VANET 환경에서 신뢰적인 에이전트 선출을 이용한 Safe-Tunneling Zone

오하나○ 김아란 신용태
숭실대학교
{hnoh○, arkim}@cherry.ssu.ac.kr shin@ssu.ac.kr

Safe-Tunneling Zone using election the reliable agent in VANET

Ha-Na Oh○ A-Ran Kim Young-Tae Shin
SoongSil Univ.

요 약

본 논문은 Vehicular Ad-hoc Network(VANET)환경에서 V2V간의 신뢰적 통신을 지원하기 위해 Safe-Tunneling Zone을 제안한다. 기존의 무선 환경에서는 신뢰적인 경로산출을 위해 ARAN에서 제안된 hop-by-hop 인증을 사용하여 신뢰성은 충족되나 많은 시간과 자원을 소비하는 단점이 있다. 그러나 본 논문에서 제안한 Safe-Tunneling Zone은 송·수신 하고자하는 차량이 각각 신뢰적 에이전트를 선택하고, 선택된 에이전트는 서로의 ID, Rn을 바탕으로 생성된 세션키를 교환함으로서 상호간의 인증을 수행한다. 이와 같이 본 논문에서는 Safe-Tunneling Zone을 통해 기존의 신뢰적 경로 산출 기법보다 수행과정 절차의 간소화, 자원소비 감소, 종단 간의 신뢰적 경로를 통한 데이터의 기밀성 또한 제공 가능하도록 한다.

1. 서 론

Vehicular Ad-hoc Network(VANET)은 차량에 임베디드 컴퓨터(Embedded computer), GPS(Global Positioning System), 근거리 무선장치(Short-range wireless network interface) 기술을 통합하여 OBU(On-Board Unit) 형태로 설치가 가능하게 되면서 기존의 인터넷 환경의 XML과 HTML로 구성된 컨텐츠 서비스가 V2I(Vehicle-to-Infrastructure) 기반에서 RSU(Road Side Unit)를 통하여 주행하는 차량 내에서 무선통신을 통해 제공될 수 있게 되었다. 또한, V2V(Vehicle-to-Vehicle)기반에서는 차량 간의 통신으로 차량 안전과 관련한 정보교환 서비스를 가능하게 하였다[1][2].

위와 같이 차량 네트워크 환경에서 다양한 통신 서비스가 증가함에 따라 보안 문제도 증가하고 있으며, VANET은 무선 네트워크의 속성으로 무선 네트워크 환경에서 존재하는 보안 문제 또한 그대로 가지고 있다[3]. 이러한 차량 간 전송되는 메시지의 위변조와 손실, 프라이버시 침해와 같은 보안 문제에 대한 연구가 선행되어지지 않는다면 해당 차량의 사고나 오작동을 유발한다. 따라서 본 논문에서는 송·수신 차량의 신뢰적인 메시지 전송을 위해 Safe-Tunneling Zone을 제안하였다. 제안된 Safe-Tunneling Zone은 각 차량의 인증을 위해 ID, 인증서, 세션키 등을 이용해 Tunneling을 구성하여 차량 간 신뢰적인 전송을 위한 방법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로서 ARAN 및 Mobile IP에 대해 살펴보고, 3장에서는 본 논문에서 제안하는 Safe-tunneling Zone의 구성 및 절차에 대해 설명한다. 마지막으로 4장에서 결론을 맺는다.

2. 관련연구

2.1 ARAN

Authenticated Routing for Ad hoc Networks(ARAN)은 AODV(Ad hoc On-demand Distance Vector) 라우팅 프로토콜 기반으로 Asymmetric key를 이용한 서명과 인증서를 통해 매 Hop마다 인증과정을 수행하여 각각의 노드 간에 인증을 확인하는 기법이다[4]. ARAN의 동작과정은 Certification, Authenticated route discovery, Authenticated route setup, Route maintenance, Key revocation 과정으로 수행된다. ARAN은 신뢰성이 입증된 인증서 발급 Server T가 존재한다고 가정하며, Node A는 Server T에게 인증서 발급을 요청한다. Server T는 Node A 일련의 과정을 거쳐 인증서를 발급한다. 이때, Node A는 목적지 X로 가기위해 목적지 X의 IP, A의 인증서 및 난수를 A의 개인키로 서명하여 이웃노드들에게 브로드캐스트 한다. A의 브로드캐스트를 받은 Node B는 A의 공개키를 사용하여 A의 서명을 확인한 후 Node B는 브로드캐스트 된 패킷의 역 경로를 저장한다. Node B는 패킷에 B의 개인키를 사용한 서명과 B의 인증서를 추가하여 이웃 Node에게 다시 브로드캐스트 하며, B의 브로드캐스트를 받은 Node C는 B의 공개키를 사용하여 B의 서명을 확인한다. 이 과정을 반복수행하여 목적지 X까지 도달하게 된다.

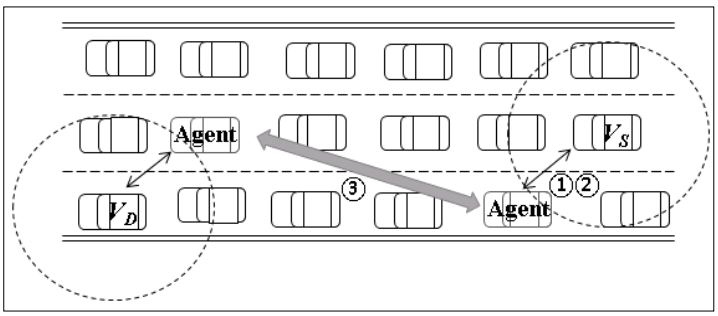
2.2 Mobile IP

Mobile IP(Internet Protocol)는 사용자가 다른 네트워크로 이동하여도 기존 서비스를 Seamless하게 지원 받

을 수 있도록 해준다[5]. 인터넷 표준을 관리하는 Internet Engineering Task Force(IETF)의 워킹그룹에서 제안되어 표준화를 진행하고 있다. Mobile IP의 동작과정은 Mobile Node(MN)가 Home 네트워크에서 다른 네트워크로 이동하게 되면 MN가 Move detection, Agent discovery, Registration 단계를 수행하며 Foreign Agent(FA)에서 등록을 하게 된다. 이때 MN는 Home Agent(HA)에게 Care of Address(CoA)를 전송하여 이동을 알림과 동시에 MN에게 온 패킷을 현재 Agent인 FA에게 전송해 줄 것을 요청한다. HA가 요청을 승낙하게 되면 HA와 FA는 Tunneling을 구성한다. 구성 후 목적지를 MN로 한 packet을 전송 시 HA는 IP 데이터그램을 IP within IP, 최소 인캡슐레이션, GRE 방법을 사용하고, FA에게 packet을 전송하여 최종목적지인 MN에게 전송된다.

3. Safe-Tunneling Zone

본 장에서는 VANET 환경에서 차량이 신뢰적 경로를 기반으로 안전한 데이터 전송을 위해 Safe-Tunneling Zone(STZ)을 제안 하였다. (그림 1)은 제안하는 STZ의 구성도를 보여준다. STZ의 구성환경은 고속도로와 같이 방향성이 일정한 차량으로 이루어진 환경이다. 모든 차량은 동일한 방향성을 가지며, 사전에 CA(Certification Authority)로부터 인증서와 공개키를 교환 하였다.



(그림 1) VANET의 Safe-Tunneling Zone의 구성도

제안하는 STZ의 구성절차는 차량 간 초기인증, 에이전트 선출 및 인증, 에이전트 간 인증으로 구성된다.

첫째, 차량 간 초기인증단계는 데이터 송·수신을 원하는 차량(V_S, V_D)간의 초기 인증을 수행한다. 둘째, 에이전트 선출 및 인증단계에서는 차량이 에이전트를 선출하기 위해 등록요구 메시지를 브로드캐스트 하고, 등록요구 메시지에 대해 가장 먼저 등록응답을 한 에이전트를 선출한다. 선출된 에이전트를 차량이 인증하기 위해 에이전트 ID, $Cert$, Rn_i을 이용하여 유효성 검증을 통해 에이전트를 인증을 하고, 인증응답 메시지를 에이전트에게 전송한다. 마지막으로 에이전트 간의 인증단계에서는 차량과 에이전트 간 인증단계에서 사용된 Rn_i을 선택한다. 각 에이전트가 선택한 $Rn1$, $Rn2$을 MD5 hash 함수를 이용 해 세션키 STK을 생성하고, 생성된 STK을 교환함으로 상호간 인증을 한다. 위 세 단계의 구성절차에 사용된 Frame format은 (그림 2)과 같다.

TYPE	Initial time	ID	Random number	SPI	Payload	Trailer

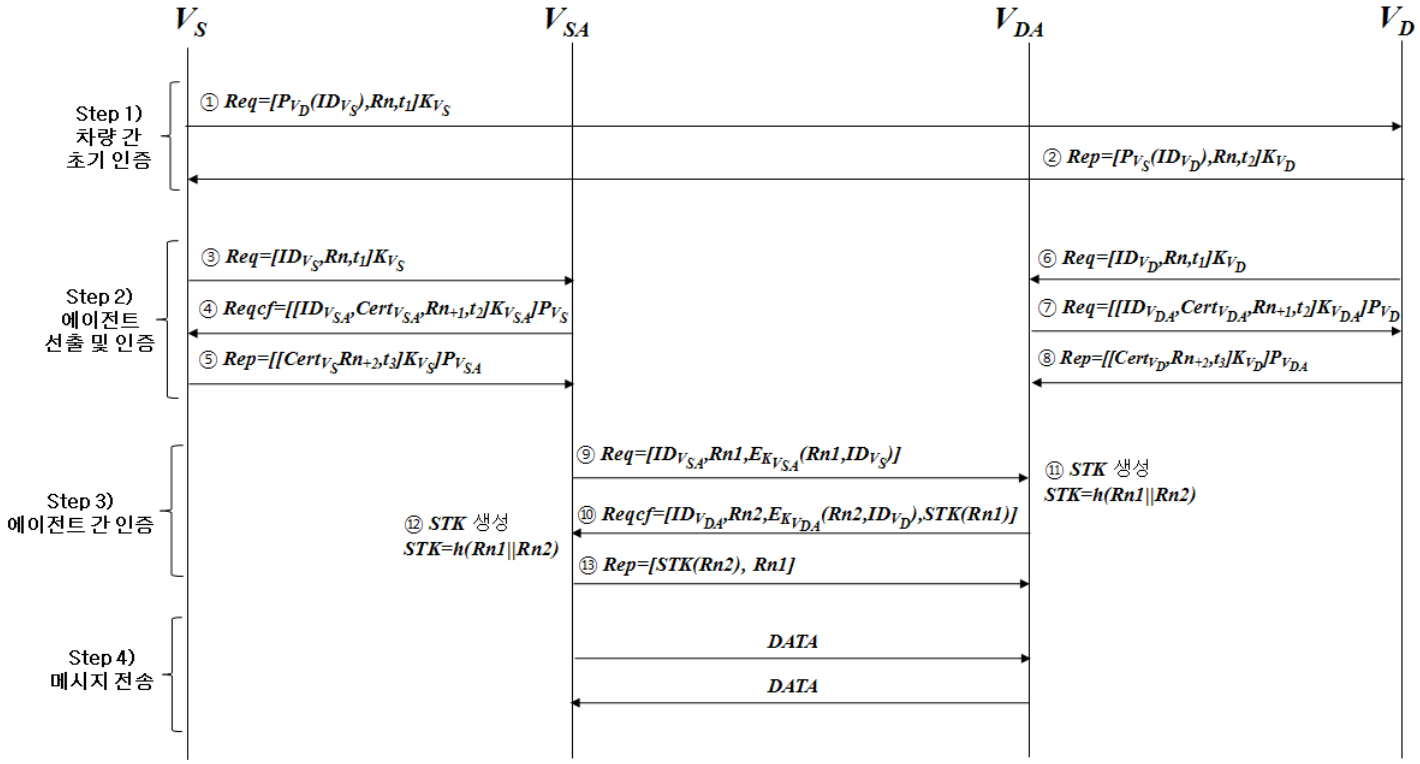
(그림 2) 에이전트 선출을 위한 Frame format

- TYPE
  1. 등록요구 : 차량이 에이전트를 선출하기위한 메시지
  2. 등록응답 : 차량의 등록요구에 대한 응답메시지
  3. 인증응답 : 에이전트의 등록 응답에 대해 차량이 에이전트를 인증 후 연결을 위해 하는 응답 메시지
  4. 메시지 전송 : 에이전트 간 Safe-Tunneling을 연결 후 차량 간 전송할 데이터
- Initial time : 차량이 등록요구 시 생성한 초기 시간
- ID : 차량 고유 식별자
- Random number(Rn) : 임의의수
- SPI : 보안 매개변수 인덱스
- Payload : 전송할 데이터
- Trailer : 에러 탐지를 위한 CRC
- Reservation : 예약필드

본 논문에서 사용되는 용어들의 표기법은 (표 1)과 같다.

(표 1) 표기법

표 기	정 의
V_S, V_D	차량 S, D
V_{SA}, V_{DA}	V_S와 V_D의 에이전트
ID_{V_X}	차량 고유 식별자(Unique identifier)
$Cert$	인증서
K_X	비밀키
P_X	공개키
STK	V_{S_A}와 V_{D_A}의 세션키
Rn_i	임의의 수
t_i	타임스탬프 값
EK_{V_X}	개인키 암호화
$h[\,]$	MD5 해시 함수



(그림 3) 제안하는 Safe-Tunneling Zone 메시지 흐름

3.1 차량 간 초기 인증

데이터 송·수신을 하기위한 차량 V_S와 V_D은 (그림 3)의 Step 1)과 같이 초기인증을 수행한다. 초기인증을 위해 공개키, 개인키, ID, Rn_i, t_i을 이용한다.

- V_S와 V_D의 초기인증 절차

① $V_S \rightarrow V_D$: $[P_{V_D}(ID_{V_S}), Rn, t_1]K_{V_S}$

② $V_S \leftarrow V_D$: $[P_{V_S}(ID_{V_D}), Rn, t_2]K_{V_D}$

3.2 신뢰적 에이전트 선출 및 인증

V_S와 V_D가 에이전트를 선출 및 인증하는 절차는 등록요구, 등록응답, 인증응답으로 이루어진다. V_S와 V_D가 에이전트를 선출하기 위해 등록요구 메시지 필드의 Initial time을 생성하여 이웃해 있는 차량들에게 브로드캐스트를 한다. 등록요구 메시지를 받은 차량들은 등록응답 메시지를 전송하며, 먼저 전송 한 차량들에 대해 에이전트로 선출된다. 세부 절차는 Step 2와 같다.

- 에이전트 선출 및 인증

③ $V_S \rightarrow V_{SA}$:

등록요구, Initial time, ID, Rn, Reservation, Trailer

$[ID_{V_S}, Rn, t_1]K_{V_S}$

④ $V_S \leftarrow V_{SA}$:

등록응답, Initial time, ID, Rn, SPI{P_X, $Cert$, MD5 hash}, Trailer

$[ID_{V_{SA}}, Cert_{V_{SA}}, Rn_{+1}, t_2]K_{V_{SA}}]P_{V_S}$

⑤ $V_S \rightarrow V_{SA}$:

인증응답, Initial time, ID, Rn, SPI{P_X, $Cert$, MD5 hash}, Trailer

$[Cert_{V_S}, Rn_{+2}, t_3]K_{V_S}]P_{V_{SA}}$

V_D와 V_{DA}도 위 와 같은 절차로 ⑥, ⑦, ⑧을 수행한다.

3.3 에이전트 간 인증

에이전트 간 인증을 위하여 Step3 ⑨와같이 V_{SA}는 V_S와의 인증 시 사용하였던 $Rn1$을 선택하여 V_S의 ID와 함께 암호화 하여 전송한다. 메시지를 받은 V_{DA}는 V_{SA}의 공개키로 복호화 하여 $K_{V_{SA}}$로 암호화 되어있는

$Rn1$ 과 V_{SA}가 대리인으로 맡고 있는 V_S의 ID가 동일한지 확인 후 V_D와 인증 시 사용하였던 $Rn2$을 선택하여 $Rn1$과 MD5 hash로 세션키 STK을 생성한다. V_{DA}는 $Rn2$와 V_D의 ID를 $K_{V_{SD}}$로 암호화하고, 생성된 STK로 $Rn1$을 암호화하여 메시지를 전송한다. V_{DA}로부터 메시지를 전달받은 V_{SA}는 복호화 하여 $Rn2$을 확인하고, ⑩과 같이 동일한 방법으로 STK을 생성하여 STK로 암호화한 $Rn1$을 확인하여 값이 맞으면 V_{DA}을 인증한다. V_{SA}은 인증응답으로 STK로 $Rn2$을 암호화하여 전송하면 V_{DA} 또한 메시지 확인 후 V_{SA}을 인증한다.

● 에이전트 간 인증

⑨ $V_{SA} \rightarrow V_{DA}$:
등록요구, Initial time, ID, Rn, SPI{MD5 hash}, Trailer
$[ID_{V_{SA}}, Rn_1, E_{V_{K_{SA}}}(Rn_1, ID_{V_S}]$

⑩ V_{DA} : $STK = h(Rn_1 \| Rn_2)$

⑪ $V_{SA} \leftarrow V_{DA}$:
등록응답, Initial time, ID, Rn, SPI{MD5 hash}, Trailer
$[ID_{V_D}, Rn_2, E_{V_{K_{DA}}}(Rn_2, ID_{V_D}), STK(Rn1)]$

⑫ V_{SA} : $STK = h(Rn_1 \| Rn_2)$

⑬ $V_{SA} \rightarrow V_{DA}$:
인증응답, Initial time, ID, Rn, Trailer
$[STK(Rn_2), Rn_1]$

위와 같은 방법으로 신뢰적인 에이전트 간 인증을 통하여 Safe-Tunneling을 구성하였고, V_S와 V_D간 메시지 전송은 Step4의 ⑭, ⑮와 같은 절차로 수행된다.

● 차량 간 메시지 전송

⑭ $V_{SA} \rightarrow V_{DA}$: 메시지전송, Initial time, ID, Rn, Payload, Trailer

⑮ $V_{SA} \leftarrow V_{DA}$: 메시지전송, Initial time, ID, Rn, Payload, Trailer

V_S와 V_D가 초기인증을 통해 서로를 인증하고, V_S와 V_{SA}, V_D와 V_{DA}가 인증하였다. 또한 V_{SA}와 V_{DA}가 인증함으로써 $V_S = V_{SA} = V_{DA} = V_D$와 같이 신뢰적인 경로를 기반으로 한 안전한 데이터 전송을 가능하도록 하였다.

4. 결 론

본 논문에서는 Vehicular Ad-hoc Network(VANET) 환경에서 V2V간의 신뢰적 통신을 지원하기 위해 Safe-Tunneling Zone을 제안하였다. 기존의 무선 환경에서는 신뢰적인 경로산출을 위해 ARAN에서 제안된 hop-by-hop 인증을 사용하여 신뢰성은 충족되었으나 많은 시간과 자원을 소비하는 단점이 있었다. 그러나 본 논문에서 제안한 Safe-Tunneling Zone은 송·수신 하고자 하는 차량에서 각각 신뢰적 에이전트를 선택하고, 선택된 에이전트는 서로의 ID, Rn을 바탕으로 생성된 세션키를 교환함으로써 서로간의 인증을 수행하였다. 이와 같이 본 논문에서 제안된 Safe-Tunneling Zone는 기존의 신뢰적 경로 산출 기법보다 수행과정 절차의 간소화와 그로인한 자원의 소비가 감소하고, 종단간의 신뢰적 경로를 통한 데이터 기밀성 또한 제공 가능하도록 하였다. 향후에는 메시지 전송 절차에서 IP within IP, 최소 인캡슐레이션 방법을 사용하여 메시지 전송의 보안을 더욱 향상시키는 연구가 이루어져야 할 것이다.

참고문헌

[1] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular Ad Hoc Networks(VANETs): Challenges and Perspectives," Proc. of Intl. Conf. on ITS Telecommunications (ITST), pp. 761-766, Jun. 2006.

[2] M. L. Sichitiu and M. Kihl, "Inter-vehicle communication systems: a survey," IEEE Communications Surveys & Tutorials, Vol. 10, Issue 2, pp. 88-105, 2008.

[3] M. Raya and J. P. Hubaux, "Securing Vehicular ad hoc networks," Journal of Computer Security, Vol. 15, pp. 39-68, 2007.

[4] Kimaya Sanzgiri, Daniel Laflamme, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer. "Authenticated Routing for Ad Hoc Networks," Selected Areas in Communications, IEEE Journal on Vol. 23, No. 3, pp. 598-610, 2005.

[5] C. E. Perkins, "IP Mobility Support for IPv4," IETF RFC 3344, Aug. 2002.