(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년05월28일
(11) 등록번호 10-1400275
(24) 등록일자 2014년05월21일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2013-0016961
(22) 출원일자 2013년02월18일
심사청구일자 2013년02월18일
(56) 선행기술조사문헌
US8230215 B2
US7934095 B2
유영준 외 2명, 차량 애드혹 네트워크 환경에서 효율적인 메시지 인증 방법, 정보보호학회논문지, 제19권, 제6호 (2009.12.)

(73) 특허권자
부경대학교 산학협력단
부산광역시 남구 신선로 365 (용당동, 부경대학교)
(72) 발명자
박영호
부산광역시 사상구 모라로52번길 9, 한양빌라 102호 (모라동)
서철
부산광역시 해운대구 해운대로483번길 15-7 ,가동301호(우동,그린빌라)
(뒷면에 계속)
(74) 대리인
특허법인 신태양

전체 청구항 수 : 총 3 항 심사관 : 양종필

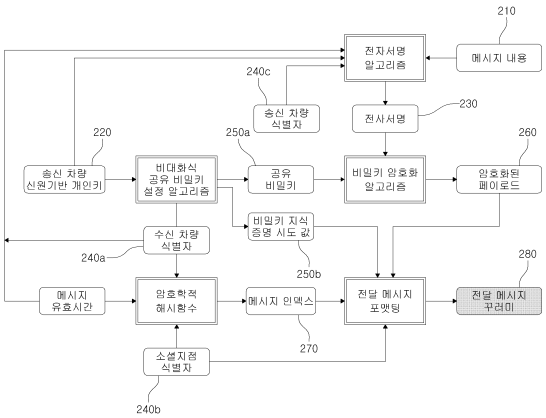
(54) 발명의 명칭 **차량 애드혹(Ad-Hoc) 네트워크에서의 메시지 전달방법**

(57) 요 약

본 발명은 차량들이 빈번하게 방문하거나 밀집되는 지역에 정해진 소셜지점(Social spot)의 노변장치의 중계기능을 통하여 차량간 메시지를 전달하는 차량 애드혹(Ad-Hoc) 네트워크에서의 메시지 전달방법에 관한 것이다.

본 발명에서는 차량의 식별자를 이용하여 메시지 수신차량을 명시하는 대신에 송신차량으로부터 수신차량으로 전달되는 메시지 꾸러미에 차량 식별자가 숨겨진 메시지 인덱스를 부가하여 소셜지점의 노변장치가 보관하게 함으로써 상기 수신차량이 자신의 차량 식별자를 노출시키지 않고서도 자신이 수신차량으로 명시된 메시지의 보관여부를 노변장치에게 질의하고 메시지를 요청할 수 있도록 하고, 메시지를 요청한 차량이 상기 송신차량에 의해 지정된 메시지 인덱스에 대응되는 정당한 수신차량인지 인증하기 위하여 신원기반 암호기술의 비대화 방식의 공유 비밀키 설정에 따라 송신차량과 지정된 수신차량만이 생성할 수 있는 비밀키에 대한 지식증명을 이용하여 소셜지점의 노변장치가 메시지의 정당한 수신차량임을 인증할 수 있도록 함으로써 차량 애드혹 네트워크를 통한 메시지 전달과정에서 메시지 도청이나 패킷분석으로부터 차량의 식별자가 노출되는 것을 방지하여 수신차량의 프라이버시를 보호할 수 있도록 하는 것이다.

대 표 도 - 도2



(72) 발명자

신상욱

부산광역시 남구 분포로 111, 134동 2204호 (용호동, LG메트로시티)

이경현

부산광역시 해운대구 마린시티2로 33 ,101동2209호(우동,해운대두산위브더제니스))

특허청구의 범위

청구항 1

송신차량이 소셜지점에 설치된 노변장치를 중계노드로 하여 수신차량에게 메시지를 전달하도록 하는 차량 애드혹(Ad-Hoc) 네트워크에서의 메시지 전달방법에 있어서,

차량 애드혹 네트워크 서비스에 등록되는 차량들과 각각의 소셜지점에 설치된 노변장치들의 안전한 메시지 전달 수행에 필요한 신원기반의 개인 키를 신뢰기관으로부터 발급받되, 차량 애드혹 네트워크 서비스에 등록되는 차량의 신원기반의 개인 키는 차량의 등록번호를 식별자(Identity)로 하여 신뢰기관이 겹선형 그룹(Bilinear group)상에서 정의되는 수학적 연산을 기반으로 하여 생성한 것이고, 소셜지점에 설치된 노변장치의 신원기반의 개인 키는 소셜지점의 지리적 위치정보를 식별자로 하여 신뢰기관이 생성한 것인 신원기반 개인키 발급단계와;

상기 소셜지점의 노변장치를 통한 메시지 전달과정에서 상기 송신차량과 수신차량 그리고 송신차량과 소셜지점의 노변장치 사이의 공유 비밀키를 각각 설정하는 공유 비밀키 설정단계와;

상기 송신차량이 자신과 수신차량 사이에 설정된 공유 비밀키를 이용하여 메시지 내용을 암호화하고, 수신차량의 식별자가 숨겨진 메시지 인덱스를 이용하여 전달하고자 하는 메시지 꾸러미(Message package)를 구성하되, 신뢰기관으로부터 발급받은 상기 송신차량의 신원기반 개인키로 전자서명을 생성하고, 전자서명이 결합된 메시지 내용을 상기 공유 비밀키 설정단계에서 계산된 비밀키로 암호화하여 페이로드(Payload)를 생성하며, 상기 소셜지점의 노변장치가 수신차량을 인증하는데 필요한 공유 비밀키에 대한 지식증명 시도값을 생성한 후 인증헤더에 포함시키고, 상기 소셜지점의 식별자와 송신차량이 지정하는 수신차량의 식별자 그리고 메시지 내용과 유효시간주기를 암호학적 해시함수(Cryptography hash function)의 입력으로 하여 해당 메시지 내용과 목적지 수신차량을 바인딩시키는 메시지 인덱스를 부가하여 상기 송신차량과 수신차량의 식별자는 메시지 꾸러미에 표시되지 않도록 하는 단계와;

차량 애드혹 네트워크 상에서 차량대 차량(V2V) 통신을 이용하여 상기 송신차량이 구성한 메시지 꾸러미(280)에 명시된 소셜지점으로 향하는 차량들의 협력에 의하여 저장-운반-전송방식으로 메시지 꾸러미(280)에 명시된 소셜지점에 설치된 노변장치까지 메시지 꾸러미(280)를 전달하는 단계와;

상기 수신차량이 소셜지점의 노변장치가 보관하고 있는 메시지 꾸러미 중에서 수신차량의 메시지 인덱스에 대응되는 정당한 수신차량임을 인증받은 후 메시지 꾸러미를 회수하는 단계와;

상기 노변장치가 보관하고 있는 메시지 꾸러미의 페이로드를 회수한 수신차량이 송신차량과의 사이에 설정된 공유 비밀키를 이용하여 암호화된 메시지 꾸러미의 페이로드를 복호화하여 상기 송신차량 식별자와 메시지 내용 그리고 송신차량의 전자서명을 추출한 후 송신차량의 전자서명을 검증하여 송신차량을 인증하되, 상기 소셜지점 노변장치로부터 수신한 암호화된 페이로드를 상기 수신차량이 송신차량의 비밀키 지식증명 시도값으로부터 설정한 송신차량과의 공유 비밀키를 이용하여 복호화하여 복원하고, 복원된 메시지 내용에서 송신차량의 식별자를 이용하여 송신차량의 신원기반 전자서명을 검증하도록 하는 메시지 복원단계를 포함하는 것을 특징으로 하는 차량 애드혹 네트워크에서의 메시지 전달방법.

청구항 2

제1항에 있어서,

상기 공유 비밀키 설정단계에서 송신차량은 암호화된 메시지 내용 전달을 위하여 자신의 신원기반 개인키와 수신차량의 공개 식별자를 이용하여 비대화식으로 수신차량과 공유할 수 있는 공유 비밀키를 설정하는 것을 특징으로 하는 차량 애드혹 네트워크에서의 메시지 전달방법.

청구항 3

제1항에 있어서,

상기 수신차량이 노변장치를 통해 메시지 꾸러미의 페이로드를 회수하는 단계에서는 상기 소셜지점의 노변장치가 상기 메시지 인덱스의 질의를 요청한 수신차량이 송신차량이 지정한 메시지 인덱스의 정당한 수신차량인지 인증하기 위하여, 상기 송신차량이 메시지 꾸러미의 인증헤더에 첨부한 공유 비밀키에 대한 지식증명 시도값을 상기 요청한 수신차량에게 제공하고;

상기 지식증명 시도값에 대하여 수신차량이 제시한 지식증명 응답을 노변장치가 비교하고 검증하도록 하여 수신차량이 자신의 차량 식별자를 노출시키지 않고서도 송신차량이 지정한 정당한 수신차량임을 증명할 수 있도록 하는 것을 특징으로 하는 차량 애드혹 네트워크에서의 메시지 전달방법.

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 차량 애드혹 네트워크에서의 메시지 전달방법에 관한 것으로, 더욱 상세하게는 컴퓨팅과 무선통신 기능을 갖춘 차량 탑재장치(OBU:On-Board Unit)를 장착한 차량들 사이의 차량 대(對) 차량(V2V:Vehicle-to-Vehicle) 통신과, 차량 대(對) 도로상에 설치된 인프라스트럭쳐(V2I:Vehicle-to-Infrastructure) 통신으로 구성되는 차량 애드혹 네트워크에서 차량들이 빈번하게 방문하거나 밀집되는 특정 구역을 일컫는 소셜지점(Social spot)에 설치된 노변장치(RSU:Road-Side Unit)를 메시지 중계노드(Relay node)로 하여, 소셜지점을 통과하는 차량들이 상기 노변장치를 통하여 메시지를 수신하는 경우에 노변장치를 통한 수신차량의 인증과정에서 수신차량의 식별자가 숨겨진 메시지 인덱스(Identity-hidden message index)기법을 이용하여, 수신차량이 자신의 식별자를 제공하지 않고서도 소셜지점의 노변장치가 보관하고 있는 메시지중에서 자신이 수신자로 지정된 메시지를 질의하고 획득하게 함으로써 통신 도청이나 패킷분석을 통해 제3자가 수신차량의 식별자를 유추하는 것을 방지토록 함과 동시에 해당 메시지 수신차량에 대한 익명성을 제공하고 프라이버시를 보호할 수 있도록 한 차량 애드혹 네트워크에서의 메시지 전달방법에 관한 것이다.

배 경 기 술

[0002] 최근, 지능형 자동차 기술과 모바일 컴퓨팅 기술의 결합으로 인하여 차량탑재장치(OBU)를 장착한 차량들간의 차량 대 차량(V2V) 통신과, 차량 대(對) 도로상에 설치된 노변장치(RSU)인 인프라스트럭쳐(V2I) 통신을 이용하여 도로상에서 차량의 안전하고 편안한 주행을 위해 교통정보서비스와 인포테인먼트(Infotainment) 서비스를 제공하기 위한 멀티-홉(Multi-Hop) 네트워크 및 차량 애드혹 네트워크 기술의 연구가 활발하게 진행되고 있다.

[0003] 상기한 멀티-홉(Multi-Hop)네트워크 서비스를 이용한 차량간 통신의 경우, 도로의 물리적 구성과 차량의 고속주행 특성으로 인하여 주변 차량들 사이에 지속적인 통신연결이 보장되지 않으므로 해당 네트워크서비스에 참여하는 원격지 차량들 사이에는 안정적인 종단간(End-to-End) 통신경로가 존재하지 않을 수도 있다는 불리함이 있다.

[0004] 반면, 실시간 속성을 엄격히 요구하지 않는 차량 애드혹 네트워크 정보서비스는 효과적인 데이터 전달을 위하여 인접한 차량들 사이의 일시적인 통신과 차량 주행경로의 특성을 고려하여 메시지의 목적지까지 저장-운반-전달(Store-Carry-Forward) 패러다임의 차량들의 협력(Coorperation)을 이용하는 지연허용 차량 네트워크(VDTNs:Vehicular Delay-Tolerant Networks) 서비스로 간주되고 있다.

이와 같은 차량 애드혹 네트워크 정보서비스와 관련하여 대한민국 공개특허공보 공개번호 제10-2006-0003756호

"애드 혹 네트워크와 기지국을 이용한 차량간 통신방법", 등록특허공보 등록번호 제10-1091787호 "차량 애드 혹 네트워크에서 적응적 브로드캐스트 방법을 수행하는 노드 장치" 등이 안출되어 있는데, 상기 "애드 혹 네트워크와 기지국을 이용한 차량간 통신방법"은 애드 혹 네트워크와 기지국을 동시에 이용함으로써 단독으로는 통신 불가능한 경우를 대비할 수 있도록 하고, 송신/수신 노드의 접속을 인접 노드, 기지국 등의 상황에 따라 세분화하여 이동성이 확보되는 차량 통신의 여러 가지 경우에 능동적으로 대비할 수 있도록 하며, 애드 혹 네트워크와 기지국 중 어느 하나를 선택함에 있어 신호의 강도에 따라 선택함으로 보다 합리적이고, 안정된 네트워크의 구성이 설정될 수 있도록 하고, 애드 혹 네트워크와 기지국을 통한 통신이 불가능한 경우 차량의 이동에 따른 새로운 접속을 계속적으로 시도함으로써 접속 실패를 방지할 수 있도록 하는 기술이다.

그리고, 상기 "차량 애드 혹 네트워크에서 적응적 브로드캐스트 방법을 수행하는 노드 장치" 는 거리 기반 브로드캐스트(DBRS) 방식 및 지역 기반 브로드캐스트(RBRS) 방식의 장점을 결합하여 변화하는 차량의 밀도에 따라 지역 기반 브로드캐스트(RBRS) 방식 및 거리 기반 브로드캐스트(DBRS) 방식을 적응적으로 선택하는 적응적 브로드캐스트 방식을 제안함으로써, 차량의 밀도에 상관 없이 우수한 브로드캐스트 성능을 제공하는 기술이다.

[0005] 그러나, 이 같은 실용적인 차량 애드혹 네트워크서비스의 구현을 위해서는 차량통신에 대한 보안을 고려하여야 하며, 특히 해당 네트워크 서비스에 참여하는 차량 및 운전자의 프라이버시를 중요하게 다루어야 한다.

[0006] 이를 위하여, 최근의 차량 애드혹 네트워크에 대한 보안연구에서는 도시환경에서 극장가나 쇼핑가와 같은 시내 주요 지점 또는 주요 도로의 톨게이트, 교차로 같이 차량의 통행량이 많거나 차량이 자주 방문하게 되는 소셜지점이라는 특정 지역에 설치된 노변장치를 메시지 중계지점으로 이용하여 데이터를 효과적으로 전달하면서 수신 차량의 프라이버시를 보호하기 위한 안전한 메시지 전달방법을 연구하고 있다.

[0007] 즉, 송신차량과 수신차량이 직접 네트워크로 연결되어 있지 않더라도 송신차량들이 자주 방문하거나 밀집되는 소셜지점에 설치되는 노변장치에게 메시지를 보관해두면 수신차량이 해당 소셜지점을 경유할 때 자신이 수신자로 지정된 메시지를 노변장치로부터 제공받도록 하는 것이다.

[0008] 도 1은 차량 애드혹(Ad-Hoc) 네트워크에서 소셜지점에 설치된 노변장치의 중계기능을 이용한 메시지 전달의 예를 나타내는 것이다.

[0009] 상기 도 1에서 차량들이 자주 방문하는 어떤 소셜지점(150)을 가정한 상태에서 어떤 송신차량(110)이 종단간 통신연결이 보장되지 않는 상태의 수신차량(130)에게 메시지를 전송하기를 원하는 경우에, 상기 송신차량(110)은 차량간 통신을 통하여 자신의 주변 차량들 중에서 소셜지점(150)을 경유하게 될 운반차량(120)을 발견한 후 상기 수신차량(130)에게 전달하고자 하는 메시지를 그 운반차량(120)에게 저장(Store)하여 해당 메시지를 소셜지점(150)으로 운반해 줄 것을 요청한다.

[0010] 상기 송신차량(110)의 요청에 따라 운반차량(120)은 송신차량(110)으로부터 자신에게 수신·저장된 메시지를 운반하여 지정된 소셜지점(150)에 도착하면, 해당 소셜지점(150)에 설치된 노변장치(140)에 메시지를 포워딩(Forwarding)하고, 상기 노변장치(140)는 수신된 메시지를 보관하였다가 나중에 소셜지점(150)을 지나는 수신차량(130)의 요청에 의해 정당한 수신차량인지의 여부를 확인하고 보관중인 메시지를 해당 수신 차량(130)에 제공하게 되는 것이다.

[0011] 이러한 소셜지점을 이용한 차량 네트워크서비스 시스템에서는 메시지의 전달시 차량의 프라이버시를 안전하게 보호할 수 있도록 하기 위한 다양한 연구들이 진행되고 있다.

[0012] 종래의 연구들은 차량의 가명(假名:Pseudonym)을 이용하여 메시지의 수신자를 지정하고, 상기의 가명을 기반으로 제공되는 익명인증서를 이용한 수신자 인증방법을 기반으로 하거나, 그룹서명(Group Signature)방법을 이용한 조건부 프라이버시 보호인증(CPPA:Conditional Privacy-Preserving Authentication)방법을 도입하고 있다.

[0013] 그러나, 상기한 가명을 기반으로 제공되는 익명인증서를 이용한 수신자 인증방법은 동일한 가명을 장시간 사용할 때 발생되는 차량의 연계(Link)와 추적(Trace)을 피하기 위하여 가명집합(Pseudonym set)을 구성하여 지속적으로 가명을 변경하여 사용해야 하며, 차량 네트워크에 참여하는 모든 차량의 가명을 사전에 알고 있어야만 하기 때문에 가명집합의 사용에 따른 익명인증서의 관리가 복잡하고 불편하다는 문제가 있다.

[0014] 또, 상기한 조건부 프라이버시 보호인증(CPPA)방법은 그룹서명 알고리즘의 많은 연산으로 인해 소셜지점의 노변장치를 통한 메시지 수신과정에서 수신차량은 노변장치와의 복잡한 인증절차를 거쳐야만 하기 때문에 시간이 많

이 소요되는 등 그 이용이 매우 불편하다는 문제가 있다.

선행기술문헌

(특허문헌 1) 대한민국 공개특허공보 공개번호 제10-2006-0003756호 "애드 혹 네트워크와 기지국을 이용한 차량 간 통신방법"

(특허문헌 2) 대한민국 등록특허공보 등록번호 제10-1091787호 "차량 애드 혹 네트워크에서 적응적 브로드캐스트 방법을 수행하는 노드 장치"

발명의 내용

해결하려는 과제

[0015] 본 발명은 이와 같은 종래의 문제점을 해결하기 위한 것으로, 그 목적은 노변장치를 통한 수신차량의 인증과정에서 수신차량의 식별자가 숨겨진 메시지인덱스(Identity-hidden message index)기법을 이용하여, 수신차량이 자신의 식별자를 제공하지 않고서도 소셜지점의 노변장치가 보관하고 있는 메시지중에서 자신이 수신자로 지정된 메시지를 질의하고 획득하게 함으로써 통신 도청이나 패킷분석을 통해 제3자가 수신차량의 식별자를 유추하는 것을 방지토록 함과 동시에 해당 메시지 수신차량에 대한 익명성을 제공하고 프라이버시를 보호할 수 있도록 한 새로운 차량 애드혹 네트워크에서의 메시지 전달방법을 제공하는 것이다.

[0016] 본 발명의 다른 목적은 신원기반의 암호기술(Identity-based cryptography)을 이용하여 송신차량과 수신차량 사이에 비대화식 키 설정(Non-interactive key agreement)기법으로 설정되는 공유 비밀키(Shared secret key)로 송신차량으로부터 전달되는 메시지를 암호화하여 오직 정당한 수신차량만이 동일한 비밀키를 계산하여 메시지를 복원할 수 있도록 함으로써 안전하게 메시지를 수신할 수 있도록 한 새로운 차량 애드혹 네트워크에서의 메시지 전달방법을 제공하는 것이다.

[0017] 본 발명의 또 다른 목적은 송신차량과 수신차량 사이에 설정된 상기 공유 비밀키에 대한 지식증명(Knowledge proof)을 이용하여 소셜지점의 노변장치에게 송신차량에 의해 지정된 메시지의 정당한 수신차량임을 증명토록 함으로써 가명의 사용에 따른 복잡한 익명인증서의 관리를 요구하지 않고서도 인증과정이 간편하고 안전하게 수행될 수 있도록 한 새로운 차량 애드혹 네트워크에서의 메시지 전달방법을 제공하는 것이다.

과제의 해결 수단

[0018] 상기의 목적을 달성하기 위하여, 본 발명은 송신차량이 소셜지점에 설치된 노변장치를 통하여 수신차량에게 메시지를 전달하도록 하는 차량 애드혹(Ad-Hoc) 네트워크에서의 메시지 전달방법에 있어서, 상기 차량 애드혹 네트워크서비스에 등록되는 차량들과 각각의 소셜지점에 설치된 노변장치들의 안전한 메시지 전달수행에 필요한 신원기반의 개인 키를 신뢰기관으로부터 발급받는 신원기반 개인키 발급단계와; 상기 소셜지점의 노변장치를 통한 메시지 전달과정에서 상기 송신차량과 수신차량 그리고 송신차량과 소셜지점의 노변장치 사이의 공유 비밀키를 각각 설정하는 공유 비밀키 설정단계와; 상기 송신차량이 자신과 수신차량 사이에 설정된 공유 비밀키를 이용하여 메시지 내용을 암호화하고, 수신차량의 식별자가 숨겨진 메시지 인덱스를 이용하여 전달하고자 하는 메시지 꾸러미(Message package)를 구성하는 단계와; 상기 송신차량이 구성한 메시지 꾸러미를 차량간 통신을 이용하여 발견한 해당 소셜지점을 경유하는 임의의 운반차량을 통하여 저장-운반한 후 소셜지점 노변장치로 메시지 꾸러미를 전송하는 단계와; 상기 수신차량이 소셜지점의 노변장치가 보관하고 있는 메시지중에서 수신차량의 메시지 인덱스에 대응되는 정당한 수신차량임을 인증받은 후 메시지를 회수하는 단계와; 상기 암호화된 메시지를 회수한 수신차량이 송신차량과의 사이에 설정된 공유 비밀키를 이용하여 암호화된 메시지를 복호화하여 상기 송신차량 식별자와 메시지 내용 그리고 송신차량의 전자서명을 추출한 후 송신차량의 전자서명을 검증하여 송신차량을 인증하는 메시지 복원단계를 포함하여 구성된다.

[0019] 본 발명의 상기 신원기반 개인키 발급단계에서 차량 애드혹 네트워크서비스에 등록되는 차량에게는 해당 차량의 등록번호를 식별자(Identity)로 하여 신뢰기관이 겹선형 그룹(Bilinear group)상에서 정의되는 수학적 연산을 기반으로 하여 생성한 차량의 신원기반 개인키가 발급되고, 소셜지점의 노변장치에게는 해당 소셜지점의 지리적 위치정보를 식별자로 하여 신뢰기관이 생성한 노변장치의 신원기반 개인키가 발급되는 특징을 갖는다.

[0020] 본 발명의 상기 공유 비밀키 설정단계에서 송신차량은 암호화된 메시지 전달을 위하여 자신의 신원기반 개인키와 수신차량의 공개 식별자를 이용하여 비대화식으로 수신차량과 공유할 수 있는 공유 비밀키를 설정하는 특징을 갖는다.

[0021] 본 발명의 상기 송신차량에 의한 메시지 꾸러미 구성단계에서 상기 송신차량은 전송 메시지에 대한 신원기반 전자서명을 생성하고, 전자서명이 결합된 메시지를 상기 공유 비밀키 설정단계에서 계산된 비밀키로 암호화하여 페이로드(Payload)를 생성하되; 상기 소셜지점의 노변장치가 수신차량을 인증하는데 필요한 공유 비밀키에 대한 지식증명 시도값을 생성한 후 인증헤더에 포함시키고; 상기 소셜지점의 식별자와 송신차량이 의도하는 수신차량의 식별자 그리고 메시지와 유효 시간주기를 암호학적 해시함수(Cryptography hash function)의 입력으로 하여 해당 메시지와 목적지 수신차량을 바인딩시키는 메시지 인덱스를 부가하여 상기 송신차량과 수신차량의 식별자는 메시지 꾸러미에 표시되지 않도록 하는 특징을 갖는다.

[0022] 본 발명의 상기 수신차량에 의한 메시지 회수단계에서는 상기 소셜지점의 노변장치가 상기 메시지 인덱스 질의를 요청한 수신차량이 송신차량이 지정한 메시지 인덱스의 정당한 수신차량인지 인증하기 위하여, 상기 송신차량이 메시지 꾸러미의 인증헤더에 첨부한 공유 비밀키에 대한 지식증명 시도값을 상기 수신차량에게 제공하고; 상기 지식증명 시도값에 대하여 수신차량이 제시한 지식증명 응답을 노변장치가 비교·검증하토록 하여 수신차량이 자신의 차량 식별자를 노출시키지 않고서도 송신차량이 지정한 정당한 수신차량임을 증명할 수 있도록 하는 특징을 갖는다.

[0023] 본 발명의 상기 수신차량의 메시지 복원단계는 상기 소셜지점의 노변장치로부터 수신한 암호화된 페이로드를 상기 수신차량이 송신차량의 비밀키 지식증명 시도값으로부터 설정한 송신차량과의 공유 비밀키를 이용하여 복호화하여 복원하고, 복원된 메시지내용에서 송신차량의 식별자를 이용하여 송신차량의 신원기반 전자서명을 검증하도록 하는 특징을 갖는다.

발명의 효과

[0024] 본 발명을 적용하면, 차량 애드혹 네트워크상에서 전달되는 메시지 꾸러미에는 차량의 식별자가 표시되지 않기 때문에 제3자가 차량 통신을 도청하더라도 메시지의 송신차량과 수신차량을 식별할 수 없게 된다.

[0025] 또, 수신차량이 공개된 소셜지점의 노변장치를 통하여 메시지를 수신하더라도 일방향성(One-way)을 가지는 암호학적 해시함수의 결과로 생성된 차량의 식별자가 숨겨진 메시지 인덱스에 의해 수신차량에 대한 식별자가 노출되지 않으므로 수신차량의 프라이버시를 보장할 수 있게 된다.

[0026] 또, 공유 비밀키 지식증명에 의해 송신차량에 의해 지정된 정당한 수신차량만이 소셜지점의 노변장치를 통해 메시지를 수신할 수 있기 때문에 종래와 같이 가명집합의 사용 및 사용되는 각각의 가명에 대응되는 복잡한 익명 인증서들의 관리가 필요하지 않으므로 시스템을 보다 효율적으로 구성할 수 있다는 효과가 있다.

도면의 간단한 설명

[0027] 도 1은 일반적인 차량 애드혹(Ad-Hoc) 네트워크에서 소셜지점에 설치된 노변장치(RSU)를 통한 메시지전달 과정

을 나타내는 구성도이다.

도 2는 본 발명에 따른 차량 애드혹 네트워크에서의 메시지 전달방법에서 송신차량이 메시지 꾸러미를 구성하는 절차를 나타내는 구성도이다.

도 3은 도 2에 나타낸 메시지 꾸러미 구성절차에 따라 최종적으로 완성된 전송 메시지의 상세 포맷을 나타내는 구성도이다.

도 4는 본 발명에 따른 차량 애드혹 네트워크에서의 메시지 전달방법에서 소셜지점의 노변장치를 통한 목적지 수신차량의 메시지 회수절차를 나타내는 구성도이다.

도 5는 본 발명에 따른 차량 애드혹 네트워크에서의 메시지 전달방법에서 수신차량이 송신차량과 비대화 방식의 공유 비밀키를 생성하는 방법을 나타내는 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0028] 이하, 첨부된 도면에 의하여 본 발명의 바람직한 실시예를 보다 상세하게 설명한다.

[0029] 도 2 내지 도 5를 참조하면, 본 발명은 차량 애드혹(Ad-Hoc) 네트워크를 통한 차량간 메시지 전달과정에서 차량 통신의 도청이나 패킷분석을 통해 제3자에게 차량의 식별자가 노출되는 것을 방지하고, 수신차량의 익명성을 보장함으로써 수신차량의 위치 프라이버시를 보호할 수 있도록 하는 것이다.

[0030] 이를 위하여, 본 발명에서는 상기 차량 애드혹 네트워크 서비스에 등록되는 차량들과 각각의 소셜지점에 설치된 노변장치들은 상호간의 안전한 메시지 전달수행을 위하여, 공신력 있는 신뢰기관으로부터 신원기반의 개인 키를 발급받게 된다(신원기반 개인키 발급단계).

[0031] 상기한 신원기반 개인키 발급단계에서 차량 애드혹 네트워크서비스에 등록되는 차량에게는 해당 차량의 차량등록번호를 식별자(Identity)로 하여 신뢰기관이 겹선형 그룹(Bilinear group)상에서 정의되는 수학적 연산을 기반으로 하여 생성한 차량의 신원기반 개인키가 발급된다.

[0032] 또, 상기 소셜지점의 노변장치에게는 해당 소셜지점의 지리적 위치정보를 식별자로 하여 신뢰기관이 생성한 노변장치의 신원기반 개인키가 발급된다.

[0033] 이 때, 상기 차량 애드혹 네트워크서비스에 등록되는 차량의 차량등록번호와 소셜지점에 설치되는 노변장치의 위치정보는 각각 자신들의 신원기반 개인키에 대응되는 공개키가 된다.

[0034] 이와 같이 신뢰기관으로부터 신원기반 개인키가 발급된 상태에서 소셜지점에 설치된 노변장치를 통하여 차량간 메시지를 전달하고자 하는 경우, 메시지를 전달하는 송신차량과 메시지를 전달받는 수신차량 및 송신차량과 수신차량 사이에서 메시지를 중계하는 역할을 하는 소셜지점의 노변장치는 각각 상호간에 공유할 수 있는 비밀키를 설정한다(공유 비밀키 설정단계).

[0035] 상기 공유 비밀키 설정단계에서 송신차량은 암호화된 메시지 전달을 위하여 자신의 신원기반 개인키와 수신차량의 공개 식별자를 이용하여 비대화식으로 수신차량과 공유할 수 있는 공유 비밀키를 설정하게 된다.

[0036] 이와 같이 송신차량과 수신차량 사이에 공유 비밀키가 설정된 상태에서 도 2에 도시된 바와 같이, 상기 송신차량은 자신과 수신차량 사이에 설정된 공유 비밀키를 이용하여 메시지 내용을 암호화하고, 수신차량의 식별자가 숨겨진 메시지 인덱스를 이용하여 전달하고자 하는 메시지 꾸러미(Message package)를 구성한다(메시지 꾸러미 구성단계).

[0037] 상기의 메시지 꾸러미 구성절차를 보다 상세하게 설명하면, 상기의 도 2에서와 같이 송신차량이 수신차량에게 메시지내용(210)을 안전하게 전달하기 위하여 먼저 신뢰기관으로부터 발급받은 송신차량의 신원기반 개인키(220)로 전자서명(230)을 생성한다.

[0038] 또, 상기 송신차량이 지정하는 메시지 수신차량의 식별자(240a)를 이용하여 신원기반의 비대화식 공유 비밀키 설정알고리즘으로 수신차량과의 공유 비밀키(250a)와 수신차량의 인증에 사용될 비밀키의 지식증명에 대한 시도값(250b)을 설정하고, 공유 비밀키(250a)를 이용하여 메시지 내용(210)과 전자서명(230)에 대한 암호화된 페이로드(260)를 생성한다.

[0039] 또, 상기 수신차량의 식별자(240a)와 소셜지점 식별자(240b)에 대한 현재 메시지 시간주기의 암호학적 해시함수의 결과로 메시지 인덱스(270)를 생성한 후, 암호화된 페이로드(260)에 메시지 인덱스(270)와 소셜지점 식별자

(240b)를 결합하여 도 3에 도시된 바와 같은 소셜지점으로 전달되는 메시지 꾸러미(280)를 구성하게 되는 것이다.

[0040] 이 과정에서 상기 송신차량과 수신차량의 식별자는 메시지 꾸러미(280)에 표시되지 않게 된다.

[0041] 상기 메시지 꾸러미(280)의 세부 포맷은 도 3에 도시된 바와 같이, 인증헤더(310) 부분에 추후 소셜지점의 노변장치에서의 수신차량의 인증에 사용될 공유 비밀키의 지식증명 수행에 필요한 지식증명 시도값(250b)이 포함된다.

[0042] 한편, 상기한 송신차량에 의하여 구성된 메시지 꾸러미(280)는 차량 애드혹 네트워크상에서 차량대 차량(V2V) 통신을 이용하여 메시지 꾸러미(280)에 명시된 소셜지점으로 향하는 차량들의 협력에 의하여 저장-운반-전송방식으로 해당 소셜지점에 설치된 노변장치까지 전달된다(메시지 꾸러미 전송단계).

[0043] 이 때, 차량 통신 기반의 저장-운반-전송방식을 이용하는 메시지 전달방법으로서 VADD(Vehicle Assisted Data Delivery) 또는 TBD(Trajectory-based Data Forwarding)와 같은 차량 애드혹 네트워크 라우팅방법이 적용될 수 있다.

[0044] 이와 같이 하여 해당 소셜지점의 노변장치에 송신차량이 전달한 메시지 꾸러미가 전송되면, 해당 노변장치는 자신의 저장소에 수신된 메시지꾸러미를 보관하고, 도 4에 도시된 바와 같이 상기 수신차량은 노변장치와의 인증절차를 통하여 노변장치가 보관하고 있는 메시지 꾸러미중에서 자신의 메시지 인덱스에 대응되는 정당한 수신차량임을 인증받은 후 메시지를 회수하게 되는 것이다(메시지 회수단계).

[0045] 상기한 메시지 회수단계에서는 송신차량에 의해 메시지 꾸러미에 첨부된 비밀키에 대한 지식증명 시도값(Challenge)으로부터 수신차량이 송신차량과 비대화 방식으로 공유 비밀키를 설정하고, 설정된 공유 비밀키에 대한 지식증명값을 소셜지점의 노변장치에게 증명하면, 수신차량이 노변장치에게 자신의 차량 식별자를 노출시키지 않고서도 송신차량이 지정한 정당한 수신차량임을 인증받게 되는 것이다.

[0046] 즉, 도 4에 도시된 바와 같이, 소셜지점을 통과하는 어떤 수신차량(410)이 자신이 수신자인 메시지 꾸러미를 소셜지점 노변장치(420)가 보관하고 있는지 여부를 확인하고자 하는 경우에, 상기 수신차량(410)은 자신의 식별자와 해당 소셜지점의 식별자를 암호학적 해시함수를 이용하여 현재 시간 주기에 유효한 메시지 인덱스를 생성하고, 해당 노변장치(420)에게 메시지 인덱스의 저장여부를 질의(430a)한다.

[0047] 이 같은 수신차량(410)의 질의에 대해 해당 노변장치(420)는 도 5에서와 같이, 자신의 저장소에서 해당 메시지 인덱스를 검색(430b)하고, 메시지 인덱스에 대응되는 메시지 꾸러미가 발견되면 수신차량(410)이 정당한 수신차량인지 인증하기 위해 인증헤더에 포함되어 있는 송신차량이 첨부한 비밀키 지식증명 시도값을 수신차량(410)에게 전송하여 비밀키 지식증명을 요구(440b)한다.

[0048] 이에 대해 상기 수신차량(410)은 도 5에서와 같이, 해당 노변장치(420)가 제시한 비밀키 지식증명 시도값과 자신의 신원기반 개인키를 이용하여 송신차량과 비대화 방식의 공유 비밀키를 설정(440a)하고, 상기 비밀키에 대한 지식증명값을 계산하여 노변장치(420)에게 응답(450a)한다.

[0049] 상기 요청 차량(410)의 응답(450a)을 수신한 노변장치(420)는 인증헤더에 포함되어 있는 송신차량이 제공한 지식증명 시도값과 메시지 수신차량(410)의 지식증명 응답값을 서로 검증하여 메시지 수신차량(410)의 정당성을 검증(450b)한다.

[0050] 이 과정에서 만일 검증에 성공하면 노변장치(420)는 메시지 인덱스에 대응되는 메시지 꾸러미의 페이로드를 수신차량(410)에게 제공(460b)한다.

[0051] 이렇게 하여 노변장치로부터 암호화된 페이로드를 회수한 수신차량(410)은 상기 송신차량과의 공유 비밀키 설정단계(440b)에서 생성된 비밀키를 이용하여 암호화된 페이로드를 복호화(460a)한 후 복호화된 메시지에 포함된 송신차량의 식별자로 송신차량의 신원기반 전자서명을 검증(470a)함으로써 송신차량에 대한 인증과 메시지 무결성을 확인하고 메시지 수신을 완료하게 되는 것이다.

부호의 설명

[0052] 210 : 메시지 내용 260 : 암호화된 페이로드

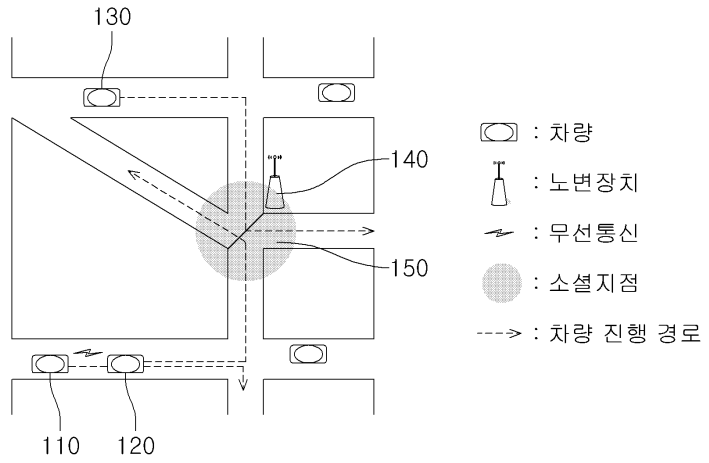
270 : 메시지 인덱스　　280 : 메시지 꾸러미

310 : 인증헤더　　410 : 수신차량

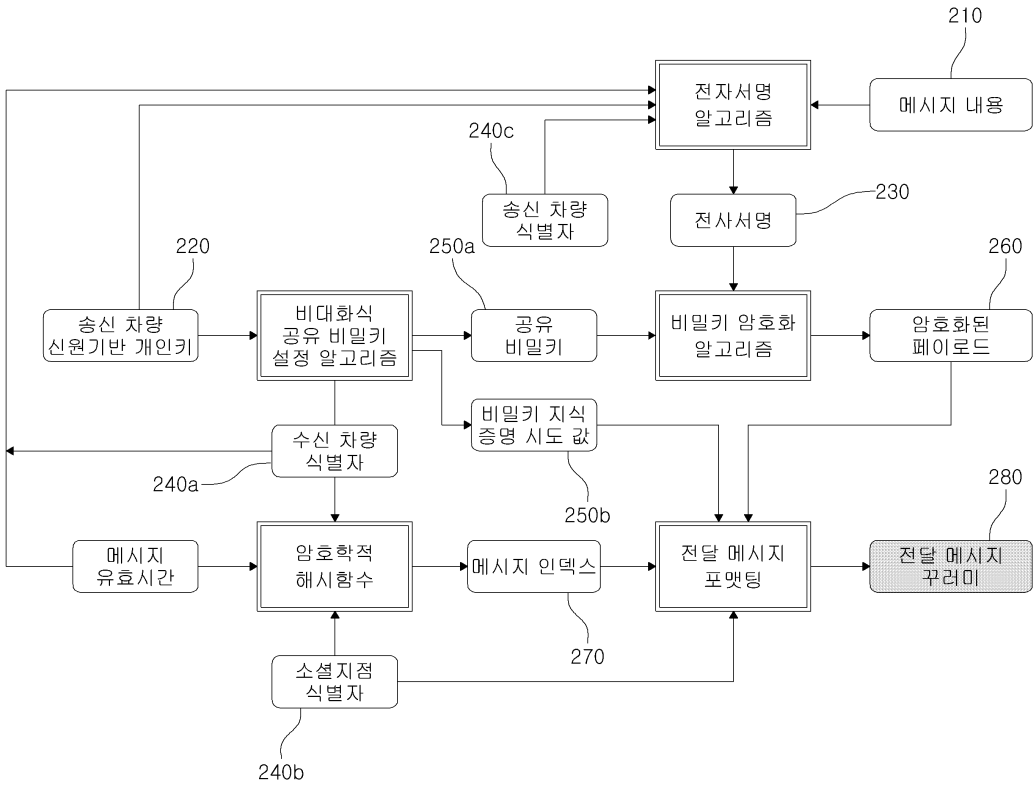
420 : 노변장치

도면

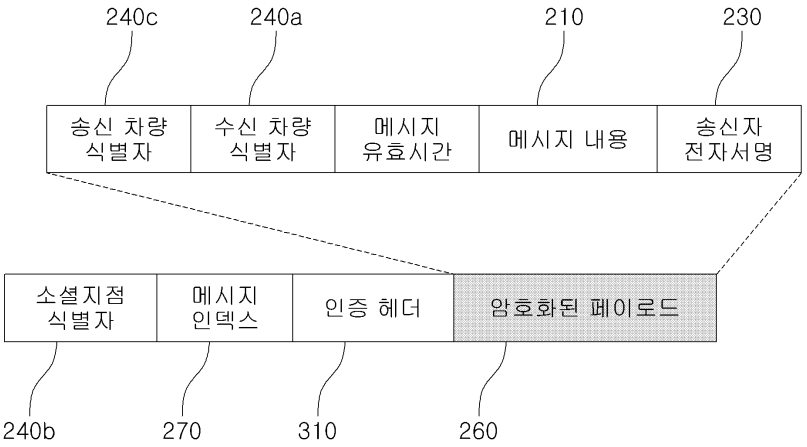
도면1



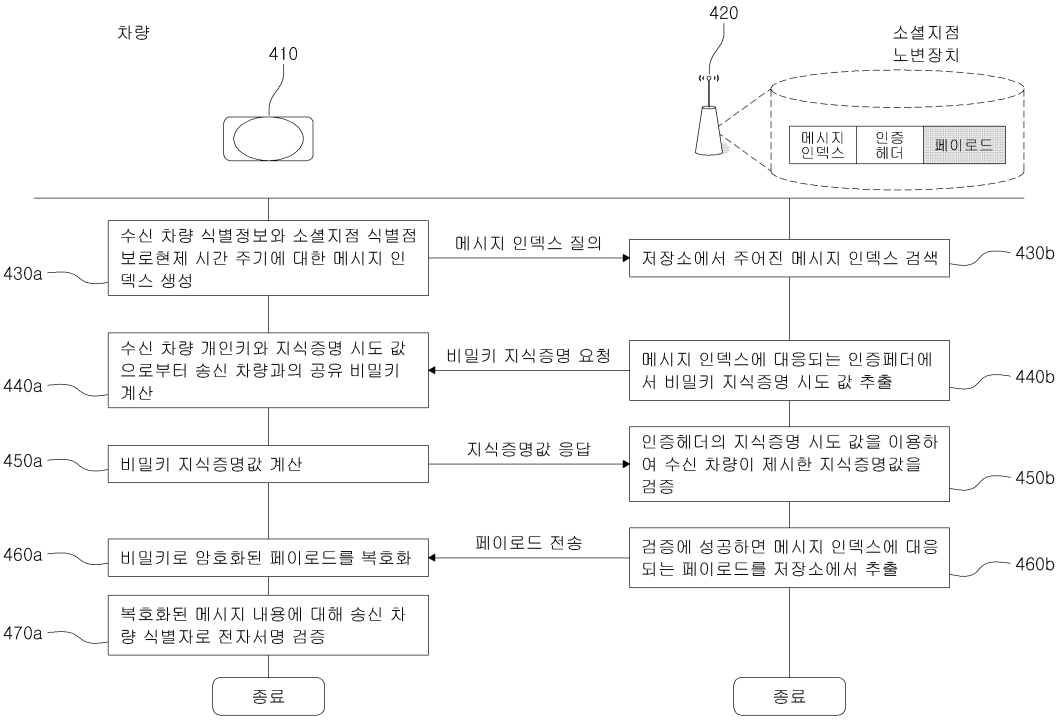
도면2



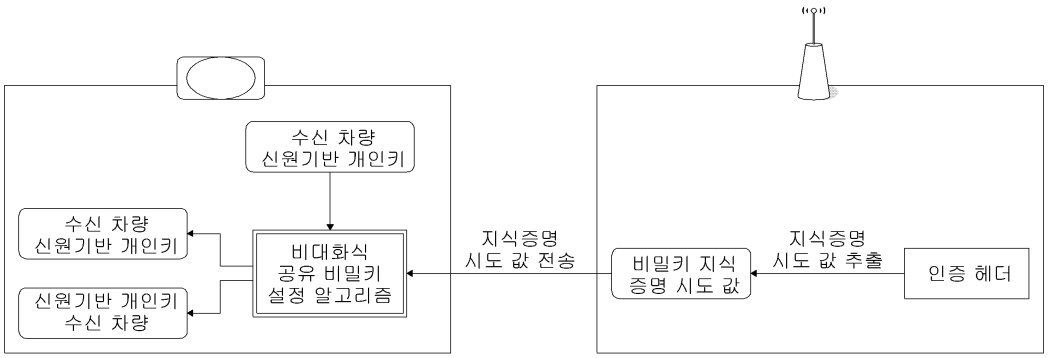
도면3


240c
240a
210
230
송신 차량 식별자
수신 차량 식별자
메시지 유효시간
메시지 내용
송신자 전자서명
소셜지점 식별자
메시지 인덱스
인증 헤더
암호화된 페이로드
240b
270
310
260

도면4


차량
410
420
소셜지점 노변장치
메시지 인덱스
인증 헤더
페이로드
수신 차량 식별정보와 소셜지점 식별정보로현제 시간 주기에 대한 메시지 인덱스 생성
430a
메시지 인덱스 질의
저장소에서 주어진 메시지 인덱스 검색
430b
수신 차량 개인키와 지식증명 시도 값으로부터 송신 차량과의 공유 비밀키 계산
440a
비밀키 지식증명 요청
메시지 인덱스에 대응되는 인증페더에서 비밀키 지식증명 시도 값 추출
440b
비밀키 지식증명값 계산
450a
지식증명값 응답
인증헤더의 지식증명 시도 값을 이용하여 수신 차량이 제시한 지식증명값을 검증
450b
비밀키로 암호화된 페이로드를 복호화
460a
페이로드 전송
검증에 성공하면 메시지 인덱스에 대응되는 페이로드를 저장소에서 추출
460b
복호화된 메시지 내용에 대해 송신 차량 식별자로 전자서명 검증
470a
종료
종료

도면5


수신 차량 신원기반 개인키
수신 차량 신원기반 개인키
신원기반 개인키 수신 차량
비대화식 공유 비밀키 설정 알고리즘
지식증명 시도 값 전송
비밀키 지식 증명 시도 값
지식증명 시도 값 추출
인증 헤더