(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0153382
(43) 공개일자 2023년11월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/3239 (2013.01)
H04L 9/3247 (2013.01)
(21) 출원번호 10-2023-7029655
(22) 출원일자(국제) 2022년01월04일
심사청구일자 없음
(85) 번역문제출일자 2023년08월31일
(86) 국제출원번호 PCT/US2022/011077
(87) 국제공개번호 WO 2022/191908
국제공개일자 2022년09월15일
(30) 우선권주장
63/158,955 2021년03월10일 미국(US)
(뒷면에 계속)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
화이트, 윌리엄
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
마슈, 션 빈센트
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인 남앤남

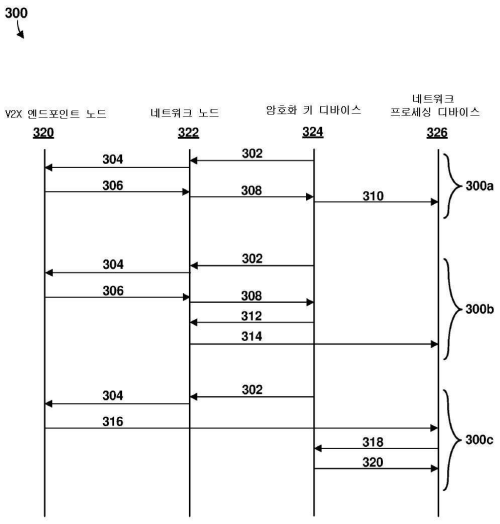
전체 청구항 수 : 총 33 항

(54) 발명의 명칭 **V2X(Vehicle-To-Everything) 메시지에서 평문 및 암호문 인증**

(57) 요 약

V2X(vehicle-to-everything) 메시지의 평문 및 암호문을 인증하기 위한 방법들을 구현하기 위한 방법들 및 디바이스들 및 시스템들은 V2X 메시지로 전송될 평문 메시지로부터 암호문을 생성하고, 암호문의 해시 및 평문 메시지의 해시를 생성하고, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 생성하고, 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 V2X 메시지를 네트워크 노드로 송신하는 것을 포함한다. 평문 메시지의 해시, 및 디지털 서명은 V2X 엔드포인트 노드가 연접에 서명했음을 네트워크 노드가 검증할 수 있도록 구성될 수 있다.

대 표 도 - 도3a



(52) CPC특허분류
H04L 2209/68 (2013.01)
H04L 2209/76 (2013.01)
H04L 2209/84 (2013.01)

(72) 발명자
반 듀렌, 드류 포스터
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
쿠마르, 비렌드라
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

(30) 우선권주장
63/180,450 2021년04월27일 미국(US)
17/497,120 2021년10월08일 미국(US)

명 세 서

청구범위

청구항 1

메시지의 평문 및 암호문을 인증하기 위해 엔드포인트 노드의 프로세서에 의해 수행되는 방법으로서,

메시지에서 전송될 평문 메시지로부터 암호문을 생성하는 단계;

상기 암호문의 해시와 상기 평문 메시지의 해시를 생성하는 단계;

상기 암호문의 해시와 상기 평문 메시지의 해시의 연접(concatenation)의 디지털 서명을 생성하는 단계; 및

상기 암호문, 상기 평문 메시지의 해시 및 상기 디지털 서명을 포함하는 메시지를 네트워크 노드로 송신하는 단계를 포함하고,

상기 암호문, 상기 평문 메시지의 해시 및 상기 디지털 서명은 상기 엔드포인트 노드가 서명된 연접에 서명했음을 상기 네트워크 노드가 검증할 수 있게 하도록 구성되는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

청구항 2

제1항에 있어서,

상기 엔드포인트 노드는 V2X(vehicle-to-everything) 엔드포인트 노드를 포함하고, 상기 메시지는 V2X 메시지를 포함하는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

청구항 3

제1항에 있어서,

상기 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지 또는 비상 응답자 메시지 중 하나로 구성되는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

청구항 4

제1항에 있어서,

상기 평문 메시지는 통행료 정보, 주차 액세스 정보, 도로 상태 정보, 지오네트워킹 정보 및 비상 응답자 정보 중 하나를 포함하는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

청구항 5

제1항에 있어서,

상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접은 상기 암호문 또는 상기 암호문의 해시의 식별 및 상기 평문 메시지 또는 상기 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

청구항 6

엔드포인트 노드로서,

프로세서를 포함하며,

상기 프로세서는,

메시지에서 전송될 평문 메시지로부터 암호문을 생성하고;

상기 암호문의 해시와 상기 평문 메시지의 해시를 생성하고;

상기 암호문의 해시와 상기 평문 메시지의 해시의 연접의 디지털 서명을 생성하고; 그리고

상기 암호문, 상기 평문 메시지의 해시 및 상기 디지털 서명을 포함하는 메시지를 네트워크 노드로 송신하도록

프로세서-실행가능 명령들로 구성되고,

상기 암호문, 상기 평문 메시지의 해시 및 상기 디지털 서명은 상기 엔드포인트 노드가 서명된 연접에 서명했음을 상기 네트워크 노드가 검증할 수 있도록 구성되는, 엔드포인트 노드.

청구항 7

제6항에 있어서,

상기 엔드포인트 노드는 V2X(vehicle-to-everything) 엔드포인트 노드를 포함하고, 상기 메시지는 V2X 메시지를 포함하는, 엔드포인트 노드.

청구항 8

제6항에 있어서,

상기 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지 또는 비상 응답자 메시지 중 하나로 구성되는, 엔드포인트 노드.

청구항 9

제6항에 있어서,

상기 평문 메시지는 통행료 정보, 주차 액세스 정보, 도로 상태 정보, 지오네트워킹 정보 및 비상 응답자 정보 중 하나를 포함하는, 엔드포인트 노드.

청구항 10

제6항에 있어서,

상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접은 상기 암호문 또는 상기 암호문의 해시의 식별 및 상기 평문 메시지 또는 상기 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하는, 엔드포인트 노드.

청구항 11

메시지를 프로세싱하기 위해 네트워크 노드의 프로세서에 의해 수행되는 방법으로서,

엔드포인트 노드로부터 암호문, 평문 메시지의 해시 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 연접의 디지털 서명을 포함하는 메시지를 수신하는 단계;

상기 엔드포인트 노드가 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접에 서명했는지 여부를 결정하는 단계; 및

상기 엔드포인트 노드가 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접에 서명했다는 결정에 응답하여, 상기 암호문, 상기 평문 메시지의 해시 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접의 상기 디지털 서명을 암호화 키 디바이스로 송신하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

청구항 12

제11항에 있어서,

상기 메시지는 V2X(vehicle-to-everything) 메시지를 포함하고, 상기 엔드포인트 노드는 V2X 엔드포인트 노드를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

청구항 13

제11항에 있어서,

상기 엔드포인트 노드가 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접에 서명했는지 여부를 결정하는 단계는,

상기 암호문의 해시를 생성하는 단계;

상기 평문 메시지의 해시와 상기 생성된 암호문의 해시를 연접하는 단계; 및

상기 엔드포인트 노드의 공개 키를 사용하여 상기 디지털 서명을 검증하기 위한 입력으로 상기 평문 메시지의 해시와 상기 생성된 암호문의 해시의 상기 연접을 제공하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

청구항 14

제11항에 있어서,

상기 암호문의 해시를 생성하는 단계는 인증된 엔드포인트 노드에 의해 사용되는 것으로 알려진 해시 알고리즘을 사용하여 상기 암호문의 해시를 생성하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

청구항 15

제11항에 있어서,

상기 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지 또는 비상 응답자 메시지 중 하나로 구성되는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

청구항 16

제11항에 있어서,

상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접은 상기 암호문 또는 상기 암호문의 해시의 식별 및 상기 평문 메시지 또는 상기 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

청구항 17

제11항에 있어서,

상기 암호문, 상기 평문 메시지의 해시, 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접의 상기 디지털 서명을 암호화 키 디바이스로 송신하는 단계는 상기 암호문, 상기 평문 메시지의 해시, 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접의 상기 디지털 서명을 암호화 키 서버로 송신하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

청구항 18

제11항에 있어서,

상기 암호문, 상기 평문 메시지의 해시, 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접의 상기 디지털 서명을 암호화 키 디바이스로 송신하는 단계는 상기 암호문, 상기 평문 메시지의 해시, 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접의 상기 디지털 서명을 암호화 키 모듈로 송신하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

청구항 19

네트워크 노드로서,

프로세서를 포함하며,

상기 프로세서는,

엔드포인트 노드로부터 암호문, 평문 메시지의 해시 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 연접의 디지털 서명을 포함하는 메시지를 수신하고;

상기 엔드포인트 노드가 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접에 서명했는지 여부를 결정하고; 그리고

상기 엔드포인트 노드가 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접에 서명했다는 결정에 응답하여, 상기 암호문, 상기 평문 메시지의 해시 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접의 상기 디지털 서명을 암호화 키 디바이스로 송신하도록

프로세서-실행가능 명령들로 구성되는, 네트워크 노드.

청구항 20

제19항에 있어서,

상기 메시지는 V2X(vehicle-to-everything) 메시지를 포함하고, 상기 엔드포인트 노드는 V2X 엔드포인트 노드를 포함하는, 네트워크 노드.

청구항 21

제19항에 있어서,

상기 프로세서는 추가로,

상기 암호문의 해시를 생성하고;

상기 평문 메시지의 해시와 상기 생성된 암호문의 해시를 연접하고; 그리고

상기 엔드포인트 노드의 공개 키를 사용하여 상기 디지털 서명을 검증하기 위한 입력으로 상기 평문 메시지의 해시와 상기 생성된 암호문의 해시의 상기 연접을 제공하도록

프로세서-실행가능 명령들로 구성되는, 네트워크 노드.

청구항 22

제19항에 있어서,

상기 프로세서는 추가로, 인증된 엔드포인트 노드에 의해 사용되는 것으로 알려진 해시 알고리즘을 사용하여 상기 암호문의 해시를 생성하도록 프로세서-실행가능 명령들로 구성되는, 네트워크 노드.

청구항 23

제19항에 있어서,

상기 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지 또는 비상 응답자 메시지 중 하나로 구성되는, 네트워크 노드.

청구항 24

제19항에 있어서,

상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접은 상기 암호문 또는 상기 암호문의 해시의 식별 및 상기 평문 메시지 또는 상기 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하는, 네트워크 노드.

청구항 25

제19항에 있어서,

상기 프로세서는 추가로, 상기 암호문, 상기 평문 메시지의 해시, 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접의 상기 디지털 서명을 암호화 키 서버로 송신하도록 프로세서-실행가능 명령들로 구성되는, 네트워크 노드.

청구항 26

제19항에 있어서,

상기 프로세서는 추가로, 상기 암호문, 상기 평문 메시지의 해시, 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접의 상기 디지털 서명을 암호화 키 모듈로 송신하도록 프로세서-실행가능 명령들로 구성되는,

네트워크 노드.

청구항 27

메시지의 평문 및 암호문을 인증하기 위해 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법으로서,

암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 상기 평문 메시지의 암호문의 해시, 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 단계;

상기 엔드포인트 노드가 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접에 서명했는지 여부를 결정하는 단계; 및

상기 엔드포인트 노드가 상기 암호문과 상기 평문 메시지의 연접에 서명했다는 결정에 응답하여 상기 엔드포인트 노드에 대한 데이터 트랜잭션을 수행하는 단계를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

청구항 28

제27항에 있어서,

상기 메시지는 V2X(vehicle-to-everything) 메시지를 포함하고, 상기 엔드포인트 노드는 V2X 엔드포인트 노드를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

청구항 29

제27항에 있어서,

상기 엔드포인트 노드가 상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접에 서명했는지 여부를 결정하는 단계는,

상기 평문 메시지의 해시를 생성하는 단계;

상기 생성된 평문 메시지의 해시와 상기 암호문의 해시를 연접하는 단계; 및

상기 엔드포인트 노드의 공개 키를 사용하여 상기 디지털 서명을 검증하기 위한 입력으로 상기 생성된 평문 메시지의 해시와 상기 암호문의 해시의 상기 연접을 제공하는 단계를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

청구항 30

제27항에 있어서,

상기 평문 메시지는 통행료 정보, 주차 액세스 정보, 도로 상태 정보, 지오네트워킹 정보 및 비상 응답자 정보 중 하나를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

청구항 31

제27항에 있어서,

상기 암호문의 해시와 상기 평문 메시지의 해시의 상기 연접은 상기 암호문 또는 상기 암호문의 해시의 식별 및 상기 평문 메시지 또는 상기 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

청구항 32

제27항에 있어서,

상기 암호화 키 디바이스로부터, 상기 엔드포인트 노드에 의해 발신된 평문 메시지, 상기 평문 메시지의 암호문의 해시, 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 단계는 암호화 키 서버로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 상기 평문 메시지의 암호문의 해시, 상기 암호문의 해시와 상기 평문 메시지 해시의 연접의 디지털 서명을 수신하는 단계를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

청구항 33

제27항에 있어서,

상기 암호화 키 디바이스로부터, 상기 엔드포인트 노드에 의해 발신된 평문 메시지, 상기 평문 메시지의 암호문의 해시, 및 상기 암호문의 해시와 상기 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 단계는 암호화 키 모듈로부터, 상기 엔드포인트 노드에 의해 발신된 평문 메시지, 상기 평문 메시지의 암호문의 해시, 상기 암호문의 해시와 상기 평문 메시지 해시의 연접의 디지털 서명을 수신하는 단계를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은 "Authenticating Plaintext And Ciphertext In A Vehicle-To-Everything (V2X) Message"이라는 명칭으로 2021년 3월 10일자로 출원된 미국 가특허 출원 제63/158,955호 및 "Authenticating Plaintext And Ciphertext In A Vehicle-To-Everything (V2X) Message With Enhanced Security"라는 명칭으로 2021년 4월 27자로 출원된 미국 가특허 출원 제63/180,450호에 대한 우선권의 이익을 주장하고, 이로써, 그 전체 내용들은 모든 목적들을 위해 본원에 참조로 포함된다.

배 경 기 술

[0002] [0002] 세계의 다수의 지역들은 차량 기반 통신 시스템들 및 기능에 대한 표준들을 개발하고 있다. 북미에서 사용하기 위한 IEEE(Institute of Electrical and Electronics Engineers) 및 SAE(Society of Automotive Engineers), 또는 유럽에서 사용하기 위한 ETSI(European Telecommunications Standards Institute) 및 CEN(European Committee for Standardization)에서 개발한 표준들이 있다. IEEE 802.11p 표준은 DSRC(Dedicated Short Range Communication) 및 ITS-G5 통신 표준들에 대한 기반이다. IEEE 1609는 IEEE 802.11p에 기반한 상위 계층 표준이다. C-V2X(Cellular Vehicle-to-Everything) 표준은 3세대 파트너십 프로젝트의 후원으로 개발된 경쟁 표준이다. 이러한 표준들은 차량 기반 무선 통신의 기반 역할을 하고, 지능형 고속도로들, 자율 및 반자율 차량들을 지원하고, 고속도로 교통 시스템들의 전반적인 효율성과 안전성을 개선하는 데 사용될 수 있다. 다른 V2X 무선 기술들은 또한 세계의 상이한 지역들에서 고려 중이다. 본원에 설명된 기법들은 모든 V2X 무선 기술에 적용 가능하다.

[0003] [0003] C-V2X 프로토콜은 향상된 도로 안전 및 자율 주행을 위해 360° 비가시선 인식과 더 높은 레벨의 예측 가능성을 함께 제공하는 2 개의 가지 전송 모드들을 정의한다. 제1 전송 모드는 V2V(Vehicle-to-Vehicle), V2I(Vehicle-to-Infrastructure), V2P(Vehicle-to-Pedestrian)를 포함하고, 셀룰러 네트워크와 독립적인 전용 지능형 교통 시스템(ITS) 5.9 기가헤르쯔(GHz) 스펙트럼에서 향상된 통신 범위 및 신뢰성을 제공하는 직접 C-V2X를 포함한다. 제2 전송 모드는 3세대 무선 이동 통신 기술(3G)들(예를 들어, GSM(global system for mobile communications) 진화(EDGE) 시스템들, 코드 분할 다중 액세스(CDMA) 2000 시스템들 등), 4세대 무선 이동 통신 기술(4G)들(예를 들어, LTE(Long Term Evolution) 시스템들, LTE-Advanced 시스템들, 모바일 WiMAX(Mobile Worldwide Interoperability for Microwave Access) 시스템들, 등), 5세대 뉴 라디오 무선 이동 통신 기술들(5G NR 시스템들 등) 등과 같은 모바일 광대역 시스템들 및 기술들에서 차량 대 네트워크 통신들(V2N)을 포함한다.

[0004] [0004] V2X 시스템의 요소는 차량이 북미에서는 BSM(Basic Safety Message) 또는 유럽에서 CAM(Cooperative Awareness Message)을 브로드캐스트하는 능력이고, 다른 차량들은 교통 안전을 개선하기 위해 수신하고 프로세싱할 수 있다. 전송 및 수신 차량들에서 이러한 메시지들의 프로세싱은 V2X(vehicle-to-everything) 기능을 제공하는 온보드 장비(본원에서 "V2X 온보드 장비"로 지칭됨)에서 발생한다.

발명의 내용

[0005] [0005] 다양한 양태들은 메시지의 평문 및 암호문을 인증하기 위해 엔드포인트 노드들에 의해 수행되는 방법들 및 시스템들을 포함한다. 일부 양태들은 메시지로 전송될 평문 메시지로부터 암호문을 생성하고, 암호문의 해시 및 평문 메시지의 해시를 생성하고, 암호문의 해시 및 평문 메시지의 해시의 연접의 디지털 서명을 생성하고, 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 메시지를 네트워크 노드로 송신하는 것을 포

함할 수 있다. 일부 양태들에서, 암호문, 평문 메시지의 해시, 및 디지털 서명은 엔드포인트 노드가 서명된 연접에 서명한 것을 네트워크 노드가 검증할 수 있도록 구성될 수 있다. 일부 양태들에서, 엔드포인트 노드는 V2X(vehicle-to-everything) 엔드포인트 노드를 포함할 수 있고, 메시지는 V2X 메시지를 포함할 수 있다.

[0006] [0006] 일부 양태들에서, 메시지는 제한된 대역폭 무선 통신 링크를 통한 전송을 위해 구성될 수 있다. 일부 양태들에서, 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지, 또는 비상 응답자 메시지 중 하나로 구성될 수 있다. 일부 양태들에서, 평문 메시지는 통행료 정보, 주차 액세스 정보, 도로 상태 정보, 지오네트워킹 정보 및 비상 응답자 정보 중 하나를 포함할 수 있다. 일부 양태들에서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문의 식별 또는 암호문의 해시 및 평문 메시지의 식별 또는 평문 메시지의 해시를 포함하는 데이터 구조를 포함할 수 있다.

[0007] [0007] 다양한 양태들은 메시지를 프로세싱하기 위해 네트워크 노드의 프로세서에 의해 수행되는 방법들 및 시스템들을 포함한다. 일부 양태들은 엔드포인트 노드로부터 암호문, 평문 메시지의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 포함하는 메시지를 수신하고, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하고, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시 연접에 서명했다는 결정에 대한 응답으로 암호문, 평문 메시지의 해시, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 디바이스로 송신하는 것을 포함할 수 있다.

[0008] [0008] 일부 양태들에서, 메시지는 V2X 메시지를 포함할 수 있고 엔드포인트 노드는 V2X 엔드포인트 노드를 포함할 수 있다. 일부 양태들에서, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하는 것은 암호문의 해시를 생성하는 것, 평문 메시지의 해시와 생성된 암호문의 해시를 연접하는 것, 및 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 평문 메시지의 해시와 생성된 암호문의 해시의 연접을 제공하는 것을 포함할 수 있다. 일부 양태들에서, 암호문의 해시를 생성하는 것은 인증된 엔드포인트 노드에 의해 사용되는 것으로 알려진 해시 알고리즘을 사용하여 암호문의 해시를 생성하는 것을 포함할 수 있다. 일부 양태들에서, 메시지는 제한된 대역폭 무선 통신 링크를 통한 전송을 위해 구성될 수 있다. 일부 양태들에서, 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지, 또는 비상 응답자 메시지 중 하나로 구성될 수 있다.

[0009] [0009] 일부 양태들에서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문의 해시의 식별 및 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함할 수 있다. 일부 양태들에서, 암호문, 평문 메시지의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 디바이스로 송신하는 것은 암호문, 평문 메시지의 해시, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 서버로 송신하는 것을 포함할 수 있다. 일부 양태들에서, 암호문, 평문 메시지의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 디바이스로 송신하는 것은 암호문, 평문 메시지의 해시, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 모듈로 송신하는 것을 포함할 수 있다.

[0010] [0010] 다양한 양태들은 메시지의 평문 및 암호문을 인증하기 위해 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법들 및 시스템들을 포함한다. 일부 양태들은 암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 것, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하는 것 및 엔드포인트 노드가 암호문과 평문 메시지의 연접에 서명했다는 결정에 대한 응답으로 엔드포인트 노드에 대한 데이터 트랜잭션을 수행하는 것을 포함할 수 있다.

[0011] [0011] 일부 양태들에서, 메시지는 V2X 메시지를 포함할 수 있고 엔드포인트 노드는 V2X 엔드포인트 노드를 포함할 수 있다. 일부 양태들에서, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하는 것은 평문 메시지의 해시를 생성하는 것, 생성된 평문 메시지의 해시와 암호문의 해시를 연접하는 것, 및 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 생성된 평문 메시지의 해시와 암호문의 해시의 연접을 제공하는 것을 포함할 수 있다.

[0012] [0012] 일부 양태들에서, 평문 메시지는 통행료 정보, 주차 액세스 정보, 도로 상태 정보, 지오네트워킹 정보 및 비상 응답자 정보 중 하나를 포함할 수 있다. 일부 양태들에서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문의 식별 또는 암호문의 해시 및 평문 메시지의 식별 또는 평문 메시지의 해시를 포함하는 데이터 구조를 포함할 수 있다. 일부 양태들에서, 암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 것은 암호화 키 서버로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 암호

문의 해시와 평문 메시지 해시의 연접의 디지털 서명을 수신하는 것을 포함할 수 있다. 일부 양태들에서, 암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 것은 암호화 키 모듈로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 것을 포함할 수 있다.

[0013] [0013] 다양한 양태들은 메시지 내의 평문 및 암호문을 인증하기 위한 시스템을 포함하고, 시스템은 메시지에서 전송될 평문 메시지로부터 암호문을 생성하고, 암호문의 해시 및 평문 메시지의 해시를 생성하고, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 생성하고, 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 메시지를 송신하기 위한 프로세서-실행가능 명령들로 구성된 프로세서를 포함하는 엔드포인트 노드를 포함한다.

[0014] [0014] 시스템은 또한 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 메시지를 엔드포인트 노드로부터 수신하고, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하고, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했다는 결정에 대한 응답으로 암호문, 평문 메시지의 해시 및 디지털 서명을 암호화 키 디바이스로 송신하는 프로세서-실행가능 명령들로 구성된 프로세서를 포함하는 네트워크 노드를 포함할 수 있다. 시스템은 또한, 암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하고, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하고, 엔드포인트 노드가 암호문과 평문 메시지의 연접에 서명했다는 결정에 대한 응답으로 엔드포인트 노드에 대한 데이터 트랜잭션을 수행하는 프로세서-실행가능 명령들로 구성된 프로세서를 포함하는 네트워크 프로세싱 디바이스를 포함할 수 있다.

[0015] [0015] 추가 양태들은 엔드포인트 노드, 네트워크 노드, 및/또는 위에 요약된 방법들 중 임의의 방법의 동작들을 수행하도록 구성된 프로세서 및 메모리를 포함하는 컴퓨팅 디바이스를 포함한다. 추가 양태들은 엔드포인트 노드, 네트워크 노드, 및/또는 위에서 요약된 방법들 중 임의의 방법에 대응하는 기능들을 수행하기 위한 다양한 수단을 갖는 컴퓨팅 디바이스를 포함할 수 있다. 추가 양태들은 엔드포인트 노드, 네트워크 노드, 및/또는 컴퓨팅 디바이스의 프로세서가 위에 요약된 방법들 중 임의의 방법에 대응하는 다양한 동작들을 수행하게 하도록 구성된 프로세서-실행가능 명령들이 저장되어 있는 비일시적 프로세서-판독가능 저장 매체를 포함할 수 있다.

도면의 간단한 설명

[0016] [0016] 본원에 포함되고 본 명세서의 일부를 구성하는 첨부 도면들은 청구범위의 예시적인 실시예들을 예시하고, 제공된 일반적인 설명 및 상세한 설명과 함께, 본원의 특징들을 설명하는 역할을 한다.

[0017] [0017] 도 1a는 다양한 실시예들을 구현하기에 적합한 예시적인 V2X 시스템을 예시하는 시스템 블록도이다.

[0018] [0018] 도 1b는 다양한 실시예들을 구현하기에 적합한 예시적인 V2X 통신 프로토콜 스택을 예시하는 개념도이다.

[0019] [0019] 도 2는 다양한 실시예들을 구현하기에 적합한 예시적인 차량 시스템의 구성요소 다이어그램이다.

[0020] [0020] 도 3a는 V2X 메시지에서 평문 및 암호문을 인증하는 방법 동안 기지국과 무선 디바이스 사이의 네트워크 요소들 사이에서 교환되는 통신의 예들을 예시하는 메시지 흐름도이다.

[0021] [0021] 도 3b는 다양한 실시예들을 구현하기에 적합한 예시적인 데이터 구조를 예시한다.

[0022] [0022] 도 4는 다양한 실시예들에 따른 V2X 메시지의 평문 및 암호문을 인증하기 위해 V2X의 프로세서에 의해 수행되는 방법을 예시하는 프로세스 흐름도이다.

[0023] [0023] 도 5는 다양한 실시예들에 따라 V2X 메시지를 프로세싱하기 위해 네트워크 노드의 프로세서에 의해 수행되는 방법을 예시하는 프로세스 흐름도이다.

[0024] [0024] 도 6은 다양한 실시예들에 따라 V2X 메시지의 평문 및 암호문을 인증하기 위해 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법을 예시하는 프로세스 흐름도이다.

[0025] [0025] 도 7은 다양한 실시예들과 함께 사용하기에 적합한 예시적인 모바일 컴퓨팅 디바이스를 예시하는 구성요

소 블록도이다.

[0026] 도 8은 다양한 실시예들과 함께 사용하기에 적합한 예시적인 모바일 컴퓨팅 디바이스를 예시하는 구성요소 블록도이다.

[0027] 도 9는 다양한 실시예들과 함께 사용하기에 적합한 예시적인 V2X 온보드 장비를 예시하는 구성요소 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0017] [0028] 다양한 실시예들은 첨부된 도면들을 참조하여 상세히 설명될 것이다. 가능하면, 동일한 참조 번호들은 동일하거나 유사한 부분들을 지칭하기 위해 도면들 전체에서 사용될 것이다. 특정 예들 및 구현들에 대해 이루어진 참조들은 예시를 위한 것이고, 청구범위를 제한하려는 의도가 아니다.

[0018] [0029] V2X 통신들에 일반적으로 사용되는 무선 통신 링크들은 대역폭이 제한된다. 일부 상황들에서, V2X 엔드포인트 노드(예를 들어, 차량)는 암호화된 평문 콘텐츠를 갖는 V2X 메시지를 송신할 수 있다. V2X 메시지는 중간 네트워크 노드(예를 들어, 노변 장치(RSU), 갠트리 배치 유닛(gantry-deployed unit) 등)에 의해 수신될 수 있고, 이는 메시지의 오버-디-에어 전송이 에러들을 메시지에 도입하지 않았음을 검증한다. 이어서, 중간 네트워크 노드는 메시지 콘텐츠를 해독하고 메시지 콘텐츠에 기반한 동작을 수행하는 프로세싱 네트워크 노드로 메시지를 전달할 수 있다. 2 개의 디지털 서명들이 V2X 메시지에 대해 생성될 수 있지만, 하나는 평문용이고 하나는 암호화된 평문(즉, 암호문)용이고, 이렇게 하면 V2X 메시지에 의해 초래되는 대역폭 오버헤드, 및 V2X 메시지에 대한 2 개의 서명들을 생성하는 계산 오버헤드가 증가한다.

[0019] [0030] 다양한 실시예들은 지능형 교통 시스템(ITS)에서 V2X(vehicle-to-everything) 메시지의 평문 및 암호문을 인증하기 위한 방법들 및 메커니즘들을 포함한다. 다양한 실시예들은 V2X 엔드포인트 노드(차량의 V2X 온보드 장비, 모바일 폰, 랩톱, 태블릿 또는 다른 적합한 컴퓨팅 디바이스와 같은 모바일 컴퓨팅 디바이스일 수 있음), 중간 노드(예를 들어, 다른 차량 또는 모바일 컴퓨팅 디바이스, 노변 장치(RSU), 갠트리 유닛(예를 들어, 통행료 갠트리 유닛)), 네트워크 프로세싱 디바이스(예를 들어, 통행료 또는 주차 지불 프로세싱, 도로 상태 모니터링, 상용차들 스크리닝 및 다른 적합한 애플리케이션들 같은 데이터 트랜잭션에 사용될 수 있는 서버)와 같은 다양한 네트워크 요소들이 V2X 메시지의 평문과 암호문을 인증할 수 있게 한다. 다양한 실시예들에 의해 지원되는 인증 방법들은 V2X 대역폭-제약 메시지들에 특히 유용하다.

[0020] [0031] V2X 프로세싱 및 통신 시스템들은 자동차들, 트럭들, 버스들, 트레일러들, 자율주행 차량들, 로봇 시스템들 등과 같은 다양한 차량들에 구현될 수 있다. 또한, ITS 또는 다른 V2X 시스템은 노변 장치들, 액세스 노드들, 및 무선 릴레이 노드들과 같은 다수의 고정 장비 설비들을 포함한다. 추가로, 다양한 실시예들은 ITS 기능과 관련이 없지만 유료 주차장들, 다양한 상용 애플리케이션들을 위한 무선 지불 시스템들, 응급 의료 서비스들 등과 같은 V2X 능력들을 이용하는 시스템들에서 유용할 수 있다. 다양한 실시예들은 V2X 통신 인프라를 사용하는 임의의 다양한 V2X-장착 차량, 고정 설비들 및 다른 디바이스들에서 구현될 수 있다. 다양한 실시예들의 모든 구현들을 포함하기 위해, "V2X 엔드포인트 노드"라는 용어는 이 설명 및 청구범위에서 일반적으로 V2X 통신 기능을 구현하는 모바일, 세미-모바일 또는 고정 시스템을 지칭하는 데 사용된다. 설명을 위해 사용되는 V2X 엔드포인트 노드의 비제한적인 예는 유료 도로를 여행하는 동안 통행료를 지불하는 자동차와 같은 차량이지만, 이것 및 다른 예들에 대한 참조들은 V2X 엔드포인트 노드를 열거한 청구범위를 제한하려는 의도가 아니다. 일부 구현들은 통신 링크들의 적어도 일부(예를 들어, 세그먼트들, 홉(hop)들 등)가 제한된 대역폭, 채널 용량 등과 같은 제약된 통신 자원들을 갖는 통신 매체를 통해 인증된 암호화된 메시지들이 전송될 수 있는 임의의 통신 시스템에서 사용될 수 있다.

[0021] [0032] V2X 메시지들의 무결성, 진위성 및 일부 경우들에서, 기밀성의 검증은 자율 및 반자율 차량들을 위한 다양한 기능들을 수행하고 ITS에서 다양한 서비스들을 지원하는 데 유용하다. 다양한 실시예들에서, V2X 엔드포인트 노드(예를 들어, V2X-장착 차량)는 중간 네트워크 노드(예를 들어, 노변 장치 또는 다른 ITS 노드)를 통해 네트워크 프로세싱 디바이스에 정보를 송신하도록 요청될 수 있다. 암호화 키 디바이스는 암호화 키를 생성하고 암호화 키를 중간 네트워크 노드로 송신할 수 있다. 일부 실시예들에서, 암호화 키 디바이스는 암호화 키 서버와 같은 별도의 디바이스일 수 있다. 일부 실시예들에서, 암호화 키 디바이스는 중간 네트워크 노드(또는 네트워크 프로세싱 디바이스)의 모듈, 유닛 또는 기능일 수 있다. 중간 네트워크 노드는 V2X가 소정 정보를 제공하라는 요청과 함께 암호화 키를 V2X 엔드포인트 노드로 송신할 수 있다. V2X 엔드포인트 노드는 응답 메시지를 생성하고, 메시지의 디지털 서명을 생성하고, 메시지를 암호화하고, 암호화된 메시지의 디지털 서명을 생

성할 수 있다. V2X 엔드포인트 노드는 암호화된 메시지와 디지털 서명을 중간 네트워크 노드로 송신할 수 있다. 중간 네트워크 노드는 V2X 엔드포인트 노드에서 송신된 메시지들의 무결성을 검증하는 암호화된 메시지의 디지털 서명을 검증할 수 있다. 중간 네트워크 노드는 암호화된 메시지를 암호화 키 디바이스로 전달할 수 있고, 암호화 키 디바이스는 메시지를 해독하고 해독된 메시지와 메시지의 디지털 서명을 네트워크 프로세싱 디바이스로 송신한다. 네트워크 프로세싱 디바이스는 메시지의 디지털 서명을 검증할 수 있고, V2X 엔드포인트 노드로부터의 메시지와 관련된 일부 액션 또는 동작을 수행할 수 있다.

[0022] [0033] 다양한 실시예들의 예시적인 애플리케이션은 V2X-장착 차량이 유료 도로에서 이동하거나 유료 주차장에 진입하는 것과 같은 V2X 엔드포인트 노드에 대한 요금 징수 또는 통행료 징수 동작을 수행하는 것을 포함한다. 통행료 갠트리 디바이스(또는 다른 적합한 디바이스)는 V2X 엔드포인트 노드를 검출하고 요금 징수 동작을 위한 정보를 요청하는 메시지(예를 들어, TAM(tolling advertisement message))를 V2X 모드로 송신할 수 있다. V2X 엔드포인트 노드는 응답 메시지, 메시지의 디지털 서명, 메시지의 암호화된 버전 및 암호화된 메시지의 디지털 서명을 포함하는 TUM(tolling upload message)으로 응답할 수 있다. 통행료 갠트리 디바이스는 암호화된 메시지의 디지털 서명을 사용하여 TUM의 오버-디-에어 전송이 메시지에 에러들을 도입하지 않았음을 검증할 수 있다. 통행료(수수료) 서비스 제공자의 네트워크 노드는 (해독 후) 메시지의 디지털 서명을 사용하여 (메시지의 디지털 서명이 검증된 경우) 수수료 징수를 위한 관련 금융 트랜잭션을 수행할 수 있다.

[0023] [0034] 위에서 언급한 바와 같이, 2 개의 디지털 서명들이 생성되고, 하나는 메시지(즉, 평문)이고 하나는 메시지의 암호화된 버전(즉, 암호문)이다. 그러나, 2 개의 별개의 디지털 서명들을 생성하고 송신하는 것은 무선 통신을 통해 이 정보를 전송하는 데 필요한 무선 주파수(RF) 오버헤드를 증가시킨다. 예를 들어, 일부 통신 프로토콜 구현들에서, 각각의 추가 서명은 단일 메시지에 100 바이트 이상을 추가할 수 있다. 다수의 V2X 엔드포인트 노드들, 중간 노드들 및 네트워크 노드들이 이러한 메시지들을 생성, 암호화, 해독 및 프로세싱할 때, 추가 오버헤드는 통신 시스템 자원들, 특히 V2X 통신 시스템 같은 대역폭-제약된 시스템의 통신 자원들에 상당한 악영향을 미칠 수 있다.

[0024] [0035] 다양한 실시예들은 효율을 개선하고 이러한 V2X 메시지들을 취급하는 데 필요한 프로세싱 및 통신 링크 오버헤드를 줄이는 방식으로 V2X 메시지에서 평문 및 암호문을 인증하는 방법들을 수행하도록 구성된 방법들, V2X 프로세싱 디바이스들, 및 시스템들을 포함한다. 일부 실시예들에서, V2X 엔드포인트 노드(예를 들어, 차량의 V2X 온보드 장비의 V2X 프로세싱 디바이스)는 V2X 메시지로 전송될 평문 메시지로부터 암호문을 생성하고, 암호문의 해시 및 평문 메시지의 해시를 생성하고, 암호문의 해시와 평문 메시지의 해시 연접의 디지털 서명을 생성하고, 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 V2X 메시지를 네트워크 노드로 송신할 수 있다. 일부 실시예들에서, 암호문, 평문 메시지의 해시, 및 디지털 서명은 네트워크 노드로 하여금 무선 디바이스가 암호문의 해시와 평문 메시지의 해시의 서명된 연접에 서명했음을 검증할 수 있도록 구성될 수 있다.

[0025] [0036] 다양한 실시예들에서, 암호문의 해시와 평문 메시지의 해시는 임의의 순서로 연접될 수 있다. 일부 실시예들에서, 암호문의 해시 및/또는 평문 메시지의 해시는 암호문 해시와 평문 메시지 해시의 메시지 위치(예를 들어, 정의된 바이트 범위)를 정의하는 데이터 구조에 포함될 수 있다(예를 들어, ASN.1(Abstract Syntax Notation One) 또는 다른 적합한 데이터 구조 설명 언어와 같은 데이터 구조 설명 언저에 의해 설명될 수 있음). 일부 실시예들에서, 암호문의 해시 및/또는 평문 메시지의 해시는 암호문 및/또는 암호문의 해시의 위치들 또는 그들 사이의 경계를 식별하는 표시(예를 들어, 시작 바이트 값 또는 필드 길이 값) 및 평문 메시지 및/또는 평문 메시지의 해시의 식별을 포함할 수 있다.

[0026] [0037] 일부 실시예들에서, V2X 메시지는 대역폭 제약 V2X 무선 통신 링크와 같은 제한된 대역폭 무선 통신 링크를 통한 전송을 위해 구성된다. 일부 실시예들에서, V2X 메시지는 하나 이상의 기능들 또는 시스템들에 따라 구성될 수 있다. 일부 실시예들에서, 평문 메시지는 V2X 엔드포인트 노드와 관련된 통행료 징수 또는 수수료 징수 동작을 가능하게 할 수 있는 V2X 엔드포인트 노드에 관한 또는 이와 연관된 민감한 금융 정보(예를 들어, 계좌 번호, 신용 카드 번호 등)를 포함할 수 있다. 예를 들어, V2X 메시지는 통행료 메시지(예를 들어, 요금 징수 또는 통행료 징수 시스템을 위한), 주차 액세스 메시지(예를 들어, 주차 지불 시스템을 위한), 도로 상태 메시지(예를 들어, 다른 차량, RSU, 또는 교통에 관한 네트워크 노드, 관찰된 차량 거동, 도로 손상, 얼음 또는 홍수 등과 같은 위험한 도로 상태에 대한 메시지), 지오네트워킹 메시지(예를 들어, 지오네트워킹 메시지 또는 메시징 시스템에 사용하기 위한), 비상 응답자 메시지(예를 들어, 경찰, 소방서, 응급 의료 기술자 또는 다른 비상 응답자 시스템) 또는 다른 적합한 메시지 또는 메시징 시스템으로 구성될 수 있다.

[0027] [0038] 일부 실시예들에서, 평문 메시지는 보호 및 인증이 적절한 개인 신원, 의료 정보, 기밀 정보 또는 독점

정보와 같은 비재무적 민감 정보를 포함할 수 있다. 일부 실시예들에서, 평문 메시지는 주차 위치, 타이머 기간 및/또는 주차 요금과 같은 주차 액세스 정보를 포함할 수 있다. 일부 실시예들에서, 평문 메시지는 도로 상태 정보를 포함할 수 있다. 일부 실시예들에서, 평문 메시지는 지오네트워킹 정보를 포함할 수 있다. 일부 실시예들에서, 평문 메시지는 위험한 상태, 사건, 사고 등에 대한 정보, 용의자들 또는 피해자들에 대한 신원 정보, 의료 정보, 개인 식별 정보(PII) 등과 같은 비상 응답자 정보를 포함할 수 있다. 일부 구현들에서, 평문 메시지의 콘텐츠는 기밀 정보 또는 민감 성격의 정보, 또는 법률 또는 규정에 의해 기밀로 취급되어야 하는 정보(예를 들어, 금융 계정 정보, 의료 정보 등)를 포함할 수 있다.

[0028] [0039] 일부 실시예들에서, 네트워크 노드(예를 들어, 차량, RSU, 갠트리 유닛, 에지 컴퓨팅 디바이스 등과 같은 중간 네트워크 노드)는 암호문, 평문 메시지의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 포함하는 V2X 메시지를 V2X 엔드포인트 노드로부터 수신할 수 있다. 네트워크 노드는, V2X 엔드포인트 노드가 암호문의 해시를 생성하고, 생성된 암호문의 해시를 사용하여 수신된 평문 메시지의 해시와 생성된 암호문의 해시의 연접을 구성하고, 그리고 V2X 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 수신된 평문 메시지의 해시와 생성된 암호문의 해시의 연접을 사용함으로써 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를, 결정할 수 있다. V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했다는 결정에 응답하여, 네트워크 노드는 암호문, 평문 메시지의 해시 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 디바이스로 송신할 수 있다.

[0029] [0040] 일부 실시예들에서, 컴퓨팅 디바이스(예를 들어, 지불 프로세싱 서버, 도로 상태 정보를 프로세싱하도록 구성된 컴퓨팅 디바이스, 비상 응답자 메시지들 및 정보를 프로세싱하도록 구성된 컴퓨팅 디바이스, 또는 다른 적합한 컴퓨팅 디바이스)는 암호화 키 디바이스로부터 V2X 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문 해시, 및 암호문 해시와 평문 메시지 해시의 연접의 디지털 서명을 수신할 수 있다. 컴퓨팅 디바이스는, V2X 엔드포인트 노드가 평문 메시지의 해시를 생성하고, 평문 메시지의 해시를 사용하여 생성된 평문 메시지의 해시와 수신된 암호문의 해시의 연접을 구성하고, 그리고 V2X 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 생성된 평문 메시지의 해시와 수신된 암호문의 해시의 연접을 사용함으로써 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를, 결정할 수 있다. 컴퓨팅 디바이스는 V2X 엔드포인트 노드가 암호문과 평문 메시지의 연접에 서명했다는 결정에 응답하여 V2X 엔드포인트 노드에 대한 데이터 트랜잭션을 수행할 수 있다.

[0030] [0041] 다양한 실시예들은 프로세싱 및 통신 링크 효율을 개선하고, 이러한 V2X 메시지들을 취급하는 데 필요한 프로세싱 및 통신 링크 오버헤드를 줄이는 방식으로 V2X 메시지에서 평문 및 암호문을 인증하는 방법들을 수행하도록 구성된 방법들, V2X 프로세싱 디바이스들, 및 시스템들을 포함한다.

[0031] [0042] 참조의 용이함을 위해, 실시예들 중 일부는 V2X 시스템들 및 프로토콜들을 사용하는 차량을 참조하여 본 출원에서 설명된다. 그러나, 다양한 실시예들이 V2X 또는 차량 기반 통신 표준들, 메시지들, 프로토콜들 또는 기술들 중 일부 또는 전부를 포함함이 이해되어야 한다. 따라서, 애플리케이션의 어느 것도 청구범위에서 이와 같이 명시적으로 열거되지 않으면 특정 시스템(예를 들어, V2X) 또는 메시지 또는 메시징 프로토콜(예를 들어, BSM(Basic Safety Message)들)에 대한 청구범위로 제한되지 않아야 한다. 게다가, 본원에서 설명되는 실시예들은 차량 내 V2X 프로세싱 시스템을 지칭할 수 있다. V2X 프로세싱 시스템이 모바일 디바이스들, 모바일 컴퓨터들, RSU들 및 도로 및 차량 상태들을 모니터링하고 V2X 통신들에 참여하도록 장착된 다른 디바이스들에서 동작하거나 그들에 포함될 수 있는 다른 실시예들이 고려된다.

[0032] [0043] 도 1a는 다양한 실시예들을 구현하기에 적합한 예시적인 V2X 시스템(100)을 예시하는 시스템 블록도이다. 도 1b는 다양한 실시예들을 구현하기에 적합한 예시적인 V2X 통신 프로토콜 스택(150)을 예시하는 개념도이다. 도 1a 및 도 1b를 참조하여, 차량(12, 14, 16)은 V2X 온보드 장비(102, 104, 106)를 각각 포함할 수 있고, 이들은 다른 차량의 온보드 장비(예를 들어, 102, 104, 106)에 의한 수신 및 프로세싱을 위해 기본 안전 메시지(Basic Safety Message)들(112, 114, 116)을 주기적으로 브로드캐스팅하는 것을 포함하여 V2X 메시지들을 송신 및 수신하도록 구성될 수 있다.

[0033] [0044] 차량 위치, 속도, 방향, 제동과 같은 거동 및 다른 정보를 공유함으로써, 차량들은 안전한 이격을 유지하고 잠재적인 충돌들을 식별하고 피할 수 있다. 예를 들어, 선행 차량(16)으로부터 기본 안전 메시지들(114)을 수신하는 후행 차량(12)은 차량(16)의 속도와 위치를 결정할 수 있어, 차량(12)이 속도를 매칭하고 안전한 이격 거리(20)를 유지할 수 있게 한다. 선행 차량들(16)이 브레이크들을 적용할 때 기본 안전 메시지들(114)을 통해 알림을 받음으로써, 선행 차량(16)이 급정지하더라도 후행 차량(12)의 V2X 장비(102)는 동시에 브레이크들

을 적용하여 안전한 이격 거리(20)를 유지할 수 있다. 다른 예로, 트럭 차량(14) 내의 V2X 장비(104)는 2 개의 차량들(12, 16)으로부터 기본 안전 메시지들(112, 116)을 수신하고, 따라서 트럭 차량(14)이 충돌을 피하기 위해 교차로에서 정지해야 함을 알릴 수 있다. 추가로, 차량 V2X 온보드 장비(102, 104, 106) 각각은 임의의 다양한 근접 통신 프로토콜들을 사용하여 서로 통신할 수 있다.

[0034] [0045] 게다가, 차량들은 기본 안전 메시지들 및 다른 V2X 통신들에 관한 데이터 및 정보를 통신 네트워크(18)(예를 들어, V2X, 셀룰러, WiFi 등)를 통해 통신 링크들(122, 124, 146)을 거쳐 다양한 네트워크 요소들(132, 134, 136)로 전송할 수 있다. 예를 들어, 네트워크 요소(132)는 RSU, 갠트리 유닛 등으로 통합되거나 이와 통신할 수 있다. 네트워크 요소(134, 136)는 지불 프로세싱, 도로 상태 모니터링, 긴급 제공자 메시지 프로세싱 등과 같은 차량(12, 14, 16)과 관련된 기능 또는 서비스를 수행하도록 구성될 수 있다. 네트워크 요소(134, 136)는 유선 또는 무선 네트워크들(142, 144)을 통해 서로 통신하여 지불 프로세싱, 도로 상태 모니터링, 긴급 제공자 메시지 핸들링 및 유사한 서비스들과 연관된 정보를 교환하도록 구성될 수 있다.

[0035] [0046] 도 2는 다양한 실시예들을 구현하기에 적합한 예시적인 차량 시스템(200)의 구성요소 다이어그램이다. 도 1a 내지 도 2를 참조하여, 시스템(200)은 V2X 프로세싱 디바이스(204)(예를 들어, 텔레매틱스 제어 유닛 또는 온보드 유닛(TCU/OBU))를 포함하는 차량(202)을 포함할 수 있다. V2X 프로세싱 디바이스(202)는 차량 내 네트워크(210), 인포테인먼트 시스템(212), 다양한 센서들(214), 다양한 액추에이터들(216) 및 무선 주파수(RF) 모듈(218)과 같은 다양한 시스템들 및 디바이스들과 통신할 수 있다. V2X 프로세싱 디바이스(202)는 또한 다양한 다른 차량들(220), 노변 장치들(222), 기지국들(224) 및 다른 외부 디바이스들과 통신할 수 있다. TCU/OBU(204)는 아래에서 더 설명되는 바와 같이 평문 및 암호문을 인증하기 위한 동작들을 수행하도록 구성될 수 있다.

[0036] [0047] V2X 프로세싱 디바이스(204)는 V2X 안테나(예를 들어, RF 모듈(218))를 포함할 수 있고, 다른 차량(220), 노변 장치(222) 및 기지국(224) 또는 다른 적합한 네트워크 액세스 포인트와 같은 하나 이상의 ITS 참가자들(예를 들어, 스테이션들)과 통신하도록 구성될 수 있다. 다양한 실시예들에서, V2X 프로세싱 디바이스(202)는 차량 내 네트워크(210), 인포테인먼트 시스템(212), 다양한 센서들(214), 다양한 액추에이터들(216) 및 RF 모듈(218)과 같은 복수의 정보 소스들로부터 정보를 수신할 수 있다. V2X 프로세싱 디바이스(204)는 복수의 정보 소스들(210-218) 중 하나, V2X 프로세싱 디바이스(204)에서 실행되는 애플리케이션 또는 서비스, 또는 차량의 다른 시스템과 같은 차량의 시스템에서 오작동 상태를 검출할 수 있다.

[0037] [0048] 차량 내 네트워크(210)의 예들은 계측 제어기 통신망(CAN: Controller Area Network), LIN(Local Interconnect Network), FlexRay 프로토콜을 사용하는 네트워크, 차량 네트워크 시스템(MOST: Media Oriented Systems Transport) 네트워크, 자동차 이더넷 네트워크를 포함한다. 차량 센서들(214)의 예들은 (GNSS(Global Navigation Satellite System) 시스템과 같은) 위치 결정 시스템, 카메라, 레이더, 라이다, 초음파 센서들, 적외선 센서들, 및 다른 적합한 센서 디바이스들 및 시스템들을 포함한다. 차량 액추에이터들(216)의 예들은 조향, 브레이크들, 엔진 동작, 조명들, 방향 신호들 등과 같은 다양한 물리적 제어 시스템들을 포함한다.

[0038] [0049] 도 3a는 V2X 메시지에서 평문 및 암호문을 인증하는 방법 동안 기지국과 무선 디바이스 사이의 네트워크 요소들 사이에서 교환되는 통신의 예들을 예시하는 메시지 흐름도(300)이다. 도 3b는 다양한 실시예들을 구현하기에 적합한 예시적인 데이터 구조(350)를 예시한다. 도 1 내지 도 3b를 참조하여, 네트워크 요소들은 V2X 엔드포인트 노드(320)(예를 들어, 차량(12, 14, 16, 202)), 네트워크 노드(322)(예를 들어, 차량들(12, 14, 16, 220) 중 다른 하나, RSU(132), 220), 암호화 키 디바이스(324)(예를 들어, 네트워크 요소(134, 136)) 및 네트워크 프로세싱 디바이스(326)(예를 들어, 네트워크 요소(134, 136))를 포함할 수 있다. 일부 실시예들에서, 암호화 키 디바이스(324)는 암호화 키 서버와 같은 별도의 디바이스일 수 있다. 일부 실시예들에서, 암호화 키 디바이스(324)는 네트워크 노드(322) 또는 네트워크 프로세싱 디바이스(326)의 모듈, 유닛 또는 기능일 수 있다.

[0039] [0050] 제1 예시적인 시나리오(300a)에서, 암호화 키 디바이스(324)는 암호화 키를 생성하고 암호화 키를 메시지(302)로 네트워크 노드(322)로 송신할 수 있다. 일부 실시예들에서, 암호화 키는 공개 키이거나 공개 키를 포함할 수 있다. 네트워크 노드(322)는 V2X가 소정 정보를 제공하라는 요청(304)과 함께 V2X 엔드포인트 노드(320)에 암호화 키를 송신할 수 있다. 요청(304)은 V2X 메시지일 수 있거나 이에 포함될 수 있다. 일반적으로, V2X 메시지들은 V2X 통신 시스템에서 사용하도록 구성되고, V2X 통신 프로토콜에 따라 포맷되고, 대역폭 및/또는 다른 자원 제약 무선 통신 링크를 통한 전송을 위해 구성된다.

[0040] [0051] V2X 엔드포인트 노드(320)는 평문 메시지를 포함하는 응답을 생성할 수 있다. V2X 엔드포인트 노드는

평문 메시지로부터 암호문을 생성할 수 있고, 암호문의 해시와 평문 메시지의 해시를 생성할 수 있다. V2X 엔드포인트 노드는 SHA-2 알고리즘 모음 등과 같은 해싱 알고리즘을 사용하여 해시(들)를 생성할 수 있다. V2X 엔드포인트 노드(320)는 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 생성할 수 있다. 다양한 실시예들에서, 암호문의 해시와 평문 메시지의 해시는 임의의 순서로 연접될 수 있다.

[0041] [0052] 일부 실시예들에서, V2X 엔드포인트 노드는 데이터 구조(350)(도 3b)와 같은 데이터 구조를 생성할 수 있고, V2X 엔드포인트 노드는 데이터 구조의 디지털 서명을 생성할 수 있다. 데이터 구조(350)는 암호문의 해시 및/또는 평문 메시지의 해시를 식별하는 마커들을 포함할 수 있다. 데이터 구조(350)는 또한 다른 데이터를 포함할 수 있다. 예를 들어, 데이터 구조(350)(예를 들어, "SignedDecryptableData")는 평문 메시지의 해시 또는 평문 메시지 자체("hOP HashOrPlaintext"), 암호문의 해시, 또는 암호문 메시지 자체("hOC HashOrCiphertext") 등과 같은 그 구조 및/또는 콘텐츠의 설명(352)을 포함할 수 있다. 데이터 구조(350)는 또한 평문 메시지의 해시 또는 평문 메시지의 설명(354), 암호문의 해시 또는 암호문의 설명(356), 및 다른 데이터 필드들, 설명자들, 마켓들 및/또는 다른 콘텐츠를 포함할 수 있다.

[0042] [0053] 도 3a로 돌아가면, V2X 엔드포인트 노드는 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 V2X 메시지(306)를 네트워크 노드(322)로 송신할 수 있다. 네트워크 노드(322)는, V2X 엔드포인트 노드(320)가 암호문의 해시를 생성하고, 생성된 암호문의 해시를 사용하여 수신된 평문 메시지의 해시와 생성된 암호문의 해시의 적절하게 인코딩된 연접을 구성하고, 그리고 V2X 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 수신된 평문 메시지의 해시와 생성된 암호문의 해시의 연접을 사용함으로써 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를, 결정할 수 있다. V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했다는 결정에 응답하여, 네트워크 노드(322)는 암호문, 평문 메시지의 해시 및 디지털 서명을 메시지(308)로 암호화 키 디바이스(324)로 송신할 수 있다.

[0043] [0054] 암호화 키 디바이스(324)는 암호문을 해독하여 평문 메시지를 생성할 수 있다. 이어서, 암호화 키 디바이스(324)는 통신(310)에서 평문 메시지, 암호문의 해시, 및 (암호문의 해시와 평문 메시지의 해시의 연접의) 디지털 서명을 네트워크 프로세싱 디바이스(326)로 송신할 수 있다.

[0044] [0055] 일부 실시예들에 따른 제2 예시적인 시나리오(300b)에서, 암호화 키 디바이스(324)는 평문 메시지를 메시지(312)로 네트워크 노드(322)에 반환할 수 있고, 네트워크 노드(322)는 평문 메시지, 암호문의 해시, 및 (암호문의 해시와 평문 메시지의 해시의 연접의) 디지털 서명을 메시지(314)로 네트워크 프로세싱 디바이스(326)로 송신할 수 있다. 일부 실시예들에서, 네트워크 노드(322) 및 암호화 키 디바이스(324)는 네트워크 노드(322)와 함께 위치되거나 통합될 수 있고, 해독 동작들은 네트워크 노드(322) 가까이에서 또는 네트워크 노드(322) 내에서 수행될 수 있다.

[0045] [0056] 일부 실시예들에 따른 제3 예시적인 시나리오(300c)에서, 엔드포인트 노드는 암호문, 평문 메시지의 해시 및 디지털 서명을 메시지(316)로 네트워크 프로세싱 디바이스(326)로 송신할 수 있다. 일부 실시예들에서, 네트워크 프로세싱 디바이스(326)는, V2X 엔드포인트 노드(320)가 암호문의 해시를 생성하고, 생성된 암호문의 해시를 사용하여 수신된 평문 메시지의 해시와 생성된 암호문의 해시의 적절하게 인코딩된 연접을 구성하고, 그리고 V2X 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 수신된 평문 메시지의 해시와 생성된 암호문의 해시의 연접을 사용함으로써 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를, 결정할 수 있다. V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했다는 결정에 응답하여, 네트워크 프로세싱 디바이스(326)는 메시지(318)에서 복호화를 위해 암호화 키 디바이스(324)에 암호문을 송신할 수 있다. 암호화 키 디바이스는 암호문을 해독할 수 있고 평문을 메시지(320)로 네트워크 프로세싱 디바이스로 송신할 수 있다. 일부 실시예들에서, 암호화 키 디바이스(324)는 네트워크 프로세싱 디바이스(326)와 함께 위치하거나 통합될 수 있고, 복호화 동작들은 네트워크 프로세싱 디바이스(326) 가까이에서 또는 네트워크 프로세싱 디바이스 내에서 수행될 수 있다.

[0046] [0057] 네트워크 프로세싱 디바이스(326)는, V2X 엔드포인트 노드가, 평문 메시지의 해시를 생성하고, 평문 메시지의 해시를 사용하여 생성된 평문 메시지의 해시와 수신된 암호문의 해시의 적절하게 인코딩된 연접을 구성하고, 그리고 V2X 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 생성된 평문 메시지의 해시와 수신된 암호문의 해시의 연접을 사용함으로써 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를, 결정할 수 있다. V2X 엔드포인트 노드가 암호문과 평문 메시지의 연접에 서명했다는 결정에 응답하여, 네트워크 프로세싱 디바이스(326)는 V2X 엔드포인트 노드에 대한 데이터 트랜잭션을 수행할 수 있다.

[0047] [0058] 다양한 실시예들에서, V2X 메시지들(304 및 306)은 하나 이상의 기능들 또는 시스템들에 따라 구성될 수 있다. 2 개의 예들로서, V2X 메시지들(304 및 306)은 (예를 들어, 요금 징수 또는 통행료 징수 시스템을 위한) 통행료 메시지들 또는 (예를 들어, 주차 지불 시스템을 위한) 주차 액세스 메시지로 구성될 수 있다. V2X 메시지들(304 및 306)은 또한 도로 상태 메시지들(예를 들어, 다른 차량, RSU 또는 트래픽에 관한 네트워크 노드, 관찰된 차량 거동, 도로 손상, 얼음 또는 홍수와 같은 위험한 도로 상태 등에 대한 메시지)로서 구성될 수 있다. V2X 메시지들(304 및 306)은 또한 (예를 들어, 지오네트워킹 메시지 또는 메시징 시스템에서 사용하기 위한) 지오네트워킹 메시지로서 구성될 수 있다. 예를 들어, V2X 엔드포인트 노드는 도로나 경로를 따라, 또는 특정 방향으로 다른 차량들, RSU들 등의 특정 세트로 전달하기 위해 V2X 메시지를 송신할 수 있다. 예를 들어, 지오네트워킹 메시지는 특정 도로를 따라 위험한 교통이나 도로 상황을 다른 차량들에 통지하는 데 사용될 수 있다. 다른 예로서, 지오네트워킹 메시지는 긴급 차량들이 접근하고 있음을 다른 차량들에 통지하기 위해 사용될 수 있어서, 다른 차량들은 일시적으로 도로를 비울 수 있다.

[0048] [0059] V2X 메시지들(304 및 306)은 또한 (예를 들어, 경찰, 소방서, 응급 의료 기술자 또는 다른 비상 응답자 시스템을 위한) 비상 응답자 메시지로서 구성될 수 있다. 예를 들어, 비상 응답자 V2X 메시지들은 위험 상황, 사건, 사고 등에 대한 정보, 용의자들 또는 피해자들에 대한 신원 정보, 의료 정보(예를 들어, 기밀로 취급되어야 함), 개인 식별 정보(PII) 등 같은 일반 대중이 아닌 다른 비상 응답자들에 의해서만 수신을 위해 의도된 정보를 포함할 수 있다. 일부 구현들에서, 평문 메시지의 콘텐츠는 기밀 정보 또는 민감 성격의 정보, 또는 법률 또는 규정에 의해 기밀로 취급되어야 하는 정보(예를 들어, 금융 계정 정보, 의료 정보 등)를 포함할 수 있다.

[0049] [0060] 도 4는 다양한 실시예들에 따라 V2X 메시지에서 평문 및 암호문을 인증하기 위해 V2X 엔드포인트 노드의 프로세서에 의해 수행되는 방법(400)을 예시하는 프로세스 흐름도이다. 도 1 내지 도 4를 참조하면, 방법(400)의 동작들은 V2X 엔드포인트 노드(예를 들어, 12, 14, 16, 202, 320)에서 V2X 프로세싱 디바이스에 의해 수행될 수 있다.

[0050] [0061] 블록(402)에서, V2X 프로세싱 디바이스는 V2X 메시지로 전송될 평문 메시지로부터 암호문을 생성할 수 있다. 예를 들어, V2X 프로세싱 디바이스는 평문 메시지를 생성하고, 이어서 평문 메시지를 암호화하여 암호문을 생성할 수 있다.

[0051] [0062] 블록(404)에서, V2X 프로세싱 디바이스는 암호문의 해시와 평문 메시지의 해시를 생성할 수 있다. 임의의 형태의 해시 함수 또는 알고리즘은 2 개의 해시들을 생성하는 데 사용될 수 있고, 상이한 해시 함수들 또는 알고리즘들은 암호문의 해시와 평문 메시지의 해시를 생성하는 데 사용될 수 있다.

[0052] [0063] 블록(406)에서, V2X 프로세싱 디바이스는 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 생성할 수 있다. 임의의 형태의 서명 기능 또는 알고리즘은 디지털 서명을 생성하는 데 사용될 수 있다.

[0053] [0064] 블록(408)에서, V2X 프로세싱 디바이스는 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 V2X 메시지를 네트워크 노드로 송신할 수 있다. 일부 실시예들에서, 암호문, 평문 메시지의 해시, 및 디지털 서명은 V2X 엔드포인트 노드가 서명된 연접에 서명했음을 네트워크 노드가 검증할 수 있도록 구성될 수 있다. 일부 실시예들에서, V2X 메시지는 하나의 V2X 엔드포인트 노드에 의해 전송되고 다른 V2X 엔드포인트 노드에 의해 수신되는 V2X 메시지와 같은 제한된 대역폭 무선 통신 링크를 통한 전송을 위해 구성될 수 있다.

[0054] [0065] 일부 실시예들에서, V2X 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지, 또는 비상 응답자 메시지로 구성될 수 있다. 일부 실시예들에서, 평문 메시지는 통행료 정보, 주차 액세스 정보, 도로 상태 정보, 지오네트워킹 정보 및 비상 응답자 정보 중 하나를 포함할 수 있다. 일부 실시예들에서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문 및/또는 암호문의 해시의 바이트 범위들 또는 경계들 및 평문 메시지 및/또는 평문 메시지의 해시의 식별을 정의하거나 지정하는 데이터 구조를 포함하거나 이에 포함될 수 있다.

[0055] [0066] 도 5는 다양한 실시예들에 따라 V2X 메시지를 프로세싱하기 위해 네트워크 노드의 프로세서에 의해 수행되는 방법(500)을 예시하는 프로세스 흐름도이다. 도 1 내지 도 5를 참조하면, 방법(500)의 동작들은 네트워크 노드(예를 들어, 12, 14, 16, 220, 132, 220, 322)에서 프로세싱 디바이스(V2X 프로세싱 디바이스일 수 있음)에 의해 수행될 수 있다.

[0056] [0067] 블록(502)에서, 프로세싱 디바이스는 V2X 엔드포인트 노드(예를 들어, 12, 14, 16, 202, 320)로부터 암호문, 평문 메시지의 해시 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 포함하는 V2X 메시지를 수신할 수 있다.

[0057] [0068] 결정 블록(504)에서, 프로세싱 디바이스는 V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정할 수 있다. 일부 실시예들에서, 프로세싱 디바이스는 암호문의 해시를 생성하고, 생성된 암호문의 해시를 사용하여 수신된 평문 메시지의 해시와 생성된 암호문의 해시의 연접을 구성하고, 그리고 V2X 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 수신된 평문 메시지의 해시와 생성된 암호문의 해시의 연접을 사용할 수 있다.

[0058] [0069] V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명하지 않았다는 결정에 응답하여(즉, 결정 블록(504) = "아니오"), 프로세싱 디바이스는 블록(506)에서 V2X 엔드포인트 노드로부터의 V2X 메시지를 거부할 수 있다. V2X 메시지를 거부하는 것은 V2X 메시지를 무시하는 것, V2X 메시지의 추가 프로세싱을 중단하는 것, 및 다른 적합한 동작들을 포함할 수 있다.

[0059] [0070] V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했다는 결정에 응답하여(즉, 결정 블록(504) = "예"), 프로세싱 디바이스는 블록(508)에서 암호문, 평문 메시지의 해시 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 디바이스로 송신할 수 있다.

[0060] [0071] 일부 실시예들에서, 프로세싱 디바이스는 인증된 V2X 엔드포인트 노드에 의해 사용되는 것으로 알려진 해시 알고리즘을 사용하여 암호문의 해시를 생성할 수 있다. 일부 실시예들에서, V2X 메시지는 제한된 대역폭 무선 통신 링크를 통한 전송을 위해 구성될 수 있다. 일부 실시예들에서, V2X 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지, 또는 비상 응답자 메시지로 구성될 수 있다. 일부 실시예들에서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문 및/또는 암호문의 해시의 식별 및 평문 메시지 및/또는 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하거나 이에 포함될 수 있다.

[0061] [0072] 도 6은 다양한 실시예들에 따라 V2X 메시지에서 평문 및 암호문을 인증하기 위해 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법(600)을 예시하는 프로세스 흐름도이다. 도 1 내지 도 6을 참조하면, 방법(600)의 동작들은 네트워크 프로세싱 디바이스(예를 들어, 134, 136)의 프로세싱 디바이스에 의해 수행될 수 있다.

[0062] [0073] 블록(602)에서, 프로세싱 디바이스는 암호화 키 디바이스(예를 들어, 324)로부터 V2X 엔드포인트 노드(예를 들어, 12, 14, 16, 202, 320)에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신할 수 있다.

[0063] [0074] 결정 블록(604)에서, 프로세싱 디바이스는 V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정할 수 있다. 일부 실시예들에서, 프로세싱 디바이스는 평문 메시지의 해시를 생성할 수 있고, 평문 메시지의 해시를 사용하여 생성된 평문 메시지의 해시와 수신된 암호문의 해시의 연접을 구성하고, 그리고 V2X 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 생성된 평문 메시지의 해시와 수신된 암호문의 해시의 연접을 사용할 수 있다. 일부 실시예들에서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문의 식별 또는 암호문의 해시 및 평문 메시지의 식별 또는 평문 메시지의 해시를 포함하는 데이터 구조를 포함할 수 있다.

[0064] [0075] V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명하지 않았다는 결정에 응답하여(즉, 결정 블록(604) = "아니오"), 프로세싱 디바이스는 블록(606)에서 V2X 엔드포인트 노드로부터의 V2X 메시지를 거부할 수 있다. V2X 메시지를 거부하는 것은 V2X 메시지를 무시하는 것, V2X 메시지의 추가 프로세싱을 중단하는 것, 및 다른 적합한 동작들을 포함할 수 있다.

[0065] [0076] V2X 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했다는 결정에 응답하여(즉, 결정 블록(604) = "예"), 프로세싱 디바이스는 V2X 엔드포인트 노드 블록(608)에 대한 데이터 트랜잭션을 수행할 수 있다.

[0066] [0077] 도 7은 다양한 실시예들과 함께 사용하기에 적합한 예시적인 모바일 컴퓨팅 디바이스(700)를 예시하는 구성요소 블록도이다. 도 1 내지 도 7을 참조하면, 다양한 실시예들은 예시적인 모바일 컴퓨팅 디바이스(700)를 포함하는 모바일 컴퓨팅 디바이스들뿐만 아니라 온보드 장비를 포함하는 매우 다양한 컴퓨팅 시스템들에서 구현될 수 있다. 모바일 컴퓨팅 디바이스(700)는 터치스크린 제어기(704) 및 내부 메모리(706)에 결합된 프로세서(702)를 포함할 수 있다. 프로세서(702)는 일반 또는 특정 프로세싱 작업들을 위해 지정된 하나 이상의 멀티코어 집적 회로들일 수 있다. 내부 메모리(706)는 휘발성 또는 비휘발성 메모리일 수 있고, 또한 보안 및/또는 암호화된 메모리, 비보안 및/또는 암호화되지 않은 메모리, 또는 이들의 임의의 조합일 수 있다. 활용될 수 있는 메모리 유형들의 예들은 DDR, LPDDR, GDDR, WIDEIO, RAM, SRAM, DRAM, P-RAM, R-RAM, M-RAM, STT-RAM, 임베디드 DRAM을 포함(그러나 이에 제한되지 않음)한다. 터치스크린 제어기(704) 및 프로세서(702)는 또한 저항

감지 터치스크린, 정전용량 감지 터치스크린, 적외선 감지 터치스크린 등과 같은 터치스크린 패널(712)에 결합될 수 있다. 추가로, 모바일 컴퓨팅 디바이스(700)의 디스플레이는 터치스크린 능력을 가질 필요가 없다.

[0067] [0078] 모바일 컴퓨팅 디바이스(700)는 하나 이상의 무선 신호 트랜시버들(708)(예를 들어, Peanut, Bluetooth, ZigBee, Wi-Fi, RF 라디오) 및 서로에 및/또는 프로세서(702)에 결합된 통신들을 송신 및 수신하기 위한 안테나(710)를 가질 수 있다. 트랜시버들(708) 및 안테나(710)는 다양한 무선 전송 프로토콜 스택 및 인터페이스들을 구현하기 위해 위에서 언급된 회로와 함께 사용될 수 있다. 모바일 컴퓨팅 디바이스(700)는 셀룰러 네트워크를 통한 통신을 가능하게 하고 프로세서에 결합되는 셀룰러 네트워크 무선 모뎀 칩(716)을 포함할 수 있다.

[0068] [0079] 모바일 컴퓨팅 디바이스(700)는 프로세서(702)에 결합된 주변 디바이스 연결 인터페이스(718)를 포함할 수 있다. 주변 디바이스 연결 인터페이스(718)는 하나의 유형의 연결을 수용하도록 단일하게 구성될 수 있거나, 또는 USB(Universal Serial Bus), FireWire, Thunderbolt 또는 PCIe와 같은 공통 또는 독점의 다양한 유형들의 물리적 및 통신 연결들을 수용하도록 구성될 수 있다. 주변 디바이스 연결 인터페이스(718)는 또한 유사하게 구성된 주변 디바이스 연결 포트(도시되지 않음)에 결합될 수 있다.

[0069] [0080] 모바일 컴퓨팅 디바이스(700)는 또한 오디오 출력들을 제공하기 위한 스피커들(714)을 포함할 수 있다. 모바일 컴퓨팅 디바이스(700)는 또한 본원에 설명된 구성요소들의 전부 또는 일부를 수용하기 위해 플라스틱, 금속 또는 재료들의 조합으로 구성된 하우징(720)을 포함할 수 있다. 통상의 기술자는 하우징(720)이 온보드 실시예에서 차량의 계기판 콘솔일 수 있음을 인식할 수 있다. 모바일 컴퓨팅 디바이스(700)는 일회용 또는 재충전가능 배터리와 같은 프로세서(702)에 결합된 전원(722)을 포함할 수 있다. 재충전가능 배터리는 또한 모바일 컴퓨팅 디바이스(700) 외부의 소스로부터 충전 전류를 수신하기 위해 주변 디바이스 연결 포트에 결합될 수 있다. 모바일 컴퓨팅 디바이스(700)는 또한 사용자 입력을 수신하기 위한 물리적 버튼(724)을 포함할 수 있다. 모바일 컴퓨팅 디바이스(700)는 또한 모바일 컴퓨팅 디바이스(700)를 턴 온 및 오프하기 위한 전원 버튼(726)을 포함할 수 있다.

[0070] [0081] 도 8은 다양한 실시예들과 함께 사용하기에 적합한 예시적인 모바일 컴퓨팅 디바이스(800)를 예시하는 구성요소 블록도이다. 도 1 내지 도 8을 참조하면, 다양한 실시예들은 랩톱 컴퓨터로 예시된 예시적인 모바일 컴퓨팅 디바이스(800)를 포함하는 매우 다양한 컴퓨팅 시스템에서 구현될 수 있다. 모바일 컴퓨팅 디바이스(800)는 컴퓨터의 포인팅 디바이스 역할을 하는 터치패드 터치 표면(817)을 포함할 수 있고, 따라서 터치 스크린 디스플레이가 장착되고 위에서 설명된 컴퓨팅 디바이스들에서 구현되는 것들과 유사한 드래그, 스크롤 및 플릭 제스처들을 수신할 수 있다. 모바일 컴퓨팅 디바이스(800)는 일반적으로 플래시 메모리의 디스크 드라이브(813)와 같은 대용량 비휘발성 메모리 및 휘발성 메모리(812)에 결합된 프로세서(802)를 포함할 것이다. 추가로, 모바일 컴퓨팅 디바이스(800)는 프로세서(802)에 결합된 무선 데이터 링크 및/또는 셀룰러 전화 트랜시버(816)에 연결될 수 있는 전자기 방사선을 송신 및 수신하기 위한 하나 이상의 안테나(808)를 가질 수 있다. 모바일 컴퓨팅 디바이스(800)는 또한 프로세서(802)에 결합된 플로피 디스크 드라이브(814) 및 컴팩트 디스크(CD) 드라이브(815)를 포함할 수 있다. 노트북 구성에서, 컴퓨터 하우징은 모두 프로세서(802)에 결합된 터치패드(817), 키보드(818) 및 디스플레이(819)를 포함한다. 컴퓨팅 디바이스의 다른 구성들은 잘 알려진 바와 같이 (예를 들어, USB 입력을 통해) 프로세서에 결합된 컴퓨터 마우스 또는 트랙볼을 포함할 수 있고, 이는 또한 다양한 실시예들과 함께 사용될 수 있다.

[0071] [0082] 도 9는 다양한 실시예들과 함께 사용하기에 적합한 예시적인 V2X 온보드 장비(900)를 예시하는 구성요소 블록도이다. 도 1 내지 도 9를 참조하면, 다양한 실시예들은 매우 다양한 V2X 온보드 장비(900)에서 구현될 수 있다. 이러한 V2X 온보드 장비(900)는 차량에 구현되어 다양한 차량 시스템들 및 센서들과 연결되도록 구성될 수 있다. V2X 온보드 장비(900)는 메모리(904)에 결합된 프로세서(902)를 포함할 수 있다. 메모리(904)는 임의의 형태의 비일시적 매체(예를 들어, 판독 전용 메모리(ROM), 플래시 메모리 등)일 수 있고 프로세서(902)로 하여금 본원에 설명된 실시예 방법들 중 임의의 방법의 동작들을 수행하게 하도록 구성된 프로세서-실행가능 명령들 및 데이터를 저장할 수 있다. 프로세서(902)는 또한 차량의 안테나(도시되지 않음)에 결합되고 V2X 메시지들을 전송 및 수신하도록 구성된 무선 트랜시버(906)에 결합될 수 있다.

[0072] [0083] 예시되고 설명된 다양한 실시예들은 청구범위의 다양한 특징들을 예시하기 위한 예들로서만 제공된다. 그러나, 임의의 주어진 실시예와 관련하여 도시되고 설명된 특징들은 반드시 연관된 실시예로 제한되지 않고 도시되고 설명된 다른 실시예들과 함께 사용되거나 조합될 수 있다. 추가로, 청구범위는 임의의 하나의 예시적인 실시예에 의해 제한되도록 의도되지 않는다. 예를 들어, 방법들(400, 500, 및 600)의 동작들 중 하나 이상은

방법들(400, 500, 및 600)의 하나 이상의 동작들로 대체되거나 조합될 수 있다.

[0073] [0084] 구현 예들은 다음 단락들에서 설명된다. 다음 구현 예들 중 일부는 예시적인 방법들의 측면에서 설명되지만, 추가 예시적인 구현들은 다음을 포함할 수 있다: 다음 구현 예들의 방법들의 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성된 프로세서를 포함하여, 온보드 유닛, 모바일 디바이스 유닛, 모바일 컴퓨팅 유닛, 또는 고정식 노변 장치, 네트워크 노드, 또는 컴퓨팅 디바이스일 수 있는 V2X 프로세싱 디바이스에 의해 구현되는 다음 단락들에서 논의되는 예시적인 방법들; 다음 구현 예들의 방법들의 기능들을 수행하기 위한 수단을 포함하는 V2X 프로세싱 디바이스, 네트워크 노드 프로세싱 디바이스, 또는 네트워크 컴퓨팅 노드 프로세싱 디바이스에 의해 구현되는 다음 단락들에서 논의되는 예시적인 방법들; 및 V2X 프로세싱 디바이스, 네트워크 노드 프로세싱 디바이스, 또는 네트워크 컴퓨팅 노드 프로세싱 디바이스의 프로세서로 하여금 다음 구현 예들의 방법들의 동작들을 수행하게 하도록 구성된 프로세서-실행가능 명령들이 저장되어 있는 비일시적 프로세서-판독가능 저장 매체로서 구현될 수 있는 다음 단락들에서 논의되는 예시적인 방법들.

[0074] [0085] 예 1. 메시지의 평문 및 암호문을 인증하기 위해 엔드포인트 노드의 프로세서에 의해 수행되는 방법으로서, 메시지에서 전송될 평문 메시지로부터 암호문을 생성하는 단계; 암호문의 해시와 평문 메시지의 해시를 생성하는 단계; 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 생성하는 단계; 및 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 메시지를 네트워크 노드로 송신하는 단계를 포함하고, 암호문, 평문 메시지의 해시 및 디지털 서명은 엔드포인트 노드가 서명된 연접에 서명했음을 네트워크 노드가 검증할 수 있게 하도록 구성되는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

[0075] [0086] 예 2. 예 1에 있어서, 엔드포인트 노드는 V2X(vehicle-to-everything) 엔드포인트 노드를 포함하고, 메시지는 V2X 메시지를 포함하는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

[0076] [0087] 예 3. 예 1 및 예 2 중 어느 한 예에 있어서, 메시지는 제한된 대역폭 무선 통신 링크를 통한 전송을 위해 구성되는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

[0077] [0088] 예 4. 예 1 내지 예 3 중 어느 한 예에 있어서, 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지 또는 비상 응답자 메시지 중 하나로 구성되는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

[0078] [0089] 예 5. 예 1 내지 예 4 중 어느 한 예에 있어서, 평문 메시지는 통행료 정보, 주차 액세스 정보, 도로 상태 정보, 지오네트워킹 정보 및 비상 응답자 정보 중 하나를 포함하는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

[0079] [0090] 예 6. 예 1 내지 예 5 중 어느 한 예에 있어서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문 또는 암호문의 해시의 식별 및 평문 메시지 또는 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

[0080] [0091] 예 7. 메시지를 프로세싱하기 위해 네트워크 노드의 프로세서에 의해 수행되는 방법으로서, 엔드포인트 노드로부터 암호문, 평문 메시지의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 포함하는 메시지를 수신하는 단계; 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하는 단계; 및 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했다는 결정에 대한 응답으로 암호문, 평문 메시지의 해시, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 디바이스로 송신하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

[0081] [0092] 예 8. 예 7에 있어서, 메시지는 V2X(vehicle-to-everything) 메시지를 포함하고, 엔드포인트 노드는 V2X 엔드포인트 노드를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

[0082] [0093] 예 9. 예 7 또는 예 8에 있어서, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하는 단계는, 암호문의 해시를 생성하는 단계; 평문 메시지의 해시와 생성된 암호문의 해시를 연접하는 단계; 및 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 평문 메시지의 해시와 생성된 암호문의 해시의 연접을 제공하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

[0083] [0094] 예 10. 예 7 내지 예 9 중 어느 한 예에 있어서, 암호문의 해시를 생성하는 단계는 인증된 엔드포인트 노드에 의해 사용되는 것으로 알려진 해시 알고리즘을 사용하여 암호문의 해시를 생성하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

[0084] [0095] 예 11. 예 7 및 예 10 중 어느 한 예에 있어서, 메시지는 제한된 대역폭 무선 통신 링크를 통한 전송을 위해 구성되는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

[0085] [0096] 예 12. 예 7 내지 예 11 중 어느 한 예에 있어서, 메시지는 통행료 메시지, 주차 액세스 메시지, 도로 상태 메시지, 지오네트워킹 메시지 또는 비상 응답자 메시지 중 하나로 구성되는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

[0086] [0097] 예 13. 예 7 내지 예 12 중 어느 한 예에 있어서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문 또는 암호문의 해시의 식별 및 평문 메시지 또는 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하는, 엔드포인트 노드의 프로세서에 의해 수행되는 방법.

[0087] [0098] 예 14. 예 7 내지 예 13 중 어느 한 예에 있어서, 암호문, 평문 메시지의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 디바이스로 송신하는 단계는 암호문, 평문 메시지의 해시, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 서버로 송신하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

[0088] [0099] 예 15. 예 7 내지 예 14 중 어느 한 예에 있어서, 암호문, 평문 메시지의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 디바이스로 송신하는 단계는 암호문, 평문 메시지의 해시, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 암호화 키 모듈로 송신하는 단계를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

[0089] [0100] 예 16. 메시지의 평문 및 암호문을 인증하기 위해 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법으로서, 암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 단계; 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하는 단계; 및 엔드포인트 노드가 암호문과 평문 메시지의 연접에 서명했다는 결정에 대한 응답으로 엔드포인트 노드에 대한 데이터 트랜잭션을 수행하는 단계를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

[0090] [0101] 예 17. 예 16에 있어서, 메시지는 V2X(vehicle-to-everything) 메시지를 포함하고, 엔드포인트 노드는 V2X 엔드포인트 노드를 포함하는, 네트워크 노드의 프로세서에 의해 수행되는 방법.

[0091] [0102] 예 18. 예 16 또는 예 17에 있어서, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하는 단계는, 평문 메시지의 해시를 생성하는 단계; 생성된 평문 메시지의 해시와 암호문의 해시를 연접하는 단계; 및 엔드포인트 노드의 공개 키를 사용하여 디지털 서명을 검증하기 위한 입력으로 생성된 평문 메시지의 해시와 암호문의 해시의 연접을 제공하는 단계를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

[0092] [0103] 예 19. 예 16 내지 예 18 중 어느 한 예에 있어서, 평문 메시지는 통행료 정보, 주차 액세스 정보, 도로 상태 정보, 지오네트워킹 정보 및 비상 응답자 정보 중 하나를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

[0093] [0104] 예 20. 예 16 내지 예 19 중 어느 한 예에 있어서, 암호문의 해시와 평문 메시지의 해시의 연접은 암호문 또는 암호문의 해시의 식별 및 평문 메시지 또는 평문 메시지의 해시의 식별을 포함하는 데이터 구조를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

[0094] [0105] 예 21. 예 16 내지 예 20 중 어느 한 예에 있어서, 암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 단계는 암호화 키 서버로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 암호문의 해시와 평문 메시지 해시의 연접의 디지털 서명을 수신하는 단계를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

[0095] [0106] 예 22. 예 16 내지 예 21 중 어느 한 예에 있어서, 암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하는 단계는 암호화 키 모듈로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 암호문의 해시와 평문 메시지 해시의 연접의 디지털 서명을 수신하는 단계를 포함하는, 컴퓨팅 디바이스의 프로세서에 의해 수행되는 방법.

[0096] [0107] 예 23. 메시지의 평문 및 암호문을 인증하기 위한 시스템으로서, 메시지에서 전송될 평문 메시지로부터

암호문을 생성하고, 암호문의 해시와 평문 메시지의 해시를 생성하고, 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 생성하고, 그리고 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 메시지를 송신하기 위한 프로세서-실행가능 명령들로 구성된 프로세서를 포함하는 엔드포인트 노드; 암호문, 평문 메시지의 해시 및 디지털 서명을 포함하는 메시지를 엔드포인트 노드로부터 수신하고, 엔드포인트 노드가 암호문의 해시와 평문 메시지 해시의 연접에 서명했는지 여부를 결정하고, 엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했다는 결정에 응답하여 암호문, 평문 메시지의 해시 및 디지털 서명을 암호화 키 디바이스로 송신하기 위한 프로세서-실행가능 명령들로 구성된 프로세서를 포함하는 네트워크 노드; 및 암호화 키 디바이스로부터, 엔드포인트 노드에 의해 발신된 평문 메시지, 평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 수신하고,엔드포인트 노드가 암호문의 해시와 평문 메시지의 해시의 연접에 서명했는지 여부를 결정하고, 그리고 엔드포인트 노드가 암호문과 평문 메시지의 연접에 서명했다는 결정에 응답하여 엔드포인트 노드에 대한 데이터 트랜잭션을 수행하기 위한 프로세서-실행가능 명령들로 구성된 프로세서를 포함하는 네트워크 프로세싱 디바이스를 포함하는, 시스템.

[0097] [0108] 전술한 방법 설명들 및 프로세스 흐름도들은 단지 예시적인 예들로서 제공되고 다양한 실시예들의 동작들이 제시된 순서대로 수행되어야 함을 요구하거나 암시하도록 의도되지 않는다. 통상의 기술자에 의해 인식될 바와 같이, 전술한 실시예들에서 동작들의 순서는 임의의 순서로 수행될 수 있다. "그후", "이어서", "다음" 등과 같은 단어는 동작들의 순서를 제한하기 위한 것이 아니고; 이 단어들은 방법들의 설명을 통해 독자를 안내하는 데 단순히 사용된다. 추가로, 예를 들어 관사들("a", "an" 또는 "the")을 사용하여 단수형의 청구항 요소들에 대한 모든 언급은 요소를 단수형으로 제한하는 것으로 해석되어서는 안 된다.

[0098] [0109] 본원에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들 및 알고리즘 동작들은 전자 하드웨어, 컴퓨터 소프트웨어 또는 이들의 조합으로 구현될 수 있다. 하드웨어와 소프트웨어의 이러한 호환성을 명확하게 예시하기 위해, 다양한 예시적인 구성요소들, 블록들, 모듈들, 회로들 및 동작들은 기능 측면에서 일반적으로 위에서 설명되었다. 이러한 기능이 하드웨어로 구현되는지 소프트웨어로 구현되는지 여부는 전체 시스템에 부과되는 특정 애플리케이션 및 설계 제약들에 의존한다. 통상의 기술자들은 각각의 특정 애플리케이션에 대해 다양한 방식들로 설명된 기능을 구현할 수 있지만, 그러한 구현 결정들은 청구범위의 범위에서 벗어나는 원인으로 해석되어서는 안 된다.

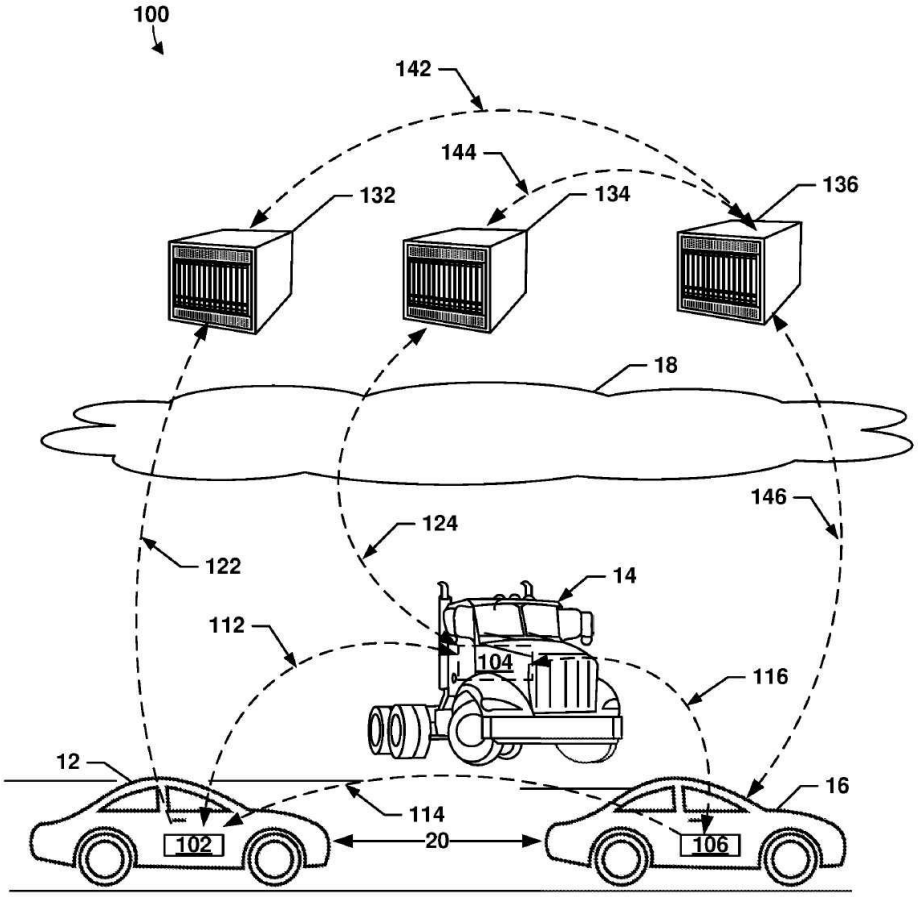
[0099] [0110] 본원에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리들, 논리 블록들, 모듈들 및 회로들을 구현하는 데 사용되는 하드웨어는 범용 프로세서, 디지털 신호 프로세서(DSP), TCUASIC(Application Specific Integrated Circuit), FPGA(Field Programmable Gate Array) 또는 다른 프로그램 가능 논리 디바이스, 이산 게이트 또는 트랜지스터 논리, 이산 하드웨어 구성요소들 또는 본원에 설명된 기능들을 수행하도록 설계된 이들의 임의의 조합으로 구현되거나 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안으로, 프로세서는 임의의 편리한 프로세서, 제어기, 마이크로제어기 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들어 DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 관련된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로서 구현될 수 있다. 대안적으로, 일부 동작들 또는 방법들은 주어진 기능에 특정한 회로에 의해 수행될 수 있다.

[0100] [0111] 하나 이상의 실시예들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 조합으로 구현될 수 있다. 소프트웨어로 구현되는 경우, 기능들은 비일시적 컴퓨터-판독가능 매체 또는 비일시적 프로세서-판독가능 매체에 하나 이상의 명령들 또는 코드로 저장될 수 있다. 본원에 개시된 방법 또는 알고리즘의 동작들은 비일시적 컴퓨터-판독가능 또는 프로세서-판독가능 저장 매체에 상주할 수 있는 프로세서-실행가능 소프트웨어 모듈에 구현될 수 있다. 비일시적 컴퓨터-판독가능 또는 프로세서-판독가능 저장 매체는 컴퓨터 또는 프로세서에 의해 액세스될 수 있는 모든 저장 매체일 수 있다. 제한이 아닌 예로서, 이러한 비일시적 컴퓨터-판독가능 또는 프로세서-판독가능 매체는 RAM, ROM, EEPROM, 플래시 메모리, CD-ROM 또는 다른 광 디스크 스토리지, 자기 디스크 스토리지 또는 다른 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 저장하는 데 사용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 본원에서 사용된 디스크(disk) 및 디스크(disc)는 CD(Compact Disc), 레이저 디스크, 광학 디스크, DVD(Digital Multimedia Disc), 플로피 디스크 및 블루 레이 디스크를 포함하고, 디스크(disk_는 일반적으로 자기적으로 데이터를 재생하지만, 디스크(disc)는 레이저로 데이터를 광학적으로 재생한다. 위의 조합들은 또한 비일시적 컴퓨터-판독가능 및 프로세서-판독가능 매체의 범위에 포함된다. 추가적으로, 방법 또는 알고리즘의 동작들은 컴퓨터 프로그램 제품에 통합될 수 있는 비일시적 프로세서-판독가능 매체 및/또는 컴퓨터-판독가능 매체에 코드들 및/또는 명령들의 하나 또는 임의의 조합 또는 세트로 상주할 수 있다.

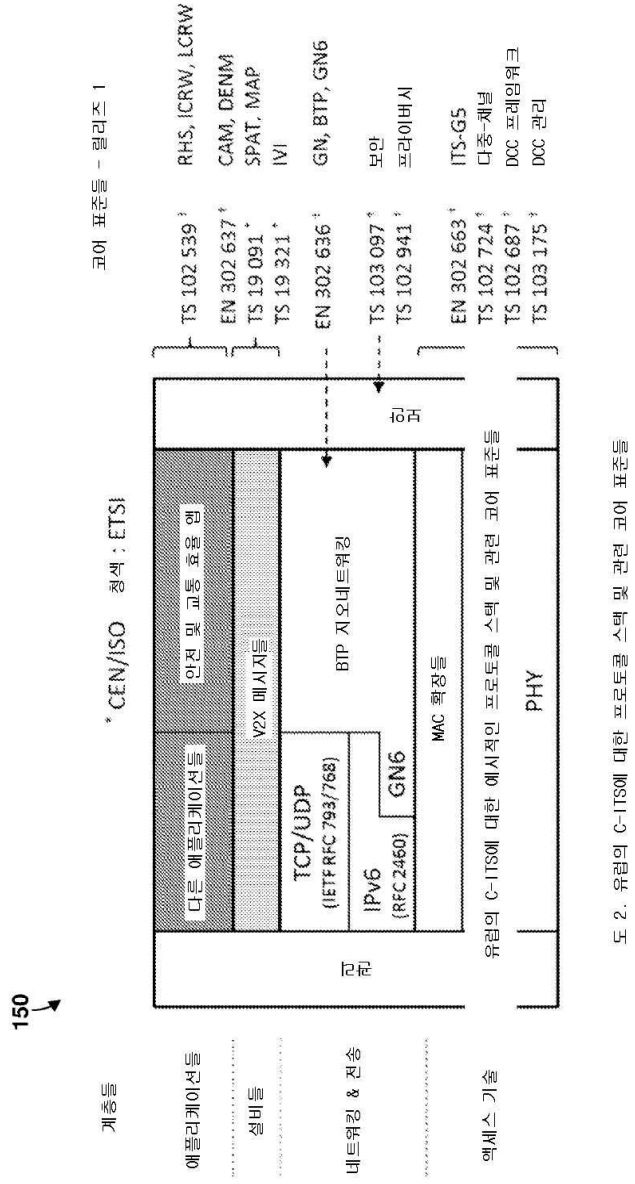
[0101] [0112] 개시된 실시예들의 이전 설명은 통상의 기술자가 청구범위를 만들거나 사용하게 할 수 있도록 제공된다. 이들 실시예들에 대한 다양한 수정들은 통상의 기술자들에게 쉽게 명백할 것이고, 본원에서 정의된 일반적 원리들은 청구범위의 범위를 벗어나지 않고 다른 실시예들에 적용될 수 있다. 따라서, 본 개시내용은 본원에 도시된 실시예들로 제한되도록 의도되지 않고, 본원에 개시된 청구범위, 원리들 및 신규 특징들과 일치하는 가장 넓은 범위에 부합되어야 한다.

도면

도면1a

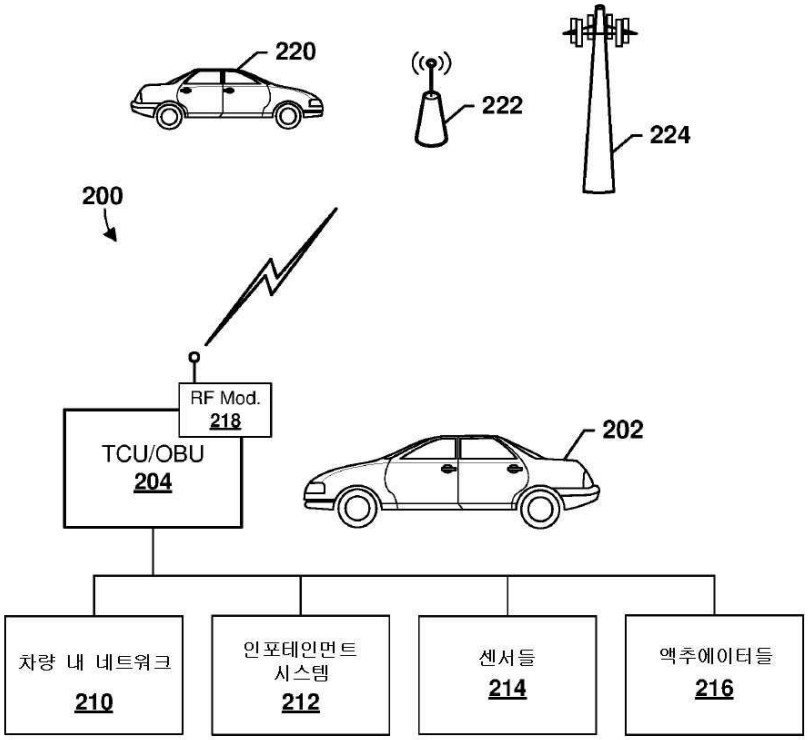


도면1b

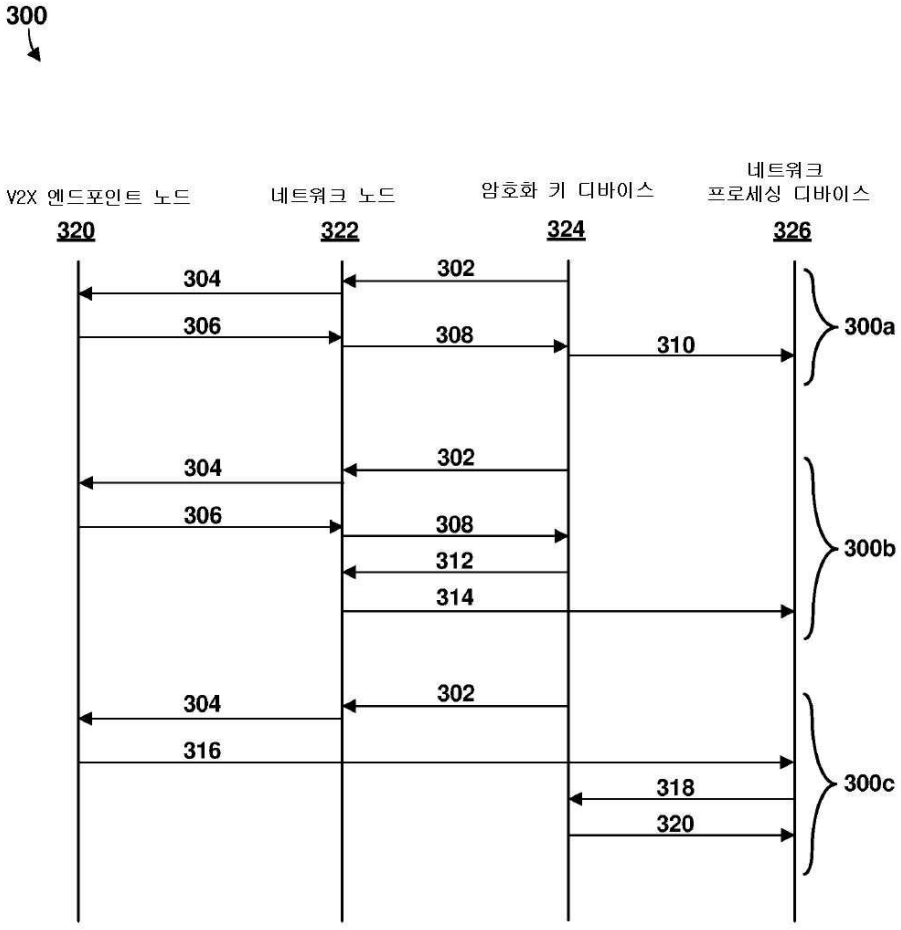


도 2. 유럽의 C-ITS에 대한 프로토콜 스택 및 관련 코어 표준들

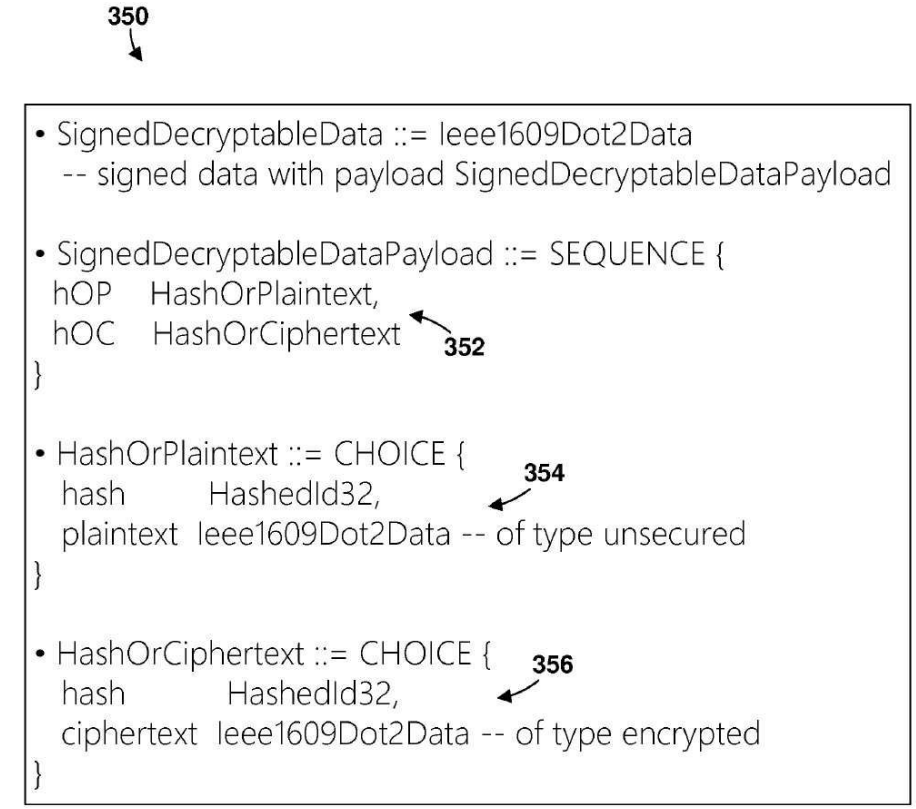
도면2


220
222
224
200
RF Mod.
218
TCU/OBU
204
202
차량 내 네트워크
210
인포테인먼트
시스템
212
센서들
214
액추에이터들
216

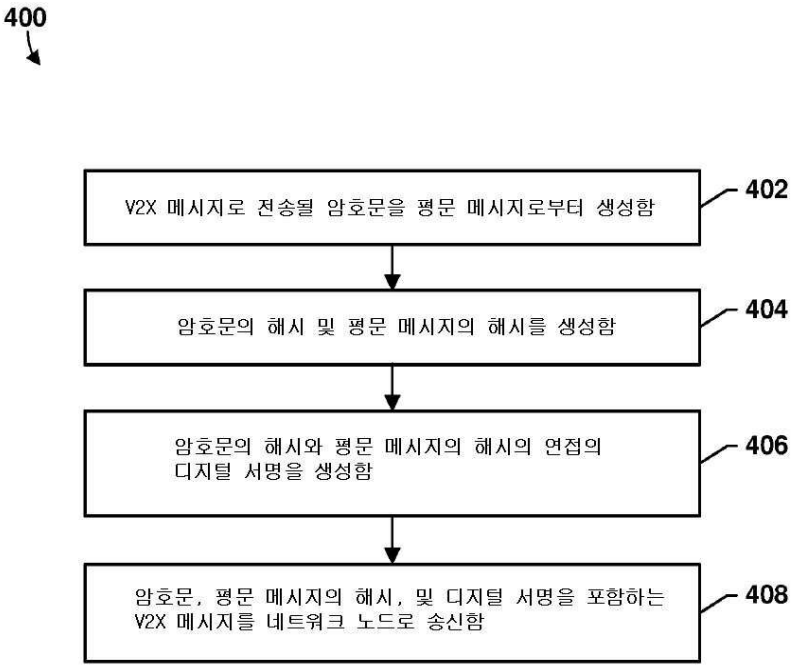
도면3a


300
V2X 엔드포인트 노드
320
네트워크 노드
322
암호화 키 디바이스
324
네트워크
프로세싱 디바이스
326
304
302
306
308
310
300a
304
302
306
308
312
314
300b
304
302
316
318
320
300c

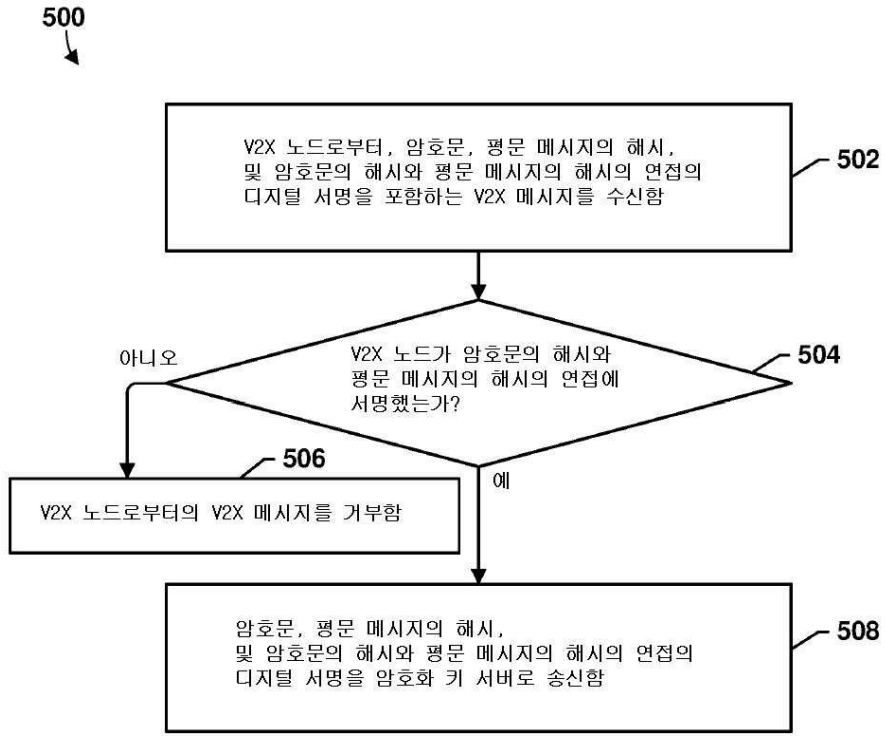
도면3b


350
• SignedDecryptableData ::= Ieee1609Dot2Data
-- signed data with payload SignedDecryptableDataPayload
• SignedDecryptableDataPayload ::= SEQUENCE {
hOP HashOrPlaintext,
hOC HashOrCiphertext
352
}
• HashOrPlaintext ::= CHOICE {
354
hash HashedId32,
plaintext Ieee1609Dot2Data -- of type unsecured
}
• HashOrCiphertext ::= CHOICE {
356
hash HashedId32,
ciphertext Ieee1609Dot2Data -- of type encrypted
}

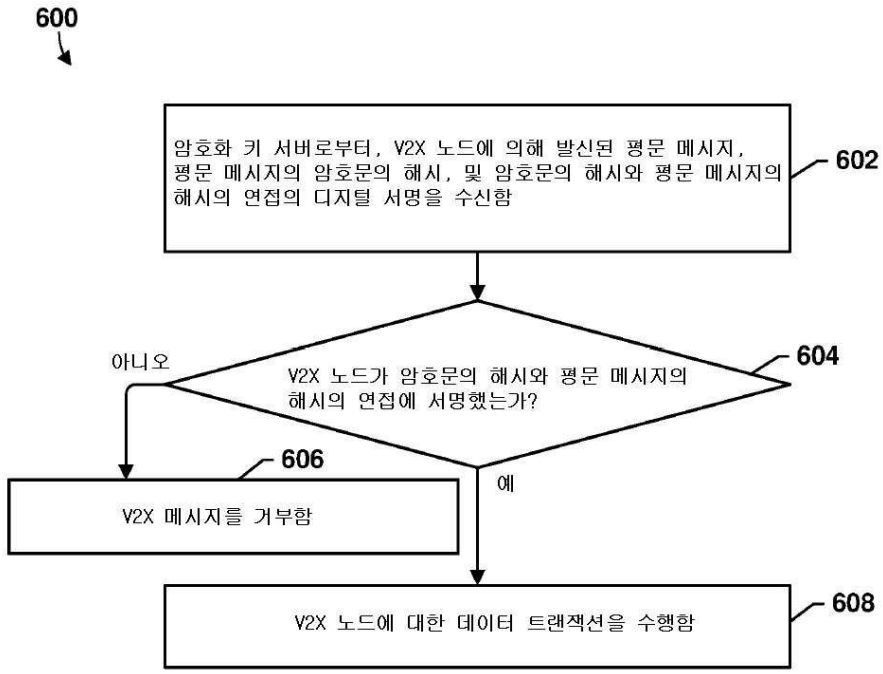
도면4


400
V2X 메시지로 전송될 암호문을 평문 메시지로부터 생성함
402
암호문의 해시 및 평문 메시지의 해시를 생성함
404
암호문의 해시와 평문 메시지의 해시의 연접의 디지털 서명을 생성함
406
암호문, 평문 메시지의 해시, 및 디지털 서명을 포함하는 V2X 메시지를 네트워크 노드로 송신함
408

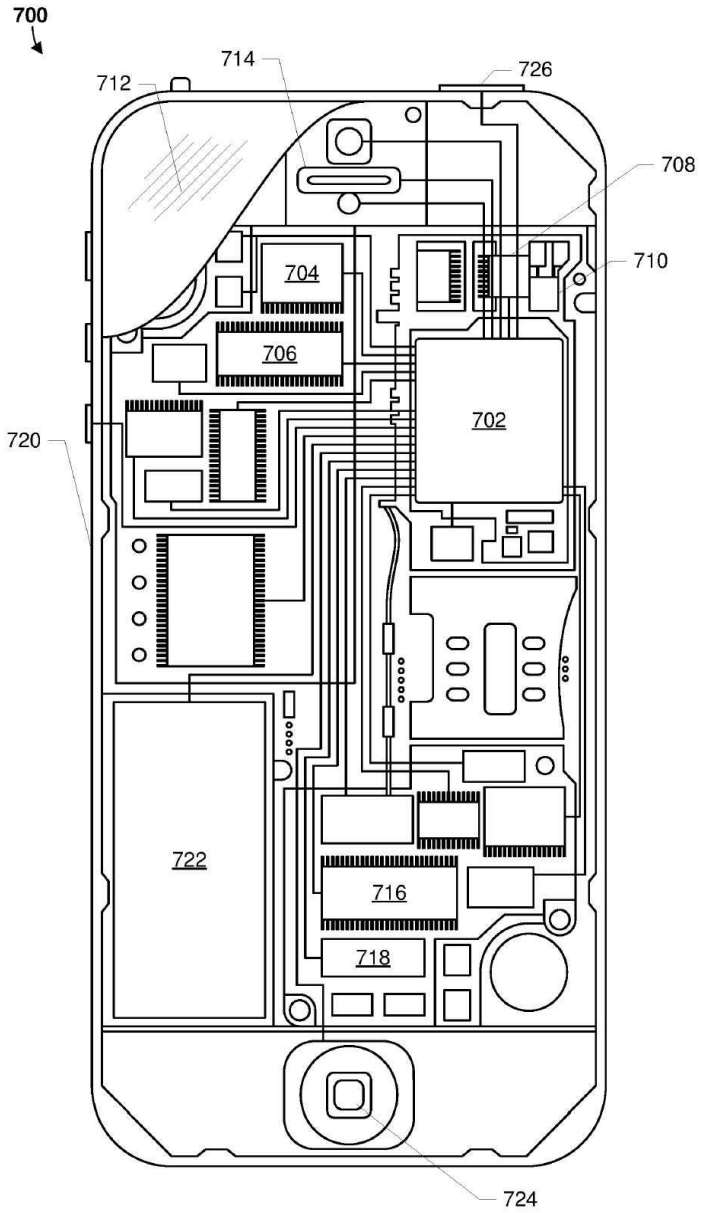
도면5


500
V2X 노드로부터, 암호문, 평문 메시지의 해시,
및 암호문의 해시와 평문 메시지의 해시의 연접의
디지털 서명을 포함하는 V2X 메시지를 수신함
502
V2X 노드가 암호문의 해시와
평문 메시지의 해시의 연접에
서명했는가?
504
아니오
예
506
V2X 노드로부터의 V2X 메시지를 거부함
암호문, 평문 메시지의 해시,
및 암호문의 해시와 평문 메시지의 해시의 연접의
디지털 서명을 암호화 키 서버로 송신함
508

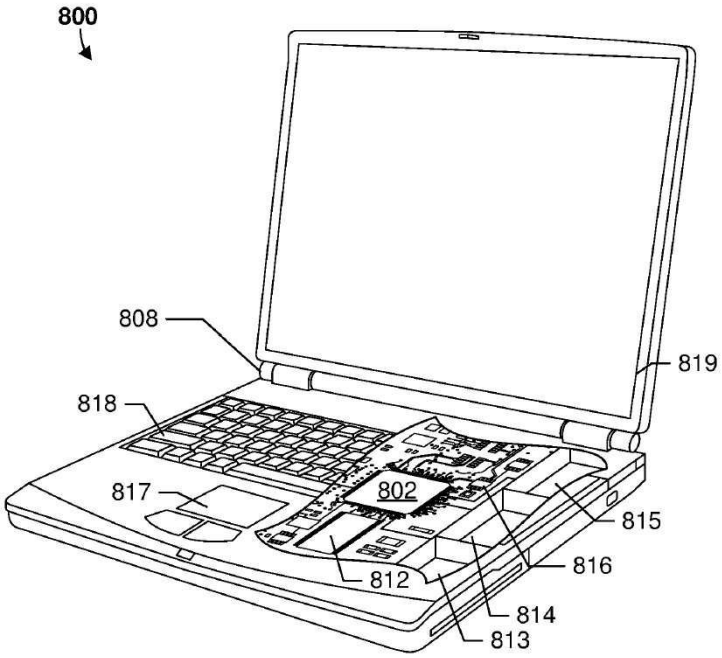
도면6


600
암호화 키 서버로부터, V2X 노드에 의해 발신된 평문 메시지,
평문 메시지의 암호문의 해시, 및 암호문의 해시와 평문 메시지의
해시의 연접의 디지털 서명을 수신함
602
V2X 노드가 암호문의 해시와 평문 메시지의
해시의 연접에 서명했는가?
604
아니오
예
606
V2X 메시지를 거부함
V2X 노드에 대한 데이터 트랜잭션을 수행함
608

도면7



도면8



도면9

