VANET환경에서의 그룹서명기반 V2V 메시지 인증 기법

김수현, 박두순*, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[kimsh, parkds, imylee]@sch.ac.kr

V2V message authentication scheme based on group signature in VANET

Su-Hyun Kim, Doo-Soon Park, Im-Yeong Lee
Department of Computer Software Engineering, Soonchunhyang University

요 약

VANET(Vehicular Ad-hoc Network)의 V2V 통신의 경우 차량 간의 안전한 통신을 위해 차량 인증 및 조건부 프라이버시 보호를 제공하기 위해서 그룹 서명 기법을 사용한 보안 기술들이 다양하게 연구되고 있다. 하지만 VANET은 MANET과 달리 빠른 이동성을 가지는 노드의 특성상 그룹 구성원의 가입과 탈퇴가 빈번하다는 문제점을 가지고 있다. 본 논문에서는 그룹 구성원의 빈번한 가입과 탈퇴를 방지하기 위해 VANET 환경에 적합하고, 그룹 관리자에 의해 생성되는 차량 개인서명키에 대한 키 위탁문제를 해결하기 위한 그룹서명방식을 제안한다.

1. 서론

최근 IT기술을 차량에 접목시키려는 노력이 가속화되고 있다. VANET(Vehicular Ad-hoc Network)은 MANET(Mobile Ad-hoc Network)의 한 형태로, 일반적으로 V2V(Vehicle to Vehicle)통신과 V2I(Vehicle to Infrastructure) 통신으로 구분된다. V2V통신은 모든 정보가 운전자의 안전에 치명적인 영향을 끼치게 됨으로써 다양한 보안요구사항을 만족하기 위해 그룹 서명 기법을 사용한 보안 기술들이 다양하게 연구되고 있다. 하지만 기존의 그룹 서명 기법을 VANET환경에서 적용하기에는 여러 가지 문제점을 가지고 있다. VANET은 MANET과 달리 노드가 빠른 속도로 이동하기 때문에 그룹 구성원의 빈번한 가입 및 탈퇴에 따른 통신 오버헤드가 매우 높고, 계산 효율성이 낮다는 문제점을 가지고 있다.

이에 따라 본 논문에서는 빈번한 그룹 가입 및 탈퇴를 방지하기 위해 차량의 속도를 고려한 일정 시간 간격의 가입요청 메시지를 적용하여 그룹 서명 방식을 제안하였다.

2. 보안 요구 사항

VANET에서는 안전한 차량 네트워크 서비스를 제공하기 위해서 다음과 같은 보안 요구 사항을 만족해야 한다.

・인증 : 차량 간 송수신되는 메시지에 대한 출처가 정당한 그룹 구성원이라는 것을 검증 할 수 있어야 한다.

・추적성 : 차량 메시지에 의한 분쟁 발생 시 그룹 관리자 비밀키에 의해 서명으로부터 신원추적이 가능해야 한다.

・조건부 프라이버시 : 메시지에 대한 출처를 제 3자가 알 수 없어야 한다. 이러한 프라이버시 제공 기술뿐만 아니라 분쟁이 발생할 경우 그룹 서명된 메시지는 그룹 관리자에 의해 개봉되어 신분을 확인 할 수 있어야 한다.

3. 제안방식

3.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템 계수를 사용하여 프로토콜을 설계한다.

ID_* : 차량 *의 식별자	P : 타원곡선상 위의 점
p : 소수 ≥ 512bit	Y_{GA} : 그룹서명키
q : 소수 ≥ 160bit	d_* : 차량 *의 개인서명키
s : 그룹 비밀키	$H()$: 일방향 해쉬 함수
T_{exp} : 차량공개키 유효시간	T_i : i번째 가입요청 메시지

3.2 그룹 가입 및 개인서명키 분배 단계

Step 1: 차량 그룹 관리자는 그룹 구성원의 개인서명키와 그룹 서명키를 안전하게 전송하기 위해 아래와 같은 각 정보를 구성한다.

- $n=p \cdot q$, $e \cdot d=1 (\mathrm{mod}\ \varnothing(n))$

* 교신저자 : parkds@sch.ac.kr

- 공개 정보 : n, e
- 비밀 정보 : p, q, d
- 그룹비밀키 : $s \in Z_q^*$
- 그룹서명키 : $Y_{GA}=sP$

Step 2: 그룹에 등록하고자 하는 차량v는 자신의 식별정보와 그룹가입 요청메시지를 일정 시간간격으로 보내게 된다.

- ID_v , T_{first}
- ID_v , T_{second}

Step 3: 그룹 관리자는 사용자의 식별정보와 가입요청메시지를 확인 후 가입 허가 메시지를 차량v에 전송한다.

- $ID_{GA}||ID_V||P$

Step 4: 차량 v는 개인서명키 생성을 위해 차량 그룹관리자가 알 수 없는 랜덤값 r을 선택 후 δ값을 계산한다. 차량 그룹관리자의 공개정보 값으로 지수승연산 후 그룹관리자에게 전송한다.

- 랜덤 $r \in Z_q^*$
- $\delta=H(ID_V||P)+rP$
- δ^e

Step 5: 차량v에게 받은 δ값을 복호화한 후, 자신의 비밀키 s를 곱셈연산 후 그룹 공개키화 함께 전송한다.

- sδ
- $(s\delta||Y_{GA}||T_{exp})$

Step 6: 차량v는 차량 그룹 관리자에게 받은 값과 자신이 생성한 값을 이용하여 개인 서명키를 계산하고, 그룹서명키 Y_{GA} 또한 같이 저장하게 된다.

- $d_v=s\delta-r\delta$
- Y_{GA}

3.3 차량 간 통신 단계

Step 1: 차량 v는 자신의 개인서명키를 이용하여 메시지를 서명하게 된다.

- $U=(M||ID_v)\oplus H(e(d_v,Y_{GA})$
- $\sigma=rP$
- UserSign M = (U,σ)

Step 2: 개인 서명된 메시지를 같은 그룹 구성원 간 검증이 가능하도록 그룹 서명키를 이용하여 그룹 서명 과정을 거친 후 브로드캐스팅하여 서명값을 전송한다.

- 랜덤 $K \in Z_q^*$
- $L=KP$
- $W=(M||U||\sigma)\oplus H(e(P,Y_{GA})^K$
- GroupSign (M||U||σ) = (L,W)

Step 3: 브로드캐스팅 된 메시지를 받은 그룹 구성원은 메시지를 그룹서명키를 통해 검증하여 정당한 그룹 구성원으로부터 전송된 메시지임을 확인한다.

- GroupSign Verify(L,W)
- $W\oplus H(e(Y_{GA},L) = (M||U||\sigma)$

3.4 사용자 추적 단계

Step 1: 그룹 구성원은 그룹서명키를 통해 복호화된 서명값 (U,σ)을 차량 그룹 관리자에게 전송하게 된다.

- GroupSign Verify(L,W)
- $W\oplus H(e(Y_{GA},L) = (M||U||\sigma)$

Step 2: (U,σ)를 전송받은 차량 그룹 관리자는 자신의 비밀키 s를 이용하여 차량v의 식별자를 추출한다.

- UserSign Verify(U,σ)
- $U\oplus H(e((Y_{GA}-\sigma)\delta,s) = (M||ID_v)$

4. 제안방식 분석

· 프라이버시 보장 : 브로드캐스팅 되는 메시지에서 그룹 구성원들은 개인서명 (U,σ)에 대한 검증은 이루어 질 수 없다.

· 추적성 : TA는 분쟁 발생 시 차량 그룹 관리자에 의해 요청된 차량의 식별자를 확인하는 과정을 제공하고 있다.

· 키 위탁 문제 : 차량 v만이 알고 있는 랜덤값 r을 이용해 δ값을 계산하게 된다. 그룹 관리자는 자신의 비밀키를 연산한 값을 전송함으로써 차량 v는 자신만이 알고 있는 r값을 노출시키지 않고 개인서명키를 생성 가능하게 된다.

· 중간자 공격 : 안전하게 서명키를 생성하기 위해서 서명키 자체를 통신로 상에 노출 시키지 않고, 차량 v만이 개인서명키를 생성하게 된다. 따라서 공격자는 중간자 공격을 통해 획득한 메시지로 서명키를 생성할 수 없게 된다.

5. 결론 및 향후 연구 방향

본 논문에서는 VANET환경에서 빈번한 그룹 가입 및 탈퇴를 방지하기 위해 차량의 속도를 고려한 일정 시간 간격의 가입요청 메시지를 적용하여 그룹 서명 방식을 제안하였다.

향후에는 본 논문에서 제안한 그룹서명을 이용한 V2V 통신 기법과 인프라를 이용하여 다양한 서비스를 제공하는 V2I 통신 환경을 연계함으로써 보다 활용도 높은 연구가 필요할 것으로 사료된다.

참고문헌

[1] J. Guo, J.P. Baugh, and S. Wang, “A Group Signature Based Secure and Privacy- Preserving Vehicular Communication Framework,”Proceedings of 2007 Mobile Networking for Vehicular Environments, pp. 103-108, May 2007.

[2] D. Chaum and E. van Heyst, "Group signatures", Advances in Cryptology-EUROCRYPT'91, LNCS 547, Springer, 1992, pp.257-265

[3] J. Zhang, L. Ma, W. Su, and Y. Wang, “Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks,” Proceedings of the First International Symposium on Data, Privacy, and E-Commerce, pp. 138-142,Nov. 2007.