VANET에서 카운팅 블룸 필터를 사용한 효율적인 그룹 키 관리 기법

이수연* · 안효범**

요 약

VANET(Vehicular Ad-hoc Network)은 원활한 교통 소통, 사고 방지 등 여러 가지 편리한 기능들을 제공하지만 그 기반을 애드혹 네트워크에 두고 있기 때문에 애드혹 망에서 발생하는 보안 문제를 가지고 있다. VANET에서 사용자의 프라이버시를 보호하기 위해 그룹 서명방식 등이 연구되어졌다. 그러나 그룹 간에 그룹 키 생성 단계 및 그룹 키 갱신 단계에서 RSU(Road-Side Unit) 및 차량의 계산상 오버헤드가 발생한다. 본 논문에서는 효율적인 그룹 키 관리 기술을 제안한다. 즉, 그룹 키 생성 및 갱신 단계에서 $CBF(Counting\,Bloom\,Filter)$를 사용하므로 RSU 및 차량의 계산상 오버헤드를 감소시킨다. 또한, RSU와 차량에서 그룹 키를 자체적으로 갱신하여 관리하는 기법이다.

An Efficient Group Key Management Scheme using Counting Bloom Filter in VANET

SuYoun Lee* · HyoBeom Ahn**

ABSTRACT

VANET(Vehicular Ad-hoc Network) is a kind of ad hoc networks which is consist of intelligence vehicular ad nodes, and has become a hot emerging research project in many fields. It provides traffic safety, cooperative driving and etc. but has also some security problems that can be occurred in general ad hoc networks. In VANET, it has been studies that group signature method for user privacy. However, among a group of group key generation phase and group key update phase, RSU(Road-Side Unit) and the computational overhead of the vehicle occur. In this paper, we propose an efficient group key management techniques with CBF(Counting Bloom Filter). Our group key management method is reduced to the computational overhead of RSU and vehicles at the group key generation and renewal stage. In addition, our method is a technique to update group key itself

Key words : VANET, Counting Bloom Filer, Group Key Management

접수일(2013년 9월 3일), 수정일(1차: 2013년 9월 12일), 게재확정일(2013년 9월 23일)

* 백석문화대학교 인터넷정보학부
** 공주대학교 정보통신공학부 (교신저자)

1. 서 론

차량 애드혹 네트워크 (Vehicular Ad-hoc NETwork; VANET)는 MANET (Mobile Ad-hoc NETwork)의 한 형태로 다수의 차량이 무선통신을 이용하여 차량과 차량 (Vehicular to Vehicular: V2V) 또는 차량과 기지국(Vehicular to Interface: V2I)의 네트워킹을 자율적으로 형성하는 차세대 네트워킹 기술이다.

VANET에서 제공되고 있는 차량 통신은 교통정보 제공 서비스, 인터넷 접속 서비스, 엔터테인먼트 서비스 등을 주목적으로 V2I통신이 활용되며 차량안전 관리 정보 교환, 교차로 진입 제어, 차량 주변의 상황을 고려한 실시간 서비스 등을 주목적으로 하는 V2V통신이 이용된다. V2I에서는 기존의 무선 환경에서 존재하는 보안 위협과 차량의 고속이동 및 네트워크 환경의 급격한 변화 때문에 발생하는 다양한 보안 위협이 존재한다. 뿐만 아니라 차량의 이동 정보가 쉽게 노출될 수 있는 문제점이 있어 개인의 프라이버시가 침해될 수 있다. 이를 해결하기 위해 기존에 많은 연구가 이루어졌고 익명 ID기반 집합 방식[1], 그룹서명 방식 [2]등이 프라이버시 침해를 방지하기 위한 해법을 제시했다. 하지만 관련된 연구에서 제시된 기법은 그룹 키 생성 단계 및 그룹 키 갱신 단계에서 그룹 관리자(RSU) 및 차량의 계산상 오버헤드가 발생하는 문제점을 갖고 있다. 따라서 본 논문에서는 카운팅 블룸 필터(CBF: $Counting\,Bloom\,Filter$)를 사용하여 효율적인 그룹 키 관리 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문과 관련된 기존 VANET 연구 결과를 소개한다. 3장에서는 본 논문에서 이론적 배경이 되는 카운팅 블룸 필터를 알아보고 이를 사용한 VANET를 위한 효율적인 그룹 키 관리 기법을 소개한다. 4장에서 결론과 향후 연구방향을 제시한다.

2. 관련 연구

2.1 보안요구사항

차량 애드혹 네트워크에서는 기본의 네트워크와 유사하지만 특히 다음의 보안 요구사항에 대하여 고려하여야 한다.

▪ 인증(Authentication)

차량 메시지에 대한 출처가 정당한 사용자라는 것을 검증할 수 있어야 하며, 전송되는 메시지는 중간에 위조 및 변조 되지 않았음을 확인 할 수 있어야 한다.

▪ 조건부 프라이버시 (Conditional Privacy)

차량 메시지의 출처에 대해서 제 3자가 알 수 없어야 하고, 분쟁이 발생할 경우 서명된 메시지를 신뢰할 수 있는 제 3의 기관이 개봉하여 신분을 확인 할 수 있어야 한다.

▪ 부인 방지 (Non-repudiation)

분쟁과 연관된 차량이 보낸 메시지에 대해서 부인하거나 반박할 수 없도록 보장되어야 한다.

▪ 키 교환 (Key Exchange)

기밀 통신을 요구하는 차량은 기밀 통신을 원하는 차량과 상호 신분 확인 후, 데이터를 보호할 수 있는 세션 키를 생성해야 하며, 생성된 세션 키는 다양한 공격으로부터 안전해야 한다.

위와 같은 차량 네트워크 보안 요구 사항을 만족할 수 있는 방법 중에 그룹 서명을 사용하는 것이 주목되고 있다. 왜냐하면, 안전한 차량 네트워크 서비스를 위해 그룹 서명 기법은 인증, 조건부 프라이버시, 부인 방지 등의 보안 서비스를 제공하기 때문이다

2.2 그룹 서명 방식[3]

기존에 그룹 키 관리 기법은 그룹에 참여하고자 하는 차량은 일정한 시간 간격을 두고 RSU에게 요청 메시지를 전송하게 되고 이 메시지를 RSU가 2개 이상 수신하게 된다면 자신의 속도와 방향에 유사하다고 판단하여 그룹 가입을 수락하는 메시지를 송신하게 된다. RSU가 아래와 같은 키 발급 프로토콜을 이용하여 그룹 키를 발급한다.

① 차량은 RSU에게 그룹 키 요청 메시지 전송

② 그룹관리자는 차량의 공개키로 그룹 키를 암호화하고 그룹 관리자의 서명문을 추가하여 차량에게 전송

③ 차량은 개인키로 메시지를 복호화하여 그룹 키를 획득하고 확인 메시지를 그룹 관리자에게 전송 차량은 발급 받은 그룹 키를 이용하여 모든 메시지를 암호화하여 전송하고 수신된 암호문을 그룹 키로 복호화하여 교통정보를 획득하게 된다. 또한,

악의적인 공격자에 대한 안전한 그룹 통신을 위하여 주기적인 그룹 키 갱신이 필요하다. 신규 차량 및 기존 차량에 대한 그룹 키 갱신 단계를 다음과 같다.

- 신규 차량의 경우 : 키 발급 프로토콜 수행
- 기존 차량의 경우 :

① 기존의 그룹 키로 새로운 그룹 키를 암호화하여 전송할 수 있지만 기존 사용자는 수신된 그룹 키 인증을 위해RSU는 서명 알고리즘 수행

② 신규 차량과 동일한 키 발급 프로토콜 수행

즉, 신규 차량과 기존 차량에 대한 그룹 키 갱신을 위해 RSU는 각 차량에 대한 암호화 및 서명 알고리즘을 수행해야 된다. 따라서 그룹 기밀통신의 안전성과 그룹 관리자 및 차량의 통신 오버헤드는 trade-off 관계로 정의하였지만 안전한 그룹 기밀 통신을 위한 연구가 필요하다. 이에 본 연구에서는 CBF를 활용하여 차량과 RSU가 자체적으로 그룹 키를 생성하고 관리하는 효율적인 그룹 키 관리 기술을 제안한다.

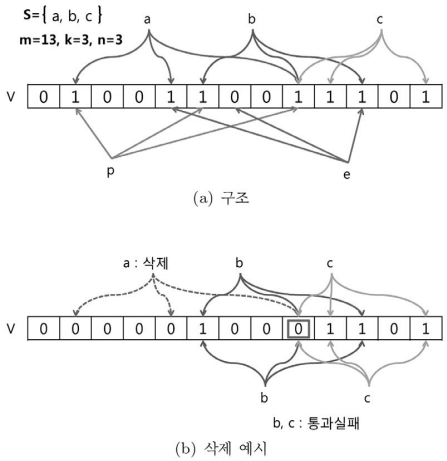
3. 효율적인 그룹 키 관리 기법

본 장에서는 제안 기술의 기반 기술인 CBF를 소개하고 그룹 키 생성 및 갱신단계에서 CBF를 이용하여 그룹 관리자 및 차량의 계산상 오버헤드를 줄이고 효율적인 그룹 키 관리 기술을 소개한다.

3.1 블룸 필터(Bloom Filter)[4,5]

불룸 필터는 간단한 비트-벡터 형태의 데이터 구조를 갖는 필터로서 저장된 정보와 입력 값을 비교하여 주어진 집합에 입력과 일치하는 값이 존재하는 지를 알려주는 방법으로 1970년 Burton Bloom에 의해 개발 되었다. 블룸 필터는 전체 도메인 U의 어떤 집합 $S=(s_{1,}s_{2,}.....s_n)$의 키 값을 비트벡터 V로 표현하는 방법이다.

블룸 필터의 동작과정은 다음과 같다. 처음 비트벡터 V의 모든 비트는 0으로 초기화 되어있다. 블룸필터는 k개의 해시함수 $h_{1,}h_{2,}.....,h_k$를 이용하여 도메인 U의 키 값을 $(1,2,....,m)$으로 사상시킨다. $s\in S$ 인 각 항목은 해시함수를 사용하여 비트벡터 V 의 $h_1(s),h_2(s),.....,h_k(s)$위치를 1로 바꾼다. 만약 $t\in S$ 인지 검사하기 위해서는 비트벡터 V의 $h_1(t),h_2(t),.....,h_k(t)$ 위치의 비트를 확인한다. 그 비트들 중 하나라도 0이면 $t\in S$임이 분명하다. 하지만 $t\notin S$ 라 할지라도 모든 비트가 1이 될 수 있는 데 이것은 불룸 필터에 존재하는 오류로서 긍정 오류(false positive)라고 한다. (그림 1)에서 보면 항목 e는 블룸 필터를 통과하지 못한다. 비트에 0이 존재하기 때문이다. 항목 p는 $p\notin S$지만 블룸 필터 검사를 통과할 수 있으므로 긍정오류가 발생하는 항목이다. 따라서 블룸 필터를 설계할 때 블룸 필터 크기를 증가시켜 긍정 오류의 비율을 조절할 수 있다.



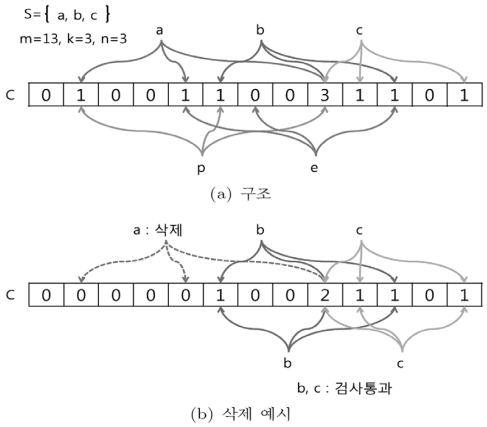
(그림 1) 불룸 필터 과정

블룸필터는 적은 메모리를 사용하고도 많은 항목을 표현할 수 있다. 예를 들어, 네트워크 라우터의 경로 테이블을 참고하는 프로그램이 있을 때 전체 IP주소들 중 약 백만 개의 IP는 특정 노드로 보내줘야 한다고 하자. IPv6의 주소 길이는 128비트이므로 약 15.3Mbyte의 메모리가 필요하다. 블룸필터는 동일한 주소테이블을 허영 긍정 오류 1%로 설정하고 3개의 해쉬 함수를 사용하면 1/10인 1.4Mbyte로 표현 할 수 있다.

3.2 카운팅 블룸 필터(Counting Bloom Filter) [6,7]

CBF는 블룸필터의 단점이었던 항목의 삽입과 삭제를 표현하기 위해 비트벡터의 비트를 카운터로 변경하여 해당 위치에 몇 개의 항목이 입력되었는지를 나타낸다. CBF는 불룸 필터와 동일한 구조에서 카운터만 추가되었으므로 긍정오류의 발생비율이 동일하다.

전체 도메인 U의 어떤 집합 $S = (s_1, s_2, \ldots\ldots s_n)$를 길이 m인 카운터벡터 C를 통해서 표현하는 데 집합 S에 항목 t가 추가되면 k개의 해시 함수를 통해 $(1, 2, \ldots, m)$로 사상 된 $h_1(t), h_2(t), \ldots\ldots, h_k(t)$위치의 카운터를 증가시킨다. 반대로 항목이 제거되면 카운터를 감소시킨다.



(그림 2) 카운팅 불룸 필터 과정

3.3 카운팅 블룸 필터를 이용한 그룹 키 관리 기법

3.3.1 제안 된 그룹 키 관리 기법

VANET에서 프라이버시 보호를 위한 효율적인 그룹 키 관리 기술은 CBF를 사용하여 그룹 관리자(RSU)와 차량(V)이 자체적으로 그룹 키를 생성하고 갱신하는 것이다. 즉, RSU와 V는 CBF를 사용하여 그룹 키를 자체적으로 생성하고 갱신 시에는 CBF를 통해 갱신하므로 RSU와 V의 계산상 오버헤드를 줄이고 통신량을 감소시키게 된다. 제안 된 기법은 그룹 키 생성 단계, 그룹 키 발급 단계, 그룹 키 갱신 단계, 그룹 키 인증 단계로 구성된다.

[사전 단계]

각 차량 및 RSU는 네트워크상에 배포되기 전 $TA(Trusted\,Authority)$에 사전등록이 된다. RSU는 등록과정을 통해 개인키를 생성 받게 되고 차량은 TA로부터 받은 계산 값을 이용하여 개인키를 생성하게 된다. 차량과 RSU 각각 TA의 등록과정은 안전한 네트워크상에서 이루어진다고 가정한다.

[그룹 키 생성 및 발급 단계]

그룹 초기 생성 단계와 생성 후 새로운 차량 가입 과정으로 구분하여 설명한다.

■ 그룹 초기 생성

1단계) $RSU \rightarrow V_0 : E_{ks}(IV)$
2단계) $V_0 : C \leftarrow CBF(IV) + CBF(ID)$

- 1단계: 새로운 차량(V_0)이 들어오면 RSU는 차량의 공개키로 IV값을 암호화하여 차량에게 보내준다.
- 2단계: 새로운 차량(V_0)은 자신의 ID와 IV값을 CBF를 통해 생성하고 그것을 C값으로 사용한다. 여기서 C값은 비트 벡터이다.

■ 그룹 생성 후 새로운 차량 가입 시 그룹 키 생성

1단계) $RSU \rightarrow V_n : E_{ks}(C_{old})$
2단계) $RSU \rightarrow *\quad : ID = C_{old} + V_{id}$
3단계) $*\quad : ID$로부터 V_{id}추출
$V_{id} = ID - C_{old}$
$C_n = C_{old} + CBF(V_{id})$
4단계) V_n는 C_{old}를 가지고 C_n생성
$C_n = C_{old} + CBF(V_{id})$

- 1단계: RSU는 새로운 차량(V_n)에게 초기에 생성 된 그룹 키(C_{old})를 새로운 차량의 공개키로 암호화하여 보낸다.

- 2단계: RSU는 그룹 내에 있는 모든 차량들에게 이전의 그룹 키(C_{old})와 차량의 아이디(V_{id})를 비트 연산하여 새로운(ID)를 생성하여 보낸다.
- 3단계: 그룹 내에 있는 차량들은 RSU로부터 온 ID에서 이전의 그룹 키(C_{old})를 빼므로 새로운 차량의 아이디를 얻을 수 있다. 또한, 이전의 그룹 키(C_{old})와 새로운 차량은 아이디(V_{id})를 통해 새로운 그 룹 키(C_n) 생성하게 된다.
- 4단계: 새로운 차량(V_n)은 자신의 아이디와 이전 그룹 키를 통해 새로운 그룹 키(C_n) 생성한다.

[그룹 키 갱신 단계]

차량이 그룹을 탈퇴하였을 때 새로운 그룹 키 형성 과정이다.

1단계) $RSU \rightarrow * : E_c(V_{id})$
2단계) $V : C_n = C_{old} - CBF(V_{id})$

- 1단계: 차량이 그룹을 탈퇴 시 RSU는 모든 차량들에게 그룹 키 C로 탈퇴한 차량의 ID를 암호화하여 전송한다.
- 2단계: 그룹 내 차량들은 기존의 그룹 키(C_{old})에서 차량의 아이디로 생성 된 CBF 값을 빼므로 새로운 그룹 키(C_n)을 생성한다.

[그룹 키 인증 단계]

차량은 새로운 그룹 키(C_n)에 대해 RSU로부터 받은 차량의 ID(V_{id})를 그룹 키로 암호화하여 전송이 되었고 본인이 소유하고 있는 그룹 키(C_{old})를 통해 자체적으로 생성하였기 때문에 새로운 그룹 키(C_n)로 인증한다.

3.4 분석

3.4.1 프라이버시 보호

그룹 생성 후 가입 단계에서 $RSU \rightarrow * : ID = C_{old} + V_{id}$ 를 통해 차량의 ID를 이전의 그룹 키(C_{old})를 통해 만들었기 때문에 제 3의 차량이 자신의 ID를 통해 그룹에 가입을 하였어도 이전의 그룹 키(C_{old})를 알 수 없기 때문에 그룹 내 차량으로 위장하여 가입 할 수 없다.

3.4.2 효율성

그룹 관리자와 차량은 그룹 키 생성과 갱신 단계에서 새로운 그룹 키에 대해 기존의 그룹 키 서명 방식인 암호화 및 서명을 제거하여 그룹 관리자와 차량의 계산상 오버헤드를 줄였다. 즉, 카운팅 블룸 필터(CBF)를 사용하여 해쉬 함수와 비트 열 계산만이 이루어지므로 계산상 효율성이 높아졌다. 또한, 그룹 관리자와 차량 간에 이전에 사용 된 그룹 키(C_{old})를 활용하여 새로운 그룹 키(C_n)를 자체적으로 생성하고 갱신하므로 그룹 내 통신량 감소도 이루어졌다.

4. 결 론

본 논문에서는 VANET에서 프라이버시를 보호하기 위한 효율적인 그룹 키 관리 기법을 소개하였다. 제안 된 기법은 $CBF(Counting\,Bloom\,Filter)$를 사용하여 그룹 키 생성 및 갱신 단계에서 그룹 관리자(RSU)와 차량(V)에서 해쉬함수와 비트 열 계산만을 수행하여 그룹 키 인증이 가능하여졌다. 또한 그룹 관리자와 차량 간에 자체적으로 그룹 키를 생성할 수 있도록 하여 통신량 감소도 가져왔다. 향후 시뮬레이션 성능분석을 통해 제안된 방법의 우수성을 입증하고자한다.

참고문헌

[1] M..raya and J.Hubaux, "Securing vehicular ad hoc networks," J. of Computer Security, vol. 15, no. 1, pp. 39-68, Jan.2007

[2] X. Lin, X. Sun, P,-H, Ho and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications", IEEE Trans, on Vehicular Technology, vol, 56, no.6, pp.3442-3456, 2007.

[3] D. Boneh and H. Shacham,"Group signatures with verifier-local revocation," CCS 2004, pp.168-177 ,2004

[4] 6. A. Broder and M. Mitzenmacher. Network applications of Bloom filters: A survey. Internet Mathematics, 1(4):485-509, 2004.

[5] B. Chazelle, J. Kilian, R. Rubinfeld, and A. Tal," The bloomier filter : an efficient data structure for static support lookup tables," in SODA '04: Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms, (Philadelphia, PA, USA), pp.30-39, Society for Industrial and Applied Mathematics, 2004.

[6] B. Chazelle, J. Kilian, R. Rubinfeld, and A. Tal," The bloomier filter : an efficient data structure for static support lookup tables," in SODA '04: Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms, (Philadelphia, PA, USA), pp.30-39, Society for Industrial and Applied Mathematics, 2004.

[7] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol.13, pp.422-426, 1970.

[저 자 소 개]

이 수 연 (SuYoun Lee)

1990년 단국대학교 전자계산학과 (이학사)
1993년 단국대학교 전산통계학과 대학원 석사(이학석사)
2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사 (공학박사)
1997년 3월 ~ 현재 백석문화대학교 인터넷정보학부 교수

e-mail : sylee@bscu.ac.kr

안 효 범 (HyoBeom Ahn)

1992년 단국대학교 전자계산학과 (이학사)
1994년 단국대학교 전산통계학과 대학원 석사(이학석사)
2002년 단국대학교 전산통계학과 대학원 박사(이학박사)
1997년 9월 ~ 2005년 3월 천안공업대학 정보통신과 부교수
2005년 3월 ~ 현재 공주대학교 정보통신학부 교수