SMART Highway환경에서 Counting BloomFilter를 활용한 차량 간 인증 기법

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

Authentication between the vehicle scheme using Counting BloomFilter in SMART Highway

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

요 약

SMART Highway 사업은 첨단 IT통신과 자동차 및 도로 기술이 접목된 세계 최고수준의 빠르고 편안한 지능형 녹색도로 실현을 목표로 하고 있다. SMART Highway의 도로-자동차 기반 교통운영에서 핵심기술인 VANET(Vehicular Ad-hoc Network)은 다수의 차량들이 무선통신을 이용하여 차량 간 통신 또는 차량과 RSU(Road Side Unit)사이의 통신을 제공하는 차세대 네트워킹 기술이다. 특히, 운전자의 안전에 직접적인 영향을 끼칠 수 있는 V2V 통신의 경우 차량 간의 안전한 통신을 위해 차량 간 상호인증이 반드시 고려되어야 한다. 이처럼 빠른 속도로 이동하는 차량 간 인증이 원활이 이루어지기 위해서는 기존의 네트워크에서 사용된 인증방식은 그대로 적용시키기 어렵다. 따라서 본 논문에서는 다수의 차량 간 통신 시에 보다 효율적인 차량 인증을 위해 카운팅 블룸필터를 이용한 차량 인증 기법을 제안한다.

1. 서론

SMART Highway 사업은 국토해양부에서 수립한 “건설교통 R&D 혁신 로드맵에서” 선정되어 추진되는 사업으로써, 첨단 토목기술, IT기술, 차세대 자동차기술을 상호 접목하여 빠르면서도 안전한 지능형 고속도로를 개발하는 사업이다[1].

SMART Highway는 첨단 IT통신과 자동차 및 도로 기술이 접목된 세계 최고수준의 빠르고 편안한 지능형 녹색도로 실현을 목표로 하고 있다. 스마트 Highway의 핵심 목표는 설계속도 160km의 자동 사고예방감지시스템 개발을 통해 도로통행의 3대 요소인 ‘운전자-도로-차량’ 간 ‘역할 재조정’과 ‘안전성 확보’가 기술개발 핵심이다. 즉, IT기술을 도로와 자동차기술에 접목하여 자동차-운전자-도로시설 간 정보의 공유-통신-제어(communication & control)를 통해 자동차와 도로기능은 높이고, 운전자의 역할(피로도)은 감소시키며 편의성은 높이면서 초고속 안전주행과 도로용량의 증대가 SMART Highway의 구현목표이다.

SMART Highway의 도로-자동차 기반 교통운영에서 핵심기술인 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. 이처럼 빠른 속도로 이동하는 차량 간 인증이 원활이 이루어지기 위해서는 기존의 네트워크에서 사용된 인증방식은 그대로 적용시키기 어렵다. 따라서 본 논문에서는 다수의 차량 간 통신 시에 보다 효율적인 차량 인증을 위해 카운팅 블룸필터를 이용한 차량 인증 기법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 기법의 이해를 돕기 위한 관련 연구들을 소개하고, 3장에서는 제안방식에 대하여 설명한다. 4장에서는 제안 방식에 대한 효율성을 분석하고, 마지막으로 5장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

2. 관련연구

2.1 블룸 필터(Bloom Filter)

블룸필터는 H. Bloom에 의해서 제안된 통계적 특성을 가진 자료구조로써, 데이터를 공간 효율적으로 빠르게 검색할 수 있다는 장점이 있다[2]. 이러한 블룸필터는 많은 양의 데이터를 매우 작은 공간을 사용하여 저장할 수 있고, 검색 방식에 따라 다양한 환경에 적용시켜 효율적인 활용이 가능하다.

블룸필터는 m개의 비트를 가진 하나의 비트 백터(bit vector) B이며, n개의 엘리먼트를 가진 유한 집합 $S=\{x_1, x_2, ... ,x_n\}$에 각각의 요소가 포함되어있는지 쉽게 확인 가능하도록 해준다. 각 요소를 블룸필터에 맵핑(mapping) 시키기 위해서는 서로 독립적인 k개의 해시(hash)함수를 사용하여 비트벡터 B의 비트 주소공간에 맵핑(mapping) 시킨다.

2.2 카운팅 블룸필터(Counting Bloom Filter)

일반적인 블룸필터는 각 요소의 삽입은 가능하지만 삭제는 불가능하다. 특정 요소를 삭제하게 된다면 해시 함수들에 의해 정해진 위치들의 비트 값을 “1”에서 “0”으로 다시 설정한다는 것인데, 이 때 삭제하고자 하는 요소가 아닌 다른 요소의 비트 값을 “0”으로 설정할 수도 있게 되는 것이다. 이로 인해 블룸필터 내에 존재 하지만 존재하지 않는다는 부정오류(False negative)가 발생하게 된다. 이러한 문제점을 해결하기 위해 제안된 카운팅 블룸필터는 비트벡터의 비트를 카운터로 변경하여 해당 위치에 몇 개의 항목이 입력되었는지를 나타낸다. 카운팅 블룸필터는 기존 블룸필터에서 카운터만 추가되었으므로, 긍정 오류의 발생 확률은 동일하다[3]. 카운팅 블룸필터의 카운터는 3비트나 4비트를 사용하는 것이 안전하다고 알려져 있다[4].

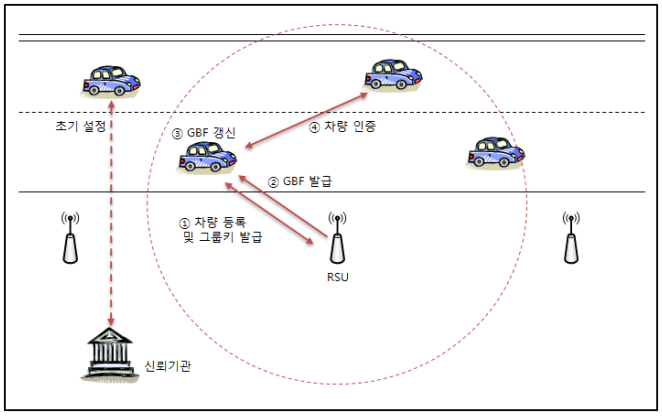
3. 제안방식

3.1 시스템 모델 및 가정

제안하는 시스템에서 모든 차량은 네트워크상에 배포되기 전 TA(Trusted Authority)에 사전등록이 된다. 또한 모든 차량은 차량에 탑재된 OBU(On-Board Unit)의 TRH(Temper Resistant Hardware : 조작 불가능한 하드웨어)를 이용하여 통신 시 모든 연산을 수행하게 되고, 통신 범위 내 그룹을 생성하기 위해 RSU는 통신 범위에 도달하는 차량에게 메시지를 보내 하나의 통신 그룹을 형성하게 된다. RSU는 항상 신뢰받는 객체이며, OBU에 비하여 월등한 연산능력을 가지고 있다고 가정한다.

3.2 시스템 계수

본 제안방식에서는 다음과 같은 시스템 계수를 사용하여 프로토콜을 설계한다.



(그림 1) 제안방식 시나리오

- RIDi : OBU에 의해 생성된 차량 i의 식별자
- PID : (ID_1, ID_2) 쌍
- P : 타원 곡선상위의 점
- G : P에 의해 생성되는 순환군
- q : G의 위수
- P_{pub1}, P_{pub2} : TA의 마스터키 (s_1,s_2)에 의해 생성된 공개키 쌍
- 공개 파라미터 : $(G, q, P, P_{pub1}, P_{pub2})$
- GK : 그룹키
- GBF : 통신 그룹 내 차량 PID 정보의 블룸필터 생성 값
- T_s : 타임스탬프
- T_{REVOK} : 그룹키 폐기 시간

3.3 초기 설정 과정

Step 1: 차량V는 TA(Trust Authority)를 통해 공유한 공개 파라미터 G, q, P, P_{pub1}, P_{pub2}를 이용하여 PID쌍 (ID_1, ID_2)를 생성한다. P_{pub1}과 P_{pub2}는 TA가 간직하고 있는 마스터키(s_1, s_2)에 의해 생성된 공개키 쌍이다.

- $ID_1=r\cdot P$
- $ID_2=RID\cdot H(r\cdot P_{pub1})$
- $PID=(ID_1, ID_2)$

3.4 차량 등록 과정

최초 그룹 구성 시 RSU는 통신 범위에 도달하는 모든 차량에게 그룹 참가 메시지를 보내 하나의 통신 그룹을 형성하게 된다. 차량으로부터 재전송 받은 메시지를 통해 하나의 GBF(Group BloomFilter)를 생성하게 된다. 이 때, 카운팅 블룸필터를 사용하여 중복되는 요소는 카운터를 통해 비트를 증가 시킨다.

Step 1: RSU는 통신 범위에 도달하는 차량들에게 RSU의 식별자가 포함된 인증서와 그룹키를 차량의 공개키로 암호화하여 전송하게 된다.

- $RSU\rightarrow V : E_{KUv}(GK||y_n||T_s||T_{REVOK}||CERT_{RSU})$

Step 2: RSU의 식별자를 확인한 차량은 사전에 생성한 자신의 임시 아이디와 함께 RSU의 공개키로 암호화 한다. 차량은 수시로 메시지를 보내면서 그룹에 속해 있음을 알린다.

-V→RSU : $E_{KU_{RSU}}(RSU_{ID}||PID_V)$

Step : RSU는 전송받은 값을 바탕으로 GBF(Group BloomFilter)를 생성한다. 이 때, 차량의 탈퇴에 대비해 효율적인 갱신을 위해 카운팅 블룸필터를 사용한다.

- $H_1(RSU_{ID}||PID_V)$, $H_2(RSU_{ID}||PID_V)$,
.... ,$H_i(RSU_{ID}||PID_V)$=GBF

3.5 발급 단계

RSU는 같은 그룹으로 구성된 차량에게 차량목록으로 계산된 블룸필터 값을 브로드캐스팅하게 된다.

Step 1: RSU는 사전에 배포된 그룹키로 암호화하여 차량 인증에 필요한 GBF를 브로드캐스팅 하게 된다.

-RSU → * : $E_{GK}(GBF||T_s||T_{REVOK})$

3.6 Group BloomFilter 갱신 단계

RSU는 차량으로부터 PID를 포함한 정보가 더 이상 수신되지 않을 경우, 통신 범위를 벗어난 것으로 판단하여 GBF를 새롭게 갱신하게 된다. 새롭게 갱신된 GBF는 발급 단계와 마찬가지로 통신 범위 내 모든 차량에게 브로드캐스팅 된다. 차량은 이전의 GBF를 폐기하고, 새롭게 갱신된 GBF를 이용하여 차량 간 인증을 하게 된다.

3.7 차량 간 인증 단계

차량 간 통신 시 그룹키를 통해 모든 메시지를 암호화하여 송수신 하게 된다. 이때, 각 차량은 그룹키로 암호화된 메시지와 함께 수신되는 다른 차량의 PID를 RSU로부터 받은 GBF와 비교하여 정당한 차량으로부터 온 메시지인지 검증하게 된다.

Step 1: 각 차량은 그룹키로 암호화된 메시지와 자신의 PID를 통신 범위 내의 차량과 송수신 하게 된다.

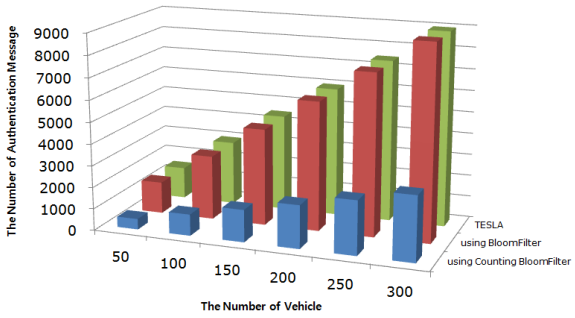
- $V_1 \rightarrow V_2$: $E_{GKn}(M)||PID_{v1}$

4. 제안방식 분석

4.1 통신 횟수

Smart highway 환경에서는 고속도로 상에서 차량의 속도가 160Km를 유지하는 것을 목표로 하기 때문에, WAVE통신의 범위 2Km를 통과하기까지 약 44초의 시간이 걸린다. 이를 실제 환경에 적용한다고 가정하였을 경우 다양한 환경적 요인을 감안하여 60초의 시간동안 발생할 수 있는 차량 간 인증메시지 통신 횟수를 비교하였다.

RSU의 통신 범위 내에 50~300대의 차량이 각각 존재한다고 가정하고, 1초에 한 대씩 통신범위를 벗어나는 경우에 이루어지는 인증 메시지 전송 횟수이다(그림 3). 일반적인 경우 상대 차량이 통신 범위를 벗어나기까지 300ms마다 인증 메시지를 송수신하게 된다. 하지만 본 제안방식의 경우 상대 차량이 통신 범위를 벗어나기 전까지 별도의 인증메시지 교환이 필요 없고, 통신 범위 내에 차량이 존재하지 않을 때에만 새롭게 갱신된 블룸필터를 이용하여 다른 차량과 인증이 이루어지므로 보다 효율적이라고 할 수 있다.



(그림 3) 인증메시지 전송 통신 횟수

4.2 메시지 크기

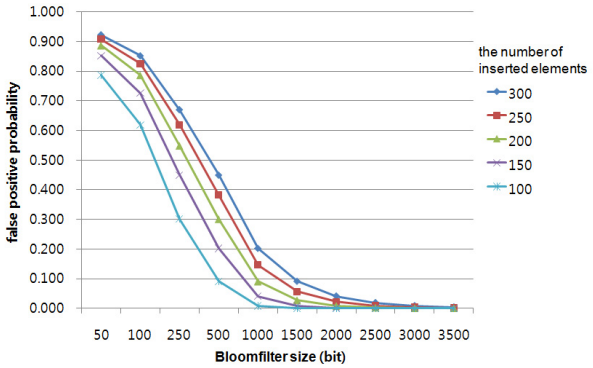
본 제안방식에서 사용된 블룸필터는 모든 차량의 인증 메시지를 저장해야하는 기존 방식과 달리 모든 차량의 인증 정보를 하나의 블룸필터에 저장하여 보관하기 때문에 공간적인 측면에서 매우 효율적이라고 할 수 있다.

하지만 BloomFilter를 사용함에 있어 가장 먼저 고려해 볼 사항이 바로 긍정오류 발생 확률이다. BloomFilter는 통계적 특성을 가진 자료구조로써 많은 양의 데이터를 줄여서 공간 효율적으로 빠르게 검색 가능하다는 장점이 존재하지만, 긍정오류가 발생하게 된다. 긍정오류란 필터 내에 데이터가 존재하지 않지만 존재한다고 검색이 되는 것이다.

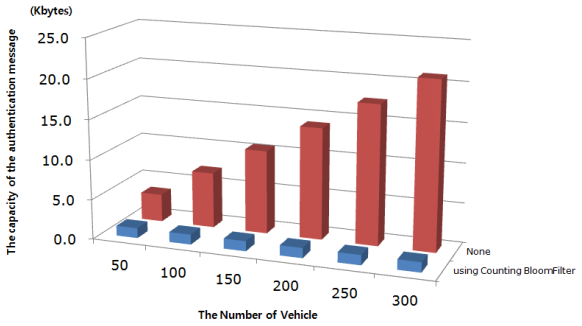
이러한 오탐 발생확률을 줄이기 위해선 일반적으로 해싱 함수의 개수를 늘리거나, 저장 공간을 늘리는 방법을 채택한다. 하지만 해싱 함수의 개수를 늘리게 되면 그만큼 연산량이 증가하기 때문에 저장 공간을 늘리는 방법을 선택하였다. 아래 식은 긍정오류 발생확률 p를 발생시키기 위해서 필요한 저장 공간을 계산하는 방법이다[2].

- BloomFilter의 크기 : m
- 입력되는 원소의 개수 : n
- 긍정오류 발생 확률 : p
- 계산식 : $m = -\frac{n \ln p}{(\ln 2)^2}$

위 식을 바탕으로 (그림 4)와 같은 그래프를 도출해 낼 수 있다. (그림 4)의 세로축은 긍정오류 발생 확률, 가로축



(그림 4) 긍정오류 검출 확률



(그림 5) 인증메시지 크기 비교

은 BloomFilter의 크기로 300개의 차량 인증 정보를 저장하는 BloomFilter의 경우 저장 공간이 약 2500bit이상이 된다면, 긍정오류 발생 확률은 약 0.8%로 굉장히 낮다고 할 수 있다. 물론 크기를 3500bit로 더 증가시킨다면 약 0.01% 이하의 확률로 더욱 낮아지게 된다.

일반적인 네트워크 노드 인증 정보 NAI(Network Access Identifier)는 최소 72바이트에서 최고 253바이트의 메시지 길이를 보장해야 한다[5]. 블룸필터를 적용한 인증 정보의 크기는 긍정오류 검출 확률을 고려하여 300대 정도의 차량 인증 정보를 안전하게 저장하기 위해서 약 3500비트의 크기가 되어야 하며, 본 논문에서 사용될 카운팅 블룸필터의 경우 한 블럭당 3비트가 카운팅에 사용되기 때문에 1300바이트의 저장공간을 필요로 한다.

차량 한 대가 저장해야 하는 인증 메시지 하나의 크기는 기존방식에 비해 크다고 할 수 있지만, 차량의 대수에 비례하여 증가하는 메시지 크기와 달리 하나의 블룸필터 메시지가 모든 차량의 인증정보를 포함한 크기이기 때문에 차량 대수에 독립적이라고 할 수 있다(그림 5).

5. 결론 및 향후 연구 방향

본 논문에서는 다수의 차량이 존재하는 VANET 환경에서 각 차량의 오버헤드를 줄이기 위해, RSU로부터 수신된 인증정보가 포함된 카운팅 블룸필터를 이용하는 인증 기법을 제안하였다.

이처럼 블룸필터를 활용하여 통신 횟수 및 저장 공간에 대한 효율성을 극대화 시켰다. 또한 일반적인 블룸필터를 사용하게 될 경우 발생할 수 있는 문제점을 카운팅 블룸필터를 사용함으로써 해결하였다.

향후에는 본 논문에서 제안한 인증 기법을 기반으로 다양한 환경적 요인을 고려한 시뮬레이션을 구축하여, 기존의 다양한 기법들과 보다 구체적으로 비교 분석이 필요할 것으로 사료된다.

참고문헌

[1] 이기영, 이혁준, “스마트하이웨이를 위한 유비쿼터스 교통정보 서비스 시스템”, 2009, 정보과학회지 제27권 9호, 한국정보과학회

[2] B. Bloom, Space/Time Trade-Offs in Hash Coding with Allowable Errors, Comm. ACM, vol. 13, no. 7, May 1970, pp. 422-426

[3] S.-W. Lee, D.-J. Park, T.-S. Chung, D.-H. Lee, S. Park, and H.-J. Song, "A log buffer-based flash translation layer using fully-associative sector translation," ACM Trans. Embed. Comput. Syst., vol.6, no.3, p.18, 2007.

[4] L. Fan, P. Cao, J. Almeida, and A. Z. Broder, "Summary cache: a scalable wide-area web cache sharing protocol," IEEE/ACM Trans. Netw., vol.8, no.3, pp.281-293, 2000.

[5] B. Aboba et al. “The Network Access Identifier”, FRC 4282, January 1999.