【명세서】

(앞쪽)

【발명(고안)의 명칭】

자율주행 차량의 보안을 위한 체인구조의 커넥티드카 시스템

【기술분야】

본 발명은 현재 활발하게 개발 및 상용화 중인 자율주행 자동차의 보안을 위해 커넥티드카와 체인구조를 적용한 자율주행 자동차의 보안에 관한 것이다. 특히 본 고안은 블록체인 기술에 기반하여 차량과 차량 간의 연결을 통해 보안을 더욱 강하게 해주는 것이다.

【발명(고안)의 배경이 되는 기술】

현재 다양한 각종 운송수단 회사들은 각자 저마다의 운송수단에 인공지능 혹은 자율주행을 결합한 운송수단을 선보이고 있고, 현재 적지 않은 회사들이 이 자율주행을 탑재한 개인용 운송수단을 상용화하였다. 현재 대부분의 자율주행 운송수단은 고수준(High-Level)의 자율주행이 아닌 인간의 개입이 많이 필요한 저수준(Low-Level)의 자율주행 시스템을 탑재한 운송수단이지만 본 과제에서 제시하였듯이 미래에서는 고수준의 자율주행을 탑재한 운송수단이 많이 상용화되리라 예상한다.

하지만 이 고수준의 자율주행은 앞서 언급한 저수준 자율주행의 인간 개입보다 더 적은 개입을 요구하거나, 인간의 개입이 요구되지 않는다. 따라서 이 자율주행을 개발하는 회사는 시스템의 보안에 더욱 더 큰 노력을 기울여야 할 것이다. 하지만 어떤 자동차 자체의 단일적인 시스템에서 보안을 유지하고 이를 스스로 보안에 대한 증명 - 어떤 자동차의 운행 데이터(속도, 방향 등)가 올바른지 확인 - 하기는 쉽지 않을 것이다. 보안을 아무리 강화한다 한들, 각각의 시스템이 보유한 정보의 위변조 방지를 완벽하게 막는 것은 어려워 보인다.

거대한 이동 수단은 자칫하면 무기가 될 수 있다. 거대한 이동 수단이 아닌 소형 혹은 중형의 이동 수단도 무기가 될 수 있는 것은 마찬가지이다. 혹여 이 이동 수단들이 해킹 혹은 시스템의 오류로 인해서 오작동하게 된다면 민간에 큰 피해를 발생시킬 수 있다.

따라서 이러한 문제점 및 보안의 우려 사항을 예방하기 위해 단일적인 보안 시스템보다는 조금 더 강력한 보안 시스템이 강구될 필요성이 있다.

【선행기술문헌】

【특허문헌】

대한민국 특허 제1021004260000호 “이동통신망 플랫폼과 커넥티드카 플랫폼 간의 연동을 위한 장치 및 방법”

【발명(고안)의 내용】

【해결하고자 하는 과제】

보안과 관련된 기존 기술의 문제점을 해결하려는 방법을 제공하는 것을 이 고안의 목적으로 한다. 종래 기술들은 커넥티드를 강조하며 인터넷과의 연동성만 강조하였다. 하지만 이는 인터넷이라는 누구나 접근 가능한 통신매체를 이용함에 따라 보안의 위험도가 많이 증가하게 된다. 또한, 인터넷이라는 것에 크게 의존하게 된다면 인터넷이 원활하게 제공되지 않는 지역 혹은 시점에 큰 문제를 초래할 수 있다.

【과제의 해결 수단】

본 고안인 자율주행 차량의 보안을 위한 체인구조의 커넥티드카 시스템의 실시 예는, 본 시스템에서 고안한 네트워크, 위 네트워크를 이용해 근거리 차량과의 통신을 위한 통신부, 위 통신장치에 전원 공급을 하기 위한 전원부, 자율주행 차량에 설치된 DSSAD 혹은 자율주행 차량의 정보를 전달받기 위한 연결부, DSSAD에서 전달받은 정보를 본 시스템에서 고안한 통신 네트워크에 맞게 변환하는 변환부를 제공한다.

본 고안의 다른 실시예는 다른 차량들로부터 전달받은 자기 차량의 정보를, 현재 자기 차량이 가지고 있는 정보와 일치하는지 확인하기 위해 대조하는 단계, 만약 여러 정보에 대한 대조의 결과가 일치하지 않는다면 이를 다시 원래의 상태라 판단되는 상태로 복구시키는 단계를 포함한 체인구조의 커넥티드카 시스템을 제공할 수 있다.

위에 서술된 해결 수단은 간략하게 표현된 예시로 이는 언제든 변경될 수 있으며 다양한 실시예가 존재 할 수 있다.

【발명(고안)의 효과】

본 고안의 사용으로 인해 지금의 보안 성능보다 더 뛰어난 보안 성능을 제공할 수 있고 과도하게 의존하고 있는 인터넷에 대해 의존성을 낮출 수 있다.

단순히 공격을 방어하는 것이 아닌, 정보가 변동이 생기더라도 다른 차들과 통신을 통해 받은 정보를 대조함으로써 방어에 실패하더라도 상태 복구를 진행하여 방어 실패 이후의 대책을 제공할 수 있다.

【도면의 간단한 설명】

도 1은 본 고안의 일 실시예에 따른 체인구조 커넥티드카 시스템의 구성도이다.

도 2는 본 고안의 일 실시예 네트워크에 사용되는 블록의 구성도 이다.

도 3은 본 고안의 일 실시예에 따른 통신장치의 구성도 이다.

【발명(고안)을 실시하기 위한 구체적인 내용】

【실시예】

아래 첨부된 도면을 참조하여 본 고안의 구성 및 원리에 대해 자세하게 설명한다.

도 1은 본 고안에 따른 체인구조 커넥티드가 시스템의 구성도의 일 실시 예이다. 본 도 1은 어떤 시스템 간의 통신이 이루어지는지 및 어떤 사물들이 통신에 참여하는지에 대한 구성도이다. 우선 통신장비를 보유하고 있는 차량(100) 간의 통신(130) 관계에 관해 상세 된 도안이다. 본 시스템이 제안하는 통신은 차량(100)뿐 아니라 전기를 공급할 수 있는 가로등(120) 및 교통과 관련된 기구들이 통신에 관여한다. 차량(100)은 통신(130)으로 전달받은 정보를 주행 상태 대조 및 공격 이후의 주행 상태 복원에 이용할 수 있고, 가로등(120)을 통해 전달받은 정보를 이용해 교통 혼잡도 혹은 도로 교통과 관련된 사항을 확인할 수 있다.

앞서 언급된 ‘교통과 관련된 기구’라는 것에는 도로교통법시행규칙 제4조에 언급된 ‘신호기’ 및 제6조 (신호등)에 해당하는 기구를 뜻한다.

도 2는 본 고안에 따른 체인구조 커넥티드카 시스템의 네트워크에 사용되는 블록 구성도(200)의 일 실시예 이다. 블록 해시(210)는 해당 블록의 식별자 해시이다. 버전(220)은 해당 블록의 소프트웨어 버전이다. 앞 블록의 해시(230)은 현재 블록 생성 시간(250)의 바로 앞선 시간에 생성된 블록의 해시를 뜻한다. 머클 해시(240)는 차량의 운행 정보들을 각각에 대해 2진 트리 형태로 구성할 때 트리 루트, 즉 최상위 루트에 위치하는 해시값이다. 블록 생성 시간(250)은 블록이 생성된 시간이다. 해시 계산을 위한 임의의 값은 여러 시점의 블록 해시(210)를 계산하기 위한 임의의 값이다. 본 네트워크는 SHA 256 암호화를 이용하는데 이때 데이터를 암호화하기 위해 존재하는 값이다. 블록 생성 시점의 자기 및 주변 차량의 운행 정보(270)는 앞서 도 1에서 설명되었던 차량(100)에 의한 통신(130)의 정보에 해당

한다.

블록 생성 시점의 자기 및 주변 차량의 운행 정보(270)은 블록 생성 시간(250)의 직전에 통신 받은 주변 차량의 운행 정보를 저장한다. 본 블록(200)은 5초 간격으로 새로운 블록(200)을 생성하며 차량 간의 통신(100) 및 운행 정보 저장은 1초 간격으로 진행되는 것으로 제공한다.

도 3은 본 고안에 따른 체인구조 커넥티드카 시스템의 통신 장치의 구성도(300)이다. 다른 차량(100)으로부터 통신 받은 정보에 대한 블록(200)인지 혹은 차량의 운행 정보 인지를 검사한다. 이후 이 데이터가 운행 정보라면 블록(200)을 생성하기 위한 운행 정보 누적 장치(320)로 전달되고, 만약 이것이 블록(200)이라면 대조기(340)로 전달된다. 운행 정보 누적 장치(320)에서는 다른 차량(100)으로부터 전달받은 정보와 자기 차량(100)으로부터 전달받은 운행 정보를 5초간 누적한다. 이후 누적된 운행 정보는 5초 간격으로 블록 생성기(350)로 전달되어 새로운 블록을 생성한다. 블록 생성기(350)에서 블록이 생성된 직후에는 통신장비를 통해 다른 차량(100)으로 배포된다. 대조기(340)에서 전달받은 블록은 블록 생성기(350)에서 생성한 블록(200)과 대조를 통해 차량 운행 정보가 올바른지 확인한다. 만약 이 대조기(340)에서 대조된 블록(200)이 일치한다면 다른 차량으로부터 전달받은 블록은(200) 폐기(330)된다. 만약 이 블록(200)과 블록 생성기(350)에서 생성된 블록(200)이 일치하지 않다면 차량 운행 정보의 변조가 발생하였으므로 복구상태 진입(360)을 시작한다..

위 대조기(340)에서 대조되는 블록(200)은 동일시점에 각각의 차량에서 블록 생성기(350)에 의해 생성된 블록이 대조된다. 블록(200)의 대조는 각 블록(200)에 저장된 머클 해시(240)를 우선적으로 대조한다. 만약 이 머클 해시(240)가 일치하지 않는다고 판단된다면 블록 생성 시점의 자기 및 주변 차량의 운행 정보(270)를 대조하여 운행 상태의 일치성을 확인한다.

만약 구성도(300)의 대조기(340)에서 운행 정보가 일치하지 않는다고 판단된다면 복구 상태 진입(360)을 하게 되는데 이 복구 상태는 이전 블록의 운행 정보 혹은 정상이라고 판단되는 블록(200)에 저장된 다른 차량(100)들의 운행 상태의 평균 상태로 운행 상태를 조정하게 된다.

【산업상 이용가능성】

본 고안에 따른 자율주행 차량의 보안을 위한 체인구조의 커넥티드카 시스템은 다양한 해킹 및 변조에 대해 대응 및 대처를 위해 사용 될 수 있기에 산업상 이용가능성은 매우 높다고 할 수 있다.

【부호의 설명】

100: 자율주행 차량의 보안을 위한 체인구조의 커넥티드카 시스템이 탑재된 차량

110: 도로의 중앙 분리대

120: 도로의 가로등

130: 차량간 통신

200: 블록

210: 블록 해시

220: 블록의 소프트웨어 버전

230: 앞 블록의 해시

240: 머클 해시

250: 블록 생성 시간(시점)

260: 해시 계산을 위한 임의의 값

270: 블록 생성 시점의 자기 및 주변 차량의 운행 정보

300: 통신 장치의 구성도

310: 블록 / 운행 데이터 분류기

320: 운행 정보 누적 장치

330: 대조 이후 정상 블록 폐기

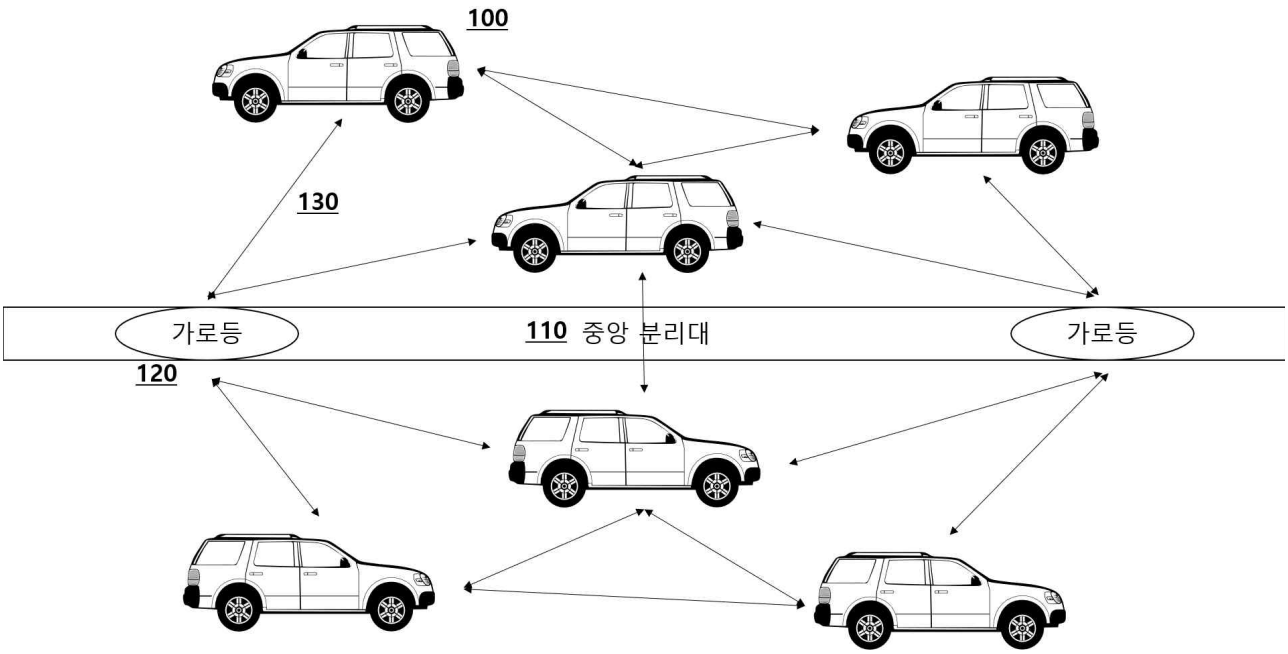
340: 블록 대조기

350: 자기 차량 블록 생성기

360: 복구 상태 진입

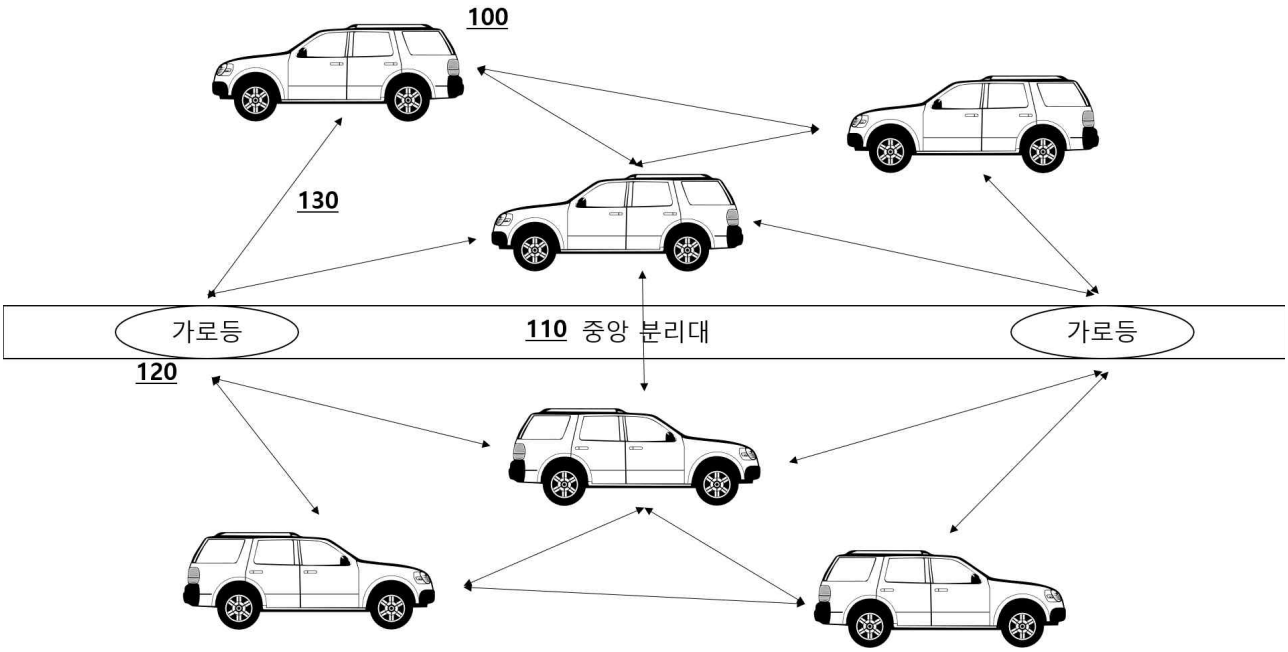
370: 다른 차량 및 통신 장치로의 블록 배포

【대표도】



【도면】

【도면 1】

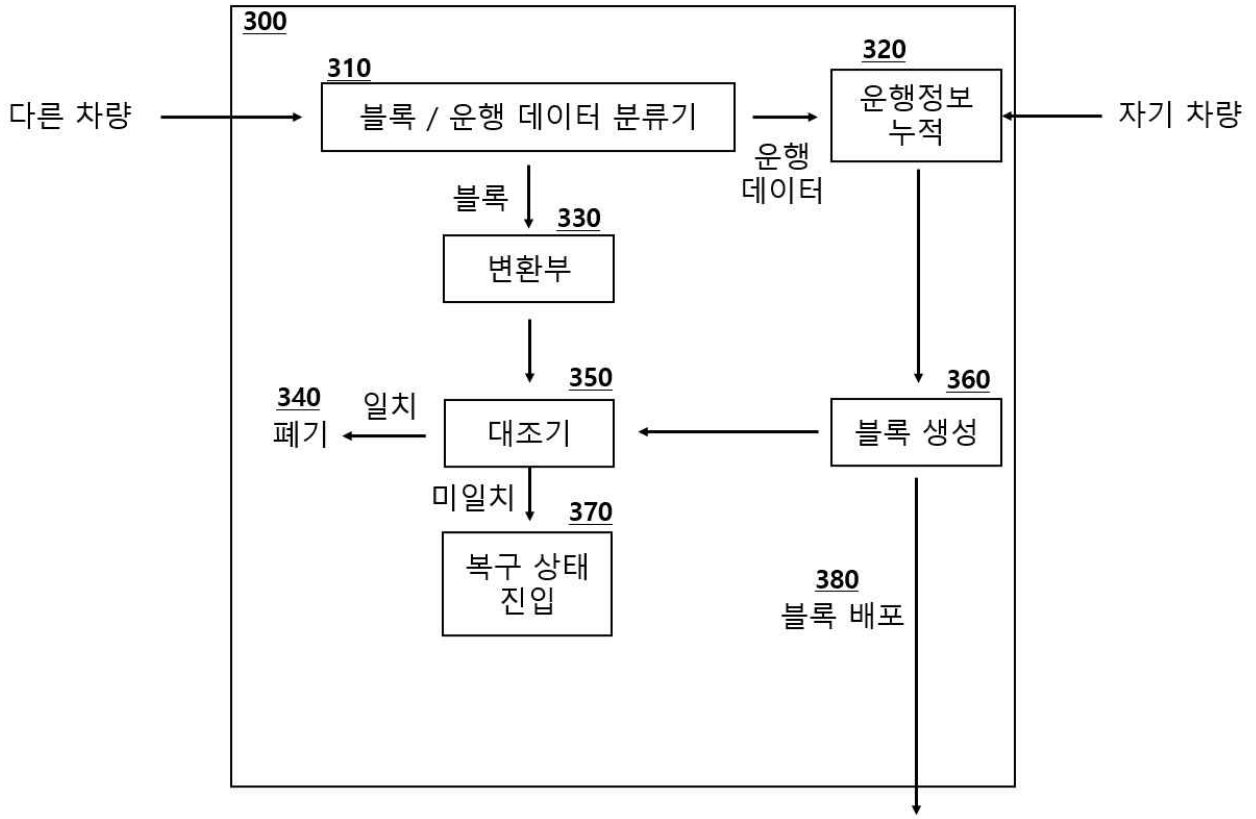


【도면 2】

200

210 블록 해시		
220 버전	230 앞 블록의 해시	240 머클 해시
250 블록 생성 시간	260 해시 계산을 위한 임의의 값	
270 블록 생성 시점의 자기 및 주변 차량의 운행 정보		

【도면 3】



210㎜×297㎜(보존용지(2종) 70g/㎡)