(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년07월31일
(11) 등록번호 10-1759136
(24) 등록일자 2017년07월12일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 29/06* (2006.01)
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/0625 (2013.01)
H04L 63/0435 (2013.01)
(21) 출원번호 10-2015-0160871
(22) 출원일자 2015년11월17일
심사청구일자 2015년11월17일
(65) 공개번호 10-2017-0057576
(43) 공개일자 2017년05월25일
(56) 선행기술조사문헌
KR101356476 B1*
KR100932274 B1*
KR101165350 B1*
KR1020150060093 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
현대자동차주식회사
서울특별시 서초구 헌릉로 12 (양재동)
(72) 발명자
이승철
서울특별시 강남구 개포로 303, 102동 1002호(개포동, 현대1차아파트)
(74) 대리인
박영복

전체 청구항 수 : 총 17 항 심사관 : 김성태

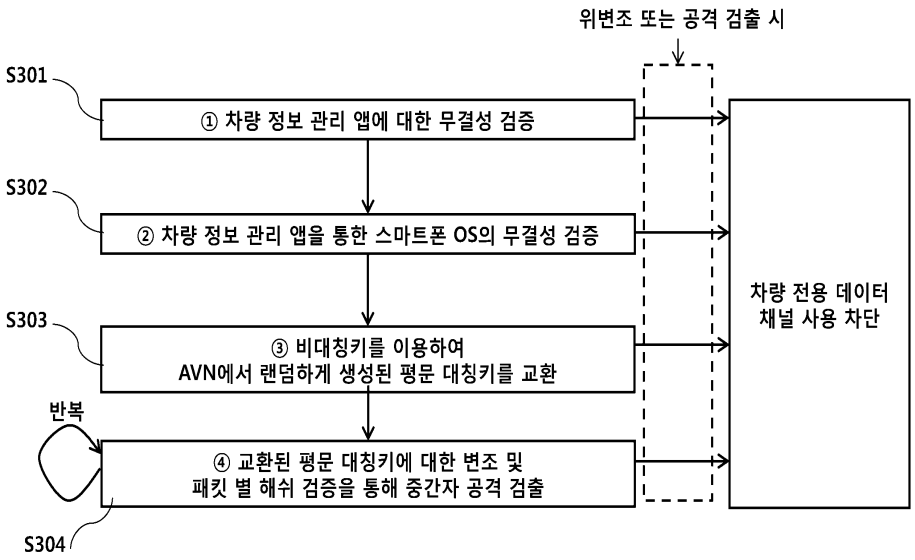
(54) 발명의 명칭 **차량 헤드 유닛과 외부 기기 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치**

(57) 요 약

본 발명은 차량 헤드 유닛과 외부 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치에 관한 것으로서, 본 발명의 일 실시예에 따른 차량 헤드 유닛에서의 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법은 상기 단말에 탑재된 응용 소프트웨어 및 운영 체제의 무결성 검증을 요청하는 소정 무결

(뒷면에 계속)

대 표 도 - 도3



성 검증 요청 메시지를 상기 단말에 전송하는 단계와 상기 단말로부터 무결성 검증 결과 메시지를 수신하는 단계와 상기 무결성 검증 결과 메시지에 따라 상기 응용 소프트웨어 및 상기 운영 체제의 무결성 검증에 성공한 경우, 상기 단말과 평문 대칭키를 교환하는 단계와 상기 평문 대칭키 교환에 성공하면, 상기 단말과 차량 전용 데이터 채널을 설정하고, 상기 평문 대칭키로 암호화된 패킷을 설정된 상기 차량 전용 데이터 채널을 통해 송수신하는 단계를 포함할 수 있다. 따라서, 본 발명은 차량 헤드 유닛과 외부 단말 연동 시 차량 정보에 대한 보안성을 강화시킬 수 있는 장점이 있다.

(52) CPC특허분류
H04L 63/061 (2013.01)
H04L 63/1416 (2013.01)
H04L 63/1466 (2013.01)
H04L 9/0861 (2013.01)
H04L 9/30 (2013.01)

명 세 서

청구범위

청구항 1

차량 헤드 유닛에서의 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법에 있어서,

상기 단말에 탑재된 응용 소프트웨어 및 운영 체제의 무결성 검증을 요청하는 소정 무결성 검증 요청 메시지를 상기 단말에 전송하는 단계;

상기 단말로부터 무결성 검증 결과 메시지를 수신하는 단계;

상기 무결성 검증 결과 메시지에 따라 상기 응용 소프트웨어 및 상기 운영 체제의 무결성 검증에 성공한 경우, 상기 단말과 평문 대칭키를 교환하는 단계; 및

상기 평문 대칭키 교환에 성공하면, 상기 단말과 차량 전용 데이터 채널을 설정하고, 상기 평문 대칭키로 암호화된 패킷을 설정된 상기 차량 전용 데이터 채널을 통해 송수신하는 단계

를 포함하고, 상기 응용 소프트웨어 및 상기 운영 체제 중 적어도 하나의 상기 무결성 검증이 실패하면, 상기 차량 전용 데이터 채널의 설정을 차단하고, 상기 단말상에서 상기 응용 소프트웨어에 대한 무결성 검증이 성공하면, 상기 무결성 검증된 상기 응용 소프트웨어에 의해 상기 운영 체제에 대한 무결성이 검증되는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 2

제1항에 있어서,

상기 평문 대칭키를 교환하는 단계는

제1 평문 대칭키를 생성하는 단계;

상기 제1 평문 대칭키를 상기 단말의 공개키를 이용하여 암호화하여 상기 단말에 전송하는 단계;

상기 차량 헤드 유닛의 공개키로 암호화된 상기 제1 평문 대칭키를 수신하는 단계; 및

상기 차량 헤드 유닛의 개인키를 이용하여 상기 수신된 제1 평문 대칭키를 복호화하는 단계

를 포함하되, 상기 생성된 제1 평문 대칭키와 상기 복호화된 제1 평문 대칭키가 동일하면, 상기 평문 대칭키 교환이 성공한 것으로 판단하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 3

제2항에 있어서,

상기 생성된 제1 평문 대칭키와 상기 복호화된 제1 평문 대칭키가 상이하면, 상기 평문 대칭키 교환이 실패한 것으로 판단하되, 상기 평문 대칭키 교환이 실패하면, 상기 차량 전용 데이터 채널의 설정을 차단하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 4

삭제

청구항 5

제2항에 있어서,

상기 평문 대칭키는 소정 대칭키 생성 함수에 랜덤 값을 입력하여 생성되는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 6

제1항에 있어서,

상기 차량 전용 데이터 채널을 통해 송수신되는 패킷은 상기 차량 헤드 유닛이 탑재된 차량의 동작을 제어하기 위한 제어 명령, 상기 차량 내 제어기들로부터 수집된 차량 정보 중 적어도 하나를 포함하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 7

제6항에 있어서,

상기 차량 정보는 주행 정보, 연비 정보, 고장 정보, 조향 정보, 스티어링휠 제어 정보, 타이어 압력 정보, 엔진 오일 상태 정보, 연료 상태 정보, 공조기 상태 정보 중 적어도 하나를 포함하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 8

삭제

청구항 9

제2항에 있어서,

상기 차량 전용 데이터 채널을 통해 송수신하는 단계는

전송 대상 패킷을 소정 크기의 블록을 분할하는 단계;

소정 정의된 규칙에 따라 상기 제1 평문 대칭키를 이용하여 제2 평문 대칭키를 생성하는 단계; 및

상기 분할된 블록 별 상기 제2 평문 대칭키를 통해 암호화하여 암호화 블록을 생성하고, 상기 분할된 블록 별 제1 평문 대칭키(K1)로 해쉬하여 생성된 데이터를 해당 암호화 블록에 패딩하여 전송하는 단계

를 포함하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 10

제2항에 있어서,

상기 차량 전용 데이터 채널을 통해 송수신하는 단계는

상기 차량 전용 데이터 채널을 통해 패킷이 수신되면, 소정 정의된 규칙에 따라 상기 제1 평문 대칭키를 이용하여 제2 평문 대칭키를 생성하는 단계;

상기 수신된 패킷에 포함된 암호화된 블록 별 상기 제2 평문 대칭키로 복호화하여 제1 데이터를 추출하는 단계; 및

해당 암호화된 블록 별 연접된 패딩 데이터를 상기 제1 평문 대칭키로 복호화하여 제2 데이터를 추출하는 단계

를 포함하되, 상기 제1 데이터와 상기 제2 데이터가 상이하면, 상기 단말상에 중간자 공격이 발생된 것으로 판단하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 11

제10항에 있어서,

상기 중간자 공격이 발생된 것으로 판단되면, 상기 설정된 차량 전용 데이터 채널을 해제하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 12

제10항에 있어서,

상기 제1 데이터와 상기 제2 데이터가 동일하면, 상기 암호화된 블록 별 추출된 상기 제1 데이터를 연접하여 패킷을 생성하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 13

차량 헤드 유닛과 연동되는 단말에서의 차량 전용 데이터 채널 보안 서비스 제공 방법에 있어서,

상기 차량 헤드 유닛으로부터 무결성 검증 요청 메시지를 수신하는 단계;

상기 단말에 탑재된 응용 소프트웨어 및 운영 체제에 대한 무결성 검증을 수행하는 단계;

상기 수행된 무결성 검증에 대한 결과 메시지를 상기 차량 헤드 유닛에 전송하는 단계; 및

상기 무결성 검증에 성공한 경우, 상기 차량 헤드 유닛에 의해 생성된 평문 대칭키를 교환하는 단계; 및

상기 평문 대칭키 교환에 성공하면, 상기 차량 헤드 유닛과 차량 전용 데이터 채널을 설정하고, 상기 평문 대칭키로 암호화된 패킷을 설정된 상기 차량 전용 데이터 채널을 통해 송수신하는 단계

를 포함하고, 상기 응용 소프트웨어 및 상기 운영 체제 중 적어도 하나의 상기 무결성 검증이 실패하면, 상기 차량 전용 데이터 채널의 설정이 차단되고, 상기 단말상에서 상기 응용 소프트웨어에 대한 무결성 검증이 성공하면, 상기 무결성 검증된 상기 응용 소프트웨어에 의해 상기 운영 체제에 대한 무결성이 검증되는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 14

제13항에 있어서,

상기 평문 대칭키를 교환하는 단계는

상기 단말의 공개키로 암호화된 제1 평문 대칭키를 상기 차량 헤드 유닛으로부터 수신하는 단계; 및

상기 제1 평문 대칭키를 상기 단말의 개인키를 이용하여 복호화한 후 상기 차량 헤드 유닛의 공개키로 암호화하여 상기 차량 헤드 유닛에 전송하는 단계

를 포함하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 15

삭제

청구항 16

제14항에 있어서,

상기 차량 전용 데이터 채널을 통해 송수신하는 단계는

전송 대상 패킷을 소정 크기의 블록을 분할하는 단계;

소정 정의된 규칙에 따라 상기 제1 평문 대칭키를 이용하여 제2 평문 대칭키를 생성하는 단계; 및

상기 분할된 블록 별 상기 제2 평문 대칭키를 통해 암호화하여 암호화 블록을 생성하고, 상기 분할된 블록 별 제1 평문 대칭키(K1)로 해쉬하여 생성된 데이터를 해당 암호화 블록에 패딩하여 전송하는 단계

를 포함하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 17

제14항에 있어서,

상기 차량 전용 데이터 채널을 통해 송수신하는 단계

상기 차량 전용 데이터 채널을 통해 패킷이 수신되면, 소정 정의된 규칙에 따라 상기 제1 평문 대칭키를 이용하여 제2 평문 대칭키를 생성하는 단계;

상기 수신된 패킷에 포함된 암호화된 블록 별 상기 제2 평문 대칭키로 복호화하여 제1 데이터를 추출하는 단계; 및

해당 암호화된 블록 별 연접된 패딩 데이터를 상기 제1 평문 대칭키로 복호화하여 제2 데이터를 추출하는 단계

를 포함하되, 상기 제1 데이터와 상기 제2 데이터가 상이하면, 중간자 공격이 발생된 것으로 판단하고, 상기 수신된 패킷을 폐기하는, 차량 전용 데이터 채널 보안 서비스 제공 방법.

청구항 18

유선 또는 무선 통신 연결을 통해 단말과 연동되어 패킷을 송수신하는 차량 헤드 유닛에 있어서,

상기 단말에 탑재된 응용 소프트웨어 및 운영 체제의 무결성 검증을 요청하는 소정 무결성 검증 요청 메시지를 상기 단말에 전송하고, 상기 단말로부터 수신된 무결성 검증 결과에 기반하여 상기 단말과 제1 평문 대칭키를 교환하고, 상기 제1 평문 대칭키 교환에 성공하면 상기 단말과 차량 전용 데이터 채널을 설정하여 상기 패킷을 송수신하는 차량 정보 제공 모듈; 및

상기 차량 전용 데이터 채널을 통해 패킷이 수신되면, 상기 제1 평문 대칭키 및 상기 제1 평문 대칭키로 변조된 제2 평문 대칭키를 통해 상기 수신된 패킷을 복호화하여 수신된 상기 패킷에 대한 중간자 공격 발생 여부를 검출하는 중간자 공격 검출 모듈

을 포함하고, 상기 응용 소프트웨어 및 상기 운영 체제 중 적어도 하나의 상기 무결성 검증이 실패하면 상기 차량 전용 데이터 채널의 설정을 차단하고, 상기 단말상에서 상기 응용 소프트웨어에 대한 무결성 검증이 성공하면 상기 무결성 검증된 상기 응용 소프트웨어에 의해 상기 운영 체제에 대한 무결성이 검증되고, 상기 중간자 공격 발생이 검출되면, 수신된 상기 패킷이 폐기되고, 상기 설정된 차량 전용 데이터 채널이 해제되는, 차량 헤드 유닛.

청구항 19

유선 또는 무선 통신 연결을 통해 차량 헤드 유닛과 연동되는 단말에 있어서,

상기 차량 헤드 유닛으로부터 무결성 검증 요청 메시지를 수신되면 탑재된 응용 소프트웨어에 대한 무결성 검증을 수행하는 무결성 검증 모듈; 및

상기 응용 소프트웨어에 대한 상기 무결성 검증이 성공하면, 탑재된 운영 체제에 대한 무결성 검증을 수행하고, 상기 응용 소프트웨어 및 상기 운영 체제에 대한 무결성 검증 결과를 상기 차량 헤드 유닛에 전송하고, 상기 차량 헤드 유닛과 평문 대칭키를 교환하는 차량 정보 관리 앱

을 포함하고, 상기 평문 대칭키 교환에 성공하면, 상기 차량 헤드 유닛과 상기 차량 정보 관리 앱 사이에 차량 전용 데이터 채널이 설정되고, 상기 평문 대칭키로 암호화된 패킷이 설정된 상기 차량 전용 데이터 채널을 통해 송수신되며, 상기 응용 소프트웨어 및 상기 운영 체제 중 적어도 하나의 상기 무결성 검증이 실패하면, 상기 차량 전용 데이터 채널의 설정이 차단되는 것을 특징으로 하는, 단말.

청구항 20

제1항 내지 제3항, 제5항 내지 제7항, 제9항 내지 제12항 중 어느 한 항에 기재된 방법을 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 차량 헤드 유닛과 외부 기기 연동 시 보안 서비스를 제공하는 방법에 관한 것으로서, 상세하게, 차량 관련 정보를 송수신하기 위한 응용 소프트웨어 및 운영 체제에 대한 무결성 검증뿐만 아니라 차량 관련 정보 송수신에 사용되는 차량 전용 데이터 채널에 대한 보안을 강화하는 것이 가능한 차량 헤드 유닛과 외부 기기 연동 시 차량 전용 데이터 채널에 대한 보안 서비스를 제공하는 방법 및 그를 위한 장치에 관한 것이다.

배 경 기 술

[0002] 최근 차량에 탑재되는 AVN(Audio Video Navigation) 또는 차량 헤드 유닛(Vehicle Head Unit)과 외부 단말(또는 외부 기기)-예를 들면, 스마트폰-을 연동하기 위한 다양한 기술이 개발되고 있다.

[0003] 일 예로, 최근 스마트폰 제조사인 애플(Apple)과 안드로이드 OS 공급자인 구글(Google)은 각각 독자 규격인 CarPlay와 구글 안드로이드 오토(Google Android Auto)를 출시하였으며, 이를 통해, 사용자는 iOS가 탑재된 스

마트폰과 안드로이드 OS가 탑재된 스마트폰을 차량 헤드 유닛과 유선 또는 무선으로 연결하여 스마트폰의 제2 디스플레이로 차량 헤드 유닛의 디스플레이를 사용할 수 있게 되었다.

[0004] 또한, Car Connective Consortium에 의해 주도되고 있는 MirrorLink 솔루션도 여러 OEM에 의하여 점차 확대 적용되고 있으며, 중국의 경우에도 바이두, 텐센트 등의 시장을 주도하는 IT 업체에 의해 독자 규격화한 차량 AVN 스마트폰 연동 기능이 개발되고 있는 실정이다.

[0005] 스마트폰과 차량 AVN을 연동하는 기능은 스마트폰의 다양한 앱들을 차량에서 편리하게 사용할 수 있도록 하고, 애플/구글/바이두 등이 이미 구축해 놓은 에코시스템을 통하여 차량에 적합한 앱들을 유통하고, 해당 앱들을 수시로 업데이트하는 것이 가능하므로, 기존 차량이 가지고 있는 한계인 에코시스템 부재, 업그레이드 및 연결성 제약 등의 문제를 효과적으로 극복하여 줄 수 있는 장점이 있다. 따라서, 차량 AVN 스마트폰 연동 기능은 기존 IT 제품 대비 뒤쳐질 수 있는 차량 AVN의 상품성을 보완할 수 있는 기술로 기대되고 있다.

[0006] 또한, 최근 출시되는 차량 및 스마트폰에는 차량 관련 각종 제어 정보 및 차량에서 취득 가능한 각종 정보-예를 들면, 주행 정보, 연비 정보, 고장 정보 등을 포함함-를 송수신하기 위한 차량 전용 데이터 채널이 지원되고 있다.

[0007] 하지만, 차량에서는 스마트폰의 유효성을 인증하기 위한 보안 인증 수단이 구비되어 있지 않아, 스마트폰의 해킹에 따른 차량 전용 데이터 채널을 통해 송수신되는 각종 제어 신호 및 데이터가 보안에 취약한 문제점이 있었다.

[0008] 차량 전용 데이터 채널을 통해 송수신되는 정보는 차량 안전에 치명적인 정보들을 포함하고 있으므로, 해당 정보가 유출되거나 변경되는 경우, 차량 안전 운행에 치명적인 영향을 미칠 수 있다. 따라서, 차량 AVN과 스마트폰 연동에서 해킹 감지 여부에 따라 차량 전용 데이터 채널에 대한 사용을 제한할 필요가 있다.

[0009] 또한, 더욱 심각하게는 애플/구글 등의 소프트웨어가 배포되는 과정에서 악의적인 해커에 의하여 코드가 위조 또는 변조된 경우, AVN 내에는 잠재적인 보안 위험성을 가진 코드가 설치되고, 그에 따른 차량 보안 위험성이 증가할 수 있다.

[0010] 현재 스마트폰과 차량 AVN을 연동하는 기술은 도 1에 도시된 바와 같이 USB/ WIFI/블루투스와 같은 물리적인 통신 수단을 이용하여 상호 연결되고, 스마트폰에서 비디오나 오디오와 같은 데이터를 전송하면, AVN에서 수신된 데이터를 디코딩하고 랜더링하여 출력하였다. 또한, AVN은 구비된 터치 화면 또는(및) 키 버튼 등의 입력 수단을 통해 입력된 입력 데이터, 음성 인식/전화 연동 등을 위한 오디오 데이터 및 AVN에 구비된 GPS 모듈을 통해 획득된 측위 데이터 등을 스마트폰에 전송할 수 있다. 또한, AVN은 스마트폰에 탑재된 특정앱과 차량 전용 데이터 채널을 설정하고, 설정된 차량 전용 데이터 채널을 통해 각종 차량 제어 정보 및 상태 정보를 송수신할 수 있다. 일 예로, AVN은 차량 전용 데이터 채널을 통해 차량 내 고장 정보, 주행 정보, 연비 정보 등을 스마트폰에 전송하고, 스마트폰은 차량 정보 수집을 위한 각종 제어 명령 및 긴급 제동과 같은 차량의 동작을 제어하기 위한 각종 제어 명령을 차량 전용 데이터 채널을 통해 AVN에 전송할 수 있다.

[0011] 현재, 차량 AVN과 스마트폰의 연동에 있어서, 스마트폰에서 차량 AVN의 무결성을 소프트웨어 또는 하드웨어적으로 인증하는 규격은 정의되어 있으나, 차량 AVN에서 스마트폰에 탑재된 소프트웨어 및 운영 체제에 대한 무결성을 인증하는 규격은 정의되어 있지 않은 상태이다.

[0012] 일반적으로, AVN과 같은 차량 헤드 유닛은 물리적으로 통제된 환경에서 사용되고, 차량 헤드 유닛 자체가 항상 네트워크에 연결되거나 사용자에 의해 소프트웨어 및 펌웨어가 상시 업데이트되지 않으므로, 보안 위험성이 스마트폰에 비해 낮은 특징이 있다.

[0013] 하지만, 스마트폰은 항상 네트워크에 접속되어 있어서, 외부의 악의적인 해킹에 항상 노출되어 있으며, 이에 따라 악성 코드가 삽입된 소프트웨어가 설치될 수 있다.

[0014] 스마트폰에 해킹이 발생되면, 해커가 원격으로 해당 스마트폰을 제어하여 긴급 제동, 스트어링휠 임의 조작 등의 제어 명령을 차량에 전송하여 차량 안전에 심각한 문제를 야기시킬 수 있다.

발명의 내용

해결하려는 과제

[0015] 본 발명은 상술한 종래 기술의 문제점을 해결하기 위해 고안된 것으로, 본 발명의 목적은 차량 AVN과 외부 단말

연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치를 제공하는 것이다.

[0016] 본 발명의 다른 목적은 외부 단말에 탑재된 응용 소프트웨어 및 운영 체제에 대한 무결성을 검증함으로써, 위변조된 응용 소프트웨어 및 운영 체제를 통한 해킹 시도를 미연에 방지하는 것이 가능한 차량 헤드 유닛과 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치를 제공하는 것이다.

[0017] 본 발명의 또 다른 목적은 차량 전용 데이터 채널을 통해 전송되는 패킷의 암호화를 통해 차량 보안 데이터, 차량 제어 명령에 대한 기밀성을 유지할 수 있을 뿐만 아니라 패킷의 해킹 여부-즉, 중간자 공격 발생 여부-를 감지하여 차량 전용 데이터 채널의 사용을 적응적으로 제어하는 것이 가능한 차량 헤드 유닛과 외부 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치를 제공하는 것이다.

[0018] 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0019] 본 발명은 차량 헤드 유닛과 외부 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치를 제공한다.

[0020] 본 발명의 일 실시예에 따른 차량 헤드 유닛에서의 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법은 상기 단말에 탑재된 응용 소프트웨어 및 운영 체제의 무결성 검증을 요청하는 소정 무결성 검증 요청 메시지를 상기 단말에 전송하는 단계와 상기 단말로부터 무결성 검증 결과 메시지를 수신하는 단계와 상기 무결성 검증 결과 메시지에 따라 상기 응용 소프트웨어 및 상기 운영 체제의 무결성 검증에 성공한 경우, 상기 단말과 평문 대칭키를 교환하는 단계와 상기 평문 대칭키 교환에 성공하면, 상기 단말과 차량 전용 데이터 채널을 설정하고, 상기 평문 대칭키로 암호화된 패킷을 설정된 상기 차량 전용 데이터 채널을 통해 송수신하는 단계를 포함할 수 있다.

[0021] 여기서, 상기 평문 대칭키를 교환하는 단계는 제1 평문 대칭키를 생성하는 단계와 상기 제1 평문 대칭키를 상기 단말의 공개키를 이용하여 암호화하여 상기 단말에 전송하는 단계와 상기 차량 헤드 유닛의 공개키로 암호화된 상기 제1 평문 대칭키를 수신하는 단계와 상기 차량 헤드 유닛의 개인키를 이용하여 상기 수신된 제1 평문 대칭키를 복호화하는 단계를 포함하되, 상기 생성된 제1 평문 대칭키와 상기 복호화된 제1 평문 대칭키가 동일하면, 상기 평문 대칭키 교환이 성공한 것으로 판단할 수 있다.

[0022] 또한, 상기 생성된 제1 평문 대칭키와 상기 복호화된 제1 평문 대칭키가 상이하면, 상기 평문 대칭키 교환이 실패한 것으로 판단하되, 상기 평문 대칭키 교환이 실패하면, 상기 차량 전용 데이터 채널의 설정을 차단할 수 있다.

[0023] 또한, 상기 응용 소프트웨어 및 상기 운영 체제 중 적어도 하나의 상기 무결성 검증이 실패하면, 상기 차량 전용 데이터 채널의 설정을 차단할 수 있다.

[0024] 또한, 최초 생성되는 상기 평문 대칭키는 소정 대칭키 생성 함수에 랜덤 값을 입력하여 생성될 수 있다.

[0025] 또한, 상기 차량 전용 데이터 채널을 통해 송수신되는 패킷은 상기 차량 헤드 유닛이 탑재된 차량의 동작을 제어하기 위한 제어 명령, 상기 차량 내 제어기들로부터 수집된 차량 정보 중 적어도 하나를 포함할 수 있다.

[0026] 여기서, 상기 차량 정보는 주행 정보, 연비 정보, 고장 정보, 조향 정보, 스티어링휠 제어 정보, 타이어 압력 정보, 엔진 오일 상태 정보, 연료 상태 정보, 공조기 상태 정보 중 적어도 하나를 포함할 수 있다.

[0027] 또한, 상기 단말상에서 상기 응용 소프트웨어에 대한 무결성 검증에 성공하면, 상기 무결성 검증된 상기 응용 소프트웨어에 의해 상기 운영 체제에 대한 무결성이 검증될 수 있다.

[0028] 또한, 상기 차량 전용 데이터 채널을 통해 송수신하는 단계는 전송 대상 패킷을 소정 크기의 블록을 분할하는 단계와 소정 정의된 규칙에 따라 상기 제1 평문 대칭키를 이용하여 제2 평문 대칭키를 생성하는 단계와 상기 분할된 블록 별 상기 제2 평문 대칭키를 통해 암호화하여 암호화 블록을 생성하고, 상기 분할된 블록 별 제1 평문 대칭키(K1)로 해쉬하여 생성된 데이터를 해당 암호화 블록에 패딩하여 전송하는 단계를 포함할 수 있다.

[0029] 또한, 상기 차량 전용 데이터 채널을 통해 송수신하는 단계는 상기 차량 전용 데이터 채널을 통해 패킷이 수신되면, 소정 정의된 규칙에 따라 상기 제1 평문 대칭키를 이용하여 제2 평문 대칭키를 생성하는 단계와 상기 수

신된 패킷에 포함된 암호화된 블록 별 상기 제2 평문 대칭키로 복호화하여 제1 데이터를 추출하는 단계와 해당 암호화된 블록 별 연접된 패딩 데이터를 상기 제1 평문 대칭키로 복호화하여 제2 데이터를 추출하는 단계를 포함하되, 상기 제1 데이터와 상기 제2 데이터가 상이하면, 상기 단말상에 중간자 공격이 발생된 것으로 판단할 수 있다.

[0030] 여기서, 상기 중간자 공격이 발생된 것으로 판단되면, 상기 설정된 차량 전용 데이터 채널이 해제될 수 있다.

[0031] 또한, 상기 제1 데이터와 상기 제2 데이터가 동일하면, 상기 암호화된 블록 별 추출된 상기 제1 데이터를 연접하여 패킷을 생성할 수 있다.

[0032] 본 발명의 다른 일 실시예에 따른 차량 헤드 유닛과 연동되는 단말에서의 차량 전용 데이터 채널 보안 서비스 제공 방법은 상기 차량 헤드 유닛으로부터 무결성 검증 요청 메시지를 수신하는 단계와 상기 단말에 탑재된 응용 소프트웨어 및 운영 체제에 대한 무결성 검증을 수행하는 단계와 상기 수행된 무결성 검증에 대한 결과 메시지를 상기 차량 헤드 유닛에 전송하는 단계와 상기 무결성 검증에 성공한 경우, 상기 차량 헤드 유닛에 의해 생성된 평문 대칭키를 교환하는 단계와 상기 평문 대칭키 교환에 성공하면, 상기 차량 헤드 유닛과 차량 전용 데이터 채널을 설정하고, 상기 평문 대칭키로 암호화된 패킷을 설정된 상기 차량 전용 데이터 채널을 통해 송수신하는 단계를 포함할 수 있다.

[0033] 여기서, 상기 평문 대칭키를 교환하는 단계는 상기 단말의 공개키로 암호화된 제1 평문 대칭키를 상기 차량 헤드 유닛으로부터 수신하는 단계와 상기 제1 평문 대칭키를 상기 단말의 개인키를 이용하여 복호화한 후 상기 차량 헤드 유닛의 공개키로 암호화하여 상기 차량 헤드 유닛에 전송하는 단계를 포함할 수 있다.

[0034] 또한, 상기 응용 소프트웨어 및 상기 운영 체제 중 적어도 하나의 상기 무결성 검증에 실패하면, 상기 차량 전용 데이터 채널의 설정이 차단될 수 있다.

[0035] 또한, 상기 차량 전용 데이터 채널을 통해 송수신하는 단계는 전송 대상 패킷을 소정 크기의 블록을 분할하는 단계와 소정 정의된 규칙에 따라 상기 제1 평문 대칭키를 이용하여 제2 평문 대칭키를 생성하는 단계와 상기 분할된 블록 별 상기 제2 평문 대칭키를 통해 암호화하여 암호화 블록을 생성하고, 상기 분할된 블록 별 제1 평문 대칭키(K1)로 해쉬하여 생성된 데이터를 해당 암호화 블록에 패딩하여 전송하는 단계를 포함할 수 있다.

[0036] 또한, 상기 차량 전용 데이터 채널을 통해 송수신하는 단계는 상기 차량 전용 데이터 채널을 통해 패킷이 수신되면, 소정 정의된 규칙에 따라 상기 제1 평문 대칭키를 이용하여 제2 평문 대칭키를 생성하는 단계와 상기 수신된 패킷에 포함된 암호화된 블록 별 상기 제2 평문 대칭키로 복호화하여 제1 데이터를 추출하는 단계와 해당 암호화된 블록 별 연접된 패딩 데이터를 상기 제1 평문 대칭키로 복호화하여 제2 데이터를 추출하는 단계를 포함하되, 상기 제1 데이터와 상기 제2 데이터가 상이하면, 중간자 공격이 발생된 것으로 판단하고, 상기 수신된 패킷을 폐기할 수 있다.

[0037] 본 발명의 또 다른 일 실시예에 따른 유선 또는 무선 통신 연결을 통해 단말과 연동되어 패킷을 송수신하는 차량 헤드 유닛은 상기 단말에 탑재된 응용 소프트웨어 및 운영 체제의 무결성 검증을 요청하는 소정 무결성 검증 요청 메시지를 상기 단말에 전송하고, 상기 단말로부터 수신된 무결성 검증 결과에 기반하여 상기 단말과 제1 평문 대칭키를 교환하고, 상기 제1 평문 대칭키 교환에 성공하면 상기 단말과 차량 전용 데이터 채널을 설정하여 상기 패킷을 송수신하는 차량 정보 제공 모듈과 상기 차량 전용 데이터 채널을 통해 패킷이 수신되면, 상기 제1 평문 대칭키 및 상기 제1 평문 대칭키로 변조된 제2 평문 대칭키를 통해 상기 수신된 패킷을 복호화하여 수신된 상기 패킷에 대한 중간자 공격 발생 여부를 검출하는 중간자 공격 검출 모듈을 포함하되, 상기 중간자 공격 발생이 검출되면, 수신된 상기 패킷이 폐기되고, 상기 설정된 차량 전용 데이터 채널이 해제될 수 있다.

[0038] 본 발명의 또 다른 일 실시예에 따른 유선 또는 무선 통신 연결을 통해 차량 헤드 유닛과 연동되는 단말은 상기 차량 헤드 유닛으로부터 무결성 검증 요청 메시지를 수신되면 탑재된 응용 소프트웨어에 대한 무결성 검증을 수행하는 무결성 검증 모듈과 상기 응용 소프트웨어에 대한 상기 무결성 검증이 성공하면, 탑재된 운용 체제에 대한 무결성 검증을 수행하고, 상기 응용 소프트웨어 및 상기 운영 체제에 대한 상기 무결성 검증 결과를 상기 차량 헤드 유닛에 전송하고, 상기 차량 헤드 유닛과 평문 대칭키를 교환하는 차량 정보 관리 앱을 포함하되, 상기 평문 대칭키 교환에 성공하면, 상기 차량 헤드 유닛과 상기 차량 정보 관리 앱 사이에 차량 전용 데이터 채널이 설정되고, 상기 평문 대칭키로 암호화된 패킷이 설정된 상기 차량 전용 데이터 채널을 통해 송수신되는 것을 특징으로 한다.

[0039] 본 발명의 또 다른 일 실시예는 상기한 차량 전용 데이터 채널 보안 서비스 제공 방법들 중 어느 하나의 방법을

실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공할 수 있다.

[0040] 상기 본 발명의 양태들은 본 발명의 바람직한 실시예들 중 일부에 불과하며, 본원 발명의 기술적 특징들이 반영된 다양한 실시예들이 당해 기술분야의 통상적인 지식을 가진 자에 의해 이하 상술할 본 발명의 상세한 설명을 기반으로 도출되고 이해될 수 있다.

발명의 효과

[0041] 본 발명에 따른 방법 및 장치에 대한 효과에 대해 설명하면 다음과 같다.

[0042] 본 발명은 차량 헤드 유닛과 외부 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치를 제공하는 장점이 있다.

[0043] 또한, 본 발명은 외부 단말에 탑재된 응용 소프트웨어 및 운영 체제에 대한 무결성을 검증함으로써, 위변조된 응용 소프트웨어 및 운영 체제를 통한 해킹 시도를 미연에 방지하는 것이 가능한 차량 헤드 유닛과 외부 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치를 제공하는 장점이 있다.

[0044] 또한, 본 발명은 차량 전용 데이터 채널을 통해 전송되는 패킷의 암호화를 통해 차량 보안 데이터에 대한 기밀성을 유지할 수 있을 뿐만 아니라 패킷의 해킹 여부-즉, 중간자 공격-를 확인하는 것이 가능한 차량 헤드 유닛과 외부 단말 연동 시 차량 전용 데이터 채널 보안 서비스 제공 방법 및 그를 위한 장치를 제공하는 장점이 있다.

[0045] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0046] 이하에 첨부되는 도면들은 본 발명에 관한 이해를 돕기 위한 것으로, 상세한 설명과 함께 본 발명에 대한 실시예들을 제공한다. 다만, 본 발명의 기술적 특징이 특정 도면에 한정되는 것은 아니며, 각 도면에서 개시하는 특징들은 서로 조합되어 새로운 실시예로 구성될 수 있다.

도 1은 종래 기술에 따른 차량 AVN 스마트폰 연동 시스템의 구성을 설명하기 위한 도면이다.

도 2는 본 발명의 일 실시예에 따른 차량 AVN 스마트폰 연동 기능을 제공하기 위해 구현된 AVN 시스템의 계층 구조를 보여준다.

도 3은 본 발명의 일 실시예에 따른 차량 헤드 유닛과 외부 단말 연동 시 차량 전용 데이터 채널에 대한 보안 서비스를 제공하는 방법을 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 스마트폰에 탑재된 응용 소프트웨어 및 운영 체제의 무결성을 검증하는 절차를 설명하기 위한 도면이다.

도 5는 본 발명의 일 실시예에 따른 차량 전용 데이터 채널의 암호화에 사용될 평문 대칭키를 교환하는 절차를 설명하기 위한 흐름도이다.

도 6 내지 7은 본 발명의 일 실시예에 따른 송신단에서 전송 대상 패킷을 암호화하여 전송하는 방법을 설명하기 도면이다.

도 8 내지 9는 본 발명의 일 실시예에 따른 수신단에서 수신된 패킷을 복호하는 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0047] 이하, 본 발명의 실시예들이 적용되는 장치 및 다양한 방법들에 대하여 도면을 참조하여 보다 상세하게 설명한다. 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

[0048] 이상에서, 본 발명의 실시예를 구성하는 모든 구성 요소들이 하나로 결합되거나 결합되어 동작하는 것으로 설명되었다고 해서, 본 발명이 반드시 이러한 실시예에 한정되는 것은 아니다. 즉, 본 발명의 목적 범위 안에서라면, 그 모든 구성 요소들이 하나 이상으로 선택적으로 결합하여 동작할 수도 있다. 또한, 그 모든 구성

요소들이 각각 하나의 독립적인 하드웨어로 구현될 수 있지만, 각 구성 요소들의 그 일부 또는 전부가 선택적으로 조합되어 하나 또는 복수 개의 하드웨어에서 조합된 일부 또는 전부의 기능을 수행하는 프로그램 모듈을 갖는 컴퓨터 프로그램으로서 구현될 수도 있다. 그 컴퓨터 프로그램을 구성하는 코드들 및 코드 세그먼트들은 본 발명의 기술 분야의 당업자에 의해 용이하게 추론될 수 있을 것이다. 이러한 컴퓨터 프로그램은 컴퓨터가 읽을 수 있는 저장매체(Computer Readable Media)에 저장되어 컴퓨터에 의하여 읽혀지고 실행됨으로써, 본 발명의 실시예를 구현할 수 있다. 컴퓨터 프로그램의 저장매체로서는 자기 기록매체, 광 기록매체 등이 포함될 수 있다.

[0049] 또한, 이상에서 기재된 "포함하다", "구성하다" 또는 "가지다" 등의 용어는, 특별히 반대되는 기재가 없는 한, 해당 구성 요소가 내재될 수 있음을 의미하는 것이므로, 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것으로 해석되어야 한다. 기술적이거나 과학적인 용어를 포함한 모든 용어들은, 다르게 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 사전에 정의된 용어와 같이 일반적으로 사용되는 용어들은 관련 기술의 문맥 상의 의미와 일치하는 것으로 해석되어야 하며, 본 발명에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0050] 또한, 본 발명의 구성 요소를 설명하는 데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다. 어떤 구성 요소가 다른 구성 요소에 "연결", "결합" 또는 "접속"된다고 기재된 경우, 그 구성 요소는 그 다른 구성 요소에 직접적으로 연결되거나 또는 접속될 수 있지만, 각 구성 요소 사이에 또 다른 구성 요소가 "연결", "결합" 또는 "접속"될 수도 있다고 이해되어야 할 것이다.

[0051] 이하의 설명에서, 차량 헤드 유닛에는 AVN(Audio Video Navigation) 기능이 탑재될 수 있으며, 차량 헤드 유닛과 AVN을 혼용해서 사용하기로 한다.

[0052] 또한, 본원 발명에 따른 외부 단말은 스마트폰을 포함할 수 있으며, 설명의 편의를 위해 외부 단말, 단말과 스마트폰을 혼용해서 사용하기로 한다.

[0053] 또한, 본원 발명에 따른 스마트폰 또는 차량 헤드 유닛에 탑재되어 차량 내 수집된 정보 또는 차량 보안 관련 정보 또는 차량 제어 명령 등을 송수신하는 응용 소프트웨어를 차량 전용 앱 또는 차량 정보 관리 앱이라 명하기로 한다. 반면, 차량 헤드 유닛에 탑재된 AVN 기능을 사용하기 위해 스마트폰에 탑재되는 응용 소프트웨어를 차량 전용 앱과 구별하기 위한 AVN 연동 앱이라 명하기로 한다.

[0054] 도 2는 본 발명의 일 실시예에 따른 차량 AVN 스마트폰 연동 기능을 제공하기 위해 구현된 AVN 시스템의 계층 구조를 보여준다.

[0055] 도 2를 참조하면, AVN 시스템은 AVN 응용(211), 스마트폰 연동 앱(212), 스마트폰 연동 앱 플러그인(213) 등을 포함하는 응용 계층(210), 미들웨어(Middleware) 및 사용자 인터페이스 프레임웍(UI Framework)을 제공하는 미들웨어 계층(220), 운영 체제(Operating System, 230) 계층, 하드웨어(Hardware, 260) 계층 등을 포함하여 구성될 수 있다.

[0056] AVN 응용(211)은 오디오, 비디오, 네비게이션 등의 기능을 제공하기 위한 응용 소프트웨어로서, 차량 헤드 유닛의 직접적인 제어를 통해 각종 AVN 기능을 사용자에 제공하기 위한 응용 소프트웨어일 수 있다.

[0057] 스마트폰 연동 앱(212)은 스마트폰과의 통신 연결을 통해 AVN 기능을 원격으로 제어하기 위한 AVN 연동 앱과 차량 내 탑재된 제어기들로부터 각종 차량 전용 정보를 실시간 수집하고, 스마트폰으로부터 수신된 소정 제어 명령에 따라 수집된 차량 정보를 유선 또는 무선으로 연결된 스마트폰에 전송하는 차량 정보 제공 앱 등을 포함할 수 있다.

[0058] 이때, AVN 연동 앱과 차량 정보 제공 앱을 위해 설정되는 채널은 서로 독립적으로 설정될 수 있다. 즉, AVN 시스템(200)에 탑재되는 차량 정보 제공 앱은 별도의 차량 전용 데이터 채널을 통해 차량 내부 정보 및 차량 제어 명령을 송수신할 수 있다.

[0059] 하드웨어(260) 계층은 AVN 기능을 제어하기 위한 LCD와 같은 디스플레이 장치, 스피커와 같은 오디오 장치, 키버튼 및 조그휠과 같은 입력 장치뿐만 아니라 차량 내 통신을 위한 CAN과 같은 차량 내 통신 모듈, 외부 사용자 디바이스와의 통신을 위한 USB 포트, WIFI 통신 모듈, 블루투스 통신 모듈 등이 탑재될 수 있다.

[0060] 본 발명에 따른 AVN 시스템은 차량 내 통신을 통해 각종 차량 상태 정보를 수집할 수 있다. 일 예로, 차량 상태 정보는 주행 정보, 연비 정보, 고장 정보, 조향 정보, 스티어링휠 제어 정보, 타이어 압력 정보, 엔진 오일 상

태 정보, 연료 상태 정보, 공조기 상태 정보 등을 포함할 수 있으나, 이에 한정되지는 않으며, 차량 내 탑재된 각종 제어기들로부터 수집 가능한 모든 정보를 포함할 수 있다.

[0061] 도 3은 본 발명의 일 실시예에 따른 차량 AVN과 스마트폰 연동 시 차량 전용 데이터 채널에 대한 보안 서비스를 제공하는 방법을 설명하기 위한 도면이다.

[0062] 도 3을 참조하면, AVN 시스템은 스마트폰의 접속이 확인되면, 스마트폰에 탑재된 차량 정보 관리 앱에 대한 무결성을 검증하는 절차를 수행할 수 있다(S301).

[0063] 차량 정보 관리 앱에 대한 무결성 검증에 성공한 경우, AVN 시스템은 검증된 차량 정보 관리 앱을 통해 스마트폰에 탑재된 운영 체제에 대한 무결성 검증 절차를 수행할 수 있다(S302).

[0064] 만약, 상기 301 단계에서, 차량 정보 관리 앱에 대한 무결성 검증에 실패한 경우, AVN 시스템은 해당 스마트폰에 대한 차량 전용 데이터 채널 사용을 차단할 수 있다.

[0065] 또한, 상기 302 단계에서, 스마트폰에 탑재된 운영 체제에 대한 무결성 검증에 실패한 경우, AVN 시스템은 해당 스마트폰에 대한 차량 전용 데이터 채널 사용을 차단할 수 있다.

[0066] 상기 302 단계에서, 운영 체제에 대한 무결성 검증이 성공한 경우, AVN 시스템은 비대칭키를 이용하여 AVN 시스템에서 랜덤하게 생성한 평문 대칭키를 교환하는 절차를 수행할 수 있다(S303). 여기서, AVN 시스템에서 사용되는 비대칭키는 AVN 시스템에 유지된 스마트폰 공개 키 및 AVN 개인 키를 포함할 수 있다. 반면, 스마트폰에서 평문 대칭키 교환 절차에 사용하는 비대칭키는 AVN 공개 키 및 스마트폰 개인 키를 포함할 수 있다. 평문 대칭키 교환 절차는 후술할 도 5를 통해 상세히 설명하기로 한다.

[0067] AVN 시스템은 평문 대칭키 교환에 성공한 경우, 해당 스마트폰과 차량 전용 데이터 채널을 설정하고, 설정된 차량 전용 데이터 채널을 통해 데이터를 송수신할 수 있다. 이때, 차량 전용 데이터 채널을 통해 전송되는 패킷은 송신단에서 암호화되어 전송된다. 수신단은 수신된 패킷을 복호하여 중간자 공격을 검출할 수 있다(S304).

[0068] 특히, AVN 시스템은 교환된 평문 대칭키를 실시간 변조하여 전송 대상 패킷을 암호화한 후, 암호화된 패킷을 차량 전용 데이터 채널을 통해 스마트폰에 전송할 수 있다. 또한, AVN 시스템은 차량 전용 데이터 채널을 통해 패킷이 수신되면, 교환된 평문 대칭키를 실시간 변조하여 수신된 패킷을 복호하고, 패킷 별 해쉬 검증을 통해 중간자 공격을 검출할 수 있다. 패킷 별 해쉬 검증을 통한 중간자 공격 검출은 후술할 도 6 내지 도 9의 설명을 통해 보다 명확해질 것이다.

[0069] 상기한 304 단계에서, 중간자 공격이 검출된 경우, AVN 시스템은 설정된 차량 전용 데이터 채널에 대한 사용을 차단 또는 해제할 수 있다.

[0070] 도 4는 본 발명의 일 실시예에 따른 스마트폰에 탑재된 응용 소프트웨어 및 운영 체제의 무결성을 검증하는 절차를 설명하기 위한 도면이다.

[0071] 도 4를 참조하면, 차량 헤드 유닛(410)은 차량 정보 제공 모듈(411), 외부 통신 모듈(412), 중간자 공격 검출 모듈(413) 및 차량 내 통신 모듈(414) 등을 포함하여 구성될 수 있다.

[0072] 스마트폰(420)은 무결성 검증 모듈(421), 차량 정보 관리 앱(422), 운영 체제(423) 및 통신 모듈(424)을 포함하여 구성될 수 있다.

[0073] 차량 정보 제공 모듈(411)은 스마트폰의 접속이 확인되면, 차량 정보 관리 앱(422) 및 운영 체제(423)에 대한 무결성 검증 요청 메시지를 스마트폰(420)에 전송할 수 있다.

[0074] 스마트폰의 통신 모듈(423)은 수신된 무결성 검증 요청 메시지를 운영 체제(423)를 통해 또는 직접 무결성 검증 모듈(421)에 전송할 수 있다.

[0075] 무결성 검증 모듈(421)은 차량 정보 관리 앱(422)에 대한 무결성을 검증할 수 있다.

[0076] 만약, 차량 정보 관리 앱(422)에 대한 무결성 검증이 성공한 경우, 무결성 검증 모듈(421)은 차량 정보 관리 앱(422)이 운영 체제(423)에 대한 무결성 검증을 수행하도록 제어할 수 있다.

[0077] 차량 정보 관리 앱(422)은 운영 체제(423)에 대한 무결성 검증을 수행하고, 무결성 검증 결과를 운영 체제(423) 또는(및) 통신 모듈(423)을 통해 차량 헤드 유닛(410)에 전송할 수 있다.

[0078] 만약, 차량 정보 관리 앱(422)에 대한 무결성을 검증에 실패한 경우, 무결성 검증 모듈(421)은 차량 정보 관리

앱(422)이 유효하지 않음을 지시하는 소정 무결성 검증 결과 메시지를 운영 체제(423) 또는(및) 통신 모듈(423)을 통해 차량 헤드 유닛(410)에 전송할 수 있다.

[0079] 차량 정보 제공 모듈(411)은 외부 통신 모듈(412)을 통해 수신된 무결성 검증 결과 메시지에 기반하여 차량 정보 관리 앱(422) 또는(및) 운영 체제(423)이 유효한지 여부를 확인할 수 있다.

[0080] 차량 정보 제공 모듈(411)은 차량 정보 관리 앱(422) 및 운영 체제(423)가 유효한 것으로 확인되면, 차량 정보 관리 앱(422)과 차량 전용 데이터 채널을 설정하고, 설정된 차량 전용 데이터 채널을 통해 패킷을 송수신할 수 있다.

[0081] 만약, 차량 정보 관리 앱(422), 운영 체제(423) 중 적어도 하나가 유효하지 않은 것으로 확인되면, 차량 정보 제공 모듈(411)은 해당 스마트폰과의 차량 전용 데이터 채널 설정을 차단할 수 있다.

[0082] 중간자 공격 검출 모듈(413)은 외부 통신 모듈(412)로부터 암호화된 패킷이 수신되면, 이를 복호하고, 복호된 패킷에 기반하여 중간자 공격을 검출할 수 있다.

[0083] 중간자 공격 검출 모듈(413)은 중간자 공격이 검출되면, 해킹이 발생되었음을 지시하는 소정 해킹 발생 보고 메시지를 차량 정보 제공 모듈(411)에 전송할 수 있다. 이때, 차량 정보 제공 모듈(411)은 해킹 발생 보고 메시지에 따라 설정된 차량 전용 데이터 채널을 해제시킬 수 있다.

[0084] 만약, 중간자 공격이 검출되지 않은 경우, 중간자 공격 검출 모듈(413)은 복호된 패킷을 차량 정보 제공 모듈(411)에 전달할 수 있다.

[0085] 차량 정보 제공 모듈(411)은 차량 정보 관리 앱(422)으로부터 수신된 소정 제어 명령에 따라 차량 내 통신 모듈(414)을 통해 수집한 각종 차량 정보를 암호화한 후 외부 통신 모듈(412)를 통해 차량 정보 관리 앱(422)에 전송할 수 있다. 이때, 차량 정보 전송에 사용되는 채널은 상기한 차량 전용 데이터 채널이다.

[0086] 도 5는 본 발명의 일 실시예에 따른 차량 전용 데이터 채널의 암호화에 사용될 평문 대칭키를 교환하는 절차를 설명하기 위한 흐름도이다.

[0087] 도 5를 참조하면, 차량 헤드 유닛(510)에는 스마트폰 공개키(S_public_key) 및 AVN 개인키(AVN_private_key)가 유지되고, 스마트폰(520)에는 AVN 공개키(AVN_public_key) 및 스마트폰 개인키(S_private_key) 유지될 수 있다(S501 내지 S502).

[0088] 차량 헤드 유닛(510)은 소정 대칭키 생성 함수에 랜덤 Seed값을 입력하여 평문 대칭키 생성할 수 있다(S503). 여기서, 평문 대칭키의 길이는 128bits일 수 있으나, 이에 한정되지는 않는다.

[0089] 차량 헤드 유닛(510)은 생성된 평문 대칭키를 스마트폰 공개키를 이용하여 암호화한 후, 암호화된 평문 대칭키를 스마트폰(520)에 전송할 수 있다(S504 내지 S505).

[0090] 스마트폰(520)은 스마트폰 개인키를 이용하여 암호화된 평문 대칭키를 복호하고, AVN 공개키를 이용하여 복호된 평문 대칭키를 다시 암호화하여 차량 헤드 유닛(510)에 전송할 수 있다(S506 내지 S508).

[0091] 차량 헤드 유닛(510)은 AVN 개인키를 이용하여 AVN 공개키로 암호화된 평문 대칭키를 복호하고, 복호된 평문 대칭키가 상기한 503 단계에서 생성된 평문 대칭키와 동일한지 여부를 확인할 수 있다(S509 내지 S510).

[0092] 확인 결과, 동일한 경우, 차량 헤드 유닛(510)은 차량 전용 데이터 채널을 설정하고, 교환된 평문 대칭키를 통해 암호화된 패킷을 송수신할 수 있다(S511).

[0093] 상기 510 단계의 확인 결과, 동일하지 않은 경우, 차량 헤드 유닛(510)은 평문 대칭키 교환에 실패한 것으로 판단하며, 평문 대칭키 교환에 실패하였음을 알리는 소정 안내 메시지를 출력할 수 있다(S512).

[0094] 도 6 내지 7은 본 발명의 일 실시예에 따른 송신단에서 전송 대상 패킷을 암호화하여 전송하는 방법을 설명하기 도면이다.

[0095] 도 6을 참조하면, 송신단은 최초 전송 대상 패킷을 소정 크기의 블록으로 분할하고, 분할된 블록을 제1 평문 대칭키(K1)를 이용하여 암호화한 후, 암호화된 블록에 Null 데이터를 패딩하여 전송할 수 있다(S601). 여기서, 송신단은 차량 헤드 유닛 또는 스마트폰일 수 있다.

[0096] 송신단은 미리 정의된 규칙에 따라 제1 평문 대칭키(K1)를 제2 평문 대칭키(K2)로 변경할 수 있다(S602). 즉, 송신단은 매 패킷 전송 시마다 평문 대칭키를 미리 정의된 규칙에 기반하여 실시간 변경할 수 있다. 일 예로,

소정 대칭키 생성 함수에 제1 평문 대칭키(K1)를 입력하여 제2 평문 대칭키(K2)가 획득될 수 있다.

[0097] 송신단은 다음 전송 대상 패킷을 소정 크기의 블록으로 분할한 후, 분할된 블록을 제2 평문 대칭키((K2)를 이용하여 암호화하고, 분할된 블록을 제1 평문 대칭키(K1)로 해쉬하여 생성된 데이터를 제2 평문 대칭키((K2)로 암호화된 블록 후미에 패딩하여 전송할 수 있다(S603).

[0098] 상기 도 6의 송신단에서의 패킷 암호화 절차를 후술할 도 7을 통해 상세히 설명하기로 한다.

[0099] 도 7을 참조하면, 송신단은 상위 계층으로부터 패킷이 수신되면, 기 교환된 제1 평문 대칭키(K1)를 입력 값으로 소정 함수에 입력하여 제2 평문 대칭키(K2)를 생성할 수 있다(S701 내지 S702).

[0100] 송신단은 수신된 패킷을 소정 길이를 갖는 n개의 블록으로 분할하고, 각각의 블록을 제2 평문 대칭키(K2)를 이용하여 암호화할 수 있다(S703 내지 S704).

[0101] 일 예로, 각각의 블록은 제2 평문 대칭키(K2)와 동일한 길이를 가질 수 있으며, 블록과 제2 평문 대칭키(K2)를 Exclusive OR 연산하여 암호화된 블록이 생성될 수 있으나, 이는 하나의 실시예에 불과하며 다른 암호화 방법이 적용될 수도 있음을 주의해야 한다.

[0102] 송신단은 제1 평문 대칭키(K1)를 이용하여 각각의 블록을 암호화(해쉬)하여 패팅 데이터를 생성하고(S706), 상기한 704 단계 내지 705 단계에서 생성된 암호화된 블록의 후미에 생성된 패팅 데이터를 단계 707에 도시된 바와 같이 삽입하여 암호화된 패킷을 생성할 수 있다.

[0103] 송신단은 기 설정된 차량 전용 데이터 채널을 통해 암호화된 패킷을 수신단에 전송할 수 있다(S708).

[0104] 도 8 내지 9는 본 발명의 일 실시예에 따른 수신단에서 수신된 패킷을 복호하는 방법을 설명하기 위한 도면이다.

[0105] 도 8을 참조하면, 수신단은 차량 전용 데이터 채널을 통해 최초로 패킷이 수신된 경우, 수신된 패킷으로부터 암호화된 블록을 추출하고, 추출된 암호화된 블록을 기 교환된 제1 평문 대칭키(K1)를 이용하여 복호화할 수 있다(S801). 여기서, 수신단은 차량 헤드 유닛 또는 스마트폰일 수 있다.

[0106] 수신단은 소정 대칭키 생성 함수에 제1 평문 대칭키(K1)를 입력하여 제2 평문 대칭키(K2)를 획득하고, 다음 수신된 패킷의 암호화된 블록을 제2 평문 대칭키((K2)를 통해 복호화하여 제1 데이터를 추출할 수 있다(S802 내지 S803). 일 예로, 대칭키 생성 함수는 소정 길이를 갖는 쉬프트 레지스터(Shift Register)일 수 있으며, 매 패킷 수신 시마다 쉬프트 레지스터에 저장된 값이 1비트씩 순환 이동되어 새로운 평문 대칭키가 생성될 수 있다. 즉, 매 패킷 송수신마다 시점마다 평문 대칭키가 변조될 수 있으며, 이에 따라 차량 전용 데이터 채널이 대한 보안이 강화될 수 있다. 다른 일 예로, 수신단은 미리 정의된 규칙에 따라 제1 평문 대칭키(K1)를 이용하여 제2 평문 대칭키(K2)를 변조할 수도 있다.

[0107] 수신단은 암호화된 블록에 연접된 패딩 데이터를 제1 평문 대칭키(K1)로 복호화하여 제2 데이터 추출할 수 있다(S804).

[0108] 연이어, 수신단은 제1 데이터와 제2 데이터가 동일한지 여부를 확인할 수 있다(S805).

[0109] 확인 결과, 동일한 경우, 수신단은 상기 제1 데이터를 연접하여 패킷을 생성한 후 상위 계층에 생성된 패킷을 전달할 수 있다(S806). 이때, 설정된 차량 전용 데이터 채널을 유지될 수 있다.

[0110] 상기 805 단계의 확인 결과, 동일하지 않은 경우, 수신단은 해당 패킷을 폐기하고 설정된 차량 전용 데이터 채널의 사용을 차단할 수 있다(S807). 일 예로, 수신단은 동일하지 않은 경우, 스마트폰 OS 단에서의 중간자 공격이 발생된 것으로 판단하여 설정된 차량 전용 데이터 채널을 해제할 수 있다.

[0111] 이하에서는 도 9를 참조하여, 상기한 도 8의 수신단에서의 패킷 복호화 절차를 상세히 설명하기로 한다.

[0112] 도 9을 참조하면, 수신단은 차량 전용 데이터 채널을 통해 패킷이 수신되면, 수신된 패킷에 포함된 암호화 블록을 추출하고, 추출된 암호화 블록 별 제2 평문 대칭키(K2)를 이용하여 복호화하여 제1 데이터를 추출하고, 해당 암호화 블록에 대응하여 삽입된 패딩을 제1 평문 대칭키(K1)를 이용하여 복호화하여 제2 데이터를 추출할 수 있다(S901 내지 S903).

[0113] 수신단은 제1 데이터와 제2 데이터가 동일한지 여부를 확인할 수 있다(S904).

[0114] 확인 결과, 동일한 경우, 수신단은 암호화 블록 별 삽입된 패딩을 제거하고, 상기 제1 데이터를 연접하여 패킷

을 생성한 후 상위 계층에 생성된 패킷을 전달할 수 있다(S905 내지 S906). 이때, 설정된 차량 전용 데이터 채널을 유지될 수 있다.

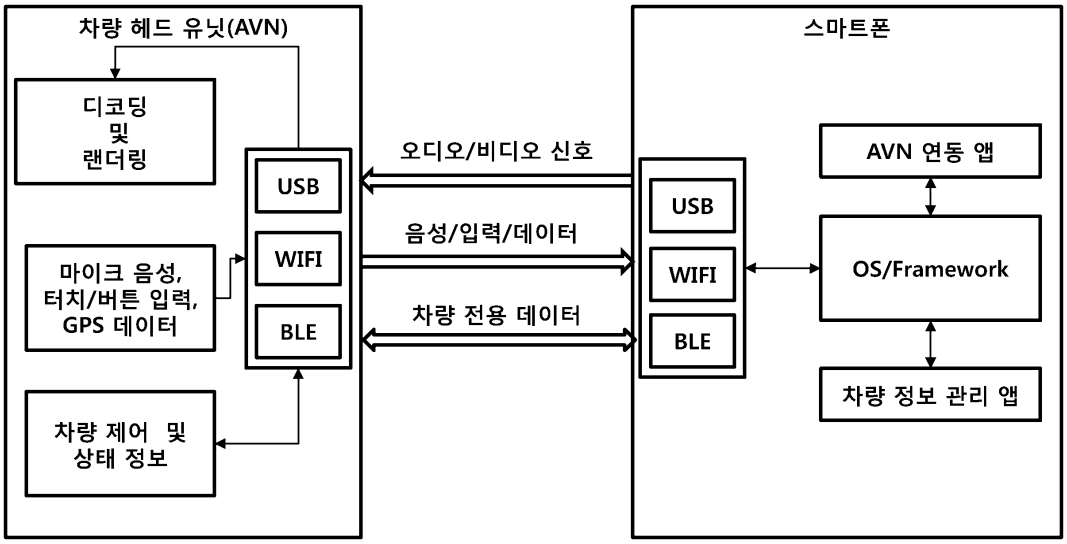
[0115] 상기한 904 단계의 확인 결과, 동일하지 않은 경우, 수신단은 해당 수신 패킷을 폐기하고 설정된 차량 전용 데이터 채널의 사용을 차단할 수 있다(S907). 일 예로, 수신단은 동일하지 않은 경우, 스마트폰 OS 단에서의 중간자 공격이 발생된 것으로 판단하여 설정된 차량 전용 데이터 채널을 해제할 수 있다.

[0116] 본 발명은 본 발명의 정신 및 필수적 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있음은 당업자에게 자명하다.

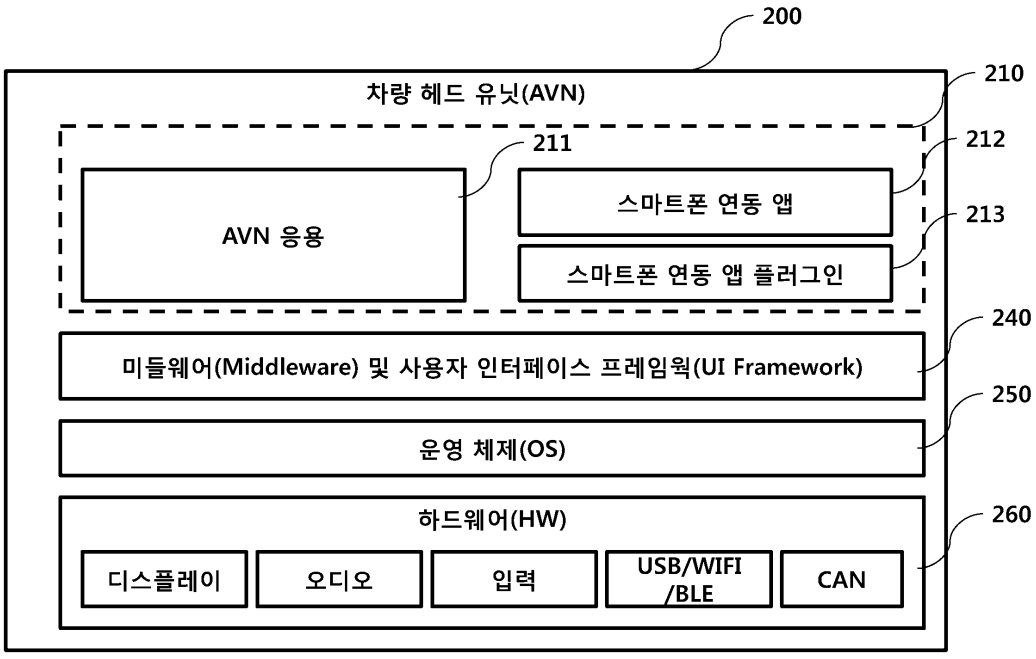
[0117] 따라서, 상기의 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니되고 예시적인 것으로 고려되어야 한다. 본 발명의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 발명의 등가적 범위 내에서의 모든 변경은 본 발명의 범위에 포함된다.

도면

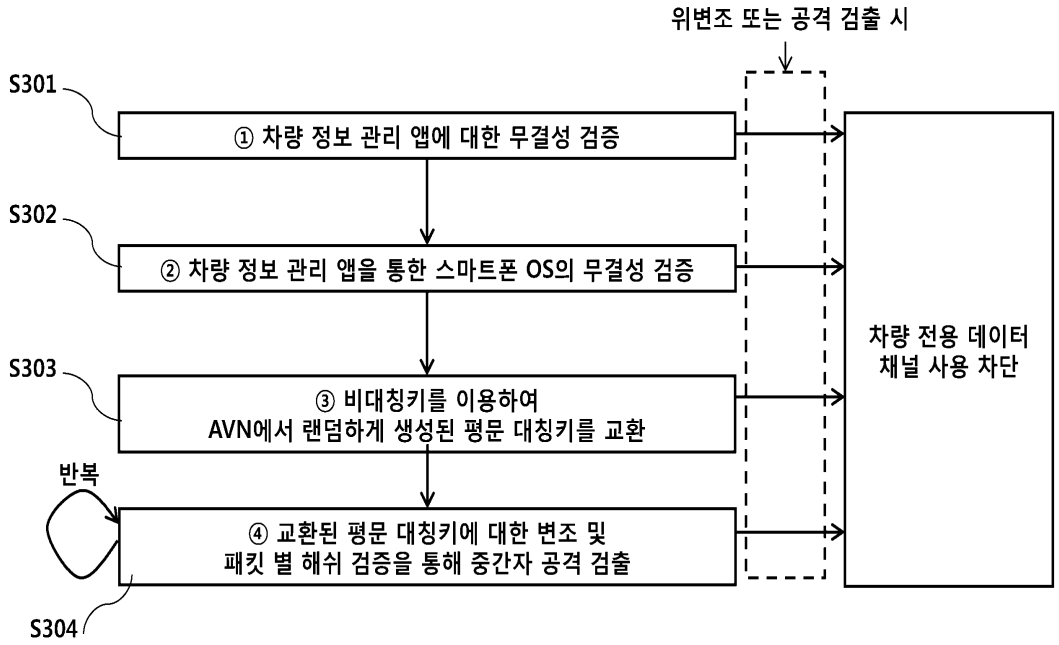
도면1



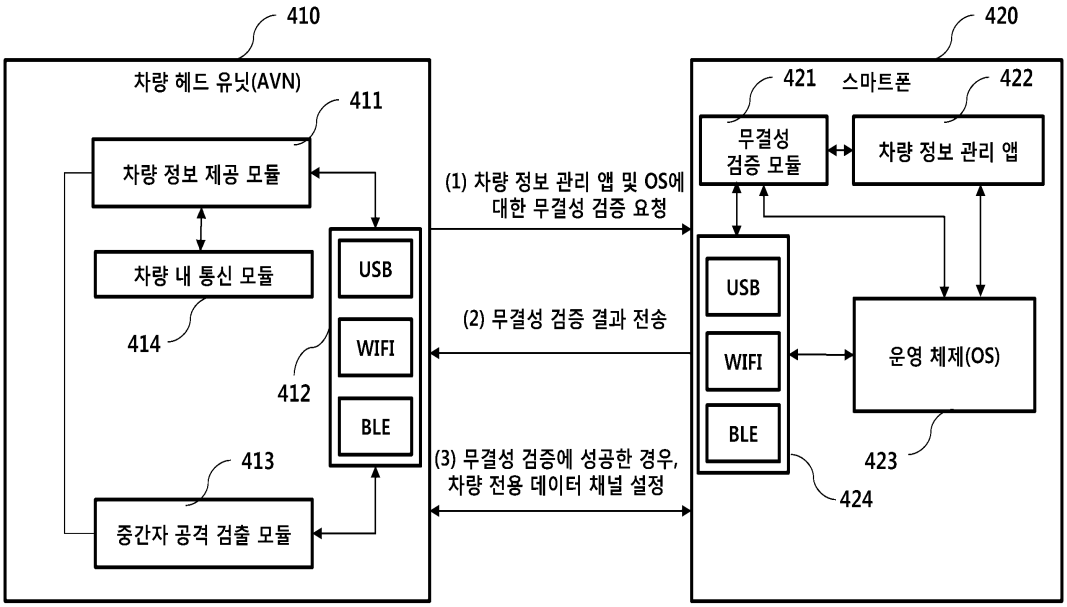
도면2



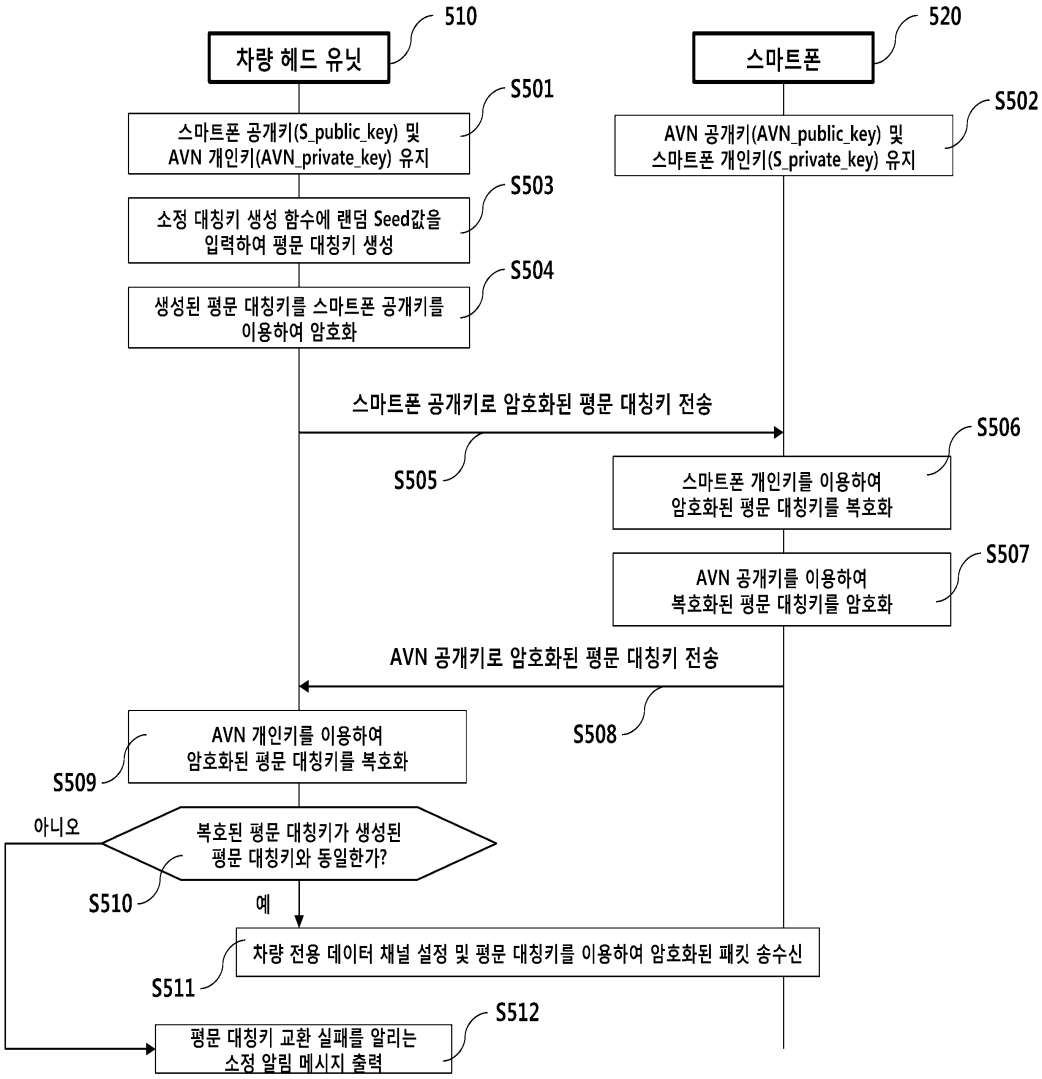
도면3


위변조 또는 공격 검출 시
S301
① 차량 정보 관리 앱에 대한 무결성 검증
S302
② 차량 정보 관리 앱을 통한 스마트폰 OS의 무결성 검증
S303
③ 비대칭키를 이용하여
AVN에서 랜덤하게 생성된 평문 대칭키를 교환
반복
④ 교환된 평문 대칭키에 대한 변조 및
패킷 별 해쉬 검증을 통해 중간자 공격 검출
S304
차량 전용 데이터
채널 사용 차단

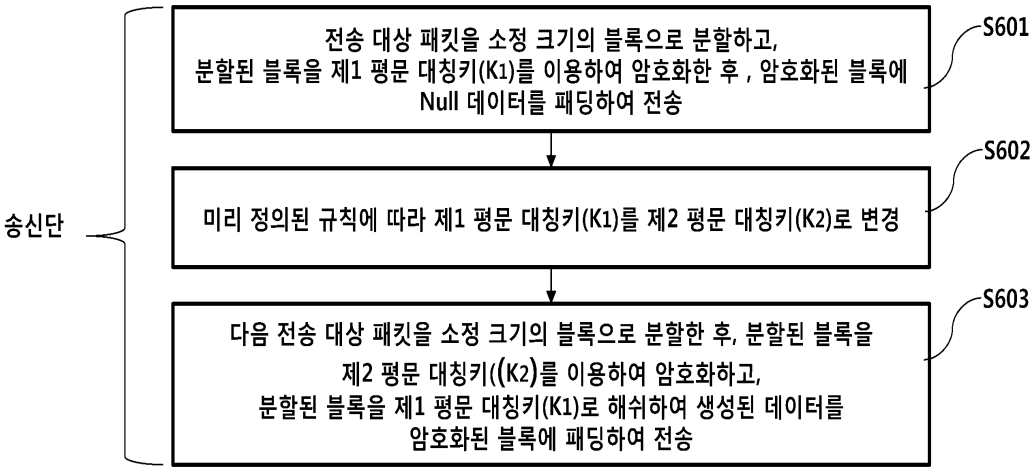
도면4


410
차량 헤드 유닛(AVN)
411
차량 정보 제공 모듈
차량 내 통신 모듈
414
USB
WIFI
412
BLE
413
중간자 공격 검출 모듈
(1) 차량 정보 관리 앱 및 OS에
대한 무결성 검증 요청
(2) 무결성 검증 결과 전송
(3) 무결성 검증에 성공한 경우,
차량 전용 데이터 채널 설정
420
421
스마트폰
422
무결성
검증 모듈
차량 정보 관리 앱
USB
WIFI
BLE
운영 체제(OS)
423
424

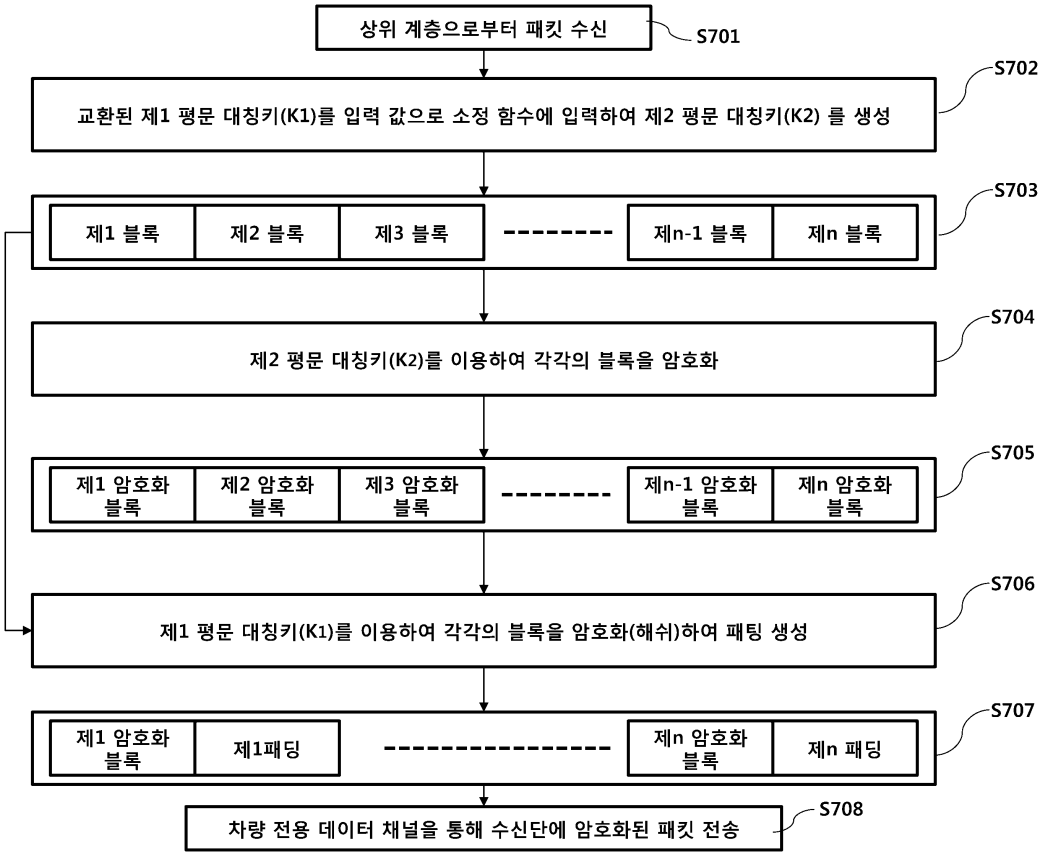
도면5


510
차량 헤드 유닛
520
스마트폰
S501
스마트폰 공개키(S_public_key) 및
AVN 개인키(AVN_private_key) 유지
S502
AVN 공개키(AVN_public_key) 및
스마트폰 개인키(S_private_key) 유지
S503
소정 대칭키 생성 함수에 랜덤 Seed값을
입력하여 평문 대칭키 생성
S504
생성된 평문 대칭키를 스마트폰 공개키를
이용하여 암호화
스마트폰 공개키로 암호화된 평문 대칭키 전송
S505
S506
스마트폰 개인키를 이용하여
암호화된 평문 대칭키를 복호화
S507
AVN 공개키를 이용하여
복호화된 평문 대칭키를 암호화
AVN 공개키로 암호화된 평문 대칭키 전송
S508
AVN 개인키를 이용하여
암호화된 평문 대칭키를 복호화
S509
아니오
복호된 평문 대칭키가 생성된
평문 대칭키와 동일한가?
S510
예
차량 전용 데이터 채널 설정 및 평문 대칭키를 이용하여 암호화된 패킷 송수신
S511
S512
평문 대칭키 교환 실패를 알리는
소정 알림 메시지 출력

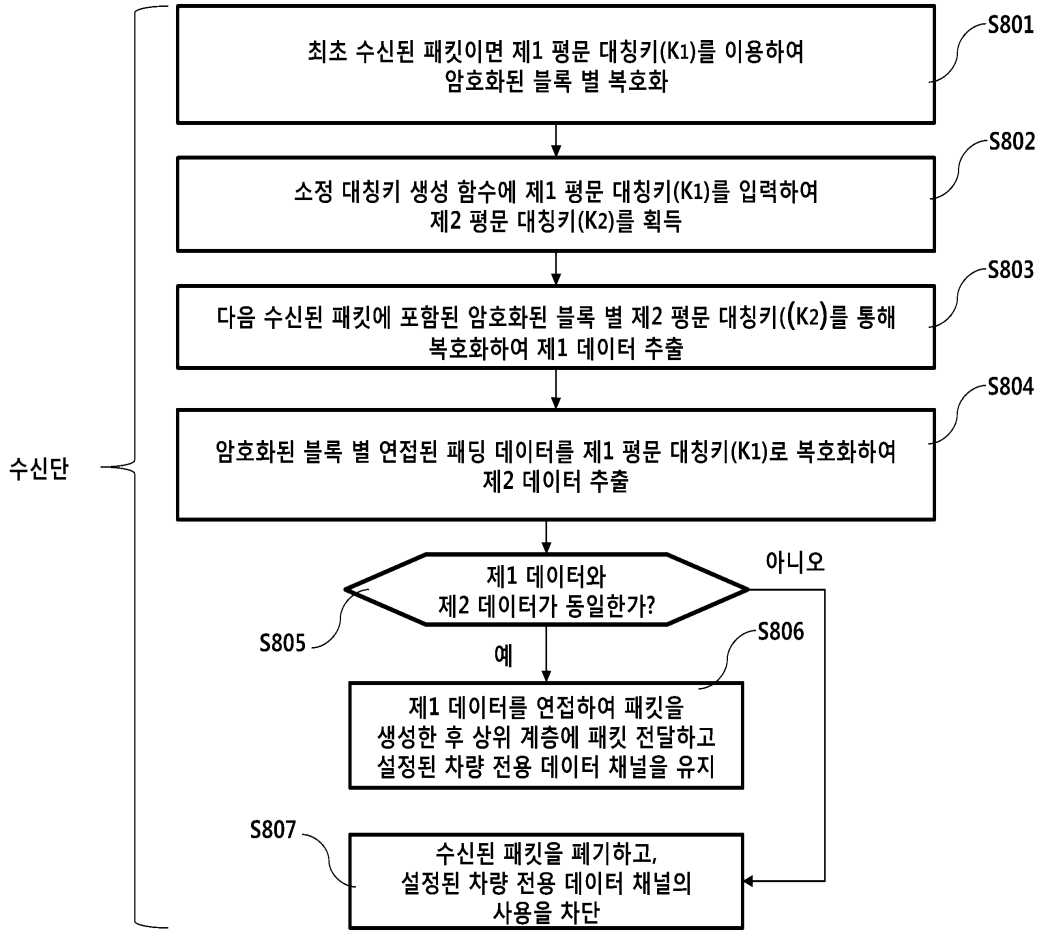
도면6


송신단
전송 대상 패킷을 소정 크기의 블록으로 분할하고,
분할된 블록을 제1 평문 대칭키(K1)를 이용하여 암호화한 후 , 암호화된 블록에
Null 데이터를 패딩하여 전송
S601
미리 정의된 규칙에 따라 제1 평문 대칭키(K1)를 제2 평문 대칭키(K2)로 변경
S602
다음 전송 대상 패킷을 소정 크기의 블록으로 분할한 후, 분할된 블록을
제2 평문 대칭키((K2)를 이용하여 암호화하고,
분할된 블록을 제1 평문 대칭키(K1)로 해쉬하여 생성된 데이터를
암호화된 블록에 패딩하여 전송
S603

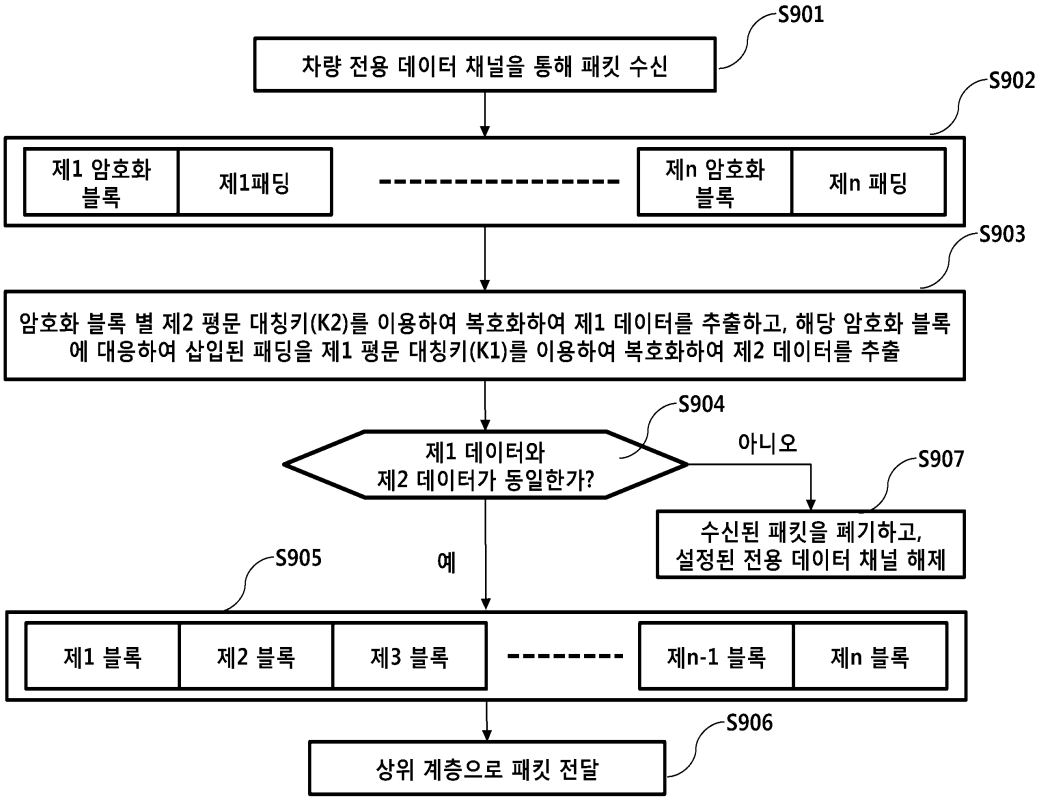
도면7


상위 계층으로부터 패킷 수신
S701
교환된 제1 평문 대칭키(K1)를 입력 값으로 소정 함수에 입력하여 제2 평문 대칭키(K2) 를 생성
S702
제1 블록
제2 블록
제3 블록
제n-1 블록
제n 블록
S703
제2 평문 대칭키(K2)를 이용하여 각각의 블록을 암호화
S704
제1 암호화 블록
제2 암호화 블록
제3 암호화 블록
제n-1 암호화 블록
제n 암호화 블록
S705
제1 평문 대칭키(K1)를 이용하여 각각의 블록을 암호화(해쉬)하여 패팅 생성
S706
제1 암호화 블록
제1패딩
제n 암호화 블록
제n 패딩
S707
차량 전용 데이터 채널을 통해 수신단에 암호화된 패킷 전송
S708

도면8


수신단
최초 수신된 패킷이면 제1 평문 대칭키(K1)를 이용하여 암호화된 블록 별 복호화
S801
소정 대칭키 생성 함수에 제1 평문 대칭키(K1)를 입력하여 제2 평문 대칭키(K2)를 획득
S802
다음 수신된 패킷에 포함된 암호화된 블록 별 제2 평문 대칭키((K2)를 통해 복호화하여 제1 데이터 추출
S803
암호화된 블록 별 연접된 패딩 데이터를 제1 평문 대칭키(K1)로 복호화하여 제2 데이터 추출
S804
제1 데이터와 제2 데이터가 동일한가?
S805
아니오
예
S806
제1 데이터를 연접하여 패킷을 생성한 후 상위 계층에 패킷 전달하고 설정된 차량 전용 데이터 채널을 유지
S807
수신된 패킷을 폐기하고, 설정된 차량 전용 데이터 채널의 사용을 차단

도면9



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 19항

【변경전】

상기 무결성 검증 결과를

【변경후】

무결성 검증 결과를