이딩 모델이 있습니다. 전송 된 신호 전력은 거리에 따라 $d^{-\alpha}$로 감소 할 수 있는데, 여기서 α는 경로 손실 지수이다. 경로 손실 거리가 자기 차량 A와 목표 차량 B

사이의 거리 D (= rΘ) 일 때, 페이딩 채널 계수 h_{AB}는 다음과 같다.

[0039] $$h_{AB} = \left|\frac{1}{(r\theta)^{\alpha}}\right|$$

[0040] 또한, 경로 손실 거리가 호스트 차량 (A)과 도청 자 (E) 사이의 거리 (r) 일 때, 페이딩 채널 효율 h_{AE}는 다음과 같다.

[0041] $$h_{AE} = \left|\frac{1}{r^{\alpha}}\right|$$

[0042] 따라서 이 시스템 모델에서 보안 용량 C_s는 다음과 같다.

[0043] $$C_s = \log_2\left(1+\frac{P}{N_0(r\theta)^{2\alpha}}\right) - \log_2\left(1+\frac{P}{N_0 r^{2\alpha}}\right)$$

[0044] 호스트 차량의 속도가 정당한 터미널 사이의 안전 거리 d_s와 관련이 있다. $d_s = v_1 \tau$. 속도 관점에서, 호스트 차량 (A)과 목표 차량 (B) 사이의 거리 (D)는 다음과 같이 주어진다.

[0045] $$D = r\theta = v\tau$$

[0046] 여기서, v는 호스트 차량 (A)의 현재 속도이고, τ는 ACC 시스템의 상수 파라미터이다.

[0047] 결과적으로, 이 시스템 모델에서 보안 용량 C_s는 다음과 같이 주어진다.

[0048] $$C_s = \log_2\left(1+\frac{P}{N_0(v\tau)^{2\alpha}}\right) - \log_2\left(1+\frac{P}{N_0 r^{2\alpha}}\right).$$

[0049] 분석의 단순성을 위해 거리 r은 고정되어 있다고 가정했다. 그런 다음 보안 용량 Cs는 단지 두 개의 가변 파라미터 v와 α로 표현되는 함수이다. 도 4는 차량 속도 v에 따른 보안 용량 Cs를 예시적으로 보여준다.

[0050] 도 4 도시 된 바와 같이, 보안 용량 C_s가 경로 손실 계수 α와 차량 속도 v에 크게 영향을 받는다. 첫째로, 차량 속도 v가 증가 할 때 보안 용량 C_s는 경로 손실 계수 α에 관계없이 감소한다. 두번째로, 더 큰 경로 손실 계수 α가, 더 큰 보안 용량 Cs을 갖는다.

[0051] 도 5는 차량 속도에 따른 보안 용량을 변화를 예시적으로 보여주는 도면이다. 또한 호스트 차량 A의 속도 증가가 보안 용량 C_s의 감소를 가져올 것으로 예상된다. 설명의 편의를 위해 자율 주행 차량이 고속도로를 주행하고 있다고 가정한다. 시뮬레이션에서, 도 5는 80 Km/h, 100 Km/h 및 120 Km/h의 상이한 속도에 따른 비밀 용량 (C_s)을 도시한다. 이 시뮬레이션에서 A와 E 사이의 거리 r이 1000m이고, 페이딩 채널 모델은 레일리 페이딩 채널 모델이라고 가정한다. 도 5에 도시 된 바와 같이, 80 Km / h에서의 기밀성이 가장 높고 120 Km / h에서의 기밀성이 가장 낮다. 차량의 고속이 보안 용량을 감소시킬 수 있음을 확인된다. 보안 환경을 고려할 때 차량 속도에 따라 전송 전력 P 또는 전송 속도를 최적화 해야 한다.

[0052] 도 6는 서로 다른 전송 전력에서 차량 속도에 따른 보안 용량의 변화를 예시적으로 보여주는 도면이다. 도 6에 도시 된 바와 같이, 송신 전력비 P/N_0로 보안 용량의 변화를 발견 할 수 있다. 보안 용량은 송신 전력비 P/N_0의 크기에 비례한다는 것을 알 수 있다. 즉, 도 6을 참조하면, 송신 전력비 (P/N_0)가 클수록 비밀 수용 용량 (C_s)이 커진다.

[0053] 도 7은 서로 다른 차량의 응답 속도에서 차량 속도에 따른 보안 용량의 변화를 예시적으로 보여주는 도면이다. 또한, ACC 시스템의 반응 속도에 따라 시스템의 비밀 수용 능력이 도시된다. 도 7에 도시 된 바와 같이, 시스템의 응답 속도가 빠를수록 비밀 수용 능력이 커진다.

[0054] 따라서, 차량 통신에서 일정한 보안 능력을 유지하기 위해 차량 속도 및 송신 전력비 P/N_0를 적절하게 선택하는 것이 중요하다. 이것은 차량 통신에서 일정 수준의 보안을 유지하기 위한 몇 가지 기준으로 비밀 수용 능력을 정의 할 수 있음을 의미한다.

[0055] 상술된 바와 같이, 보안 용량은 차량 속도, 송신 전력의 크기 및 시스템 파라미터에 의해 결정될 수 있다. 요약

하면, 비밀 수용 능력의 도식은 다음 표에 의해 결정될 수 있습니다.

[0056] 표 1은 다양한 파라미터들과 보안 용량 사이의 관계를 예시적으로 보여준다.

표 1

[0057]

Vehicle Speed	Up	Down	Secrecy Capacity
	Down	Up	
Transmission Power	Up	Up	
	Down	Down	
System Parameter (Response Time)	Up	Down	
	Down	Up	

[0058] **릴레이 기반 시스템 모델(SYSTEM MODEL BASED ON RELAY)**

[0059] 상술 된 바와 같이, 차량 속도가 증가함에 따라 보안 용량은 감소한다. 차량 속도가 증가함에 따라 감소된 보안 용량은 협동 릴레이 통신에 의해 보상될 수 있다. V2V 통신에서 호스트 차량 A와 목표 차량 B 사이의 하나의 릴레이 R에 채택하여 비밀 수용 능력을 향상시킬 수 있다. 일반적으로 협력 릴레이 통신의 보안 용량은 릴레이가 없는 직접 통신보다 높다. 보안 용량의 분석을 단순화하기 위해, 도 8에 도시 된 바와 같이, 시스템 모델이 호스트 차량 (A)과 타겟 차량 (B) 사이에 하나의 릴레이 (R)를 포함한다고 가정한다.

[0060] 합법적인 채널의 채널 용량은 다음과 같이 표현된다.

[0061]
$$C_1(A,B) = W\log_2\left(1+\left(\frac{P_A h_{AB}}{P_R h_{RB}+\sigma_B^2}\right)\right)$$

[0062] 여기서, P_A는 호스트 차량 A와 릴레이 R의 송신 전력, h_{AB}는 호스트 차량 A와 목표 차량 B 사이의 채널 이득, h_{RB}는 릴레이 R과 목표 차량 B 사이의 채널 이득 , σ_B^2는 목표 차량 B에서의 부가적인 백색 가우스 잡음이며, W는 대역폭이다.

[0063] 도청 채널의 채널 용량은 다음과 같다.

[0064]
$$C_2(A,E) = W\log_2\left(1+\left(\frac{P_A h_{AE}}{P_R h_{RE}+\sigma_E^2}\right)\right)$$

[0065] 여기서, h_{AE}는 차량 A와 도청 자 E 사이의 채널 이득이고, σ_E^2는 차량 B에서의 부가적인 백색 가우스 잡음이다. 그러면, 협력 릴레이 통신을 통한 보안 용량은 다음과 같다.

[0066]
$$C_R = W\left[\log_2\left(1+\left(\frac{P_A h_{AB}}{P_R h_{RB}+\sigma_B^2}\right)\right)-\log_2\left(1+\left(\frac{P_A h_{AE}}{P_R h_{RE}+\sigma_E^2}\right)\right)\right]$$

[0067] 도 9는 릴레이 존재 유무에 따른 보안 용량의 변화를 예시적으로 보여주는 도면이다. 도 9을 참조하면, 릴레이 R이 보안 용량을 향상시키는 데 도움이 된다. 즉, 릴레이를 사용하는 V2V 통신이 보안 용량을 향상시킬 수 있다. 릴레이와 보안 용량 사이의 관계는 아래의 표와 같이 정리 될 수 있다.

[0068] 표 2는 릴레이 모드와 보안 용량 사이의 관계를 보여준다.

표 2

[0069]

Relay	Off	Down	Secrecy Capacity
	On	Up	

[0070] **평균 보안 용량(ERGODIC SECRECY CAPACITY)**비밀 유지 용량은 시간 경과에 따른 채널 변동을 고려하지 않는다. 그래서 도입된 개념이 평균 보안 용량(ergodic secret capacity; ESC)이다. 평균 보안 용량은 합법적인 사용자와 도청 자에 대한 비밀 비율의 시간 평균으로 정의된다. MIMO 시스템에서의 평균(ergodic) 페이딩 채널의

경우, 페이딩 채널 계수는 독립적이며 동일하게 분포된다. 이와 같이, 차량 네트워크에서, 자기 차량 A, 목표 차량 B 및 도청자 E의 각각은 각각의 채널 사용에 대해 상이한 페이딩 상태를 경험할 수 있다. 모든 단말이 현재의 페이딩 상태 (CSI)에 대한 완전한 CSI (channel state information;채널 상태 정보)를 갖는다고 가정하면, 평균 보안 용량은 다음과 같다.

[0071] $$C_S = \max_{E_A[\gamma]\le P} E_A \log_2\left(1+\frac{\gamma|h_{AB}|^2}{\sigma_B^2}\right) - \log_2\left(1+\frac{\gamma|h_{AE}|^2}{\sigma_E^2}\right)$$

[0072] 여기서 γ 전력 계수이고 $A = \left\{h_{AB},\ h_{AE} : \frac{|h_{AB}|^2}{\sigma_B^2} > \frac{|h_{AE}|^2}{\sigma_E^2}\right\}$이다.

[0073] 도 10은 평균 보안 용량 및 AWGN(additive white Gaussian noise) 채널 용량을 예시적으로 비교한 도면이다. 도 10에 도시된 바와 같이, AWGN 채널 용량은 평균 보안 용량 보다 크다.

[0075] **보안 용량을 이용한 차량 통신(V2V COMMUNICATION USING SECRECY CAPACITY)**

[0076] 최근 5G 이동 통신망에서 차량 통신 용량을 계산하는데 관심을 갖는다. 상술된 바와 같이, 차량 속도와 보안 용량, 그리고 릴레이 존재와 보안 용량 사이에는 밀접한 관계를 갖는다.

[0077] 도 11은 본 발명의 실시 예에 따른 차량 통신을 예시적으로 보여주는 도면이다. 비밀 용량 값에 따라 협력 릴레이 통신에 의해 수행되는 V2V 통신이 제한될 수 있다.

[0078] V2V 통신 과정은 다음과 같이 진행될 수 있다.

[0079] 1) 호스트 차량은 타겟 차량으로부터 CSI (channel state information)을 수신한다.

[0080] 2) 호스트 차량은 타겟 차량과의 연결을 위한 보안 용량을 계산한다.

[0081] 3) 계산된 보안 용량이 사전에 결정된 값보다 큰 지를 판별한다. 여기서 사전에 결정된 값은 차량의 속도의 범위에 따라 다르게 설정될 수 있다.

[0082] 4) 만일 보안 용량이 사전에 결정된 값보다 크다면, 호스트 차량은 타겟 차량과 직접적으로 통신을 수행할 수 있다.

[0083] 5-1) 실시 예에 있어서, 보안 용량이 사전에 결정된 값보다 크지 않다면, 호스트 차량은 협력 릴레이 통신을 이용하는 간접 통신을 타겟 차량과 수행할 수 있다. 차량 네트워크에서 릴레이 선택은 전력 소비, 혹은 보안 용량 등을 고려하여 최적의 알고리즘에 의해 선택될 수 있다. 예를 들어, 최적화 알고리즘은 호스트 차량의 송신 전력을 제어하여 V2V 통신의 보안을 향상시킬 수 있다. V2V 통신은 보안 용량에 기초한 협동 릴레이 통신에 의한 물리 계층 보안 강화를 유도한다.

[0084] 5-2) 다른 실시 예에 있어서, 보안 용량이 사전에 결정된 값보다 크지 않다면, 호스트 차량은 사전에 결정된 만큼 송신 전력을 증가시키고, 그 후에 타겟 차량과 통신을 수행할 수 있다.

[0085] 한편, 호스트 차량은 보안 용량의 결과에 따라 5G 모바일 네트워크와 같은 V2I 통신을 선택할 수 있다.

[0086] 또한 5G 차량 통신을 위한 새로운 CSI (채널 상태 정보)를 정의 할 것이다. 제안하는 주요 내용은 채널 상태 정보(CSI)에 SNR 값에 포함하는 것이다. 초기 통신을 시도 할 때, 수신기 및 수신기가 수신 된 전력을 알고 있기 때문에 송신 전력을 알고 있다면 수신기에서 SNR 값을 계산하는 것은 어렵지 않다. 모든 수신기는 SNR 값을 계산하여 채널 상태 정보에 포함시킬 수 있다. 이 제안을 위해서는 먼저 관련 표준 협회에서 충분한 토론을 해야 할 것이다.

[0087] **물리 계층 보안 강화(PHYSICAL LAYER SECURITY ENHANCEMENT)**

[0088] 기본적으로 V2V 통신은 보안 용량에 기반한 물리 계층 보안을 만족시킨다다. 또한 압축 감지(compressive sensing)를 기반으로 한 물리 계층 암호화를 사용하여 보안을 강화할 수 있다. 압축 감지 (Compressive sensing) 암호화는 물리적 계층에서 간단한 복잡성이 낮은 암호로 합리적으로 안전한 전송을 제공 할 수 있으므로 매력적인 솔루션이 될 수 있다. 일반적으로 압축 감지 방식은 나이 퀴스트 비율 (Nyquist rate) 이하의 신호를 샘플링 할 수 있다.

[0089] 도 12는 압축 센싱을 이용한 물리 계층 보안을 증대시키는 방법을 개념적으로 설명하는 도면이다.

[0090] 호스트 차량 (A)과 타겟 차량 (B) 사이의 V2V 통신에 따르면, 압축 감지 암호화는 선택적 일 수 있다. 호스트 차량 (A)은 기밀 능력의 값에 따라 압축 감지 암호화를 사용할지를 결정할 수 있다.

[0091] 차량 네트워크에서 차량의 보안 용량과 차량 속도 사이의 관계에 따르면, 고속의 차량의 경우 저속의 차량보다 보안 용량이 감소된다. 보안 환경을 고려할 때 차량 속도에 따라 전송 전력 또는 전송 속도를 최적화 할 필요가 있다. 또한 릴레이를 사용하는 V2V 통신이 보안 용량을 향상시킬 수 있다. 따라서 차량 사용자는 차량 속도에 따라 보안 용량을 높이기 위해 릴레이를 선택하는 최적화 된 선택 릴레이 알고리즘을 통해 V2V 통신이 수행되어야 한다. 또한 압축 감지 암호화를 사용하여 물리 계층 보안이 도입될 수 있다. 앞으로는 물리 계층 보안을 통해 차량 네트워크에서의 보다 효율적인 설계 및 보다 빠르고 안전한 통신과 같은 개선을 이끌어 낼 것이다.

[0092] 도 13은 본 발명의 실시 예에 따른 차량 통신 방법을 예시적으로 보여주는 흐름도이다. 도 1 내지 도 13을 참조하면, 차량 통신 방법은 다음과 같이 진행될 수 있다.

[0093] 호스트 차량은 채널 상태 정보를 이용하여 보안 용량을 계산할 수 있다(S110). 호스트 차량은 계산된 보안 용량을 사전에 결정된 값 이상으로 유지하도록 전송 전력, 릴레이 모드, 속도 등 조절하고, 이 후 타겟 차량과 통신을 수행할 수 있다(S120).

[0094] 본 발명에 따른 단계들 및/또는 동작들은 기술분야의 통상의 기술자에 의해 이해될 수 있는 것과 같이, 다른 순서로, 또는 병렬적으로, 또는 다른 에포크(epoch) 등을 위해 다른 실시 예들에서 동시에 일어날 수 있다.

[0095] 실시 예에 따라서는, 단계들 및/또는 동작들의 일부 또는 전부는 하나 이상의 비-일시적 컴퓨터-판독가능 매체에 저장된 명령, 프로그램, 상호작용 데이터 구조(interactive data structure), 클라이언트 및/또는 서버를 구동하는 하나 이상의 프로세서들을 사용하여 적어도 일부가 구현되거나 또는 수행될 수 있다. 하나 이상의 비-일시적 컴퓨터-판독가능 매체는 예시적으로 소프트웨어, 펌웨어, 하드웨어, 및/또는 그것들의 어떠한 조합일 수 있다. 또한, 본 명세서에서 논의된 "모듈"의 기능은 소프트웨어, 펌웨어, 하드웨어, 및/또는 그것들의 어떠한 조합으로 구현될 수 있다.

[0096] 본 발명의 실시 예들의 하나 이상의 동작들/단계들/모듈들을 구현/수행하기 위한 하나 이상의 비-일시적 컴퓨터-판독가능 매체 및/또는 수단들은 ASICs(application-specific integrated circuits), 표준 집적 회로들, 마이크로 컨트롤러를 포함하는, 적절한 명령들을 수행하는 컨트롤러, 및/또는 임베디드 컨트롤러, FPGAs(field-programmable gate arrays), CPLDs(complex programmable logic devices), 및 그와 같은 것들을 포함할 수 있지만, 여기에 한정되지는 않는다.

[0097] 한편, 상술 된 본 발명의 내용은 발명을 실시하기 위한 구체적인 실시 예들에 불과하다. 본 발명은 구체적이고 실제로 이용할 수 있는 수단 자체뿐 아니라, 장차 기술로 활용할 수 있는 추상적이고 개념적인 아이디어인 기술적 사상을 포함할 것이다.

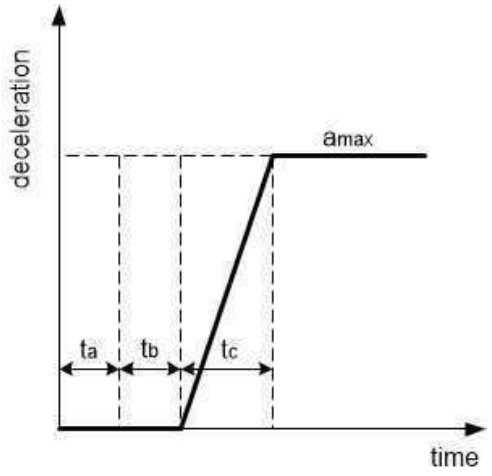
부호의 설명

[0098] ACC: 적응형 크루즈 제어

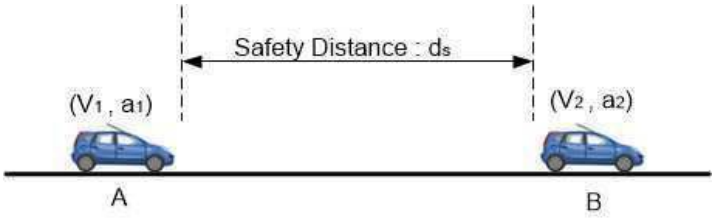
V2V: 차량 대 차량

도면

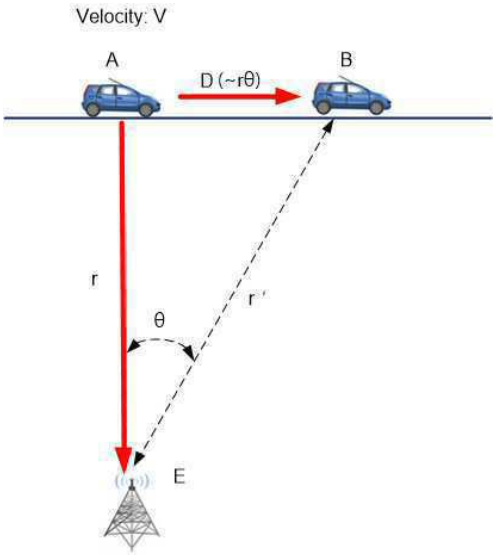
도면1



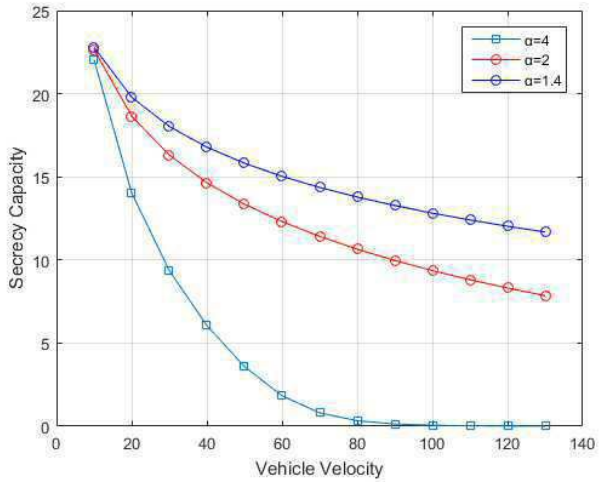
도면2



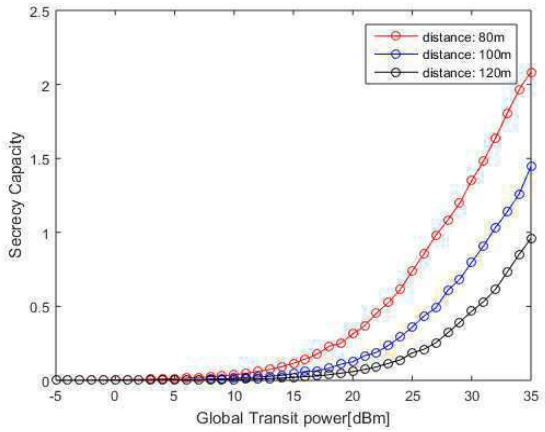
도면3



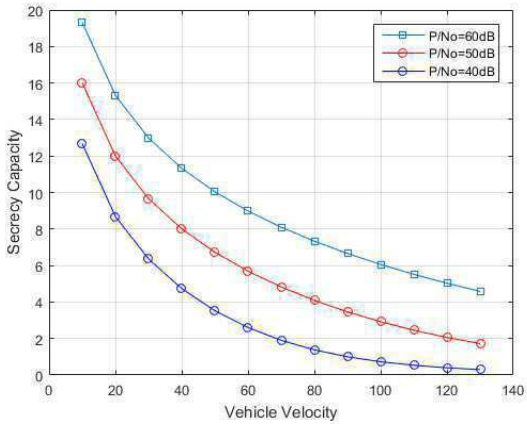
도면4


α=4
α=2
α=1.4
Secrecy Capacity
Vehicle Velocity

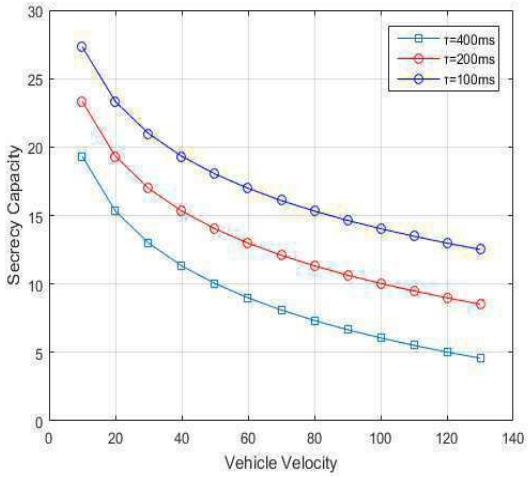
도면5


distance: 80m
distance: 100m
distance: 120m
Secrecy Capacity
Global Transit power[dBm]

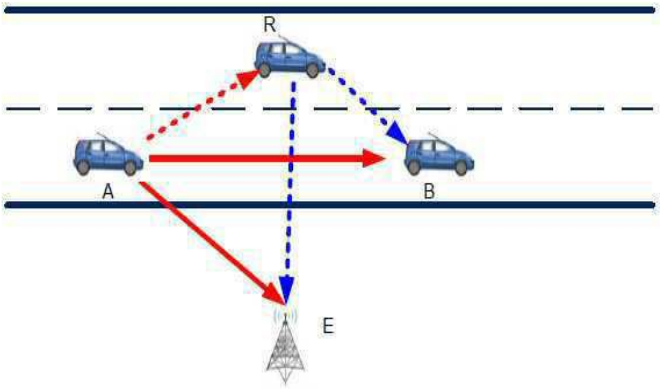
도면6


P/No=60dB
P/No=50dB
P/No=40dB
Secrecy Capacity
Vehicle Velocity

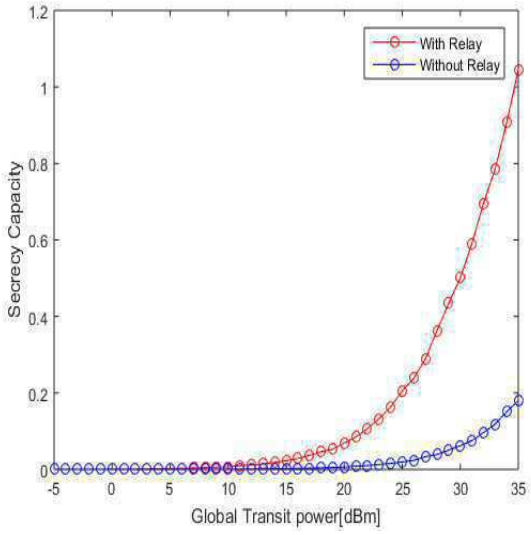
도면7


τ=400ms
τ=200ms
τ=100ms
Secrecy Capacity
Vehicle Velocity
0
5
10
15
20
25
30
0
20
40
60
80
100
120
140

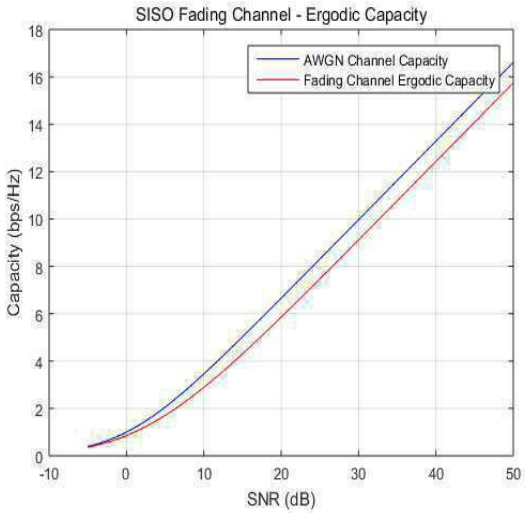
도면8


R
A
B
E

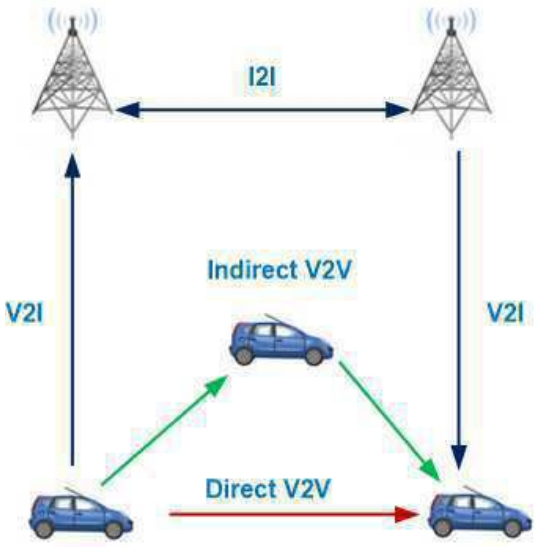
도면9


With Relay
Without Relay
Secrecy Capacity
Global Transit power[dBm]
0
0.2
0.4
0.6
0.8
1
1.2
-5
0
5
10
15
20
25
30
35

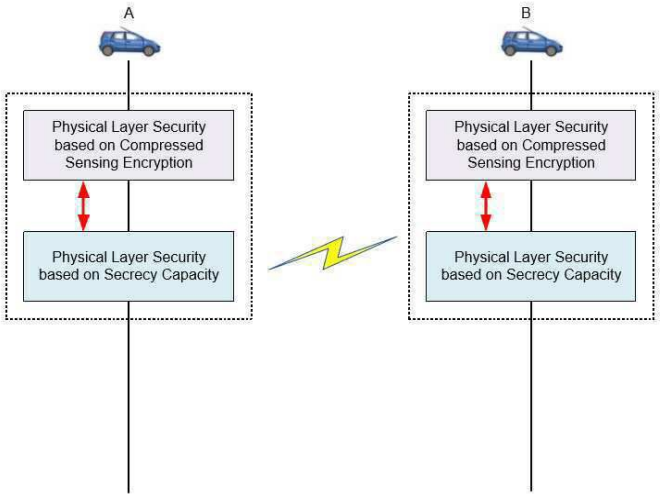
도면10



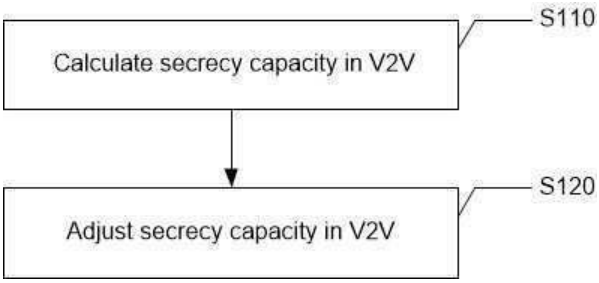
도면11



도면12



도면13


S110
Calculate secrecy capacity in V2V
S120
Adjust secrecy capacity in V2V