VANET 환경에서 효율적인 통신 보안 기술을 위한 시뮬레이션 구현

최성진, 김수현, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[starcsj87, kimsh, imylee]@sch.ac.kr

Implementation of simulation for efficient communication security technologies in VANET

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

요 약

SMART Highway는 다수의 차량들이 무선통신을 이용하여 차량 간 통신 또는 차량과 도로의 인프라 장비 사이에서의 통신을 제공하는 차세대 네트워킹 기술로 VANET이 핵심기술이 된다. 이러한 환경에서는 기존의 네트워크와 달리 사람의 생명과 직접적으로 연결되어 있기 때문에 보안이 매우 중요한 핵심사항이 된다. 빠른 속도의 환경속에서 이동하는 차량 간 인증이 원활이 이루어지기 위해서는 기존의 네트워크에서 사용된 인증방식은 그대로 적용시키기 어렵다. 따라서 본 논문에서는 VANET 통신 환경에서의 보안 위협 분석을 통해 보안 요구사항을 도출하여, 이를 바탕으로 다수의 차량 간 통신 시에 보다 효율적인 차량 인증이 이루어지기 위하여 블룸필터를 사용한 메시지 일괄검증 기법을 사용한다. 이를 통하여 차량이 통신 범위를 벗어나기 전까지 별도의 불필요한 인증메시지 교환을 줄이고, 통신 범위 내에 차량이 존재하지 않을 때에만 새롭게 갱신된 블룸필터를 이용하여 다른 차량과 인증이 이루어지는 효율적 방식을 제안하고자 한다.

1. 서론

SMART Highway라 함은 기존의 고속도로가 가지고 있던 속도의 한계를 넘는 160km/h 이상으로 주행 할 수 있게 설계된 고속도로를 말하는 것으로 현재 국토해양부에서는 이러한 지능형 교통 시스템과 관련하여 2015년까지 도로부문 예산의 2%수준으로 투자를 단계적으로 늘리고, 2020년까지 도로-차량간, 차량-차량간 통신할 수 있는 차세대 지능형 교통 시스템(ITS:Intelligent Transportation System) 체계를 확대해나갈 계획이 추진 중 이다[1].

SMART Highway의 도로-자동차 기반 교통운영에서 핵심기술인 VANET(Vehicular Ad-hoc Network)은 MANET(Mobile Ad-hoc Network)의 한 형태로, 차량에 설치된 무선 통신기기를 통한 지능형 차량 간 그리고 차량과 노변장치간의 통신을 VANET이라고 한다. VANET은 운전자의 안전을 보장을 위해 활용되는 기술로써 산업계와 학계를 중심으로 연구가 활발히 진행되고 있다[2]. 이러한 VANET은 일반적으로 V2V(Vehicle to Vehicle)통신 또는 V2I(Vehicle to Infrastructure) 통신으로 구분된다. V2V 통신은 RSU(Road Side Units)와 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 블룸필터를 이용한 차량 인증 기법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 기법의 이해를 돕기 위한 관련 연구들을 소개하고, 3장에서는 차량 통신 네트워크 환경에서 필요로 하게 되는 보안 요구사항에 대해 설명한다. 4장에서는 제안방식에 대하여 설명을 하고, 5장에서는 시뮬레이션 구현을 통한 제안방식의 효율성을 분석하며, 마지막으로 6장에서는 결론 및 향후 연구방향을 제시하고자 한다.

2. 관련 연구

2.1 SMART Highway 연구 동향

국내에서는 정부의 SMART Highway 개발 계획의 발표 로 VANET에 관한 관심이 최근 증대되기 시작했다. 첨단 IT 및 자동차 기술 등을 이용하여, 실시간 교통정보

제공, 교통제어, 미래형 첨단 자동차의 안전주행, 도로 상태 실시간 계측, 교량 등 도로 부속물 수명 연장 등이 가능한 SMART Highway를 2016년까지 건설하는 것을 목표로 한다. SMART Highway 개발이 완료되면 무사고, 무정체 고속도로를 실현하여, 국내 거점 도시 간 이동성이 획기적으로 향상되고 자동차·물류·IT 등 관련 산업에도 큰 파급효과를 가져올 것으로 예측된다. 이러한 VANET과 관련된 기술 연구는 ETRI(전자통신연구원)에서 주로 진행되고 있다. ETRI는 2007년부터 4년간 VMC (Vehicle Multi-hop Communication)기술 개발에 착수하였다. VMC 프로젝트는 고속으로 이동하는 차량에서 다양한 텔레메틱스와 ITS 서비스를 제공하기 위한 V2V통신과 V2I 차량 통신 기술을 연구하여, 국내 표준 및 국제 ITU 표준 도출하는 것을 목표로 하고 있다[3]. 기본적으로는 미국의 차량 간 이동 통신 표준인 WAVE(Wireless Access for Vehicular Environment)에 근간을 두고 있으나, 응급 메시지를 CDMA기술을 통해 송신하여, 실시간 기능 및 신뢰성을 높이고, VANET의 다양한 네트워크 상황변화를 감내할 수 있는 기술 개발을 목표로 하고 있다.

2.2 블룸 필터(BloomFilter)

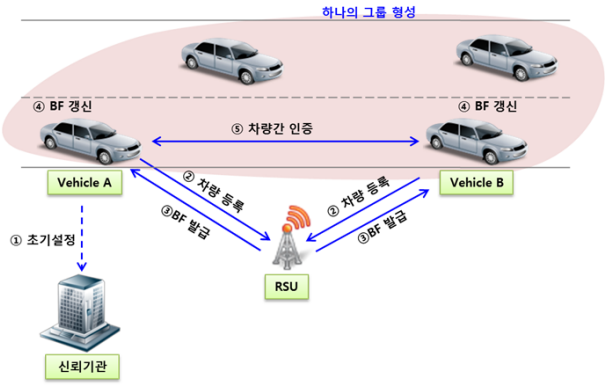
블룸필터는 H. Bloom에 의해서 제안된 통계적 특성을 가진 자료구조로써, 데이터를 공간 효율적으로 빠르게 검색할 수 있다는 장점이 있다[4]. 이러한 블룸필터는 많은 양의 데이터를 매우 작은 공간을 사용하여 저장할 수 있고, 검색 방식에 따라 다양한 환경에 적용시켜 효율적인 활용이 가능하다.

블룸필터는 m개의 비트를 가진 하나의 비트 백터(bit vector) B이며, n개의 엘리먼트를 가진 유한 집합 S={x1, x2, ... ,xn}에 각각의 요소가 포함되어있는지 쉽게 확인 가능하도록 해준다. 각 요소를 블룸필터에 맵핑시키기 위해서는 서로 독립적인 k개의 해시함수를 사용하여 비트벡터 B의 비트 주소공간에 맵핑시킨다.

3. 보안 요구사항

차량 통신 네트워크 환경에서 발생할 수 있는 보안 문제를 해결하기 위해서는 다음과 같은 보안 요구사항을 만족해야 한다[5].

- 메시지 부인 방지(Message Non-Repudiation)
  : 책임과 관계되는 요구사항으로 송신자는 메시지를 보냈다는 사실을 부인할 수 없어야 한다.
- 메시지 기밀성(Message Confidentiality)
  : 메시지는 접근이 인가되지 않은 노드로부터 안전하게 보호되어야 한다.



(그림 1) 제안방식 시나리오

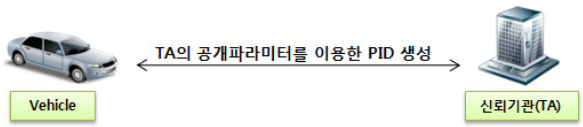
- 접근 제어(Access Control)
  : 구성 노드와 다른 노드에게서 제공받는 특정 서비스에 접속하는 것은 로컬 네트워크의 정책을 통해 결정 되어야 한다.
- 객체 인증(Entity Authentication)
  : 수신자는 송신자가 메시지를 생성했음을 확신할 수 있게 해야 하며 송신자가 현재 통신 중인 실제 송신자 네트워크의 노드임을 나타낼 수 있는 증거를 가져야 한다. 변경되지 않고 수신된 메시지는 충분히 작은 시간 내에 생성되어야 하므로 시간 정보를 이용하여 증거를 만들 수 있다.
- 가용성(Availability)
  : 네트워크와 응용프로그램은 오류가 있거나 부당한 상황에서도 사용 가능해야 한다.
- 익명성(Anonymity)
  : 어떤 차량이 메시지를 보내거나 이동 등 특정 동작을 하였을 때 다른 관찰자들이 특정 동작을 한 차량을 알 수 없어야 한다.
- 정당성 식별(Liability Identification)
  : 운전자는 다른 노드나 전송 시스템의 작동을 혼란시킨 계획적이거나 우발적인 행동에 대해 책임질 수 있어야 한다.

4. 제안방식

4.1 시스템 계수

제안하는 시스템에서 모든 차량은 네트워크상에 배포되기 전 TA(Trusted Authority)에 사전등록이 된다고 가정하며 본 제안방식에서 사용하는 시스템 계수는 다음과 같다.

- RID∗ : OBU(On-Board Unit)에 의해 생성된 차량 ∗의 식별자
- PID∗ : 차량 ∗의 ($ID*_1$, $ID*_2$) 쌍
- P_{pub1}, P_{pub2} : TA의 마스터키 (s_1,s_2)에 의해 생성된 공개키 쌍
- GK : 그룹키
- T_s : 타임스탬프



(그림 2) 초기 설정 과정

· T_{REVOK} : 그룹키 폐기 시간
· CERTIFY : 식별자
· BF : BloomFilter

4.2 초기 설정 과정

Step 1. 차량은 신뢰기관을 통해 차량 ID를 생성 한다(그림 2).

- $PID*=(ID_1, ID_2)$

4.3 차량 등록 과정

Step 1. RSU는 통신 범위에 도달하는 차량들에게 RSU의 식별자가 포함된 인증서와 그룹키를 차량 v의 공개키로 암호화하여 전송 한다(그림 3).

- RSU ⇨ Vehicle : $E_{PUv}(GK||CERTIFY_{RSU})$

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

- Vehicle ⇨ RSU : $E_{PURSU}(RSU_{ID}||PID_V)$

Step 3. RSU는 전송받은 값을 바탕으로 BloomFilter를 생성 한다.

- $H_1(RSU_{ID}||PID_V)$, $H_2(RSU_{ID}||PID_V)$,
  … $H_i(RSU_{ID}||PID_V)=BF$

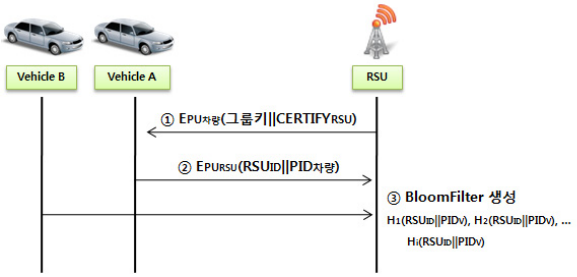
4.4 발급 단계

Step 1. RSU는 사전에 배포된 그룹키로 암호화하여 차량 인증에 필요한 BloomFilter를 브로드캐스팅 한다(그림 4).

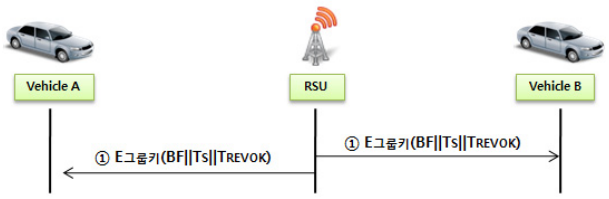
- RSU ⇨ Vehicle : $E_{GK}(BF||T_S||T_{REVOK})$

4.5 BloomFilter 갱신 단계

Step 1. RSU는 차량으로부터 PID를 포함한 정보가 더 이상 수신되지 않을 경우, 통신 범위를 벗어난 것으로 판단하여 BF를 새롭게 갱신할 것을 요청한다(그림 5).



(그림 3) 차량 등록 과정



(그림 4) 발급 단계

(그림 5) BloomFilter 갱신 단계

Step 2. RSU는 발급 단계와 마찬가지로 모든 차량에게 브로드캐스팅 한다.

Step 3. 기존의 BF를 폐기 후 갱신된 BloomFilter를 이용하여 차량 간에 인증을 한다.

4.6 차량 간 인증 단계

Step 1. 각 차량은 그룹키로 암호화된 메시지와 자신의 차량 PID를 통신 범위 내의 차량과 송수신 하게 된다(그림 6).

- Vehicle A ⇨ Vehicle B : $E_{GK}(BF)||PID_{VA}||M$

5. 제안방식 구현

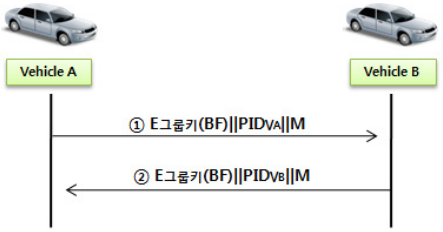
4장에서의 내용을 기반으로 차량 통신 네트워크 환경에서 BloomFilter를 이용한 차량 간 통신을 하게 되는 시뮬레이션을 구현하였다.

5.1 개발 환경

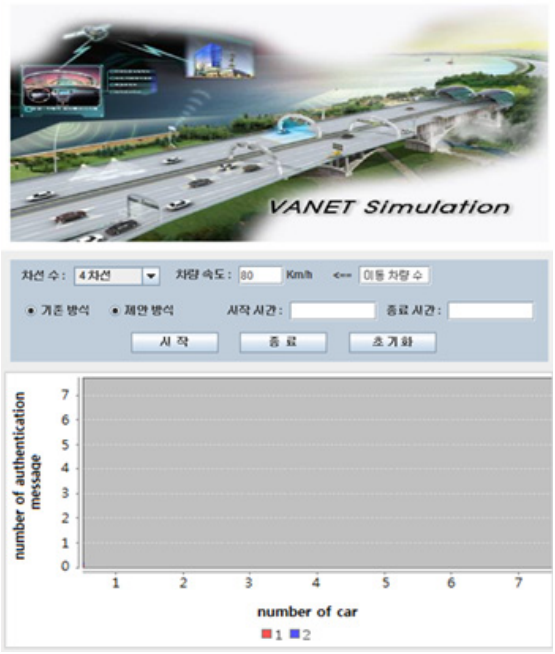
시뮬레이션의 개발환경으로는 eclipse 개발 툴을 이용하여 JAVA기반의 GUI환경의 프로그램으로 구성이 되어 있다.

5.2 시뮬레이션 구성

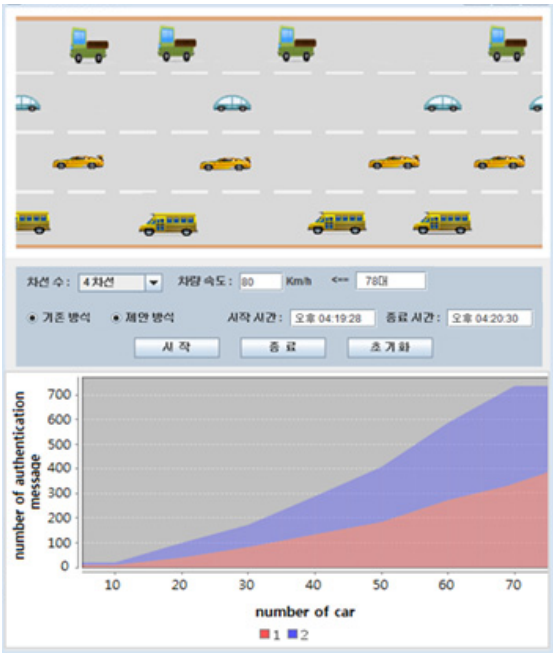
초기 화면에서는 도로의 차선 수 및 차량의 평균 이동 속도를 입력할 수 있다. 차선 수는 2차선부터 4차선까지 선택이 가능하며 화면에 보이는 도로를 1km의 하나의 RSU의 통신범위라 가정하고 해당 거리를 통과하는 차량의 속도에 따른 실제 이동량을 반영하였다(그림 7).



(그림 6) 차량 간 인증 단계



[그림 7] 초기화면



[그림 8] 실행 화면

5.3 입력에 따른 결과

사용자는 차선 수를 선택 후 차량의 평균속도를 입력하게 되고 시뮬레이션의 실행 시간으로부터 종료시간까지의 하나의 RSU 통신범위를 지나는 차량의 수를 측정하게 된다. 기존방식과 제안방식의 체크박스 선택을 통해 이에 맞는 상황을 비교하며, 이 과정에서 차량 간에 BloomFilter를 통한 통신 횟수를 비교하게 된다. 이 방식을 통해 상대 차량이 통신 범위를 벗어나기 전까지 별도의 인증메시지 교환이 필요 없고, 통신 범위 내에 차량이 존재하지 않을 때에만 새롭게 갱신된 BloomFilter를 이용하여 다른 차량과 인증이 이루어지므로 보다 효율적이라고 할 수 있다(그림8).

6. 결론 및 향후 연구 방향

본 논문에서는 다수의 차량이 존재하는 차량 통신 네트워크 환경에서의 각 차량의 복잡한 통신 절차를 줄이기 위해 RSU로부터 수신된 인증정보가 포함된 BloomFilter를 이용하는 인증 기법을 제안하였다.

이처럼 BloomFilter를 활용하여 통신 횟수 및 저장 공간에 대한 효율성을 향상 시켰으며 복잡한 절차를 보다 간소화 할 수 있었다.

향후에는 본 논문의 방식을 기반으로 좀 더 다양한 환경적 요인을 고려하여 기존의 다양한 기법들과 보다 구체적으로 비교 분석이 가능할 것으로 본다.

참고문헌

[1] ChosunBiz “지능형 교통 시스템 관련 기사”, 2012.01

[2] 조영준, 이현승, 박남제, 최두호, 원동호, 김승주, “VANET에서의 보안 기술동향”, 한국정보보호학회, 제19권 제1호, 2009.02

[3] 오현서, 최혜옥, 조한벽 “차량 통신 기술 동향” 주간 기술동향 통권 1315호, 2007.09

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

[5] 김수현 “VANET에서 그룹서명 기반의 객체 및 메시지 인증기법에 관한 연구” 순천향대학교 석사학위 논문, 2012.02