제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

# VANET환경에서 BloomFilter를 이용한 메시지 일괄검증 기법

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

# Message Batch verification scheme using Bloom Filter in VANET

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

요 약

VANET(Vehicular Ad-hoc Network)는 MANET(Mobile Ad-hoc Network)의 한 형태로, 다수의 차량들이 무선통신을 이용하여 차량 간 통신 또는 차량과 RSU(Road Side Unit)사이의 통신을 제공하는 차세대 네트워킹 기술이다. VANET환경에서 기존의 그룹 서명 방식을 이용한 메시지 서명 및 검증이 이루어진다면, 통신 차량이 많아질수록 오버헤드가 발생하는 단점을 지니고 있다. 이에 따라, 본 논문에서는 다수의 차량 간 통신 시에 보다 효율적인 메시지 검증을 위해 Bloom Filter를 이용한 메시지 일괄 검증 기법을 제안한다.

## 1. 서론

VANET(Vehicular Ad-hoc Network)은 MANET(Mobile Ad-hoc Network)의 한 형태로, 다수의 차량들이 무선통신을 이용하여 차량 간 통신 또는 차량과 RSU(Road Side Unit)사이의 통신을 제공하는 차세대 네트워킹 기술이다.

이러한 VANET은 일반적으로 V2V(Vehicle to Vehicle)통신 또는 V2I(Vehicle to Infrastructure) 통신으로 구분된다. V2V 통신은 RSU와 같은 인프라와의 통신 과정 없이 차량과 차량의 통신으로 주변 도로 상황이나 교통사고와 같은 응급 상황 전파를 통해 돌발 상황에 빠르게 대처할 수 있도록 안전 서비스 제공에 주로 사용된다. VANET의 특성상 다수의 차량이 밀집된 환경에서 메시지 서명 및 검증이 이루어진다면, 통신 차량이 많아질수록 큰 오버헤드가 발생하는 단점을 지니고 있다. 이에 따라, 본 논문에서는 다수의 차량 간 통신 시에 보다 효율적인 메시지 검증을 위해 Bloom Filter를 이용한 메시지 일괄 검증 기법을 제안한다.

## 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
- s : 그룹비밀키
- $Y_{GA}$ : 그룹서명키
- d* : 차량 *의 개인서명키
- $Z_q^*$ : 모듈러 q로의 곱셈군
- H() : 일방향 해쉬 함수
- (q, $G_1$, $G_T$, e, P, H, Y) : 공개 파라미터
- e : Bilinear map $e:G_1 \times G_1 \rightarrow G_T$

### 3.2 RSU와 차량 간 통신 단계

RSU는 같은 그룹으로 구성된 차량의 메시지를 송수신하게 되며, 메시지를 받은 RSU는 정당한 그룹 구성원으로부터 전송된 메시지인지 그룹서명키를 통해 검증하게

된다. RSU는 전송받은 메시지를 이용하여 블룸필터를 생성하고, 다시 메시지를 브로드캐스팅하게 된다.

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

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

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

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

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

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

***Step 4:*** RSU는 수신받은 메시지를 여러 개의 해쉬함수를 통해 연산 후, 블룸 필터를 이용하여 BFM을 생성한다.

- $H_1(M_1)$, $H_2(M_1)$, .... ,$H_i(M_1)=BFM_1$
  $H_1(M2)$, $H_2(M_2)$, .... ,$HS(M_2)=BFM_2$
  ...,
  $H_1(M_i)$, $H_2(M_i)$, .... ,$H_i(M_i)=BFM_i$

3.4 메시지 검증 단계

RSU가 수신한 메시지와 동일한 메시지를 수신받은 차량은 RSU가 생성하여 전송하는 블룸필터를 받게 된다. 수신차량은 블룸필터를 이용하여 다수의 메시지를 수신하더라도 한 번의 비교연산만으로 정당한 메시지인지 판별할 수 있게 된다.

## 4. 제안방식 분석

4.1 일괄 검증 기법이 적용된 차량 보안 기술들 기능 및 효율성 비교

차량 통신에 적용된 일괄 검증 기법들과 제안 프로토콜을 비교하여 [표 1]에 정리하였다.
본 제안 방식에서는 각 노드(차량)별 연산의 오버헤드를 줄이기 위해 RSU를 이용한 일괄 검증 방식을 제안하였다. RSU에서 블룸필터를 미리 생성하여 전송하기 때문에 각 노드에서는 별도의 연산 과정 없이 단순 비교 과정만으로도 일괄 검증을 통해 인증이 이루어진다.

## 5. 결론 및 향후 연구 방향

<표 1> 그룹 서명 기법이 적용된 차량 보안 기술 기능 비교

| | | [4] | [5] | 제안기법 |
|---|---|---|---|---|
| 메시지 인증 | | ○ | ○ | ○ |
| 조건부 프라이버시 | | △ | × | ○ |
| 사용자 추적 | | ○ | × | ○ |
| 키 위탁문제 해결 | | × | × | ○ |
| 일괄 검증 방식 | 노드별 연산 | 3P+M+3S | - | - |
| | 비교탐색 | | 순차탐색 | 해싱결과 탐색 |

(P: 페어링연산, M: 곱셈연산, S: 덧셈연산)

본 논문에서는 다수의 차량이 존재하는 VANET환경에서 오버헤드를 줄이기 위해 RSU를 이용한 일괄 검증 기법을 제안하였다. 그룹서명을 기반으로 이루어지기 때문에 VANET환경에서의 다양한 보안 요구사항을 만족시킬 수 있으며, Bloom Filter를 이용한 일괄검증 방식에서는 기존의 방법보다 노드별 계산 효율성을 증가시켰다. 하지만 일괄검증 기법에도 단점이 존재하는데, n개의 메시지에 대한 일괄검증이 실패하였을 경우 그 중에 잘못된 메시지를 찾기 위해 재검증해야하는 단점이 존재한다.

향후에는 본 논문에서 제안한 일괄 검증 기법을 기반으로 비정상적인 메시지를 추출하는 연구와 그룹크기에 유동적인 블룸필터 생성기법에 대한 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] A. Fiat, “Batch RSA,” Journal of Cryptogly, vol.10, no. 2, pp. 75 - 85, Mar. 1997.

[4] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, “An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks,” Proc. of the IEEE INFOCOM 2008, pp. 246-350, Apr. 2008.